Universidad Internacional de La Rioja (UNIR)

ESIT

Máster universitario en Seguridad Informática

Automatización Aprendizaje WAF

Trabajo Fin de Máster

presentado por: Pinto Melo, Víctor Alfonso

Director/a: Cuesta Gómez, David

Ciudad: Bogotá
Fecha: 30/06/2020

Resumen

En este trabajo abordaremos una forma rápida de aprendizaje automático al WAF mediante una consulta de directorio y según la política que quisiéramos implementar, sea seguridad permisiva o restrictiva, los directorios que serían validos o no al momento de consultar una aplicación, que parámetros y extensiones deberíamos permitir o restringir, en definitiva, entregaremos una línea base, en la cual mitigamos un tiempo prudencial en el aprendizaje y poder salir a producción con una política más estable, ahorrando falsos positivos o falsos negativos según sea el caso.

Palabras Clave: WAF, Automatización, aprendizaje, política de aprendizaje.

Abstract

In this work we approach a fast form of automatic learning to the WAF through a directory consultation and according to the policy that we would like to implement, permissive or restrictive maritime security, the protocols that we process valid or not when consulting an application, what parameters and extensions should allow or restrict, in short, deliver a baseline, in which we mitigate a prudential time in learning and be able to go to a production with a more stable policy, saving false positives or false negatives depending on the case.

Keywords: WAF, Automation, Learning, Learning policy

Agradecimientos:

A mi esposa e hija, que me han tenido tanta paciencia y comprensión…

A mi padre y madre, sé que estarán orgullosos…

A mis compañeros de trabajo y empresa, por su disposición y permiso para desarrollar el laboratorio

A David Cuesta, por su colaboración y orientación…

Índice

Índice de figuras

Índice de tablas

1 Introducción

1.1 Presentación

El origen del firewall data de la década de 1980, gracias a la aceptación del uso de la pila de protocolos TCP/IP, y el riesgo que presentaba el viaje de estos paquetes sin ningún control entre redes, exponiendo información incrementando el acceso no autorizado a datos sensibles. Teniendo presente que estos paquetes tenían una estructura, un encabezado, en el cual se haya conformado por el puerto de origen, puerto destino, un número de secuencia, un número de acuse de recibido, la longitud de cabecera, espacio reservado (para futuros usos), las banderas de estado, ventana de recepción, la suma de verificación, puntero urgente, unas opciones (agregar algunas características que no cubren la cabecera) y el relleno, el cual complementa la cabecera en caso de que no cumpla los 32 bits; y la parte de datos. (formato de la cabecera ip, 2020)

Conociendo lo anterior, Cheswick y Bellovin tuvieron una idea, usar el filtrado de paquetes para denegar el acceso a todo lo que no se encuentre permitido en la red (Bellovin & Cheswick, 1994). Aquí nace el concepto de firewall, a ellos se sumaron las aportaciones de Nir Zuk (1993), David Pensak (1995), Markus Ranum (1992, 1993) y Jeff Mogul (1984), unido todas las ideas surgió la propuesta de un dispositivo para asegurar nuestra red interna protegiendo de un medio inseguro, en este caso la Internet.

Ranum nos ofreció el primer producto firewall, DEC SEAL. El cual incluía un modo proxy, desarrollado por él en 1992. “DEC SEAL fue muy interesante, porque tenía un número de parte, un manual y una empresa detrás de él” (Ranum,2008).

Este último, armonizó el concepto de firewall híbrido, ya que también controlaba datos de algunas aplicaciones como RSH o FTP.

Para el año 1994 la empresa CheckPoint lanzó al mercado su producto Firewall-1 que tuvo una gran importancia en el ámbito de la seguridad, introduciendo a su vez una interfaz gráfica para la administración. (InfoWorld, 1996) En los siguientes años surgieron creaciones como Squid (1996) y Snort (1998), los cuales fueron creados con licencias gratuitas para la investigación y maduración de estas tecnologías.

En esta misma época surgieron nuevas funcionalidades que irían moldando poco a poco, surgiendo nuevos productos, entre ellos el web application firewall, gracias al incremento de los servicios web, se requería una protección a nivel de capa 7, es aquí donde, en ese entonces la compañía Perfecto Technologies desarrolla el producto AppShield para comercios virtuales, protegiéndolo contra el ingreso de caracteres ilegales en las páginas web. La empresa pasó a

llamarse Sanctum, creando un top 10 con las mejores técnicas de ataque a aplicaciones web, creando así, las bases de mercado para los WAF. (Web Application Firewall,2020).

Un WAF es un firewall para aplicaciones HTTP, Aplica un conjunto de reglas a una conversión HTTP, en general esas cubren ataques comunes como Cross-site Scripting (XSS) y SQL Injection.

Los WAF pueden venir en forma de dispositivo, un complemento del servidor o un filtro y pueden personalizarse para una aplicación web. (OWASP,2019)

1.2 Motivación

Según la consultora Gartner (Global IT spending, 2020), a nivel mundial en el año 2019 la inversión en seguridad empresarial llego a 124,000 millones de dólares, aumentó un 8% con respecto al año 2017 y no es por menos, los hackers han creado una empresa rentable, las ganancias son interesantes, han pasado de una persona en una habitación hackeando y robando contraseñas a ejércitos organizados, con herramientas especializadas para atacar organizaciones y obtener datos confidenciales.

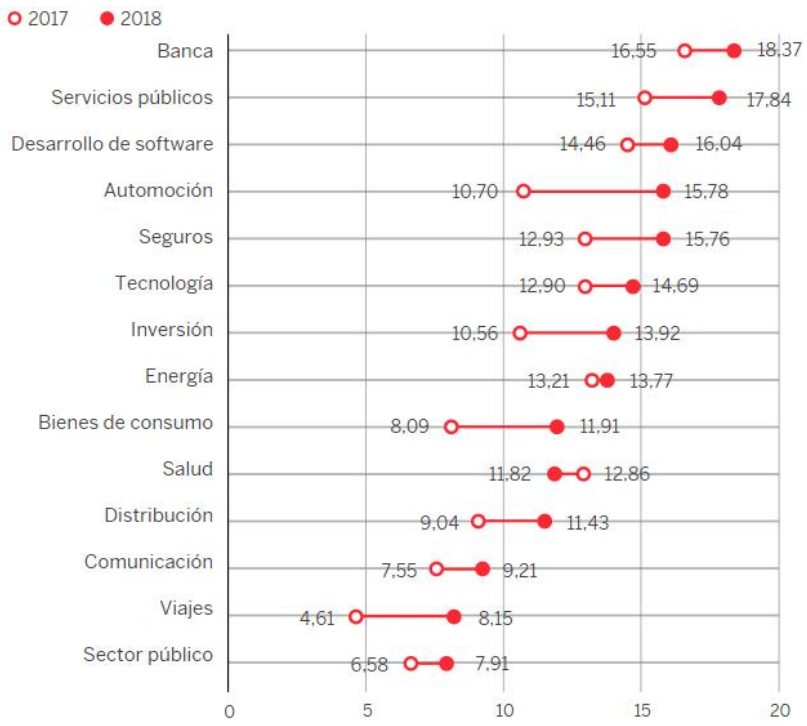

Figura 1: Costo del cibercrimen en millones de dólares (El País, 2020)

Según reporte de la empresa especializada en ciber seguridad, SonicWall, los ataques contra aplicaciones web han aumentado un 52%, el objetivo favorito es la obtención de información financiera personal. Según estadísticas recopiladas por la misma compañía hubo una

disminución en general de malware, en un 6% con respecto al año 2018, registrando para el año 2019 un total de 9.9 billones de ataques por malware.

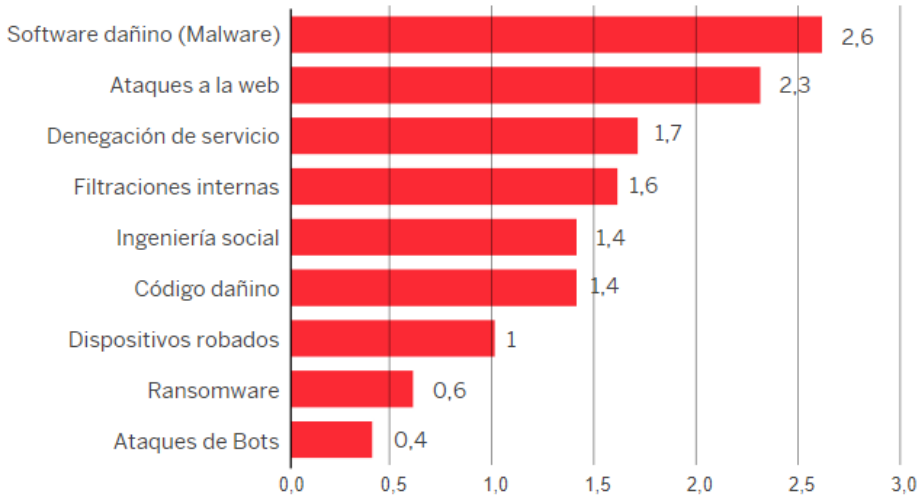

Figura 2: Cantidad de ataques por tipo (El país, 2020)

Figura 3: Estadísticas anuales de ataques por malware. (SonicWall,2020a)

Otro dato interesante que recopilo la compañía SonicWall es el incremento significativo a nivel global de ataque por parte de malware en puertos no estándar, detectando un incremento del 15% de malware que dirigía sus ataques a estos puertos. Dichos asaltos aprovechan la protección que la mayoría de las empresas utilizan en sus arquitecturas, el cortafuegos, ya que generalmente está configurado para monitorizar puertos estándar como lo son el 80 HTTP, 443 HTTPS, 25 SMTP, etc.

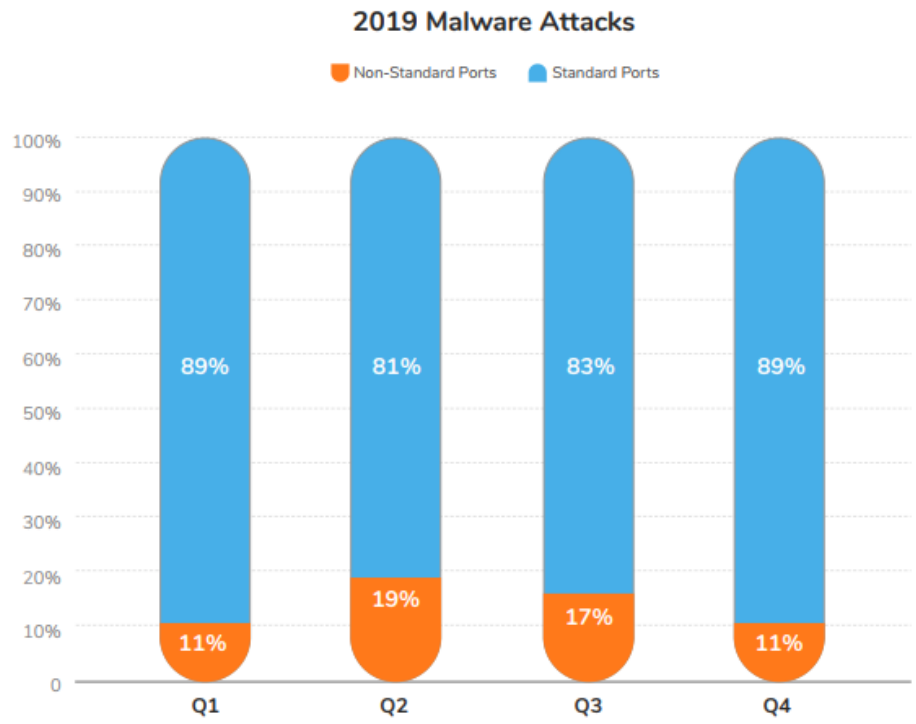

Figura 4: Ataque de malware a puertos no convencionales por trimestre año 2019 (SonicWall,2020b)

Como se indicó anteriormente, los ataques a aplicaciones web aumentaron considerablemente, según la investigación realizada por SonicWall, algunas de las aplicaciones populares que fueron objetivo de estos ataques fueron: SharePoint, Atlassian, Confluence, Drupal Oracle Weblogic, Microsoft Windows GDI, Slack, G Suite y Dropbox. (Most Targeted Web Applications, 2020)

Según el último reporte emitido por SonicWall el aumento de ataques ha bajado en general, pero se ha vuelto más especializado, la mayoría de los ataques se producen sobre la capa de aplicaciones, ya que se tiene la perspectiva de que pueda existir algún error de diseño, codificación o configuración en las aplicaciones que pueda ser explotado.

Perdidas por ciberataques

Se estima que para 2021 los daños por delitos informáticos costarán a las empresas un total de 6 billones de dólares según el reporte anual de cibercrimen de la empresa Cibersecurity Ventura. (Global Cybercrime damage, 2018)

Según el artículo, siguen manteniendo la apuesta por esta cifra, debido al incremento de ataques a compañías a nivel mundial.

Un artículo del periódico digital portafolio.co, afirma que, Hay empresas que pierden hasta $4.000 millones por ciberataques (Portafolio, 2019): “De acuerdo con un estudio realizado por

el Mintic, la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), se revela que en Colombia más del 60% de las organizaciones encuestadas incurrieron en costos cercanos al millón de pesos por daños relacionados con ciberataques, mientras que el 20% gastaron entre 1 y 15 millones de pesos, el 15% entre 15 y 235 millones y el 5% presentó valores desaforados de hasta 4.000 millones de pesos, como consecuencia de incidentes de vulneración tecnológica"

En el mismo artículo hace referencia que el 23% de los incidentes, fueron ocasionados por vulnerabilidades en el software (Mayoría de ataques cibernéticos…,2019) las vulnerabilidades comprenderían malas configuraciones, malas prácticas de codificación, uso de componentes desactualizados, falta de actualizaciones de seguridad.

Según el trabajo "*Comparativa de la eficacia de herramientas WAF y RASP frente a ataques*" (Sureda, 2017) se realizaron los ataques del OWASP Top 10 a diversos dispositivos WAF y RASP, en los cuales se concluye que la herramienta RASP Contrast, tiene un excelente índice de efectividad según las métricas utilizadas, no obstante indica que la efectividad de las herramientas WAF utilizadas está inmediatamente por debajo, inclusive se solapa con algunos resultados, lo que nos indica que los WAF son excelentes dispositivos pero se requiere de una configuración más estricta para evitar falsos positivos o lo peor, falsos negativos.

Aquí entra nuestro dispositivo especializado en seguridad de la capa 7 del modelo OSI, el WAF, el cuál a través de firmas que deben ser actualizadas regularmente y un aprendizaje, mitigará y reducirá significativamente los ataques del OWASP Top 10. Cómo se comentó anteriormente, existe una fase de learning en la cual, el dispositivo escuchará, capturará y pedirá tomar una decisión por cada parámetro, URL, script, etc que evidencie está sucediendo entre cliente y servidor. Por esta razón veo la necesidad de acelerar el aprendizaje del WAF, teniendo presente que en promedio se requieren 15 días a lo menos para que tengamos una muestra inicial e ir y depurando manualmente, captura por captura que peticiones debemos permitir y cuáles no.

La idea de este trabajo es, conociendo una aplicación web y en un ambiente de QA, desarrollar un método para consumir los servicios web, que deben estar alojados bajo el dispositivo de seguridad, pasando parámetros a dicha aplicación y mientras esto sucede, el WAF observe, capture y aprenda de manera confiable, para poder reducir los tiempos de aprendizaje y poder implementar una política más robusta en producción.

1.3 Objetivos Generales

El objetivo principal es realizar un piloto experimental, en donde conociendo la aplicación a asegurar y que a su vez debe estar implementada inicialmente bajo el WAF en QA, desarrollar

una técnica para enseñar al dispositivo de manera segura, controlada y eficiente una política de seguridad.

- Analizar trabajos similares, informes, artículos y demás que puedan ayudar a este trabajo
- Selección y configuración de una aplicación bajo WAF de QA.
- Ejecución técnica de fast learning sobre la aplicación asegurada bajo el WAF, la idea es enviar peticiones de manera controlada y eficiente para completar la fase de aprendizaje de manera más efectiva.
- Implementar la política en el ambiente productivo, haciendo una comparativa de las evidencias capturadas por la política implementada bajo el fast learning contra una política de aprendizaje convencional.

1.4 Estructura del documento

La estructura de este documento está dividida en los siguientes capítulos:

1. **Capítulo 1. Introducción**: Donde se introduce al trabajo y se describe la motivación de este.
2. **Capítulo 2. Estado del arte**: Se explican los conceptos básicos de cómo trabaja un WAF, tipos de políticas de seguridad existentes y cómo funcionan, además detallaremos la configuración de la aplicación que usaremos sobre el ambiente de QA.
3. **Capítulo 3. Objetivos y metodología del trabajo**: Se explica cuál es el objetivo general de este trabajo, así como una breve descripción del procedimiento realizado para la consecución de este.
4. **Capítulo 4. Desarrollo específico de la contribución:** Se detalla cómo se desarrolló el piloto sobre el ambiente de QA, que datos se usaron, cómo se aplicó la política su exportación e implementación en producción y las métricas comparativas entre la política de aprendizaje normal versus la que implementamos desde QA.
5. **Capítulo 5. Conclusiones y trabajos futuros:** Se describen las conclusiones sobre el presente trabajo y posibles campos futuros de investigación.
6. **Capítulo 6. Glosario**: recopilación de la terminología técnica utilizada en este documento con su explicación.
7. **Capítulo 7. Referencias:** Se detallan las referencias utilizadas y que sirvieron de referencia para el presente trabajo.
8. **Capítulo 8. Anexos:** Se adjunta información relevante sobre la consecución del aporte como lo son: capturas de pantalla, logs de resultados, tablas, etc.

2 Estado del arte

2.1 Introducción

Los firewalls de aplicaciones son dispositivos que se ponen entre la internet y la aplicación, analizando el tráfico HTTP y cada una de las peticiones y respuestas que se hacen entre cliente y servidor antes de que lleguen a su destino. Para que el WAF sepa que debe buscar en su análisis de tráfico, debe utilizar un archivo de firmas, el cual generalmente debe ser actualizado de manera regular para estar al día en nuevas técnicas de evasión, gracias a estas firmas podremos dejar al descubierto los ataques más frecuentes y usados contra aplicaciones web.

"Desafortunadamente la flexibilidad que ofrecen las soluciones heurísticas tiene un precio de falsas alarmas que se generan en circunstancias inusuales, pero no están relacionadas al ataque" Pałka, D., & Zachara, M. (2011a) Sucede frecuentemente, una aplicación productiva aún superada la fase de aprendizaje, y no ha conseguido entender completamente el comportamiento de la aplicación, capturará el tráfico y lo marcará como riesgoso, mientras no se ponga el equipo en estado de bloqueo, no sucederá nada, solo una alerta pero si este está bloqueando lo que considere un ataque, tendremos problemas en producción, personalmente he tenido que solventar estos incidentes en mi trabajo, revisar códigos de bloqueo y permitirlos si son legítimos. Sin embargo, es un problema menor en contra de lo que puede suceder en caso de que sea un ataque real y logre su cometido, es mejor prevenir que lamentar.

