



Zed Attack Proxy

(Nivel básico)

Sección de Seguridad de la información - Rodrigo Castro Díaz

Agenda

- Introducción a ZAP
- Detalles de configuración
- Escaneos pasivos y activos
- Reportes

¿Qué es ZAP?

Zed Attack Proxy (ZAP) es una herramienta gratuita de pruebas de penetración de código abierto que hace parte del Open Web Application Security Project (OWASP). ZAP está diseñado específicamente para probar aplicaciones web y es flexible y extensible.

ZAP es un proxy de estilo hombre en el medio



Si ya hay otro proxy de red en uso, como en muchos entornos corporativos, ZAP se puede configurar para conectarse a ese proxy.



Notas:

ZAP es un proxy de uso al estilo hombre en el medio, es decir que ZAP funciona poniéndose entre el navegador y la aplicación interceptando las peticiones y respuestas de la aplicación web incluso en entornos corporativos

Detalles iniciales

¿Cómo obtener ZAP?

ZAP requiere Java 8+ para ejecutarse

[Descarga instalador ZAP](#)

[kali linux](#)

Notas:

ZAP es una aplicación java, por lo tanto requiere que el sistema operativo tenga instalado java 8 o superior, por lo tanto podemos conseguir instaladores para los principales sistemas operativos e incluso en Docker

También viene incluida en diversas distribuciones de pentesting y seguridad informática como Kali Linux o Backbox

Antes de usar

¿De qué manera voy a usar ZAP? ¿Cómo proxy local, cómo servidor de pruebas?

Notas:

Debemos definir el uso que haremos de la herramienta para poder aprovechar al máximo sus capacidades, es posible que solo pensemos en probar la herramienta o realizar una prueba básica, en este caso las opciones y configuraciones por defecto serán más que suficientes

Ajustes de la JVM antes de lanzar ZAP

- Ajustes de heap

`-Xmx1024m`

[JVM options](#)

Notas:

Para sacarle el máximo provecho se permite establecer el tamaño máximo del grupo de asignación de memoria de Java para la ejecución de ZAP.

El heap es una estructura de datos especial de la JVM y es crítica para las aplicaciones porque cuando se desborda el heap la aplicación falla, por defecto estos valores suelen ser pequeños, y dependiendo del uso que le demos puede ser necesario personalizar los valores.

Dependiendo del sistema operativo, esta configuración puede variar, por lo que es aconsejable consultar la documentación oficial

- Garbage Collector

```
-XX:+UseSerialGC
-XX:+UseParallelGC
-XX:+UseConcMarkSweepGC //en desuso desde java 9
-XX:+UseG1GC
-XX:+UseZGC // recomendado en java 11
```

Notas:

Seleccionar correctamente el Garbage Collector dependiendo de la versión de JVM también impacta al funcionamiento de la herramienta

El Garbage Collector (o recolector de basura) es uno de los elementos fundamentales en la JVM se encarga de recolectar aquellos elementos que ya no son usados dentro del programa, es un procedimiento que se ejecuta de manera automática.

El algoritmo que escojamos dependerá del equipo. Si se tiene alguna restricción a nivel de hardware probablemente los primeros (serial y parallel) serán los más indicados, si la máquina es potente y el uso de la aplicación lo requiere es posible que la mejor opción sea usar los últimos (G1 o ZGC), en la versión 11 el recomendable es usar ZGC.

Configurar proxy


Por defecto, ZAP usa la dirección de 'localhost' y el puerto '8080', pero estos se pueden cambiar

[Configuring proxies](#)

Notas:

Generalmente no hay problema pero en algunos navegadores actuales para Windows, se requiere de algunas configuraciones adicionales para permitir la captura del tráfico de localhost.

Primeros pasos con ZAP

 OWASP ZAP ×

¿Usted desea permanecer en esta sesión de ZAP?

☐ Si, yo quiero continuar en esta sesión con un nombre basado en el tiempo actual

☐ Si, yo deseo permanecer en esta sesión, pero quiero especificar el nombre y la ubicación a utilizar

☒ No, por los momentos no quiero continuar en esta sesión

☐ Recuerda mi selección y no me vuelvas a realizar esta pregunta de nuevo.