"La debilidad más común en la seguridad de aplicaciones web, es la falta de una validación adecuada de las entradas procedentes del cliente o del entorno de la aplicación" (OWASP,2012) Generalmente, los desarrolladores no tienen presente en sus productos la seguridad por defecto a menos que se les exija usar un S-SDLC, mientras esto no se haga cultura, las aplicaciones están expuestas a diversos ataques, los más comunes y con mejores resultados son:

- Injection: Sucede cuando un atacante envía datos con el fin de obtener un comportamiento no deseado por parte de esta, puede ser a nivel de base de datos, protocolos como LDAP, los headers en SMTP.
- Broken Authentication: Son los métodos manuales o automáticos que utiliza un atacante para obtener el control de una cuenta en determinada aplicación web.
- Sensitive Data Exposure: Consiste en comprometer información sensible que debería ser confidencial.
- XML External Entities (XXE): Ataque que se realiza contra aplicaciones que utilizan un intérprete XML y este se encuentra configurado de manera insegura, el atacante podrá obtener información o realizar ataques mediante payloads.

- Broken Access Control: Consiste en aprovechar una página de login usada para administrar la web.
- Security Misconfigurations: Consiste en aprovechar los errores en las configuraciones de sitios web, generalmente por fuerza bruta.
- Cross-Site Scripting (XSS): Consiste en inyectar código malicioso en páginas para distribuir programas maliciosos por medio de ellas.
- Insecure Deserialization: Consiste en aprovechar las cadenas de byes deserializadas para obtener privilegios, generalmente cookies con información de usuario y roles.
- Using Components with known vulnerabilities: Como su nombre indica, es usar complementos, versiones de librerias, frameworks, etc que se encuentran desactualizadas y con vulnerabilidades conocidas.
- Insuficiente registro y monitoreo: Se requiere al menos tener un log de eventos para evidenciar que está sucediendo y tomar acciones correctivas.

2.2 Antecedentes

Las formas más usadas de implementación de WAF son las siguientes maneras:

- Modo Puente o Transparente: actúa cómo un dispositivo que conecta dos redes, sus interfaces de red no poseen una dirección IP asociada, por consiguiente, no es necesario modificar las direcciones de los servidores ni los DNS asociados al mismo, las aplicaciones que se encuentren bajo dicho dispositivo estarán protegidas.
- Modo Proxy Inverso: este modo al igual que el anterior, conecta dos redes, pero sus interfaces tienen direcciones IP, por lo cual, para el cliente el WAF sería el servidor de aplicaciones con el que interactuaría, ya que este suplantaría al servidor o servidores de aplicaciones que estén detrás, respondiendo al tráfico y analizándolo.

Algunos fabricantes incluyen en estos dispositivos características adicionales como lo son:

- Aceleración SSL: se trata de quitar la carga del cifrado a los servidores web para que el WAF realice dicha función, aunque, quedaría el tráfico descifrado desde el dispositivo hacía las aplicaciones web.
- Protección DoS: se puede configurar un perfil adicional por aplicación, donde se indican las transacciones por minuto que deberían ser normales en una aplicación, si son superadas, se rechazaría el tráfico.
- Ocultación errores por defecto: los errores por defecto muestran mucha información relevante para un atacante, cómo el tipo de servidor web usado, tecnología en que está desarrollada determinada aplicación y en ocasiones información sobre el motor de base de

datos, para ello se ofrecen ocultar los códigos de respuesta 400 y/o 500, enmascarándolos con una imagen o una redirección a otra página.

- Protección capcha: a través del WAF podemos proteger un formulario de consulta o un login si este no cuenta con la protección necesaria a nivel de código.

Los firewalls de aplicaciones tienen dos modelos a seguir para comprender el tráfico que circulará por la aplicación a proteger, aquí nace la política de seguridad, se puede elegir tanto un modelo como otro o combinar los dos, los métodos son:

- Seguridad negativa: es el modelo de más fácil implementación y administración, ya que acepta todas las peticiones entrantes y bloquea puntualmente aquellas que son consideradas amenazas, depende de una base de firmas que debe ser actualizada regularmente.
- Seguridad positiva: este modelo deniega todas las peticiones entrantes a menos que estén explícitamente permitidas (aprendidas o añadidas), tiene una ventaja enorme con respecto al anterior modelo y es que nos protegerá de tráfico desconocido, incluyendo amenazas reales, su contra son la cantidad de falsos positivos que detecta, además de lo difícil que resulta mantener la política si la aplicación web cambia con frecuencia, implementando nuevas funcionabilidades.

2.3 Trabajos relacionados

En el trabajo *Learning Web Application Firewall – Benefits and Caveats* (Palka & Zachara, 2011b) realizan un análisis de cómo funciona un WAF a nivel de configuración, mitigación de ataques, implementación. En el apartado número cinco, hacen referencia a los problemas e inconvenientes al momento de implementarlo, se analiza lo dispendioso de la gran cantidad de datos que se deben recolectar, mantener y posteriormente analizar, así mismo el problema que conlleva almacenar esta data sensible. En cuanto al aprendizaje, analizan las dos formas que se pueden implementar, el aprendizaje activo (TL) y el aprendizaje continuo (CL), resalta que el aprendizaje activo requiere un administrador del dispositivo, el cual tiene que especificar cuando se activa y se desactiva el modo de aprendizaje, mientras se encuentre activo, se recolectarán los parámetros y sus valores para tener un patrón de cotejamiento. Al finalizar la etapa de aprendizaje se entra en modo bloqueo, aquí se comparan los parámetros que ingresan con los que ya se tienen almacenados.

De este modo, resalta que no es necesario almacenar los datos, ya que la información que se utiliza es la recolectada en la etapa del aprendizaje. El lado negativo, es que se debe volver a reaprender cada vez que se introducen cambios en la aplicación protegida.

Respecto al aprendizaje continuo (CL) resalta que es más fácil de configurar ya que se requieren menos entradas manuales, pero, por obvias razones, no es muy preciso, ya que se analizan los datos que ingresan en caliente contra los que siguen, si los valores difieren se dará un falso positivo.

Allí hace una comparativa de las dificultades entre los dos métodos, pero no se aborda una forma de mitigar la complejidad que implica el aprendizaje o entrenamiento del WAF.

Otro trabajo similar, donde se detallan ¿cómo aprende un WAF? Es: *Securing information resources using web application firewalls*. (Baranov & Beybutov, 2015) en un apartado hablan del "*Machine Learning*" que utilizan las soluciones WAF, entre estas resaltan dos fabricantes, Imperva y F5, resaltan la dificultad que se tiene para implementar un aprendizaje perfecto ya que el algoritmo que se usa para esto es privativo. Mencionan la forma en la que se puede aprender de manera segura y rápida con el fabricante F5, el cual permite seleccionar una dirección IP de confianza y desde allí generar tráfico, algo similar a lo que se realizará en mi contribución. También se analiza el tiempo que utiliza en este caso Imperva para su aprendizaje que son 240 horas, después de las cuales se dará por finalizada dicha fase y se activará el modo bloqueo, en cambio para el F5 se puede parametrizar esta fase para ser más holgada, pudiendo configurar más tiempo o simplemente, volver a poner en etapa de learning una vez se haya entrado a bloqueo, esto sucede generalmente cuando se realizan cambios en una aplicación protegida.

En un trabajo enfocado a los ataques de iSQL: *Prevention of SQL injection Attacks using AWS WAF (*Kareem, 2018*)*. Expresan la preocupación de la efectividad que tienen estos ataques por la facilidad de por llevarse a cabo y los excelentes resultados que se obtiene. Cita que una de las formas más fáciles de ser detectados es gracias a los WAF, pero ratifica que solo detecta los ataques más sencillos o simples, considerando los ataques de iSQL más elaborados los que pueden pasar inadvertido por la detección de las políticas de estos dispositivos. También indican que el costo de mantenimiento es elevado, haciendo dispendioso mantenerlo operativo y la administración dedicada para que sea eficiente, se realiza un estudio detallado de cómo evitar solo ataques iSQL mediante una configuración detallada en AWS WAF, no usan un escáner de vulnerabilidades y adicional no tienen en cuenta los demás tipos de ataques.

2.4 Estado actual

Actualmente el aprendizaje de los dispositivos WAF es muy similar, una etapa inicial de creación de la política para proteger una aplicación luego comienza la fase de aprendizaje del tráfico, la cual depende el fabricante puede durar desde unas horas hasta semanas, para ello vamos a revisar algunas soluciones, comenzando con la elegida para este trabajo, el ASM de F5

y su fuerte competencia BWAF de Barracuda, adicional validaremos MODSECURITY el cual es muy popular por ser open source.

2.4.1 Application Security Manager (ASM)

Antes de crear una política, sea cual sea la tecnología se debe tener presente para qué aplicación se desarrolla, en ¿qué lenguaje está desarrollada? sobre ¿qué arquitectura está alojada? Las tecnologías que apoyan la aplicación web, etc. Lo anterior para hacer una correcta elección y configuración de una política, en ASM se trata de ser mus preciso, ya que se tienen actualizaciones de firmas para estas tecnologías, las cuales se deben tener presentes a su vez antes de comenzar.

Teniendo presente lo anterior, crear una política es sencillo, basta con ingresar al Local Traffic Manager de F5 donde se encuentra aprovisionado el módulo de ASM y nos dirigimos a la opción, Security, Application Security, Security Policies, Policies List y presionamos en crear:

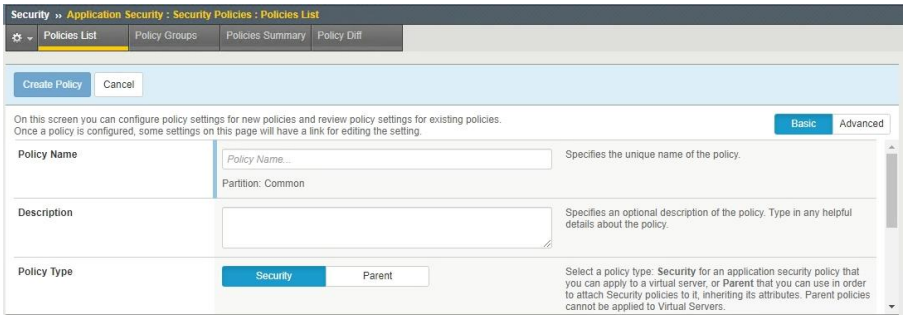

Figura 5: Menú creación de una nueva política de seguridad (Propia)

Allí debemos elegir un nombre para nuestra política, es recomendable que sea alusivo al nombre de la aplicación para poder identificarla con facilidad, una breve descripción de la misma, luego debemos elegir el tipo de política, en nuestro caso es de seguridad (parental es para agregar políticas de seguridad sobre esta, es como un repositorio) elegimos una plantilla, se recomienda la fundamental, ya que mantiene un equilibrio entre facilidad de configuración, mantenimiento e implantación, luego se elige la aplicación sobre la cuál va a trabajar esta política.

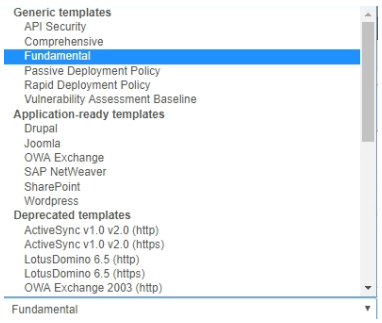

Figura 6: Tipos de plantillas de seguridad ASM (propia)

A continuación, se da a elegir al administrador, cómo será el método de aprendizaje de esta nueva política, por lo general y lo más usado es dejarla en manual y que el administrador después entre a revisar una por una las alertas y acepte o niegue el tráfico de esta.

Figura 7: Modo de aprendizaje y modo de aplicación ASM (propia)

La siguiente opción pregunta ¿cómo queremos que actúe la política de seguridad? Que inicie a bloquear lo que se considere una amenaza o que sea transparente y simplemente capture y alerte para que sea el administrador quién tome esa decisión.

El siguiente paso es seleccionar la codificación del idioma o podríamos permitir que automáticamente el WAF lo detecte, la mejor práctica es elegirlo de inmediato, además está presente una opción para elegir la efectividad o precisión de las alertas y amenazas con relación a la plantilla elegida, se divide en tres tipos, cada uno de ellos adecuado para un tipo de aplicación web diferente, en resumen, la forma rápida es recomendada para aplicaciones web pequeñas, con un tráfico muy bajo, ya que selecciona los límites de precisión bajos, por lo cual se completa más rápido pero no será tan precisa. La media es la que se recomienda comúnmente por el fabricante, ya que los valores de umbral son más altos y la efectividad aumenta, como también el tiempo en completarse y, por último, el aprendizaje lento, el cuál es recomendado para aplicaciones enormes, con bastantes opciones y un tráfico denso, tomará mucho más tiempo en completar el umbral, pero en teoría será bastante precisa, reduciendo los falsos positivos a una mínima cantidad.

El WAF nos permite ingresar manualmente qué tecnologías utilizamos en nuestra aplicación y arquitectura, por ejemplo, si utilizamos un Windows Server con un IIS y tenemos una base de datos MSSQL, le podremos agregar esos parámetros, de esta forma el tendrá una configuración base para iniciar, no es obligatorio hacerlo, ya que, al iniciar el tráfico, el dispositivo detectará las tecnologías y las mostrará en las alertas, donde el administrador indicará si es correcta o no.

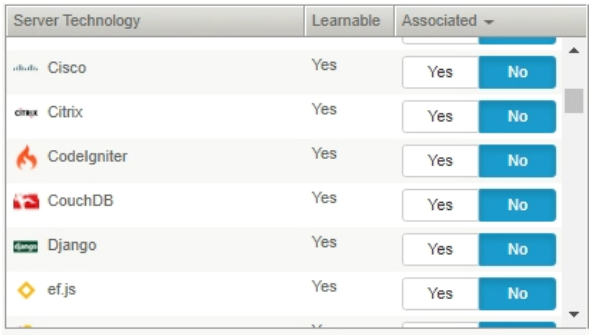

Figura 8: Tecnologías de la aplicación web en ASM (propia)

La siguiente opción nos permite elegir una dirección IP segura, desde la cual podemos alimentar la política de seguridad, navegando por la aplicación web desde un ambiente de QA generalmente.

Luego la elección de la velocidad de aprendizaje para completar la política, si las alertas las podemos pasar un modo provisional mientras decidimos si aceptamos o no la sugerencia del dispositivo, si la política debe diferenciar entre mayúsculas y minúsculas y si hace lo mismo con el tráfico HTTP y HTTPS.

Una vez realizada esta configuración, con un poco de conocimiento podríamos afinar aún más agregando por ejemplo el tamaño máximo que tendrá la URL, el número máximo de parámetros que irán en el request, etc. Esta parte es opcional, ya que el WAF arrojará estos resultados y dará una sugerencia de estos.

Al finalizar los pasos anteriores, solo resta iniciar el consumo de la aplicación utilizando la dirección que nos entrega el dispositivo y comenzar a aceptar o no las alertas que se emiten en el WAF con base a las firmas de amenazas.

La esencia de una política en ASM es su archivo de firmas, ASM Attack Signature es información acumulativa sobre los tipos de ataques y los patrones a seguir para vulnerar las aplicaciones web, este es generado regularmente por el fabricante F5, en su sitio web de descargas, como complemento se ofrece un archivo que incluye las tecnologías usadas en lado del servidor, el cual adiciona patrones de ataque específicos hacía estas, ayudando a identificar con mayor facilidad si el tráfico que circula sea legítimo o no, se dirige a un servidor web IIS o Apache, el código utilizado es PHP o ASP.NET, o la base de datos que se usa es MySQL o MSSQL, etc

ASM permite que estas actualizaciones de archivo se puedan realizar de manera automática, semi automática o completamente manual, todo depende de la configuración que se tenga en el equipo, permisos de conexión hacía el sitio del fabricante o la política de seguridad interna que maneje la compañía.

2.4.2 Barracuda Web Application Firewall

El WAF de Barracuda trae configuradas de fábrica las políticas de seguridad, las cuales pueden aplicarse a una o muchas aplicaciones web, inspeccionando el tráfico de entrada y salida para detectar ataques maliciosos dentro de los mismos. Estas políticas, pueden ser mejoradas manualmente por un administrador del equipo. (Barracuda, 2019a)

Para poder proteger la aplicación web con Barracuda WAF es necesario primero agregar el servicio dentro del dispositivo, se debe elegir la dirección IP virtual (VIP) que entregará dicha aplicación al usuario final, el puerto y el servidor donde se encuentra alojada dicha aplicación, al momento de crear esta aplicación en el WAF, automáticamente se le asigna una política por defecto, además de esta se cuenta con las siguientes políticas:

- Sharepoint
- Sharepoint 2013
- OWA
- OWA 2010
- OWA 2013
- Oracle

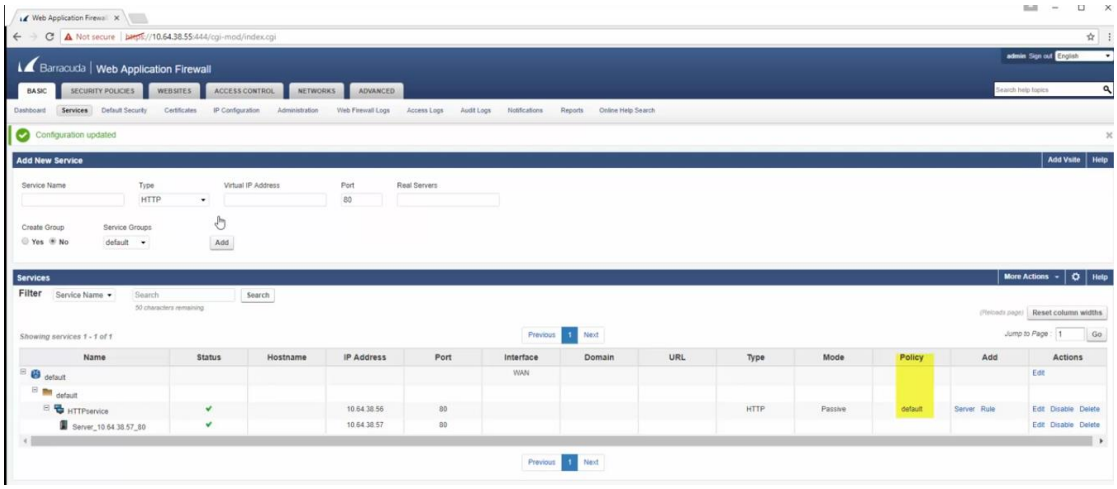

Figura 9: Pantalla para configuración nuevo servicio web. (Barracuda,2019b)

Cada política contiene nueve sub políticas las cuales se pueden editar en la página de políticas secundarias:

- Límites de solicitud:
  Definen un criterio para validar las solicitudes de entrada controlando los tamaños en los campos del encabezado HTTP, si se supera el límite superior, los paquetes serán descartados. Esta proyección ayuda a la mitigar los ataques de desbordamiento de buffer para ocasionar una denegación del servicio. (Barracuda, 2020a)

- Cookie:
  Se realiza un cifrado de las cookies utilizadas por las aplicaciones web, con el fin de proteger la información que en ocasiones viaja en ellas, de esta forma aseguramos que no se comprometa la privacidad de un usuario o aplicación. (Barracuda, 2019c)
- Protección de URL:
  Esta barrera controla los parámetros que se usan en las peticiones de las URLS, bloqueando métodos que no se usan y que podrían resultar inseguros ya que podrían inyectar scripts maliciosos. (Barracuda, 2020b)
- Protección de parámetros:
  Se configuran qué valores pueden ir en los parámetros, que caracteres pueden insertarse, de esta forma evitar scripts malintencionados. (Barracuda, 2020c)
- Encubierto:
  Con esta regla se enmascaran las respuestas de servidor, como lo son los errores por defecto que despliega alguna tecnología donde entrega información relevante de la arquitectura que se está usando. (Barracuda, 2019d)
- Protección contra robo de datos:
  Se utiliza para enmascarar información sensible que se utilice en las transacciones de la aplicación web, como lo son números de tarjetas de crédito, identificación, dirección, teléfono, etc. (Barracuda, 2020d)
- Normalización de URL:
  Todas las codificaciones son convertidas por el WAF y normalizadas a ASCII, con el fin de evitar ataques encubiertos. (Barracuda, 2019e)
- ACL Globales:
  Son reglas globales para saber que se permite compartir y que no a nivel de aplicaciones en el dispositivo. (Barracuda, 2020e)
- Política de acción:
  Son acciones que se toman cuando ocurre una violación en alguna política como lo serían una redirección, un código de bloqueo, un reto captcha, etc. (Barracuda, 2019f)

Al igual que ASM, Barracuda WAF utiliza archivos de firmas para detectar ataques, con unas características adicionales, indica que el tráfico primero atraviesa varias capas para poder normalizarse y al final, hacer una comparación exacta de qué tipo de ataque se está realizando, la idea en esto es reducir el tiempo de análisis al momento de llegar a la etapa final, otorgándole un tiempo de respuesta más oportuno. Las firmas se encuentran agrupadas, permitiendo una optimización en el uso de memoria de acuerdo con el match que haya realizado. Si una vulnerabilidad nueva es detectada, esta es cotejada contra las firmas existentes, por lo general basta con aumentar el nivel de bloqueo a uno más estricto.

"Cuando se produce un ataque, las firmas relevantes se crean de inmediato y se ponen a disposición de barracuda Web Application Firewall a través de actualizaciones de definición de ataque" (Barracuda, 2016)

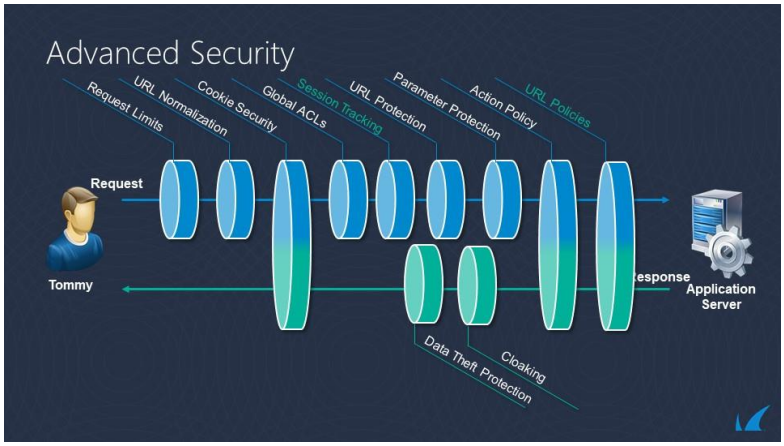

Figura 10: Seguridad Avanzada Barracuda (Barracuda, 2016)

En la imagen se describe las 9 capas que atravesaría el tráfico para normalizarse antes de poder entrar en análisis de firmas.

2.4.3 ModSecurity

Fue desarrollado en 2002 por Ivan Ristíc (ModSecurity HandBook, 2010a) como un pasatiempo para poder monitorear el tráfico HTTP en los servidores Apache, "*Inicialmente, la mayor parte de mi trabajo lo pasé luchando con Apache para ganar acceso a los cuerpos de las solicitudes, que era una habilidad crucial. Apache 1.3.x no tenía intercepción o API de filtrado, pero puede engañarlo para someterlo"* (ModSecurity HandBook, 2010b). A partir de allí el proyecto comenzó a crecer y se volvió comercial.

En el año 2006 se realizó una evaluación por Forrester Research (The Forrester wave: Web Application firewalls q2, 2006) y ModSecurity salió bien librado en las comparativas contra otros WAF, desde allí la aplicación se comenzó a evolucionar, en el mismo año fue entregada una versión renovada. A partir de acá se han realizado muchos cambios, se incluyó soporte para otras tecnologías de servidores web, como IIS y Nginx. El último cambio fue una reestructuración completa, dejando de ser un módulo transformándolo en LibmodSecurity una solución WAF competente.

Funciona con reglas, las cuales son muy personalizables además del uso de expresiones regulares en las mismas, adicional existe un proyecto que las genera y entrega en un repositorio en Github el cual pertenece a SpiderLabs y ofrece protección para las siguientes categorías de ataque:

- Protección del protocolo HTTP
- Búsqueda en listas negras en tiempo real
- Protección DoS sobre HTTP
- Protección genérica para ataques web

También se pueden comprar las reglas, las cuales son refinadas por Trustwave gracias test de penetración e investigaciones, adicional ofrecen actualizaciones a diario en las cuales se entregan actualizaciones críticas y ofrece una cobertura para más categorías de ataques, estas son algunas:

- Parches virtuales
- Reputación de direcciones IP
- Detección de Malware basado en aplicaciones Web
- Detección de ataques desde BotNet
- Detección de backdoors
- Detección de ataques DoS sobre HTTP

El funcionamiento de ModSecurity depende de dos términos: la configuración y las reglas, la configuración le indica al WAF cómo procesar los datos que obtiene y las reglas deciden qué hacer con este tráfico. La taxonomía de las reglas es la siguiente:

SecRule VARIABLES OPERADOR ACCIONES

Ejemplo:

SecRule ARGS “<script>” log,deny,status:404

En el ejemplo anterior le estamos indicando a ModSecurity que, dentro de todo el tráfico, si encuentra el texto “<script>” registre la acción en el log y a su vez niegue la transacción usando el código 404. (ModSecurity HandBook, 2010c).

3 Objetivos y metodología del trabajo

3.1 Objetivo

El objetivo de este trabajo es encontrar una técnica que permita acelerar el aprendizaje de una política de seguridad en el WAF de QA mediante un procedimiento seguro y controlado, reduciendo los falsos positivos a lo mínimo posible para poder ahorrar tiempos y costos al implementarse en el ambiente productivo.

3.1.1 Objetivos Específicos

- Crear la política en el ambiente de laboratorio, la cual aprenderá la seguridad negativa que la atraviese.
- Ejecución del laboratorio utilizando OWASP ZAP como escáner de vulnerabilidades para generar el tráfico negativo.
- Validar la cantidad de firmas activadas después del escaneo para comprobar efectividad de este.
- Crear política de control en el ambiente productivo y dejarla aprendiendo al menos por siete días.
- Concluido este periodo, validar las firmas activadas en la política productiva y realizar comparación con la generada en el laboratorio mediante OWASP ZAP.
- Implementar la política generada en el laboratorio en producción, en modo transparente para comprobar la efectividad de las firmas activadas en el laboratorio.

3.2 Metodología del trabajo

Para el desarrollo de este trabajo se tienen ideados varios pasos con los cuales se pretende ejecutar el aprendizaje acelerado, los cuales relaciono a continuación:

1) Elección de una aplicación Web en el ambiente de QA, se tiene como candidata un portal web desarrollado para facilitar la gestión y entrega de información a los clientes externos.
2) Creación y configuración de la política de seguridad sobre el WAF de QA, allí parametrizaremos y asociaremos la misma a la aplicación elegida en el punto anterior.
3) Ejecución de las pruebas de fast learnign automatizado, utilizando una aplicación que envíe parámetros de manera acelerada al mismo y un escáner de vulnerabilidades, puede ser OWASP ZAP.
4) Análisis de las evidencias halladas por la política para dicha aplicación y validar si es necesario volver a realizar el escaneo del paso anterior.
5) Exportar la política del ambiente de QA e implementarla en el ambiente productivo.

6) Revisar contra el tráfico real la aparición de sugerencias en la política de seguridad, si aún hay sugerencias o se redujeron al máximo.
7) Crear la política desde cero para la misma aplicación en producción y analizar la cantidad de apariciones versus las apariciones de la política acelerada.
8) Comparar los resultados.

4 Desarrollo especifico de la contribución

Como hemos observado, los ataques sobre la capa de aplicación son variados y los más fáciles de encontrar gracias a la cantidad de herramientas e información disponible en la Internet, de igual forma las defensas para mitigar los riesgos asociados a estos, en nuestro caso específico el firewall de aplicaciones ASM del fabricante F5, el cual nos ofrece una flexibilidad para construir una política adecuada a nuestras aplicaciones y esto es precisamente lo que queremos realizar, activar la mayor cantidad de firmas negativas en el menor tiempo posible para ahorrar riesgos innecesarios en el ambiente productivo.

4.1 Descripción del experimento

4.1.1 Entorno de laboratorio

Para la adecuación de este laboratorio se utilizaron los siguientes equipos, todos se encuentran virtualizados a excepción de la máquina de usuario confiable.

Máquina usuario: se utilizará un equipo portátil HP EliteBook Folio 1040 G3, con un procesador Intel Core i7-6600U de 2.6 GHz, memoria RAM de 8 GB. En este equipo se tendrá instalada la una máquina virtual de Kali Linux desde donde se ejecutará OWASP ZAP.

OWASP ZAP es una herramienta de seguridad catalogada como escáner de vulnerabilidades basado en el OWASP Top 10, el cual se ejecuta a modo de proxy, entre el navegador y la aplicación a analizar, enviando ataques automáticos, los cuales son de interés para acelerar el aprendizaje negativo en la aplicación del WAF.

F5 LTM con ASM QA: Dispositivo LTM virtualizado con el módulo ASM que es el Web Application Firewall a utilizar en este laboratorio, aquí se configurará la política para proteger la aplicación web. El Local Management Traffic es un balanceador de carga a nivel local, que se encarga de gestionar solicitudes a nivel de aplicaciones para mantener una alta disponibilidad en servicios web, adicional al ASM incluye varios módulos, como lo es aceleración del tráfico, gestión de certificados y manejo de cifrado y descifrado, para retirar la carga de los servidores.

Servidor QA: Se cuenta con un servidor Virtual Windows Server 2016, con un procesador Intel Xeon E5-2695 v3, 4 procesadores de 2.3 GHz, memoria RAM de 16 GB donde se encuentra alojado el servicio IIS donde con la aplicación web a probar, la cual está desarrollada sobre Microsoft .NET con una conexión a una base de datos de MSSQL.

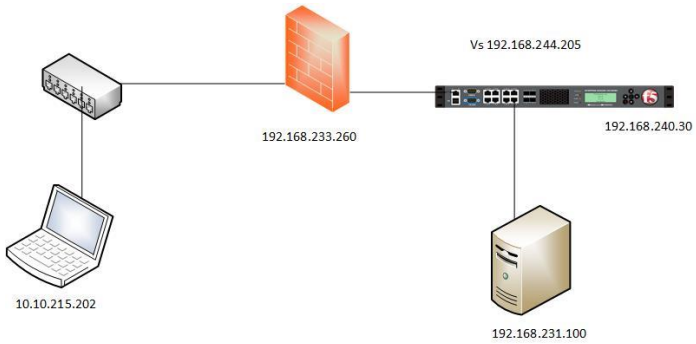

Figura 11: Arquitectura del laboratorio. (propia)

Virtual Server con Aplicación Web: En el servidor de pruebas tenemos desplegadas muchas aplicaciones web, pero nos enfocaremos en una que permite una alta interacción con los usuarios, es un portal web donde se generan reportes en formatos como .pdf, .xlsx, .txt y .csv adicional, hay información sensible y relevante sobre los movimientos de los clientes corporativos, como estados de cuentas, movimiento de dinero, información de los beneficiarios de dicho dinero, etc Esta aplicación se encuentra desarrollada con varias tecnologías, C#, Angular y JavaScript y hace conexión con una base de datos en un servidor MSSQL.

El virtual server se denomina a una dirección IP que se asigna en el LTM de F5 para presentar una aplicación al público actuando como proxy inverso, sobre esta dirección se asigna la política del ASM, la cual se encargará de ayudar en la proyección de la aplicación contra los ataques más comunes del OWASP Top 10. Para nuestro laboratorio se ha creado desde ceros la configuración también para dicha aplicación, por consiguiente, sacaremos las métricas de la cantidad de tráfico generado por la misma, así mismo en producción se sacará un promedio de conexiones en los 7 días de aprendizaje real, con esto podremos comparar que tan efectivo es realizar el aprendizaje mediante el escáner de vulnerabilidades.

4.1.2 Justificación herramientas elegidas

4.1.2.1 OWASP ZAP

OWASP ZAP es un escáner de vulnerabilidades que funciona como proxy, para poder interceptar el tráfico entre un cliente y un servidor, de uso libre y código abierto, multiplataforma, fácil instalación y uso intuitivo, con múltiples características que facilitan el análisis de aplicaciones web. En lo personal, considero este escáner como una de las mejores herramientas que puede utilizar un especialista en seguridad en sus inicios, es libre, tiene amplia documentación disponible en la internet, está soportada por OWASP y una gran comunidad de expertos en seguridad a nivel mundial.

Podemos destacar de esta herramienta su diversidad en plugin para uso en los análisis, el modo de escaneo pasivo, el crawling, analizar y modificar en tiempo real los requests hacía el

servidor, el modo ataque activo, la facilidad de configurar nuevas políticas de ataque según las necesidades, en mi opinión, una pequeña navaja suiza del análisis de vulnerabilidades en sitios web, y es precisamente esta una ventaja para mi laboratorio, contar con tantas formas de ataques (OWASP TOP 10), incrementando su cadencia, modificando en determinadas URLS que atacar, con qué técnica, con esto obtenemos un tráfico "ilegítimo" para que el WAF aprenda qué debe bloquear en esta política de seguridad negativa.

Los ataques utilizados por el escáner OWASP ZAP se basan en el OWASP TOP 10, a continuación, se realiza una breve descripción de cada uno de estos:

A1.2017 Inyección: Ocurre cuando un atacante envía datos inseguros al intérprete de la aplicación, en esta categorización se encuentran los tipos de inyección SQL, NoSQL, comandos de SO y LDAP, XPath.

A2.2017 Autenticación rota: Sucede cuando se implementa de manera inadecuada la autenticación en aplicaciones web, a los atacantes solo les bastará conocer una cuenta para poder comprometer la aplicación, también se pueden basar en métodos de fuerza bruta.

A3.2017 Exposición de datos sensibles: Se suele interceptar el tráfico en busca de protocolos de cifrado débiles o ausencia de estos para capturar información sensible, como usuarios y contraseñas.

A4.2017 Entidades externas (XXE): Se utiliza para explotar procesadores XML vulnerables, la idea es cargar un contenido hostil en el archivo XML y vulnerar el código para aprovecharse del mismo.

A5.2017 Pérdida de control de acceso: Los atacantes se aprovechan de la falta de controles de acceso para escalar privilegios, un ejemplo puede ser vulnerando alguna cuenta por defecto que tenga un rol administrador.

A6.2017 Configuración incorrecta de seguridad: Los atacantes siempre intentarán encontrar vulnerabilidades sin corregir o configuraciones por defecto para poder acceder al sistema.

A7.2017 Cross-Site Scripting (XSS): Es una de las vulnerabilidades más utilizadas, sucede cuando un atacante inserta comandos JS o HTML en una página web que no hace las validaciones correspondientes, exponiendo a los demás usuarios a la ejecución de estos comandos malintencionados en sus navegadores.

A8.2017 Deserialización insegura: Son ataques un poco más complejos de explotar, pero no, por ende, se deben menospreciar, suceden cuando se usan datos no confiables para alterar el funcionamiento de una aplicación al momento de deserializar el objeto.

A9.2017 Uso de componentes con vulnerabilidades conocidas: Es muy frecuente el uso de componentes de terceros, en ocasiones no se valida que problemas están asociados a dicho componente o si existe una versión más segura del mismo, el ataque se aprovecha de esto por medio de exploits.

A10.2917 Registro y monitoreo insuficiente: Si un sistema no tiene un control de los eventos que suceden en su sistema y que estos sean seguros, que no puedan ser modificados, estaremos ante un gran problema, ya que prácticamente estaremos ciegos ante un ataque o no podremos reaccionar de manera oportuna al mismo.

4.1.2.2 BIG IP ASM

En contraposición a la herramienta OWASP ZAP que era libre, la elección del WAF del fabricante F5 se hace por la experiencia que tengo trabajando con este dispositivo, entendiendo la necesidad de la empresa en la que laboro actualmente, su compromiso con la seguridad de la información y el riesgo al que se encuentra expuesta por el tipo de servicio financiero que presta, decidí investigar si existe una forma más efectiva de implementar una política en el menor tiempo posible, en un ambiente controlado y de fácil adaptación sobre el ambiente productivo. Aquí entra ASM, es una herramienta muy potente, flexible, robusta y con experiencia en el mercado de la seguridad, con buena documentación de acceso libre, también existe una gran comunidad de expertos a nivel mundial.

Como lo mencioné con anterioridad, el dispositivo trabaja en base a firmas, las cuales constantemente se están liberando y publicando en la página web del fabricante, adicional, también son publicadas firmas de tecnologías (aquellas que se pueden seleccionar al momento de crear la política, IIS, MSSQL, Windows Server, etc..) firmas de geolocalización por direcciones IP, firmas de anti-Bot y las actualizaciones sobre el firmware del dispositivo, haciéndola una herramienta muy completa.

4.1.3 Creación política de seguridad

Lo primero que se debe realizar es configurar la aplicación en el balanceador para tener un virtual server sobre el que se debe aplicar la política, acto seguido vamos a ir al módulo del ASM en el LTM y creamos la nueva política de la siguiente manera:

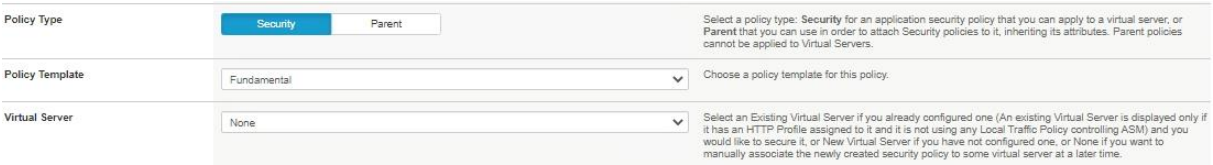

Figura 12: Elección plantilla fundamental ASM. (propia)

Elegimos el tipo de política como seguridad, ya que la idea es construirla nosotros mismos a modo de aprendizaje por tráfico generado desde la herramienta OWASP ZAP. Se elige la plantilla fundamental para crear la política por ser la mejor equilibrada, existe una plantilla que es basada en herramientas de escaneo de vulnerabilidades, pero lamentablemente está integrada con herramientas que son de paga y solicitan registro para un contacto comercial.

Lo siguiente será elegir el tipo de aprendizaje, le indicaremos que debe ser automático, para que el dispositivo intercepte el tráfico, lo analice y decida si lo considera una amenaza con referencia al archivo de firmas instalado, adicional le indicamos que debe permitir este flujo de datos continuar sin bloquearlo, así sea catalogado como una amenaza. La idea es esto es poder obtener la información de cuantas amenazas atravesaron el WAF enviadas desde el escáner de vulnerabilidades y poder aplicarlas de manera manual, así se tendrá la certeza de que la política ha recibido el tráfico malicioso deseado para su aprendizaje.