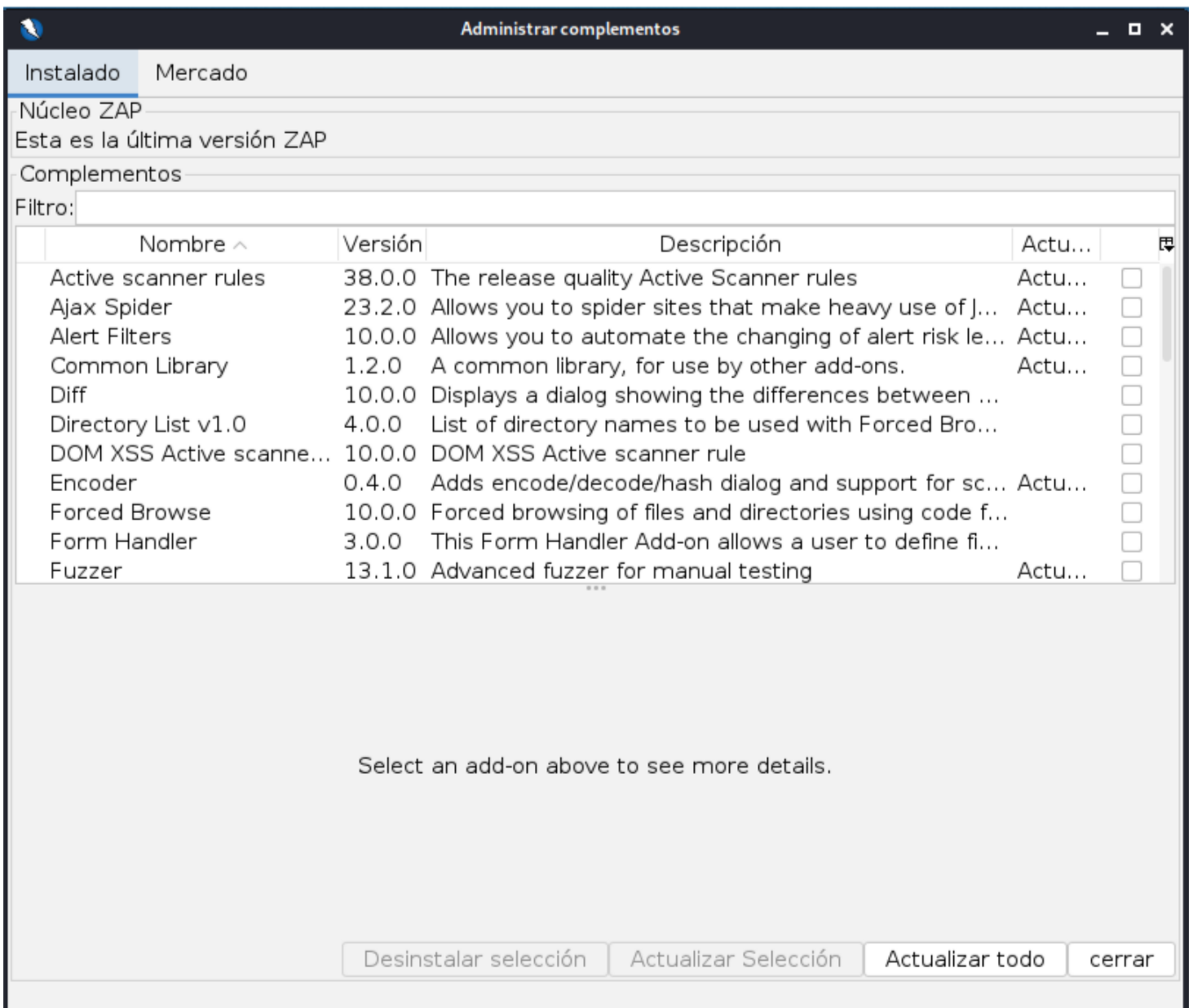
Siempre puede cambiar su decisión por medio de la pantalla de Opciones/Base de datos

Ayuda

Iniciar

Notas:

Cuando inicia ZAP, preguntará si desea mantener la sesión. De forma predeterminada, las sesiones se graban en el disco en una base de datos HSQLDB con un nombre y una ubicación predeterminados. Si no se desea permanecer en la sesión, esos archivos se eliminan cuando sale de ZAP.



Notas:

Cuando inicia ZAP por primera vez, mostrara una ventana para la actualización de los componentes de la aplicación, se recomienda actualizar todos.