Luego escogemos que el aprendizaje sea manual y el tipo de aplicación de esta política sea de transparente, en otras palabras, vamos a permitir que el WAF capture todo el tráfico, pero lo permita y seamos nosotros quienes decidamos si es válido o no.

Por último, agregamos las direcciones IP de confianza desde las cuales el WAF registrará en sus excepciones y ayudarán a generar una política de manera más rápida y eficiente, además le dejamos la velocidad de aprendizaje en media, ya que esperamos generar un tráfico moderado, como si se tratara de un sitio productivo concurrido moderadamente.

4.1.4 Ataque con OWASP ZAP

Para esto vamos a ir a la máquina virtual de Kali Linux, actualizamos la distribución para obtener los últimos parches disponibles y ejecutamos OWASP ZAP, luego agregamos la URL de la aplicación que está siendo protegida por el WAF, en este caso es: https://192.168.244.205/PortalCorporativoNuevo/Portal/

Los primeros pasos son recorrer el sitio web, utilizando el escaneo manual que ofrece la herramienta, el fin de esto es ayudar al escáner de vulnerabilidades a entender nuestro sitio, y que arme un mapa de este, a su vez activamos el crawling sobre el sitio, para que vaya inspeccionando y capturando más información relevante para la herramienta.

Una vez terminada esta primera parte, vamos a OWASP e incluiremos la URL del sitio que estamos atacando y está protegido por el WAF en el contexto actual, le indicamos al escáner que queremos que esa URL esté en la mira, de esta forma, la podremos identificar de una manera más rápida en caso de que aparezcan otras URLS diferentes a la que estamos analizando y no perder de vista el objetivo y los hallazgos asociados al mismo.

Ahora en las opciones que nos ofrece seleccionamos las tecnologías que usa nuestra aplicación web, al igual que en el WAF, en OWASP podemos indicarle que la aplicación está corriendo sobre un IIS, en un Windows Server, con un motor MSSQL y desarrollada con un lenguaje de ASP.NET con esto se pretende afinar el escaneo, para que utilice los ataques o evasiones más comunes para estos tipos de tecnologías, además no generamos tanto tráfico basura, que tal vez sea catalogado como amenaza, pero será para engrosar la política de forma no productiva.

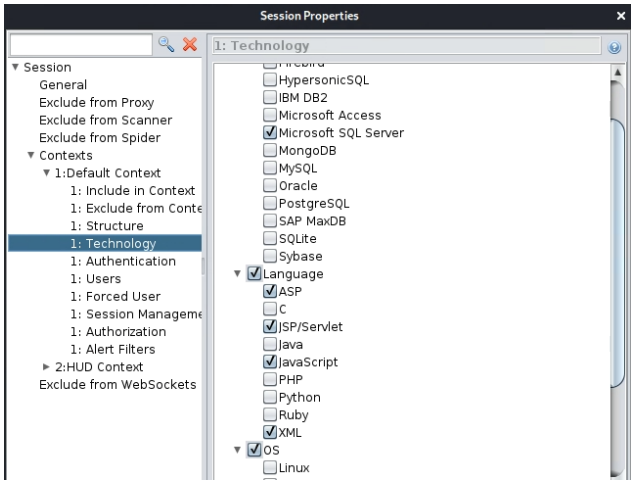

Figura 13: Tecnologías utilizadas en la aplicación web OWASP ZAP. (propia)

Con esto hemos terminado con la configuración del contexto para esta aplicación, ahora debemos configurar la política de escaneo, en la cual debemos configurar los niveles de intensidad del ataque, dejamos por defecto el nivel de alerta, pero la intensidad del ataque la dejamos en alta, con esto garantizamos que la herramienta enviará muchas peticiones tratando de encontrar vulnerabilidades. También subimos el nivel de ataque de inyección, siendo este el problema más recurrente en las aplicaciones web, queremos cubrirlo de muy buena manera para que el WAF detecte los diversos tipos de inyección que se intentarán sobre el sitio por la herramienta y almacene el conocimiento de estos para su futura implementación en producción.

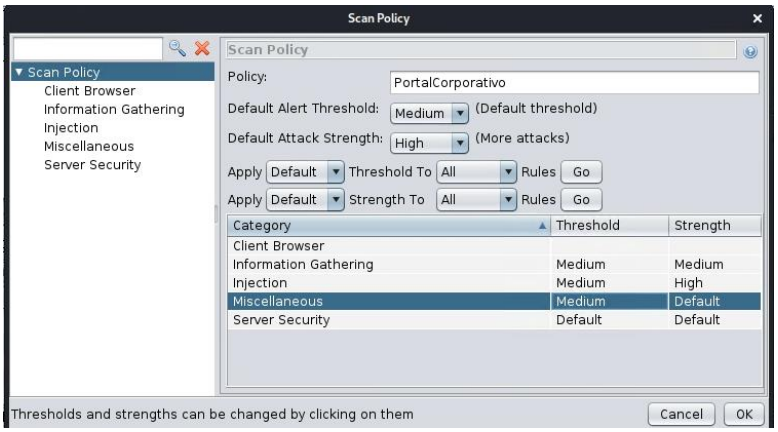

Figura 14: Política de escaneo OWASP ZAP. (propia)

Al validar la política en el WAF ya existen sugerencias de nuestro recorrido utilizando el modo de escaneo manual en OWASP, una de las sugerencias nos indica que se están utilizando caracteres no válidos, como lo son / o \ en la URI los cuales pueden tener un riesgo potencial en la aplicación web, son utilizados con frecuencia en los ataques CSRF o XSS para invocar sitios maliciosos o ejecutar comandos malintencionados respectivamente.

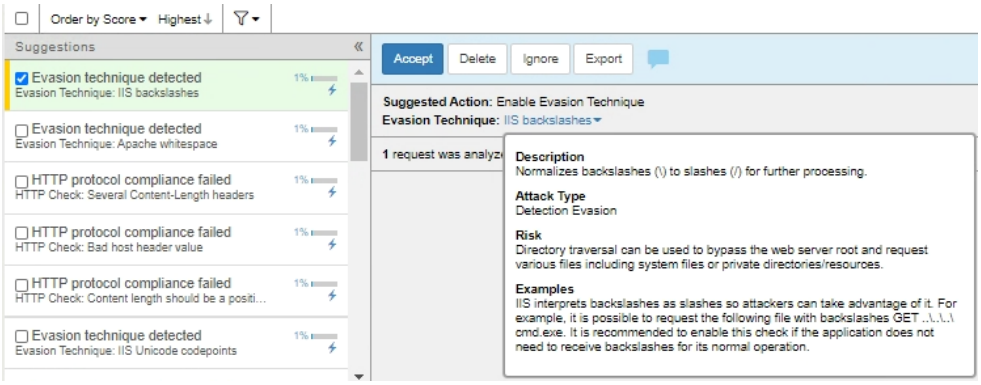

Figura 15: Sugerencia WAF caracteres inseguros. (Propia)

Debemos analizar con cuidado las sugerencias referentes a parámetros, en algunas aplicaciones desarrolladas por la empresa, hemos evidenciado envío de caracteres especiales que aparentan ser un ataque, pero no es así, ya que los desarrolladores los usan para armar objetos e invocar otras URLS.

Otro de los hallazgos que encontró el WAF es que se están enviando caracteres más allá del cierre de línea, no es algo riesgoso, pero podría considerarse sospechoso en un ambiente productivo.

Ahora debemos iniciar el escaneo automático, en el cual se realizará el ataque con las configuraciones y especificaciones realizadas en los pasos anteriores, enviando tráfico malicioso del tipo OWASP TOP 10, haciendo hincapié en los ataques de tipo inyección.

Se han realizado repetidos escaneos sobre los diferentes directorios que detecto el escáner de vulnerabilidades, la idea es hacer crecer la cantidad de tráfico y que el ASM registre esto y siga aprendiendo sobre las potenciales amenazas.

Al finalizar los ataques con la herramienta de análisis de vulnerabilidades y después de un tiempo, en el que corremos sobre la ruta principal un escaneo activo exhaustivo, casi hemos completado la política de seguridad, encontrándose sobre un 86% y con 469 anomalías detectadas en el tráfico HTTPS

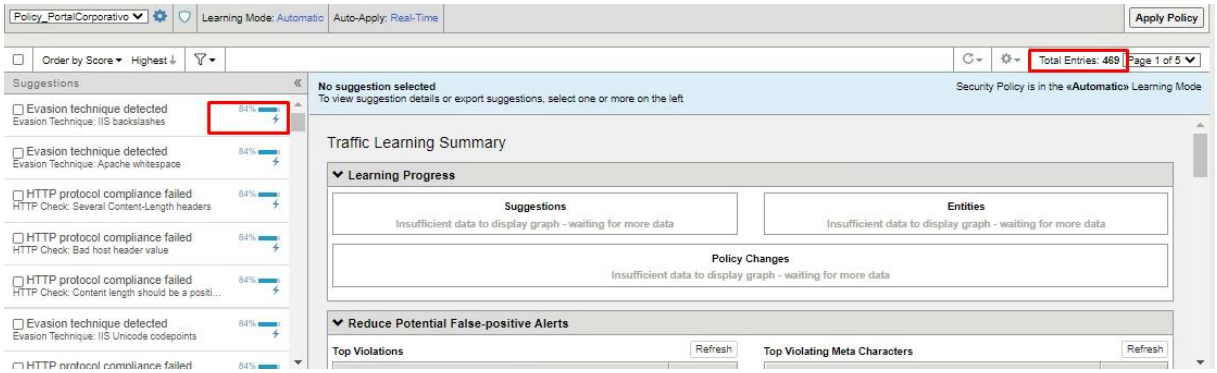

Figura 16: 469 entradas en aprendizaje. (Propia)

Al completar el escaneo, ciertas firmas se completan al 100%, estas se aplican automáticamente a la política la cual debemos validar que aún siga en modo de aprendizaje, ya que necesitamos completar la mayoría de las firmas posibles.

Se requiere un escaneo exhaustivo con el ataque alto a cada una de las carpetas del sitio para poder completar en su mayoría la política.

Para tener una métrica de esta etapa, se han gastado aproximadamente 6 horas de escaneo sobre la aplicación, no consecutivas para no generar alertas en la red interna de la organización.

Se escanearon por parte de OWASP ZAP gracias al modo Fuzz 220 URIS dentro de las cuales se descubrieron archivos que utiliza el aplicativo web.

4.1.5 Confirmando amenazas

Al llegar al 100% del aprendizaje, hemos generado suficiente tráfico para que el ASM haya registrado de sus 2642 registros de firmas, algunas alertas las cuales se encuentra agrupadas por el tipo de ataque o violación en el ASM. Como la política se configuró con un aprendizaje automático, esta entra en modo bloqueo inmediatamente, no obstante, las alertas por nuevo tráfico se seguirán generando por el periodo que dure la configuración de la política, en este caso 7 días, una vez finalizado este periodo se bloqueará cualquier tráfico ilegal sin importar

que sea legítimo, esta parte siempre es la tarea dispendiosa de la puesta en marcha en producción.

Tipo de Violación	Cantidad
Ataques de firma detectados	538
Estado de respuesta ilegal en HTTP	2
Longitud ilegal en método POST	1
Longitud ilegal en URL	1

Tabla 1: Evidencias agrupadas.

Ahora debemos aceptar todas las sugerencias que el WAF ha evidenciado, confirmándole efectivamente, que todos los hallazgos son tráfico malintencionado y que la comparación que se realizó en base a su archivo de firmas es correcta. Al finalizar la aplicación de las más de 2000 sugerencias el "Traffic and learnign" queda vacío.

Firma detectada	Total
SQL-INJ ' UNION SELECT (Parameter)	28
timeout execution attempt (Parameter)	28
Directory Traversal attempt "../" (Parameter)	28
Directory Traversal attempt (../Windows) (Parameter)	28
/windows access	28
ZAP Probe (W45pz4p) (Parameter)	28
ZAP Probe (thishouldnotexistandhopefullyitwillnot) (Parameter)	28
Session Fixation Attempt - 4 (Parameter)	28
ASP.NET injection attempt (response.write) (2) (Parameter)	28
SQL-INJ expressions like "AND 1=1" (7) (Parameter)	26
SQL-INJ expressions like "sleep()" (3) (Parameter)	26
SQL-INJ "UNION ALL SELECT NULL" (Parameter)	26
"timeout" execution attempt (2) (Parameter)	26
"Start-Sleep" execution attempt (Parameter)	26
"get-help" execution attempt (Parameter)	26
"sleep" execution attempt (3) (Parameter)	24
XSS script tag (Parameter)	22
XSS script tag end (Parameter) (2)	22
<script>alert(1);</script> (Parameter)	22
SQL-INJ expressions like "OR 1=1" (7) (Parameter)	21

Tabla 2: Top 20 evidencias por total

Después de aplicada, generamos nuevamente tráfico con OWASP ZAP utilizando la misma política de ataque creada anteriormente, con esto validaremos que nos muestra el ASM con respecto a lo que aprendió, se evidencia que se han logrado capturar algunas violaciones interesantes usando la política.

Tipo de Violación	Cantidad
Ataques de firma detectados	31
Técnica de evasión	8
Cumplimiento de protocolo HTTP	2

Tabla 3: Nuevos registros ASM

Con el nuevo tráfico generado se han detectado las siguientes amenazas, al no encontrase en etapa de bloqueo, alerta los hallazgos, para que se tengan presentes que decisión se deben tomar con los mismos, en nuestro caso y teniendo conocimiento que estamos formando una política hecha netamente con seguridad negativa, debemos seleccionar y bloquear estas nuevas alertas.

Tipo de Entidad QA	Total	No forzado
Tipos de archivos	1	0
HTTP URLs	2	0
WebSocket URLs	2	0
Parámetros	29	0
Cookies	1	0
Signatures	2642	285
Campañas de amenaza	0	N/A
Redirección de dominios	1	N/A
Cumplimiento protocolo HTTP	19	0
Técnicas de evasión	8	0
Seguridad de servicios Web	13	13

Tabla 4: Nuevos tipos de amenazas detectadas.

4.1.6 Política productiva

Cómo métrica comparativa y de control, utilizaremos en contraste una política generada en igual de condiciones, para la misma aplicación en el ambiente productivo, la cual registrará tráfico legítimo o puede que no, de usuarios reales que a diario realicen su autogestión de información por medio de esta plataforma.

Las condiciones son las mismas, misma política creada desde ceros, plantilla fundamental, aprendizaje automático a una velocidad media, la cual estará en proceso de aprendizaje por 7 días, al final de estos, procederemos a validar si es sostenible el aprendizaje por medio de un escáner de vulnerabilidades. Lo que se pretende comprar es si al realizar un escaneo de un par de horas sobre el sitio y sus subsitios y/o directorios es tan eficiente como 7 días de tráfico generado por usuarios reales y concurrentes, realizando sus operaciones normales.

Adicional a la información generada por el ASM en el LTM productivo, contamos con una herramienta complementaria, la cual nos brindará información de contadores, permitiéndonos conocer la cantidad de conexiones, desde que se active la política hasta su fin concluidos los 7 días, para esto se configura un perfil de análisis sobre BigIQ, un dispositivo

para monitorizar los balanceadores de carga, tomando métricas como logs, salud de los equipos, consumos, conexiones, tráfico generado, etc. En dicho dispositivo asociaremos un perfil de analítica que fue creado sobre la dirección virtual del portal web en producción, con esto será suficiente para que se comiencen a registrar todos los eventos que lo atraviesen, ya que esta información nos será útil a la hora de hacer la comparación final.

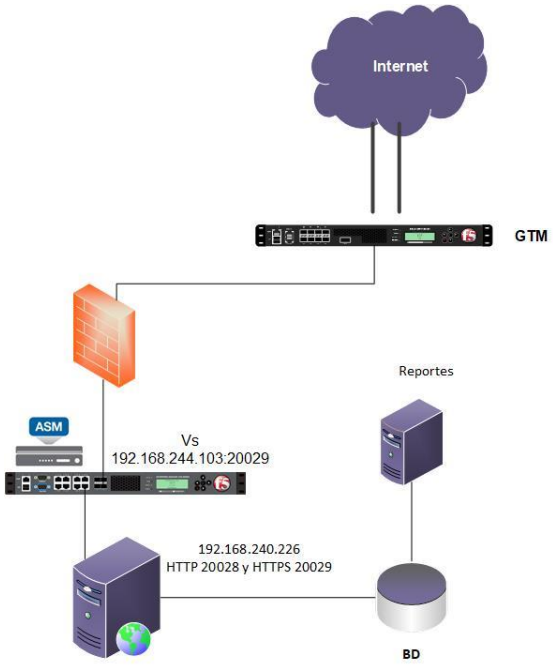

Figura 17: Arquitectura productiva Portal y ASM. (Propia)

4.1.7 Métricas política productiva

Después de siete días de creada la política sobre el ambiente productivo en modo de aprendizaje, procedemos a evaluar las métricas tomadas por el dispositivo BigIQ. La política fue activada en el ASM el 01 de junio en horas de la noche, y los eventos se comenzaron a reflejar de manera inmediata desde entonces y hasta el 08 de junio recibió peticiones de usuarios reales en modo aprendizaje, registrando el tráfico legítimo como algunas violaciones. Vamos a revisar los números respecto a esta semana de espera.

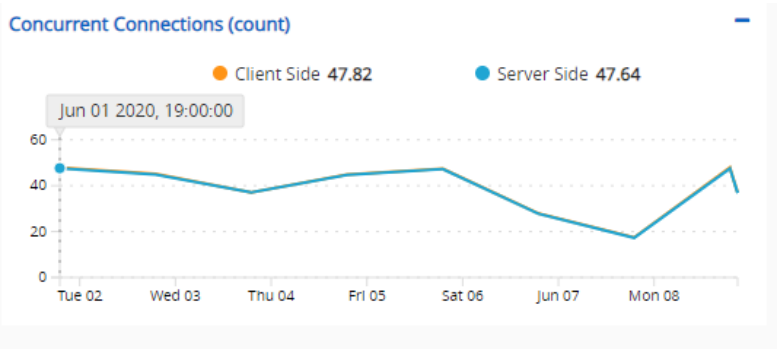

Figura 18: Máximo de conexiones concurrentes. (Propia)

Según información entregada por el perfil de analítica de BigIQ en el transcurso de una semana se tuvo un máximo al día máximo de 48 conexiones concurrentes sobre el portal web que contiene la política productiva.

En el transcurso de una semana se realizó un análisis de las conexiones establecidas sobre el sitio productivo, aquí evidenciamos la importancia de la seguridad, esta aplicación es para uso de clientes corporativos a nivel nacional en Colombia, y como podemos observar en el siguiente grafico hemos tenido transacciones desde diferentes países, algunos de ellos sospechosos por propiciar ciber ataques.

Figura 19: Transacciones por países. (propia)

Ahora si echamos un vistazo al comportamiento de la política productiva del ASM en las estadísticas del BigIQ para el portal web, se han capturado algunas alertas pero en su mayoría el tráfico es legal, desde su activación el 01 de junio en horas de la noche se puede observar el incremento en la curva hasta el martes 2 de junio, después de esto, comienza el descenso del aprendizaje y se mantiene así hasta la fecha en que se cumple el periodo de aprendizaje el 7 de junio, a partir de allí nuevamente comienza un ciclo de alertas nuevas.

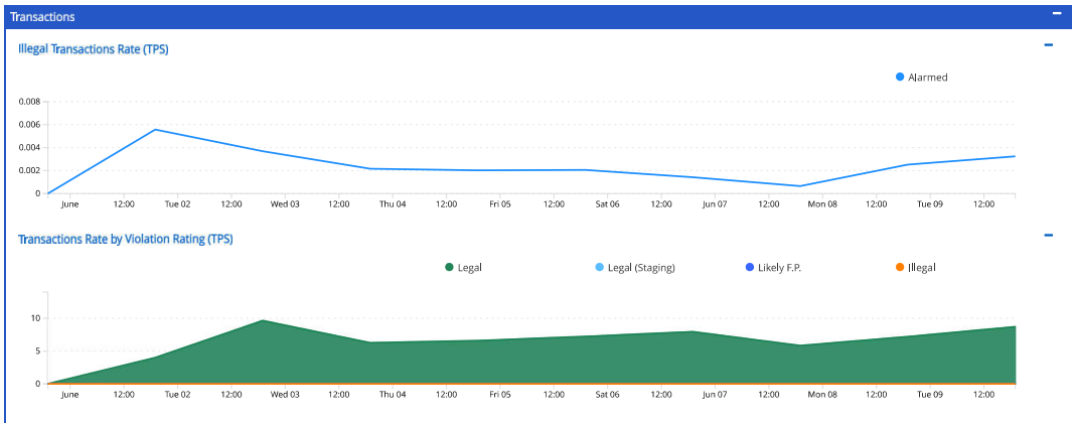

Figura 20: Transacciones en política ASM. (propia)

4.1.8 Análisis política productiva

Validando las evidencias de la política productiva, la cual ha estado un poco más de 8 días, se han alertado algunas peticiones, la cuales tienen algunas similitudes con las capturadas sobre el escaneo en el ambiente de QA, con la diferencia que en esta se tienen un alto caudal de peticiones legales, las cuales generaron algunas alertas y revisaremos a continuación:

Tipo de Entidad	Total	No forzado
Tipos de archivos	15	0
HTTP URLs	2	0
WebSocket URLs	2	0
Parámetros	2	0
Cookies	1	0
Signatures	2708	285
Campañas de amenaza	0	N/A
Redirección de dominios	0	N/A
Cumplimiento protocolo HTTP	19	0
Técnicas de evasión	8	0
Seguridad de servicios Web	13	13

Tabla 5: Amenazas detectadas política productiva. (propia)

Al hacer la comparativa entre las dos políticas, encontramos que existe una similitud entre las dos, excepto que para la implementación productiva tenemos una identificación de 15 tipos de archivos contra 1 evidenciado en la política de QA, esto se debe a los reportes que son generados desde el portal por los usuarios y sus distintas formas de exportación.

En contraparte vemos que en la política de QA capturamos 29 parámetros que fueron usados por OWASP ZAP gracias a sus ataques por diccionario en las URLS identificadas por este y en la implementación productiva solo se capturaron 2 parámetros.

En cuanto a los últimos tres ítems de las tablas, se comparten los hallazgos en las dos políticas, indicando tentativamente que en nuestro laboratorio nos hemos acercado a los consumos reales y las posibles violaciones que se podrían generar en un ambiente real.

Existe una diferencia en la política productiva y es que se activaron 2708 de las firmas registradas en su archivo de las cuales el WAF nos informa que están listas para entrar a modo bloqueo 285 en contra partida, para QA se activaron 2642 alertas sobre su archivo y de estas tenemos listas para bloqueo también 285.

Se aclara que el archivo de firmas utilizado en los ambientes de QA y producción es el mismo, si no fuese así podríamos entrar en conflicto en la migración de las políticas entre dispositivos.

Tipo de Violación	Cantidad
Estado de respuesta ilegal en HTTP	2
Longitud ilegal en método POST	1
Método ilegal	1
Longitud de consulta de cadena ilegal	1

Tabla6: Tipos de violaciones agrupados en producción. (propia)

En la política implementada en producción se obtuvieron 4 diferentes grupos de violaciones, que son las que se encuentra en la anterior tabla, allí podemos clasificar todo el tráfico "malicioso" que ASM detecto proveniente de los usuarios reales del portal web.

4.1.9 comparación de políticas

En este paso podremos observar la diferencia entre el aprendizaje rápido creado a partir de tráfico malintencionado generado con la herramienta OWASP ZAP contra el aprendizaje normal a lo largo de aproximadamente 8 días generado por usuarios reales, para esto debemos ir a uno de los dispositivos ASM, en mi caso utilizaré el de QA donde ya se encuentra la política "Policy_PortalCorporativo" y debemos importar la política del ambiente productivo "Policy_PortalCorporativo_Prod", esto con el fin de que el dispositivo nos realice una comparativa entre las dos indicándonos exactamente qué diferencias existen entre ambas. ASM nos otorga una opción de construir una política proveniente de la fusión de las dos, o de una selección específica entre ambas, por ejemplo, si quisiera algunas alertas generadas en producción copiarlas a la política de QA o si quisiera pasar los parámetros aprendidos en QA hacía la productiva.

Pero antes, observemos la cantidad de entradas totales, es decir sin agrupar en los diferentes tipos de alertas, para dejar claro este punto, en ASM al dispararse una alerta allí se almacena cierta cantidad de eventos asociados al mismo, lo que se llama una muestra, generalmente entre más ocurrencias se tenga de un tipo determinado de alerta, el WAF podrá tener un modelo más amplio, un ejemplo de esto lo podemos observar en la siguiente imagen.

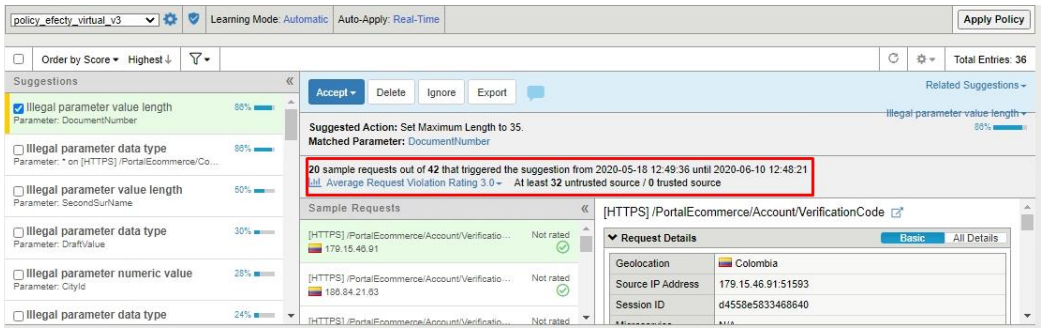

Figura 21: Ejemplo muestra de tráfico. (propia)

Del tráfico diario en un sitio web, la mayoría es legítimo, el ASM indica que cantidad de este dispara determinadas entradas o alertas, y toma una traza, indicando cuantas veces ha sucedido en totalidad y una muestra de este, generalmente esta se compone de diferentes formas en que se ha violado dicha firma, para que se tenga mayor claridad al momento de tomar una determinada decisión o si se acepta la sugerencia del dispositivo.

Teniendo presente lo anterior debemos conocer cuantas entradas se han disparado en las dos políticas, comencemos con la que fue creada en producción, la cual estuvo aproximadamente 8 días en modo de aprendizaje, con un total de 3131 entradas en los registros del ASM, estas evidencias se encontraban agrupadas en 4 tipos de alertas (tabla 6), la mayoría sugerencias de modificaciones sobre parámetros y otras aceptar códigos de respuestas del sitio web.

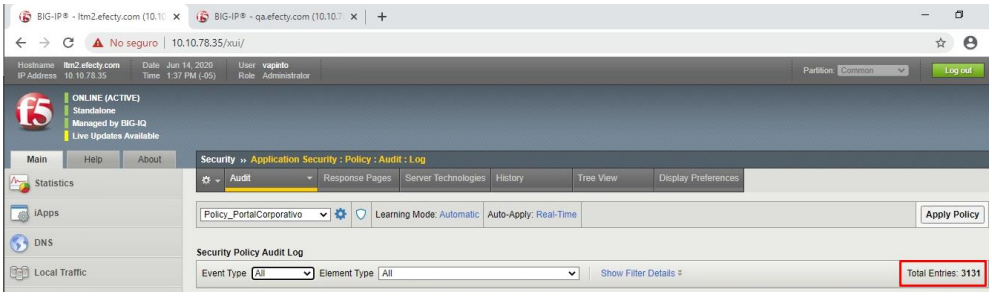

Figura 22: Total eventos detectados ASM Producción. (propia)

En contraste, la política generada a través del escáner OWASP ZAP, el cual en total se ejecutó aproximadamente 6 horas en el ambiente de QA, alcanzó a generar 3579 entradas en ASM, las cuales se encuentran agrupadas también en 4 colecciones, con la gran diferencia que en esta hemos registrado más de 500 eventos de firmas en uno de esos grupos, lo cual es interesante, ya que al hacer forzado en la política de seguridad en el WAF, si un evento similar vuelve a suceder sobre esta política será bloqueado inmediatamente.

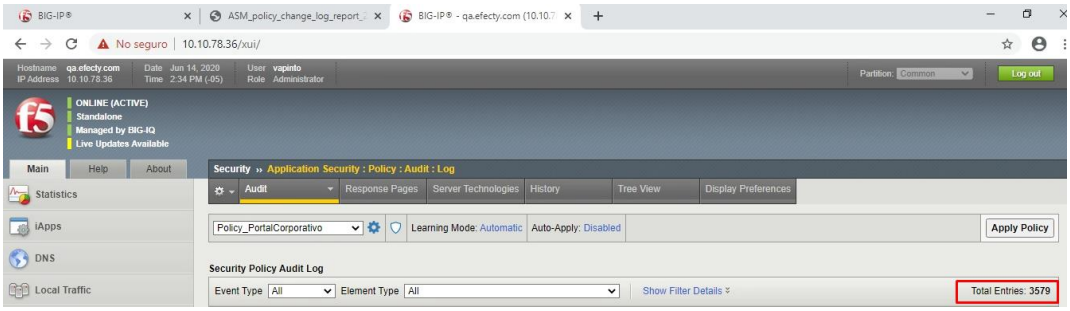

Figura 23: Total eventos detectados ASM QA. (propia)

Al utilizar la herramienta de diferenciación entre políticas del ASM encontramos la siguiente información, que es lo que se aprendió diferente a las alertas por firmas, es decir, estos son valores únicos para cada aplicación y política, para este ejemplo, nuestra implementación

productiva aprendió 69 tipos de archivos diferentes que se utilizan en el portal web, esto solo ocurrió porque los usuarios invocaron en algún momento cada uno de estos archivos, por otra parte, la implementación en QA aprendió 27 parámetros nuevos que usa la aplicación en QA, esto gracias a los directorios que utilizó OWASP ZAP para descubrirlos.

Tipo de Entidad	Existente en Política QA	Existente en Política Productiva	Entidades Diferentes
Técnicas de evasión	0	0	2
Tipo de archivo	0	69	1
Comprobación HTTP	0	0	1
HTTP URL	0	0	1
Header	0	0	2
Nombre de HOST	0	1	0
Parámetros	27	0	1
Atributos de política	0	0	1
Configuración creación de política	0	0	1
Firmas de política	0	0	5
Protección de redirección	0	0	1

Tabla 7: Diferencias aprendidas entre políticas. (Propia)

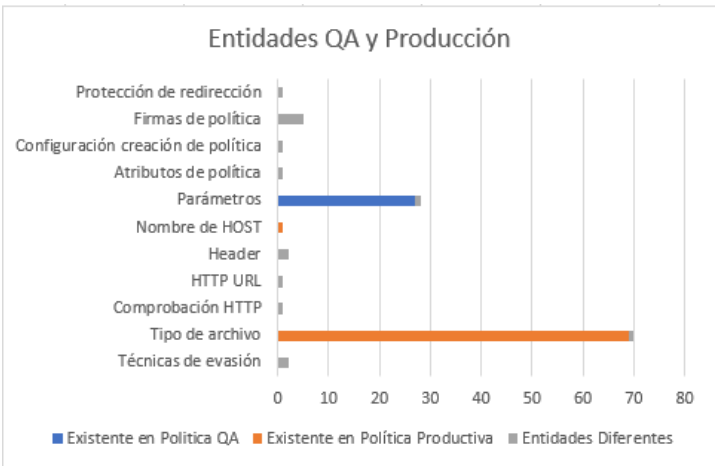

Figura 24: Gráfico de entidades en QA y producción. (propia)

Adicional a los valores aprendidos por una u otra política, también tenemos un columna con las entidades diferentes, esto indica que hay un match en ambas políticas, por ejemplo, un tipo de violación, pero en una el aprendizaje está detenido y en la otra se encuentra activo o por ejemplo, la longitud de determinado método POST en una de las políticas se modificó a 3000 caracteres mientras en la otra está por defecto en 1000, esta información ayuda, para poder tomar decisiones.

Realizando una comparación de las políticas con un editor de texto, Notepad ++, el cual hace una diferencia entre dos archivos y enseña que existe en uno y qué falta en el otro, respetando

el espaciado donde debería estar estos, nos indica que en la política generada en el laboratorio contiene un total de 28486 líneas, contra 27908 de la política de control creada en producción, al realizar la revisión a fondo, encontramos del lado de la política de control, que lo que no se comparte con la generada en QA son los tipos de archivos aprendidos, mientras que al validar que tiene la política creada en pruebas con OWASP ZAP, esta contiene las firmas activadas en el escenario controlado, las cuales se encuentran listas para entrar en bloqueo.

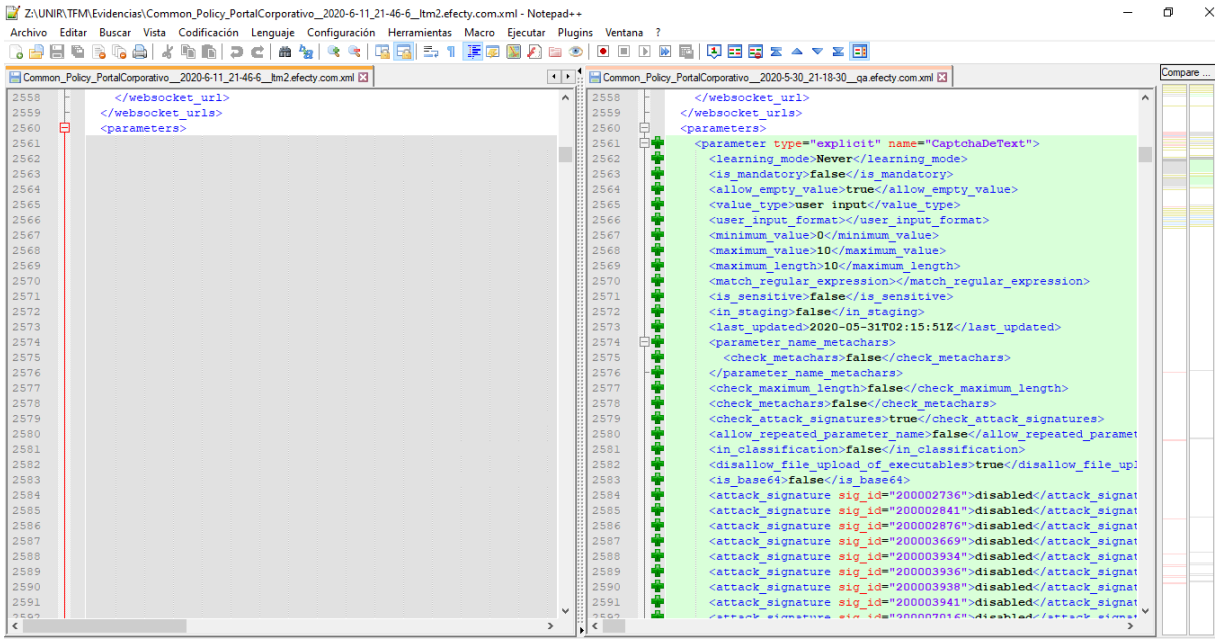

Figura 25: Comparación a nivel de XML entre políticas. (propia)

4.1.9 Implementación política de QA en producción

Conociendo las diferencias entre las políticas, tenemos presente que la implementación del ambiente de QA recibió mucho tráfico de seguridad negativa, el cual fue bloqueado aceptando las sugerencias del mismo en el dispositivo de pruebas, ahora al implementar esta política en producción tenemos presente que existe una diferencia de 69 archivos diferentes que deberá aprender, pero estas son sugerencias realizadas por el WAF, lo que realmente queremos observar es si los casi 500 eventos asociados a firmas detectados en QA, realmente están bloqueando o marcándose como tráfico ilegal, para esto procederemos a modificar la política implementada en producción por la generada en el laboratorio de QA bajo el escaneo de OWASP ZAP y la dejaremos una semana más, seguirá en modo transparente para detectar las sugerencias en el aprendizaje, se espera que estas sean mínimas ya que se ha inducido al ASM con mucho tráfico malintencionado generado de manera automatizada. La política es activada el día 14 de junio en horas de la noche, por consiguiente, debemos revisarla nuevamente 8 días después para observar las ocurrencias.

Transcurridos 8 días de implementada la política de QA en producción, la cual está en modo transparente aprendiendo aún, ha detectado activado algunas alertas en el aprendizaje, se evidencia que se ha recibido recientes ataques sobre el portal corporativo en producción, que coinciden con un ataque de FUZZING ya que se están buscando diversos directorios como los utilizados por OWASP ZAP, el tráfico es permitido, por temas de políticas corporativas no puedo proceder a bloquear este sin realizar un previo control de cambios e informando al área de seguridad para que estén al tanto (reporte que fue generado inmediatamente se evidenció esta anomalía) sin embargo, las alertas se encuentran en los logs y el mismo es marcado como tráfico ilegal, el cual sería inmediatamente bloqueado al pasar el estado de la política de transparente a bloqueo, desde su implementación se detectaron 187 nuevos eventos en una semana, los cuales se sumarían al aprendizaje de los más de 3500 eventos generados por el escáner de vulnerabilidades en QA activados en un par de horas, contra los 3136 eventos disparados en la política de control de producción, la cual estuvo aproximadamente 8 días registrando eventos reales de usuarios, esto evidencia que la política con aprendizaje acelerado obtuvo una buena información de tráfico negativo en su etapa de aprendizaje en el laboratorio efectuado, ya que solo se registraron 187 nuevos eventos, los cuales están asociados al incidente de ataque real y algunos son tipos de archivos que no se aprendieron en el laboratorio y sobre los que se debería afinar la política productiva.

5 Conclusiones y trabajos futuros

En este trabajo hemos acelerado el aprendizaje de una política de seguridad mediante el escáner de vulnerabilidades OWASP ZAP, con el cual realizamos aproximadamente 6 horas de ataques, comenzando con uno pasivo y luego con varios activos, uno sobre cada URI encontrada por el mismo con una intensidad alta en su política de ataque, mientras el WAF registraba las entradas en su panel de aprendizaje, agrupándolas por tipo, acto seguido se forzaron estas sugerencias y se implementó una política en producción desde cero con las mismas características como métrica de control, pero con la ventaja de tener más tiempo aprendiendo y en un entorno real, recibiendo tráfico legítimo.

A partir de los resultados obtenidos podemos concluir lo siguiente:

OWASP ZAP es una herramienta muy versátil y sus ataques incluyen el OWASP TOP 10, por lo cual se tendrá una línea base muy completa para iniciar un aprendizaje de política de seguridad.

El WAF ASM del fabricante F5 es muy flexible y permite detectar muchas entradas del tráfico malintencionado, así mismo la reducción de falsos positivos depende del refinamiento de la política de seguridad en etapas posteriores.

Se puede lograr una política inicial robusta utilizando OWASP ZAP, ya que los resultados obtenidos en cuanto a entradas y entidades es de calidad y en menos tiempo, en 6 horas se alcanzaron a ingresar más entradas al aprendizaje y se generaron activaciones de firmas, adicional se aprendieron bastantes parámetros gracias a los diccionarios que incluye la herramienta. Por otro lado, la política productiva al estar recibiendo tráfico real detectó 69 tipos de archivos, los cuales fueron usados por varios usuarios, activando estas sugerencias, al igual que las páginas de respuesta por defecto del IIS.

Implementar una política de seguridad es una tarea dispendiosa y de cuidado, se requiere tener un conocimiento de la aplicación que se está asegurando para evitar errores en el momento del entrar al modo bloqueo de la misma.

Los resultados son alentadores, se puede concluir de manera general que si se tiene la posibilidad de usar un escáner de vulnerabilidades para acelerar el aprendizaje negativo de una política se debería de realizar, con esto garantizamos tener unas bases firmes para empezar el modelado de la misma, sin embargo, no quiere decir que con solo realizar un par de horas de escaneo nuestra aplicación estará segura, se requiere dedicación, refinación y mantenimiento a esta, ya que todas las aplicaciones son diferentes, al igual que las variables usadas para su infraestructura (servidor web, tecnología usada para el desarrollo, motor de base de datos, etc)

cambian constantemente, adicional, se encuentran vulnerabilidades todos los días en diferentes dispositivos y tecnologías, incluyendo los mismos WAF.

La política que se aprendió en este laboratorio fue netamente seguridad negativa, esto indica que bloqueamos todo lo que tenemos en una lista negra y que no está permitido para una aplicación web.

6 Glosario

ASM: Application Security Manager, módulo WAF del fabricante F5.

BigIQ: Dispositivo para centralizar administración de otros equipos de F5 y toma de métricas.

Bot: Software que realiza tareas repetitivas

Capcha: Aplicación para distinguir un usuario real de un bot.

DNS: Sistema de nombres de dominio, su función es interpretar los nombres para buscar la dirección IP asociada a la misma en la internet.
DoS: Denegación de Servicio, ataque realizado para saturar un servicio para hacerlo colapsar.

Exploit: Técnica para aprovechar una vulnerabilidad.

Firmware: Software de bajo nivel que controla los circuitos.

Framework: Entorno de trabajo que tiene predefinido unos módulos de software.

FTP: Protocolo usado para la transferencia de archivos.

GTM: Global Traffic Manager, dispositivo para gestión de zonas, dns y tráfico público.

HTTP: Protocolo de transferencia de hipertexto, permite transmitir información en la internet.

IIS: Servidor Web de Microsoft

LDAP: Protocolo ligero de acceso a directorios, permite acceso a un directorio.

LTM: Local Traffic Manager, balanceador de carga del fabricante F5

Malware: Aplicaciones malintencionadas creadas para aprovechar vulnerabilidades en los sistemas de usuarios.

MSSQL: Servidor de base de datos de Microsoft

OSI: Modelo de interconexión de sistemas abiertos, es un estándar para poder comunicarse con otros sistemas.

OWA: Acceso web para el correo Outlook

OWASP: Proyecto de código abierto que se dedica a investigar y combatir las causas de inseguridad en las aplicaciones.

Payload: Carga útil, es el mensaje que se envía o en el escenario de un ataque, el script que se inyecta.

Puente: Dispositivo que interconecta dos redes.

QA: Hace referencia a calidad, bien sea un ambiente de pruebas QA.

RSH: Programa de consola que permite la ejecución de comandos remotamente.

SMTP: Protocolo usado para el envío de correos en redes.

S-SDLC: Ciclo de vida de desarrollo seguro.

Snort: Es un sistema de detección de intrusos.

Squid: Aplicación para hacer funciones de proxy web.

URI: Identificador uniforme de recursos, es una ruta dentro de una página web.

URL: Localizador uniforme de recursos, su función es indexar hacía un contenido o página especifica en la internet.

VIP: Terminología usada en el WAF de Barracuda para hacer referencia a una dirección IP virtual.

Virtual Server: Terminología que se utiliza por F5 para identificar una dirección IP virtual.

WAF: Firewall de aplicaciones web, funciona a nivel de capa 7 del modelo OSI.

XML: Lenguaje de marcado extensible, utilizado para almacenar datos en forma legible.

7 Referencias

Baranov, P. A., & Beybutov, E. R. (2015). Securing information resources using web application firewalls.

Barracuda. (2019c). Cómo proteger las cookies HTTP. Recuperado el 22 de febrero de 2019, a partir de: https://campus.barracuda.com/product/webapplicationfirewall/doc/4259854/how-to-secure-http-cookies

Barracuda. (2020e). Configuración ACL globales. Recuperado el 19 de mayo de 2020, a partir de: https://campus.barracuda.com/product/webapplicationfirewall/doc/4259851/configuring-global-acls

Barracuda. (2019e). Configuración de la normalización de URL. Recuperado el 24 de mayo de 2019, a partir de: https://campus.barracuda.com/product/webapplicationfirewall/doc/4259853/configuring-url-normalization

Barracuda. (2019f). Configuración de la política de acción. Recuperado el 22 de febrero de 2019, a partir de: https://campus.barracuda.com/product/webapplicationfirewall/doc/4259856/configuring-action-policy

Barracuda. (2020d). Configuración de protección contra robo de datos. Recuperado el 3 de junio de 2020, a partir de: https://campus.barracuda.com/product/webapplicationfirewall/doc/4259929/configuring-data-theft-protection

Barracuda. (2020c). Configuración de protección contra robo de parámetros. Recuperado el 03 de junio de 2020, a partir de: https://campus.barracuda.com/product/webapplicationfirewall/doc/4259929/configuring-data-theft-protection

Barracuda. (2019d). Configurando el encubrimiento. Recuperado el 22 de febrero de 2019, a partir de: https://campus.barracuda.com/product/webapplicationfirewall/doc/4259864/configuring-cloaking

Barracuda. (2020b). Configurar la protección URL. Recuperado el 03 de junio de 2020, a partir de: https://campus.barracuda.com/product/webapplicationfirewall/doc/4259876/configuring-url-protection

Barracuda. (2020a). Configurar límites de solicitud. Recuperado el 3 de junio del 2020, a partir de: https://campus.barracuda.com/product/webapplicationfirewall/doc/4259870/configuring-request-limits

Barracuda. (2016). Firmas inteligentes. Recuperado el 22 de marzo de 2016, a partir de: https://campus.barracuda.com/product/webapplicationfirewall/doc/90445705/smart-signatures/

Barracuda. (2019b). Paso 2: configurar un service. Recuperado el 13 de noviembre de 2019, a partir de: https://campus.barracuda.com/product/webapplicationfirewall/doc/4259899/step-2-configuring-a-service

Barracuda. (2019a). Políticas de seguridad. Recuperado el 21 de febrero de 2019, a partir de: https://campus.barracuda.com/product/webapplicationfirewall/doc/4259878/security-policies/

Bellovin & Cheswick. (1994). Network Firewalls

Cisomag. (2020). Attacks on Web Applications surged in 2019: report. Recuperado el 10 de febrero de 2020 a partir de: https://www.cisomag.com/attacks-on-web-applications-surged-in-2019-report/

CyberSecurity Ventures. (2018). Global Cybercrime Damages Predicted to Reach $6 Trillion annually by 2012. Recuperado el 7 de diciembre de 2018, a partir de: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Eje 21. (2019). Mayoría de ataques cibernéticos en Colombia provienen de sitios web maliciosos. Recuperado el 21 de julio de 2019, a partir de: https://www.eje21.com.co/2019/07/mayoria-de-ataques-ciberneticos-en-colombia-proviene-de-sitios-web-maliciosos/

El País. (2020). Ciberataques que matan a las empresas. Recuperado el 15 de febrero de 2020 a partir de https://elpais.com/economia/2020/02/14/actualidad/1581694252_444804.html

Forrester. (2006). The Forrester Wave: Web Application Firewalls, Q2 2006. Recuperado el 23 de junio de 2006, a partir de: https://www.forrester.com/report/The+Forrester+Wave+Web+Application+Firewalls+Q2+2006/-/E-RES38766

Gartner. (2020). Global IT spending. Recuperado el 15 de enero de 2020, a partir de https://www.gartner.com/en/newsroom/press-releases/2020-01-15-gartner-says-global-it-spending-to-reach-3point9-trillion-in-2020

InfoWorld. (1996). Internet Firewalls, It's between you and them. Recuperado el 29 de julio de 1996 a partir de https://books.google.com.co/books?id=Jj0EAAAAMBAJ&printsec=frontcover#v=onepage&q&f=false

Kareem, M. (2018). Prevention of SQL Injection Attacks using AWS WAF.

Mogul, J. (1984). Internet subnets. RFC-917, Computer Science Dept, Stanford University.

Nir Zuk. (1993). Method simulating data traffic on network in accordance with a client/sewer paradigm

OWASP. (2012). Pruebas de seguridad en aplicaciones web según OWASP. Recuperado el 4 de julio de 2009, a partir de: https://owasp.org/www-pdf-archive/OWASP_SUSCERTE.pdf

OWASP. (2019). Web Application Firewall. Recuperado el 26 de noviembre de 2019, a partir de https://owasp.org/www-community/Web_Application_Firewall

Pałka, D., & Zachara, M. (2011a). Learning web application firewall-benefits and caveats.

Pałka, D., & Zachara, M. (2011b). Learning web application firewall-benefits and caveats.

Pensak, D., & Grandinetti, M. (1995). The internet and beyond: Securing data across the enterprise. International Journal of Network Management, 5(6), 305-312.

Portafolio. (2019). Hay empresas que pierden hasta $4000 millones por ciberataques. Recuperado el 23 de julio de 2019, a partir de : https://www.portafolio.co/negocios/empresas/auditorias-ti-ahorran-perdidas-por-ciberataques-531817

Ranum, M. J. (1992, July). A network firewall. In Proceedings of the World Conference on System Administration and Security, Washington, DC.

Ranum, M. J. (1993, April). Thinking about firewalls. In Proceedings of Second International Conference on Systems and Network Security and Management (SANS-II) (Vol. 8).

Ranum, M. J. (2008). ¿Who invented the firewall? Recuperado el 15 de enero de 2008, a partir de https://www.darkreading.com/who-invented-the-firewall/d/d-id/1129238

Ristic, I. (2010a). ModSecurity Handbook. Feisty Duck.

Ristic, I. (2010b). ModSecurity Handbook. Feisty Duck.

Ristic, I. (2010c). ModSecurity Handbook. Feisty Duck.

SonicWall. (2020a). SonicWall Cyber Threar Report. Recuperado el 3 de febrero de 2020 a partir de https://www.cisomag.com/attacks-on-web-applications-surged-in-2019-report/

SonicWall. (2020b). SonicWall Cyber Threar Report. Recuperado el 3 de febrero de 2020 a partir de https://www.cisomag.com/attacks-on-web-applications-surged-in-2019-report/

Sureda, Riera. (2017) Comparativa de la eficacia de herramientas WAF y RASP frente a ataques.

Wikipedia. (2020). Web Application Firewall. Recuperado el 28 de mayo de 2020, a partir de https://es.wikipedia.org/wiki/Web_application_firewall

8 Anexos

8.1 Informe escaneo OWASP ZAP

Nivel de riesgo	Número de alertas
Alto	0
Medio	3
Bajo	10
Informativo	5

Medium (Medium)	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	https://fonts.gstatic.com/s/muli/v20/7Aulp_0qiz-aVz7u3PJLcUMYOFmQkEk30eg.woff2
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	https://fonts.gstatic.com/s/muli/v20/7Aulp_0qiz-aVz7u3PJLcUMYOFnOkEk30eg.woff2
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	https://fonts.gstatic.com/s/muli/v20/7Aulp_0qiz-aVz7u3PJLcUMYOFkpl0k30eg.woff2
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	https://fonts.gstatic.com/s/muli/v20/7Aujp_0qiz-afTfcIyoiGtm2P0wG05Fz4eqVww.woff2
Method	GET
Evidence	Access-Control-Allow-Origin: *
Instances	4
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Other information	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Reference	http://www.hpenterprisesecurity.com/vulncat/en/vulncat/vb/html5_overly_permissive_cors_policy.html

CWE Id	264
WASC Id	14
Source ID	3

Medium (Medium)	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	https://fonts.googleapis.com/css?family=Muli:300,300i,400,400i,700,700i
Method	GET
Evidence	Access-Control-Allow-Origin: *
Instances	1
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Other information	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Reference	http://www.hpenterprisesecurity.com/vulncat/en/vulncat/vb/html5_overly_permissive_cors_policy.html

CWE Id	264
WASC Id	14
Source ID	3

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	https://192.168.244.205/empresas
Method	GET
Parameter	X-Frame-Options
URL	https://192.168.244.205/Noticias/servientrega-y-efecty-de-la-mano-de-e-design-pix
Method	GET
Parameter	X-Frame-Options
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/

Method	POST
Parameter	X-Frame-Options
URL	https://192.168.244.205/empleados
Method	GET
Parameter	X-Frame-Options
URL	https://192.168.244.205/club-monedero-lightbox
Method	GET
Parameter	X-Frame-Options
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal//Recaudos/NotascreditoDebito
Method	GET
Parameter	X-Frame-Options
URL	https://192.168.244.205/inicio
Method	GET
Parameter	X-Frame-Options
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Account/OlvidoContrasena
Method	POST
Parameter	X-Frame-Options
URL	https://192.168.244.205/recargas-personas
Method	GET
Parameter	X-Frame-Options
URL	https://192.168.244.205/selecciona-el-tipo-de-pqr
Method	GET
Parameter	X-Frame-Options
URL	https://192.168.244.205/noticia
Method	GET
Parameter	X-Frame-Options
URL	https://192.168.244.205/centros-atencion/barranquilla.html
Method	GET
Parameter	X-Frame-Options
URL	https://192.168.244.205/eventos
Method	GET
Parameter	X-Frame-Options
URL	https://192.168.244.205/Noticias/efecty-en-la-feria-de-cali-2017
Method	GET
Parameter	X-Frame-Options
URL	https://192.168.244.205/Noticias/efecty-en-la-caminata-de-la-solidaridad-
Method	GET

Parameter	X-Frame-Options
URL	https://192.168.244.205/centros-atencion/pereira.html

Method	GET
Parameter	X-Frame-Options
URL	https://192.168.244.205/giros-nacionales
Method	GET
Parameter	X-Frame-Options
URL	https://192.168.244.205/centros-atencion/tunja.html
Method	GET
Parameter	X-Frame-Options
URL	https://192.168.244.205/asdfasdf
Method	GET
Parameter	X-Frame-Options
URL	https://192.168.244.205/puntos-de-atencion
Method	GET
Parameter	X-Frame-Options
Instances	114
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
Source ID	3

Low (Medium)	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://tracking-protection.cdn.mozilla.net/block-flashsubdoc-digest256/1512160865

Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/content-track-digest256/69.0/1576857797
Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/analytics-track-digest256/69.0/1581379643

Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/except-flashallow-digest256/1490633678
Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/block-flash-digest256/1496263270
Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/mozstd-trackwhite-digest256/69.0/1589483333
Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/except-flash-digest256/1494877265
Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/social-track-digest256/69.0/1583860003
Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/base-track-digest256/69.0/1583860003
Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/allow-flashallow-digest256/1490633678
Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/except-flashsubdoc-digest256/1517935265
Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/ads-track-digest256/69.0/1581543360
Method	GET
Parameter	X-Content-Type-Options
Instances	12
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

Other information	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3

Low (Medium)	**Incomplete or No Cache-control and Pragma HTTP Header Set**
Description	The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
URL	https://fonts.googleapis.com/css?family=Muli:300,300i,400,400i,700,700i
Method	GET
Parameter	Cache-Control
Evidence	private, max-age=86400
Instances	1
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13
Source ID	3

Low (Medium)	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=68.8&pver=2.2
Method	POST
Parameter	X-Content-Type-Options

Instances	1
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3

Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Content/imagenes/
Method	GET
Parameter	X-XSS-Protection
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/
Method	GET
Parameter	X-XSS-Protection
URL	https://192.168.244.205/Noticias/efecty-en-la-caminata-de-la-solidaridad-
Method	GET
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Account/OlvidoContrasena
Method	POST
Parameter	X-XSS-Protection
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Account/OlvidoContrasena
Method	GET
Parameter	X-XSS-Protection
Instances	168

Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'. The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block X-XSS-Protection: 1; report=http://www.example.com/xss The following values would disable it: X-XSS-Protection: 0
Other information	The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit). Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).
Reference	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet https://www.veracode.com/blog/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Source ID	3

Low (Medium)	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/bundles/reorjs?v=wbi38SCThObEbpdK39UGvpVP2bj1-n4Su7Sz5gnHuoA1
Method	GET
Parameter	X-Content-Type-Options

URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Content/imagenes/okImg.jpg
Method	GET
Parameter	X-Content-Type-Options
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Account/OlvidoContrasena
Method	POST
Parameter	X-Content-Type-Options
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/ScriptsTemplate/js/jquery-ui/external/jquery/jquery.js
Method	GET
Parameter	X-Content-Type-Options
Instances	380
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type- Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME- sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3

Low (Medium)	**Incomplete or No Cache-control and Pragma HTTP Header Set**
Description	The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
URL	https://192.168.244.205/efecty-negocio
Method	GET
Parameter	Cache-Control
Evidence	private
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Account/CambiarContrasena

Method	GET
Parameter	Cache-Control
Evidence	private
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Content/DataTables/datatables.min.css
Method	GET
Parameter	Cache-Control
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Account
Method	GET
Parameter	Cache-Control
Evidence	private
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal//Pago/AdministracionPagos
Method	GET
Parameter	Cache-Control
Evidence	private, s-maxage=0
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Content/assets/css/efecty-skins.css
Method	GET
Parameter	Cache-Control
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Content/assets/css/fonts/fontawesome/css/font-awesome.min.css
Method	GET
Parameter	Cache-Control
URL	https://192.168.244.205/PortalCorporativoNuevo/ApiPortal/Api/ServiceResponse/ValidarRangoFechas?fechaInicio=2020-05-01&fechaFinal=2020-05-24&Rango=ReportesFondoProyecto
Method	GET
Parameter	Cache-Control
Evidence	no-cache
URL	https://192.168.244.205/PortalCorporativo/
Method	GET
Parameter	Cache-Control
Evidence	private
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Shared/ConsultaNivelEscalamiento
Method	GET
Parameter	Cache-Control
Evidence	private, s-maxage=0
Instances	197
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13
Source ID	3

Low (Medium)	Cookie Without Secure Flag
Description	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/
Method	POST
Parameter	.ASPXAUTH
Evidence	Set-Cookie: .ASPXAUTH
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal
Method	GET
Parameter	TS01066dd7
Evidence	Set-Cookie: TS01066dd7
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal
Method	GET
Parameter	ASP.NET_SessionId
Evidence	Set-Cookie: ASP.NET_SessionId
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Shared/ReloadDataReportUsuario?tipo=110&tipo1=0&tipo2=0
Method	GET
Parameter	TS01066dd7
Evidence	Set-Cookie: TS01066dd7
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/
Method	POST
Parameter	TS01066dd7
Evidence	Set-Cookie: TS01066dd7
Instances	5
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Reference	http://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)
CWE Id	614
WASC Id	13
Source ID	3

Low (Medium)	Absence of Anti-CSRF Tokens
	No Anti-CSRF tokens were found in a HTML submission form.

Description	A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	https://192.168.244.205/
Method	GET
Evidence	<form role="form" action="/System/Search" method="post">
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/angular.js
Method	GET
Evidence	<form ng-controller="ExampleController">
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/angular.js
Method	GET
Evidence	<form name="myForm" ng-controller="ExampleController">
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/angular.js
Method	GET
Evidence	<form name="form">
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/
Method	GET
Evidence	<form action="/PortalCorporativoNuevo/Portal/" class="login-form fade-in-effect ng-pristine ng-valid in" method="post" role="form">
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/angular.js
Method	GET
Evidence	<form>
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/angular.js
Method	GET

Evidence	<form name="myForm" ng-controller="ExampleController">
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal//Pago/ReporteConsignaciones
Method	GET
Evidence	<form class="filter" name="frmReporteConsignacionesx" id="frmReporteConsignacionesx">
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/angular.js
Method	GET
Evidence	<form name="myForm" ng-controller="ExampleController">
Instances	140
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Other information	No known Anti-CSRF token [anticsrf, CSRFToken, RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret] was found in the following HTML form: [Form 1: "text"].
Reference	http://projects.webappsec.org/Cross-Site-Request-Forgery http://cwe.mitre.org/data/definitions/352.html
CWE Id	352

WASC Id	9
Source ID	3

Low (Medium)	**Information Disclosure - Debug Error Messages**
Description	The response appeared to contain common error messages returned by platforms such as ASP.NET, and Web-servers such as IIS and Apache. You can configure the list of common debug messages.
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Shared
Method	GET
Evidence	customErrors mode
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Recaudos
Method	GET
Evidence	customErrors mode
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/AdministracionUsuarios
Method	GET
Evidence	customErrors mode
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/PagosOnLine/ConsultarProductoPago
Method	GET
Evidence	customErrors mode
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/bundles
Method	GET
Evidence	customErrors mode
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Home
Method	GET
Evidence	customErrors mode
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/bundles/adOSjs
Method	GET
Evidence	customErrors mode
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/PagosOnLine
Method	GET
Evidence	customErrors mode
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/fonts
Method	GET
Evidence	customErrors mode
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Pago
Method	GET

Evidence	customErrors mode
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/DefaultCaptcha
Method	GET
Evidence	customErrors mode
Instances	11
Solution	Disable debugging messages before pushing to production.
Reference	
CWE Id	200
WASC Id	13
Source ID	3

Low (Medium)	**Cookie No HttpOnly Flag**
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Shared/ReloadDataReportUsuario?tipo=110&tipo1=0&tipo2=0
Method	GET
Parameter	TS01066dd7
Evidence	Set-Cookie: TS01066dd7
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal
Method	GET
Parameter	TS01066dd7
Evidence	Set-Cookie: TS01066dd7
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/
Method	POST
Parameter	TS01066dd7
Evidence	Set-Cookie: TS01066dd7
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/
Method	POST
Parameter	.ASPXAUTH
Evidence	Set-Cookie: .ASPXAUTH
Instances	4
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	http://www.owasp.org/index.php/HttpOnly
CWE Id	16

WASC Id	13
Source ID	3

Low (Medium)	**Cookie Without SameSite Attribute**
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/
Method	POST
Parameter	.ASPXAUTH
Evidence	Set-Cookie: .ASPXAUTH
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Shared/ReloadDataReportUsuario?tipo=110&tipo1=0&tipo2=0
Method	GET
Parameter	TS01066dd7
Evidence	Set-Cookie: TS01066dd7
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal
Method	GET
Parameter	ASP.NET_SessionId
Evidence	Set-Cookie: ASP.NET_SessionId
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal
Method	GET
Parameter	TS01066dd7
Evidence	Set-Cookie: TS01066dd7
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/
Method	POST
Parameter	TS01066dd7
Evidence	Set-Cookie: TS01066dd7
Instances	5
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	16
WASC Id	13
Source ID	3

Informational (Medium)	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/ScriptsTemplate/ui-bootstrap-tpls-0.11.2.min.js
Method	GET
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/ScriptsTemplate/app.js
Method	GET
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/plugins/dataTable/jquery.dataTables.js
Method	GET
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/ScriptsTemplate/TweenMax.min.js
Method	GET
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/ScriptsTemplate/joinable.js
Method	GET
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/moment-with-locales.js
Method	GET
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Account/OlvidoContrasena
Method	POST
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/ScriptsTemplate/directives.js
Method	GET
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Account
Method	GET
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/bootstrap-datetimepicker.js
Method	GET
Instances	72
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Other information	<!-- Mirrored from www.efecty.com.co/calculadora-giros-lightbox.html by HTTrack Website Copier/3.x [XR&CO'2014], Wed, 17 Jun 2015 18:08:00 GMT --> <!-- Mirrored from www.efecty.com.co/calculadora-giros-lightbox.html by HTTrack Website Copier/3.x [XR&CO'2014], Wed, 17 Jun 2015 18:08:02 GMT -->
Reference	
CWE Id	200
WASC Id	13

Source ID	3

Informational (Low)	Timestamp Disclosure - Unix
Description	A timestamp was disclosed by the application/web server - Unix
URL	https://tracking-protection.cdn.mozilla.net/social-track-digest256/69.0/1583860003
Method	GET
Evidence	1583860003
URL	https://tracking-protection.cdn.mozilla.net/analytics-track-digest256/69.0/1581379643
Method	GET
Evidence	1581379643
URL	https://tracking-protection.cdn.mozilla.net/block-flash-digest256/1496263270
Method	GET
Evidence	1496263270
URL	https://tracking-protection.cdn.mozilla.net/except-flash-digest256/1494877265
Method	GET
Evidence	1494877265
URL	https://tracking-protection.cdn.mozilla.net/content-track-digest256/69.0/1576857797
Method	GET
Evidence	1576857797
URL	https://tracking-protection.cdn.mozilla.net/block-flashsubdoc-digest256/1512160865
Method	GET
Evidence	1512160865
URL	https://tracking-protection.cdn.mozilla.net/base-track-digest256/69.0/1583860003
Method	GET
Evidence	1583860003
URL	https://tracking-protection.cdn.mozilla.net/except-flashallow-digest256/1490633678
Method	GET
Evidence	1490633678
URL	https://tracking-protection.cdn.mozilla.net/allow-flashallow-digest256/1490633678
Method	GET
Evidence	1490633678
URL	https://tracking-protection.cdn.mozilla.net/ads-track-digest256/69.0/1581543360
Method	GET
Evidence	1581543360
URL	https://tracking-protection.cdn.mozilla.net/except-flashsubdoc-digest256/1517935265

Method	GET
Evidence	1517935265
URL	https://tracking-protection.cdn.mozilla.net/mozstd-trackwhite-digest256/69.0/1589483333
Method	GET
Evidence	1589483333
Instances	12
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Other information	1583860003, which evaluates to: 2020-03-10 13:06:43
Reference	https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200
WASC Id	13
Source ID	3

Informational (Low)	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server - Unix
URL	https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=68.8&pver=2.2
Method	POST
Evidence	1581543360
URL	https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=68.8&pver=2.2
Method	POST
Evidence	1583860003
URL	https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=68.8&pver=2.2
Method	POST
Evidence	1512160865
URL	https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=68.8&pver=2.2
Method	POST
Evidence	1517935265
URL	https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=68.8&pver=2.2
Method	POST
Evidence	1589483333
URL	https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=68.8&pver=2.2
Method	POST

Evidence	1496263270
URL	https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=68.8&pver=2.2
Method	POST
Evidence	1494877265
URL	https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=68.8&pver=2.2
Method	POST
Evidence	1581379643
URL	https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=68.8&pver=2.2
Method	POST
Evidence	1490633678
URL	https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=68.8&pver=2.2
Method	POST
Evidence	1576857797
Instances	10
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Other information	1581543360, which evaluates to: 2020-02-12 16:36:00
Reference	https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200
WASC Id	13
Source ID	3

Informational (Low)	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server - Unix
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/ScriptsTemplate/efecty-custom.js
Method	GET
Evidence	1062462400
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/ScriptsTemplate/efecty-custom.js
Method	GET
Evidence	1293974054
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/angular.js
Method	GET
Evidence	14794066

URL	https://192.168.244.205/portal-corporativo
Method	GET
Evidence	799575979
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/angular.js
Method	GET
Evidence	22186109
URL	https://192.168.244.205/PortalCorporativoNuevo/ApiPortal/Api/ServiceResponse/ConsultarRegionales
Method	GET
Evidence	11250510
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/ScriptsTemplate/js/jquery-ui/external/jquery/jquery.js
Method	GET
Evidence	20030331
URL	https://192.168.244.205/PortalCorporativoNuevo/ApiPortal/Api/ServiceResponse/ConsultarRegionales
Method	GET
Evidence	11250540
URL	https://192.168.244.205/PortalCorporativoNuevo/Portal/Scripts/ScriptsTemplate/js/jquery-ui/external/jquery/jquery.js
Method	GET
Evidence	20110929
Instances	209
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Other information	1062462400, which evaluates to: 2003-09-01 20:26:40
Reference	https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200
WASC Id	13
Source ID	3

8.2 Diferencias significativas de las políticas

Política laboratorio QA	Política control Producción
Tipos de Archivos	
N/A	`<file_type type="explicit" name="ashx">`

```
      <learning_mode>Never</learning_mode>
      <url_length>100</url_length>
      <request_length>5000</request_length>
      <query_string_length>1000</query_string_length>
      <post_data_length>1000</post_data_length>
      <check_response>false</check_response>
      <in_staging>false</in_staging>
      <last_updated>2020-06-02T20:05:46Z</last_updated>
      <check_url_length>true</check_url_length>
      <check_request_length>true</check_request_length>
<check_query_string_length>true</check_query_string_length>
      <check_post_data_length>true</check_post_data_length>
    </file_type>
    <file_type type="explicit" name="css">
      <learning_mode>Never</learning_mode>
      <url_length>100</url_length>
      <request_length>5000</request_length>
      <query_string_length>1000</query_string_length>
      <post_data_length>1000</post_data_length>
      <check_response>false</check_response>
      <in_staging>false</in_staging>
      <last_updated>2020-06-02T16:07:34Z</last_updated>
      <check_url_length>true</check_url_length>
      <check_request_length>true</check_request_length>
<check_query_string_length>true</check_query_string_length>
      <check_post_data_length>true</check_post_data_length>
    </file_type>
    <file_type type="explicit" name="eot">
      <learning_mode>Never</learning_mode>
      <url_length>100</url_length>
      <request_length>5000</request_length>
      <query_string_length>1000</query_string_length>
      <post_data_length>1000</post_data_length>
      <check_response>false</check_response>
      <in_staging>false</in_staging>
```

```
      <last_updated>2020-06-09T16:15:39Z</last_updated>
      <check_url_length>true</check_url_length>
      <check_request_length>true</check_request_length>
<check_query_string_length>true</check_query_string_length>
      <check_post_data_length>true</check_post_data_length>
    </file_type>
    <file_type type="explicit" name="gif">
      <learning_mode>Never</learning_mode>
      <url_length>100</url_length>
      <request_length>5000</request_length>
      <query_string_length>1000</query_string_length>
      <post_data_length>1000</post_data_length>
      <check_response>false</check_response>
      <in_staging>false</in_staging>
      <last_updated>2020-06-02T18:15:39Z</last_updated>
      <check_url_length>true</check_url_length>
      <check_request_length>true</check_request_length>
<check_query_string_length>true</check_query_string_length>
      <check_post_data_length>true</check_post_data_length>
    </file_type>
    <file_type type="explicit" name="html">
      <learning_mode>Never</learning_mode>
      <url_length>100</url_length>
      <request_length>5000</request_length>
      <query_string_length>1000</query_string_length>
      <post_data_length>1000</post_data_length>
      <check_response>false</check_response>
      <in_staging>false</in_staging>
      <last_updated>2020-06-02T17:15:39Z</last_updated>
      <check_url_length>true</check_url_length>
      <check_request_length>true</check_request_length>
<check_query_string_length>true</check_query_string_length>
      <check_post_data_length>true</check_post_data_length>
    </file_type>
    <file_type type="explicit" name="ico">
```

```
      <learning_mode>Never</learning_mode>
      <url_length>100</url_length>
      <request_length>5000</request_length>
      <query_string_length>1000</query_string_length>
      <post_data_length>1000</post_data_length>
      <check_response>false</check_response>
      <in_staging>false</in_staging>
      <last_updated>2020-06-02T16:13:07Z</last_updated>
      <check_url_length>true</check_url_length>
      <check_request_length>true</check_request_length>
<check_query_string_length>true</check_query_string_length>
      <check_post_data_length>true</check_post_data_length>
    </file_type>
    <file_type type="explicit" name="jpg">
      <learning_mode>Never</learning_mode>
      <url_length>100</url_length>
      <request_length>5000</request_length>
      <query_string_length>1000</query_string_length>
      <post_data_length>1000</post_data_length>
      <check_response>false</check_response>
      <in_staging>false</in_staging>
      <last_updated>2020-06-02T16:15:39Z</last_updated>
      <check_url_length>true</check_url_length>
      <check_request_length>true</check_request_length>
<check_query_string_length>true</check_query_string_length>
      <check_post_data_length>true</check_post_data_length>
    </file_type>
    <file_type type="explicit" name="js">
      <learning_mode>Never</learning_mode>
      <url_length>100</url_length>
      <request_length>5000</request_length>
      <query_string_length>1000</query_string_length>
      <post_data_length>1000</post_data_length>
      <check_response>false</check_response>
      <in_staging>false</in_staging>
```

```
      <last_updated>2020-06-02T15:56:08Z</last_updated>
      <check_url_length>true</check_url_length>
      <check_request_length>true</check_request_length>
<check_query_string_length>true</check_query_string_length>
      <check_post_data_length>true</check_post_data_length>
    </file_type>
    <file_type type="explicit" name="no_ext">
      <learning_mode>Never</learning_mode>
      <url_length>100</url_length>
      <request_length>5000</request_length>
      <query_string_length>1000</query_string_length>
      <post_data_length>1000</post_data_length>
      <check_response>false</check_response>
      <in_staging>false</in_staging>
      <last_updated>2020-06-02T15:02:52Z</last_updated>
      <check_url_length>true</check_url_length>
      <check_request_length>true</check_request_length>
<check_query_string_length>true</check_query_string_length>
      <check_post_data_length>true</check_post_data_length>
    </file_type>
    <file_type type="explicit" name="png">
      <learning_mode>Never</learning_mode>
      <url_length>100</url_length>
      <request_length>5000</request_length>
      <query_string_length>1000</query_string_length>
      <post_data_length>1000</post_data_length>
      <check_response>false</check_response>
      <in_staging>false</in_staging>
      <last_updated>2020-06-02T16:15:39Z</last_updated>
      <check_url_length>true</check_url_length>
      <check_request_length>true</check_request_length>
<check_query_string_length>true</check_query_string_length>
      <check_post_data_length>true</check_post_data_length>
    </file_type>
    <file_type type="explicit" name="svc">
```

```
      <learning_mode>Never</learning_mode>
      <url_length>100</url_length>
      <request_length>5000</request_length>
      <query_string_length>1000</query_string_length>
      <post_data_length>5000</post_data_length>
      <check_response>false</check_response>
      <in_staging>false</in_staging>
      <last_updated>2020-06-03T09:15:39Z</last_updated>
      <check_url_length>true</check_url_length>
      <check_request_length>true</check_request_length>
<check_query_string_length>true</check_query_string_length>
      <check_post_data_length>true</check_post_data_length>
    </file_type>
    <file_type type="explicit" name="woff">
      <learning_mode>Never</learning_mode>
      <url_length>100</url_length>
      <request_length>5000</request_length>
      <query_string_length>1000</query_string_length>
      <post_data_length>1000</post_data_length>
      <check_response>false</check_response>
      <in_staging>false</in_staging>
      <last_updated>2020-06-02T16:15:39Z</last_updated>
      <check_url_length>true</check_url_length>
      <check_request_length>true</check_request_length>
<check_query_string_length>true</check_query_string_length>
      <check_post_data_length>true</check_post_data_length>
    </file_type>
    <file_type type="explicit" name="xap">
      <learning_mode>Never</learning_mode>
      <url_length>100</url_length>
      <request_length>5000</request_length>
      <query_string_length>1000</query_string_length>
      <post_data_length>1000</post_data_length>
      <check_response>false</check_response>
      <in_staging>false</in_staging>
```

```
      <last_updated>2020-06-03T12:15:39Z</last_updated>
      <check_url_length>true</check_url_length>
      <check_request_length>true</check_request_length>
<check_query_string_length>true</check_query_string_length>
      <check_post_data_length>true</check_post_data_length>
    </file_type>
    <file_type type="explicit" name="zip">
      <learning_mode>Never</learning_mode>
      <url_length>100</url_length>
      <request_length>5000</request_length>
      <query_string_length>1000</query_string_length>
      <post_data_length>1000</post_data_length>
      <check_response>false</check_response>
      <in_staging>false</in_staging>
      <last_updated>2020-06-03T12:15:39Z</last_updated>
      <check_url_length>true</check_url_length>
      <check_request_length>true</check_request_length>
<check_query_string_length>true</check_query_string_length>
      <check_post_data_length>true</check_post_data_length>
    </file_type>
<disallowed_file_types>
      <file_type name="aspx"/>
      <file_type name="bak"/>
      <file_type name="bat"/>
      <file_type name="bck"/>
      <file_type name="bin"/>
      <file_type name="bkp"/>
      <file_type name="cer"/>
      <file_type name="cfg"/>
      <file_type name="cgi"/>
      <file_type name="cmd"/>
      <file_type name="com"/>
      <file_type name="conf"/>
      <file_type name="config"/>
      <file_type name="crt"/>
```

```
<file_type name="dat"/>
<file_type name="der"/>
<file_type name="dll"/>
<file_type name="do"/>
<file_type name="eml"/>
<file_type name="exe"/>
<file_type name="exe1"/>
<file_type name="hta"/>
<file_type name="htr"/>
<file_type name="htw"/>
<file_type name="ida"/>
<file_type name="idc"/>
<file_type name="idq"/>
<file_type name="ini"/>
<file_type name="java"/>
<file_type name="jsp"/>
<file_type name="key"/>
<file_type name="log"/>
<file_type name="lua"/>
<file_type name="msi"/>
<file_type name="nws"/>
<file_type name="old"/>
<file_type name="p12"/>
<file_type name="p7b"/>
<file_type name="p7c"/>
<file_type name="pem"/>
<file_type name="pfx"/>
<file_type name="php"/>
<file_type name="pol"/>
<file_type name="printer"/>
<file_type name="py"/>
<file_type name="reg"/>
<file_type name="sav"/>
<file_type name="save"/>
<file_type name="shtm"/>
<file_type name="shtml"/>
```

<file_type name="stm"/>
<file_type name="sys"/>
<file_type name="temp"/>
<file_type name="tmp"/>
<file_type name="wmz"/>
</disallowed_file_types>

Parámetros y firmas Aprendidos

<parameter type="explicit" name="CaptchaDeText">
<learning_mode>Never</learning_mode>
<is_mandatory>false</is_mandatory>
<allow_empty_value>true</allow_empty_value>
<value_type>user input</value_type>
<user_input_format></user_input_format>
<minimum_value>0</minimum_value>
<maximum_value>10</maximum_value>
<maximum_length>10</maximum_length>

<match_regular_expression></match_regular_expression>
<is_sensitive>false</is_sensitive>
<in_staging>false</in_staging>
<last_updated>2020-05-31T02:15:51Z</last_updated>
<parameter_name_metachars>
<check_metachars>false</check_metachars>
</parameter_name_metachars>
<check_maximum_length>false</check_maximum_length>
<check_metachars>false</check_metachars>

<check_attack_signatures>true</check_attack_signatures>

<allow_repeated_parameter_name>false</allow_repeated_parameter_name>
<in_classification>false</in_classification>

<disallow_file_upload_of_executables>true</disallow_file_upload_of_executables>
<is_base64>false</is_base64>
<attack_signature sig_id="200002736">disabled</attack_signature>
<attack_signature sig_id="200002841">disabled</attack_signature>

<attack_signature sig_id="200020030">disabled</attack_signature>

```
      <attack_signature
sig_id="200002876">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>

      <attack_signature
sig_id="200003941">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="CaptchaInputText">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:51Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>
```

```
      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

      <is_base64>false</is_base64>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200002876">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>

      <attack_signature
sig_id="200003941">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="NewPassword">

      <learning_mode>Never</learning_mode>
```

```
      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:26Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

      <is_base64>false</is_base64>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200002876">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>
```

```
      <attack_signature
sig_id="200003941">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="Password">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:38Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>
```

```
<disallow_file_upload_of_executables>true</disallow_file_upload_of_executables>

      <is_base64>false</is_base64>

      <attack_signature sig_id="200002736">disabled</attack_signature>

      <attack_signature sig_id="200002838">disabled</attack_signature>

      <attack_signature sig_id="200002841">disabled</attack_signature>

      <attack_signature sig_id="200002876">disabled</attack_signature>

      <attack_signature sig_id="200003669">disabled</attack_signature>

      <attack_signature sig_id="200003934">disabled</attack_signature>

      <attack_signature sig_id="200003936">disabled</attack_signature>

      <attack_signature sig_id="200003938">disabled</attack_signature>

      <attack_signature sig_id="200003941">disabled</attack_signature>

      <attack_signature sig_id="200007016">disabled</attack_signature>

      <attack_signature sig_id="200007025">disabled</attack_signature>

      <attack_signature sig_id="200010019">disabled</attack_signature>

      <attack_signature sig_id="200015099">disabled</attack_signature>

      <attack_signature sig_id="200015101">disabled</attack_signature>

      <attack_signature sig_id="200018019">disabled</attack_signature>

      <attack_signature sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="ProductoPago">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>
```

```
<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:38Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

      <is_base64>false</is_base64>

      <attack_signature
sig_id="200000098">disabled</attack_signature>

      <attack_signature
sig_id="200001475">disabled</attack_signature>

      <attack_signature
sig_id="200002553">disabled</attack_signature>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002835">disabled</attack_signature>

      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200002876">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>

      <attack_signature
sig_id="200003941">disabled</attack_signature>
```

```
      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200101609">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="Rango">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:39Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>
```

```
<disallow_file_upload_of_executables>true</disallow_file_upload_of_executables>

      <is_base64>false</is_base64>

      <attack_signature sig_id="200000098">disabled</attack_signature>

      <attack_signature sig_id="200001475">disabled</attack_signature>

      <attack_signature sig_id="200002736">disabled</attack_signature>

      <attack_signature sig_id="200002835">disabled</attack_signature>

      <attack_signature sig_id="200002838">disabled</attack_signature>

      <attack_signature sig_id="200002876">disabled</attack_signature>

      <attack_signature sig_id="200003669">disabled</attack_signature>

      <attack_signature sig_id="200003936">disabled</attack_signature>

      <attack_signature sig_id="200003938">disabled</attack_signature>

      <attack_signature sig_id="200003941">disabled</attack_signature>

      <attack_signature sig_id="200007016">disabled</attack_signature>

      <attack_signature sig_id="200007025">disabled</attack_signature>

      <attack_signature sig_id="200010019">disabled</attack_signature>

      <attack_signature sig_id="200015099">disabled</attack_signature>

      <attack_signature sig_id="200015101">disabled</attack_signature>

      <attack_signature sig_id="200018019">disabled</attack_signature>

      <attack_signature sig_id="200101609">disabled</attack_signature>

      <attack_signature sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="RetypePassword">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>
```

```
        <minimum_value>0</minimum_value>

        <maximum_value>10</maximum_value>

        <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

        <is_sensitive>false</is_sensitive>

        <in_staging>false</in_staging>

        <last_updated>2020-05-31T02:15:26Z</last_updated>

        <parameter_name_metachars>

          <check_metachars>false</check_metachars>

        </parameter_name_metachars>

        <check_maximum_length>false</check_maximum_length>

        <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

        <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

        <is_base64>false</is_base64>

        <attack_signature
sig_id="200002736">disabled</attack_signature>

        <attack_signature
sig_id="200002838">disabled</attack_signature>

        <attack_signature
sig_id="200002841">disabled</attack_signature>

        <attack_signature
sig_id="200002876">disabled</attack_signature>

        <attack_signature
sig_id="200003669">disabled</attack_signature>

        <attack_signature
sig_id="200003934">disabled</attack_signature>

        <attack_signature
sig_id="200003936">disabled</attack_signature>

        <attack_signature
sig_id="200003938">disabled</attack_signature>

        <attack_signature
sig_id="200003941">disabled</attack_signature>

        <attack_signature
sig_id="200007016">disabled</attack_signature>

        <attack_signature
sig_id="200007025">disabled</attack_signature>
```

```
      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="Username">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:38Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

      <is_base64>false</is_base64>

      <attack_signature
sig_id="200001001">disabled</attack_signature>
```

```
      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200002876">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>

      <attack_signature
sig_id="200003941">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200101162">disabled</attack_signature>

      <attack_signature
sig_id="200101566">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="estado">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>
```

```
<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:51Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

      <is_base64>false</is_base64>

      <attack_signature
sig_id="200000098">disabled</attack_signature>

      <attack_signature
sig_id="200001475">disabled</attack_signature>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002835">disabled</attack_signature>

      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200002876">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>

      <attack_signature
sig_id="200003941">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>
```

```
      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200101609">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="fechaFin">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:51Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>
```

```
      <is_base64>false</is_base64>

      <attack_signature
sig_id="200000098">disabled</attack_signature>

      <attack_signature
sig_id="200001475">disabled</attack_signature>

      <attack_signature
sig_id="200002553">disabled</attack_signature>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002835">disabled</attack_signature>

      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200101609">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="fechaIni">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>
```

```
      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:51Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

      <is_base64>false</is_base64>

      <attack_signature
sig_id="200000098">disabled</attack_signature>

      <attack_signature
sig_id="200001475">disabled</attack_signature>

      <attack_signature
sig_id="200002553">disabled</attack_signature>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002835">disabled</attack_signature>

      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>
```

```
      <attack_signature
sig_id="200101609">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="identificacion">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:39Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

      <is_base64>false</is_base64>

      <attack_signature
sig_id="200000098">disabled</attack_signature>

      <attack_signature
sig_id="200001475">disabled</attack_signature>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002835">disabled</attack_signature>
```

```
      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200002876">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>

      <attack_signature
sig_id="200003941">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200101609">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="numLote">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>
```

```
      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:39Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

      <is_base64>false</is_base64>

      <attack_signature
sig_id="200000098">disabled</attack_signature>

      <attack_signature
sig_id="200001475">disabled</attack_signature>

      <attack_signature
sig_id="200002553">disabled</attack_signature>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002835">disabled</attack_signature>

      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200002876">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>

      <attack_signature
sig_id="200003941">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>
```

```
      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200101609">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="numOrdenServicio">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:39Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

      <is_base64>false</is_base64>
```

```
      <attack_signature
sig_id="200000098">disabled</attack_signature>

      <attack_signature
sig_id="200001475">disabled</attack_signature>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002835">disabled</attack_signature>

      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200002876">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>

      <attack_signature
sig_id="200003941">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200101609">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="numeroDocumento">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>
```

```
      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:50Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

      <is_base64>false</is_base64>

      <attack_signature
sig_id="200000098">disabled</attack_signature>

      <attack_signature
sig_id="200001475">disabled</attack_signature>

      <attack_signature
sig_id="200002553">disabled</attack_signature>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002835">disabled</attack_signature>

      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002876">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>

      <attack_signature
sig_id="200003941">disabled</attack_signature>
```

```
      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200101609">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="numeroIdentificacion">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:51Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>
```

```
<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

      <is_base64>false</is_base64>

      <attack_signature
sig_id="200000098">disabled</attack_signature>

      <attack_signature
sig_id="200001475">disabled</attack_signature>

      <attack_signature
sig_id="200002553">disabled</attack_signature>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002835">disabled</attack_signature>

      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200002876">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>

      <attack_signature
sig_id="200003941">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200101609">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="numeroOrden">
```

```
      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:50Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

      <is_base64>false</is_base64>

      <attack_signature
sig_id="200000098">disabled</attack_signature>

      <attack_signature
sig_id="200001475">disabled</attack_signature>

      <attack_signature
sig_id="200002553">disabled</attack_signature>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002835">disabled</attack_signature>

      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200002876">disabled</attack_signature>
```

```
      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>

      <attack_signature
sig_id="200003941">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200101609">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>


<attack_signature
sig_id="200000098">disabled</attack_signature>

      <attack_signature
sig_id="200001475">disabled</attack_signature>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002835">disabled</attack_signature>

      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200002876">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>
```

```
      <attack_signature
sig_id="200003941">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200101609">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="proyecto">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:38Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>
```

```
      <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

      <is_base64>false</is_base64>

      <attack_signature
sig_id="200000098">disabled</attack_signature>

      <attack_signature
sig_id="200001475">disabled</attack_signature>

      <attack_signature
sig_id="200002553">disabled</attack_signature>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002835">disabled</attack_signature>

      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200002876">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>

      <attack_signature
sig_id="200003941">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200101609">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>
```

```
    <parameter type="explicit" name="regional">
      <learning_mode>Never</learning_mode>
      <is_mandatory>false</is_mandatory>
      <allow_empty_value>true</allow_empty_value>
      <value_type>user input</value_type>
      <user_input_format></user_input_format>
      <minimum_value>0</minimum_value>
      <maximum_value>10</maximum_value>
      <maximum_length>10</maximum_length>
<match_regular_expression></match_regular_expression>
      <is_sensitive>false</is_sensitive>
      <in_staging>false</in_staging>
      <last_updated>2020-05-31T02:15:39Z</last_updated>
      <parameter_name_metachars>
        <check_metachars>false</check_metachars>
      </parameter_name_metachars>
      <check_maximum_length>false</check_maximum_length>
      <check_metachars>false</check_metachars>
<check_attack_signatures>true</check_attack_signatures>
<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>
      <in_classification>false</in_classification>
<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>
      <is_base64>false</is_base64>
      <attack_signature
sig_id="200000098">disabled</attack_signature>
      <attack_signature
sig_id="200001475">disabled</attack_signature>
      <attack_signature
sig_id="200002736">disabled</attack_signature>
      <attack_signature
sig_id="200002835">disabled</attack_signature>
      <attack_signature
sig_id="200002838">disabled</attack_signature>
      <attack_signature
sig_id="200002841">disabled</attack_signature>
      <attack_signature
sig_id="200002876">disabled</attack_signature>
```

```
      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>

      <attack_signature
sig_id="200003941">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200101609">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="t">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:51Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>
```

```
        <check_maximum_length>false</check_maximum_length>

        <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

        <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

        <is_base64>false</is_base64>

        <attack_signature
sig_id="200000098">disabled</attack_signature>

        <attack_signature
sig_id="200001475">disabled</attack_signature>

        <attack_signature
sig_id="200002736">disabled</attack_signature>

        <attack_signature
sig_id="200002841">disabled</attack_signature>

        <attack_signature
sig_id="200002876">disabled</attack_signature>

        <attack_signature
sig_id="200003669">disabled</attack_signature>

        <attack_signature
sig_id="200003934">disabled</attack_signature>

        <attack_signature
sig_id="200003936">disabled</attack_signature>

        <attack_signature
sig_id="200003938">disabled</attack_signature>

        <attack_signature
sig_id="200003941">disabled</attack_signature>

        <attack_signature
sig_id="200007016">disabled</attack_signature>

        <attack_signature
sig_id="200007025">disabled</attack_signature>

        <attack_signature
sig_id="200010019">disabled</attack_signature>

        <attack_signature
sig_id="200015098">disabled</attack_signature>

        <attack_signature
sig_id="200015099">disabled</attack_signature>

        <attack_signature
sig_id="200015101">disabled</attack_signature>

        <attack_signature
sig_id="200018019">disabled</attack_signature>

        <attack_signature
sig_id="200101609">disabled</attack_signature>
```

```
      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="tipo">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:51Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

      <is_base64>false</is_base64>

      <attack_signature
sig_id="200000098">disabled</attack_signature>

      <attack_signature
sig_id="200001475">disabled</attack_signature>

      <attack_signature
sig_id="200002553">disabled</attack_signature>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002835">disabled</attack_signature>
```

```
      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200002876">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>

      <attack_signature
sig_id="200003941">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200101609">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="tipo1">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>
```

```
      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:51Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

      <is_base64>false</is_base64>

      <attack_signature
sig_id="200000098">disabled</attack_signature>

      <attack_signature
sig_id="200001475">disabled</attack_signature>

      <attack_signature
sig_id="200002553">disabled</attack_signature>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002835">disabled</attack_signature>

      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200002876">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>

      <attack_signature
sig_id="200003941">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>
```

```
      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200101609">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="tipo2">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:51Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

      <is_base64>false</is_base64>
```

```
      <attack_signature
sig_id="200000098">disabled</attack_signature>

      <attack_signature
sig_id="200001475">disabled</attack_signature>

      <attack_signature
sig_id="200002553">disabled</attack_signature>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002835">disabled</attack_signature>

      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200002876">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>

      <attack_signature
sig_id="200003941">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200101609">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="tipoFormatoArchivo">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>
```

```
      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:39Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

      <is_base64>false</is_base64>

      <attack_signature
sig_id="200000098">disabled</attack_signature>

      <attack_signature
sig_id="200001475">disabled</attack_signature>

      <attack_signature
sig_id="200002553">disabled</attack_signature>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002835">disabled</attack_signature>

      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200002876">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>
```

```
      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>

      <attack_signature
sig_id="200003941">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200101609">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="tipoformatoarchivo">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:39Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>
```

```
<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

      <is_base64>false</is_base64>

      <attack_signature
sig_id="200000098">disabled</attack_signature>

      <attack_signature
sig_id="200001475">disabled</attack_signature>

      <attack_signature
sig_id="200002553">disabled</attack_signature>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002835">disabled</attack_signature>

      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200002876">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>

      <attack_signature
sig_id="200003941">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>
```

```
      <attack_signature
sig_id="200101609">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="usuario">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>

      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:39Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

      <is_base64>false</is_base64>

      <attack_signature
sig_id="200000098">disabled</attack_signature>

      <attack_signature
sig_id="200001475">disabled</attack_signature>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002835">disabled</attack_signature>
```

```
      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200002876">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>

      <attack_signature
sig_id="200003941">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>

      <attack_signature
sig_id="200010019">disabled</attack_signature>

      <attack_signature
sig_id="200015099">disabled</attack_signature>

      <attack_signature
sig_id="200015101">disabled</attack_signature>

      <attack_signature
sig_id="200018019">disabled</attack_signature>

      <attack_signature
sig_id="200101609">disabled</attack_signature>

      <attack_signature
sig_id="200104076">disabled</attack_signature>

    </parameter>

    <parameter type="explicit" name="v">

      <learning_mode>Never</learning_mode>

      <is_mandatory>false</is_mandatory>

      <allow_empty_value>true</allow_empty_value>

      <value_type>user input</value_type>

      <user_input_format></user_input_format>

      <minimum_value>0</minimum_value>

      <maximum_value>10</maximum_value>

      <maximum_length>10</maximum_length>


<match_regular_expression></match_regular_expression>

      <is_sensitive>false</is_sensitive>
```

```
      <in_staging>false</in_staging>

      <last_updated>2020-05-31T02:15:39Z</last_updated>

      <parameter_name_metachars>

        <check_metachars>false</check_metachars>

      </parameter_name_metachars>

      <check_maximum_length>false</check_maximum_length>

      <check_metachars>false</check_metachars>


<check_attack_signatures>true</check_attack_signatures>


<allow_repeated_parameter_name>false</allow_repeated_param
eter_name>

      <in_classification>false</in_classification>


<disallow_file_upload_of_executables>true</disallow_file_u
pload_of_executables>

      <is_base64>false</is_base64>

      <attack_signature
sig_id="200000098">disabled</attack_signature>

      <attack_signature
sig_id="200001475">disabled</attack_signature>

      <attack_signature
sig_id="200002553">disabled</attack_signature>

      <attack_signature
sig_id="200002736">disabled</attack_signature>

      <attack_signature
sig_id="200002835">disabled</attack_signature>

      <attack_signature
sig_id="200002838">disabled</attack_signature>

      <attack_signature
sig_id="200002841">disabled</attack_signature>

      <attack_signature
sig_id="200002876">disabled</attack_signature>

      <attack_signature
sig_id="200003669">disabled</attack_signature>

      <attack_signature
sig_id="200003934">disabled</attack_signature>

      <attack_signature
sig_id="200003936">disabled</attack_signature>

      <attack_signature
sig_id="200003938">disabled</attack_signature>

      <attack_signature
sig_id="200003941">disabled</attack_signature>

      <attack_signature
sig_id="200007016">disabled</attack_signature>

      <attack_signature
sig_id="200007025">disabled</attack_signature>
```

<attack_signature sig_id="200010019">disabled</attack_signature> <attack_signature sig_id="200015098">disabled</attack_signature> <attack_signature sig_id="200015099">disabled</attack_signature> <attack_signature sig_id="200015101">disabled</attack_signature> <attack_signature sig_id="200018019">disabled</attack_signature> <attack_signature sig_id="200101609">disabled</attack_signature> <attack_signature sig_id="200104076">disabled</attack_signature>	
Otras sugerencias	
N/A	<valid_host_name name="portalcorporativo.efecty.com.co"> <include_subdomains>false</include_subdomains> </valid_host_name>