Tip: En esta ventana podemos ir a la pestaña de mercado para instalar complementos adicionales y expandir funcionalidades de la herramienta

Addons

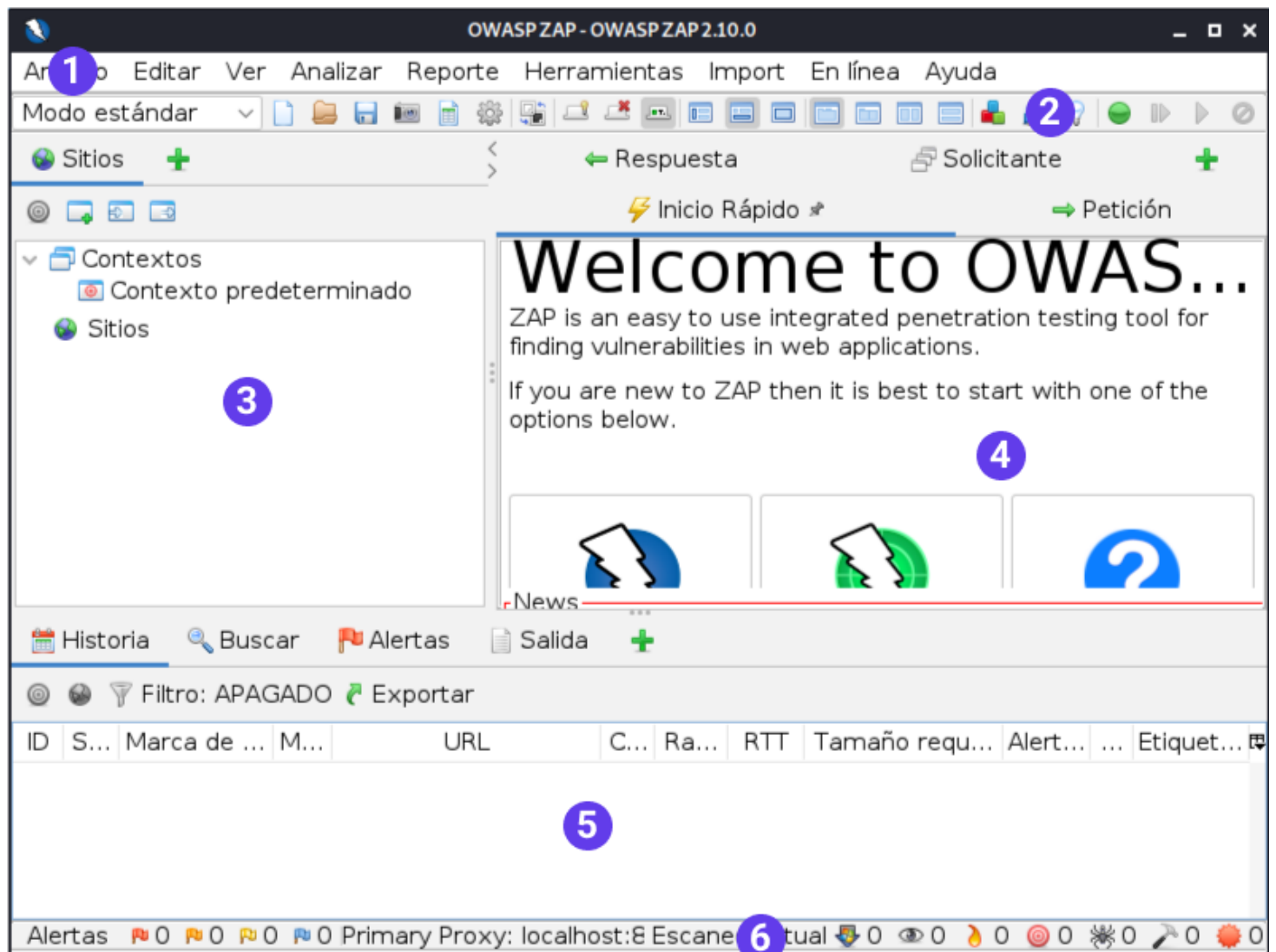
- Python Scripting y/o Ruby Scripting
- Tree Tools
- Community Scripts
- CustomReport
- Export Report

- Requester

Notas:

Estos son algunos de los complementos adicionales que podemos instalar cuya descripción encontraremos en la ventana de la aplicación

Interfaz de usuario



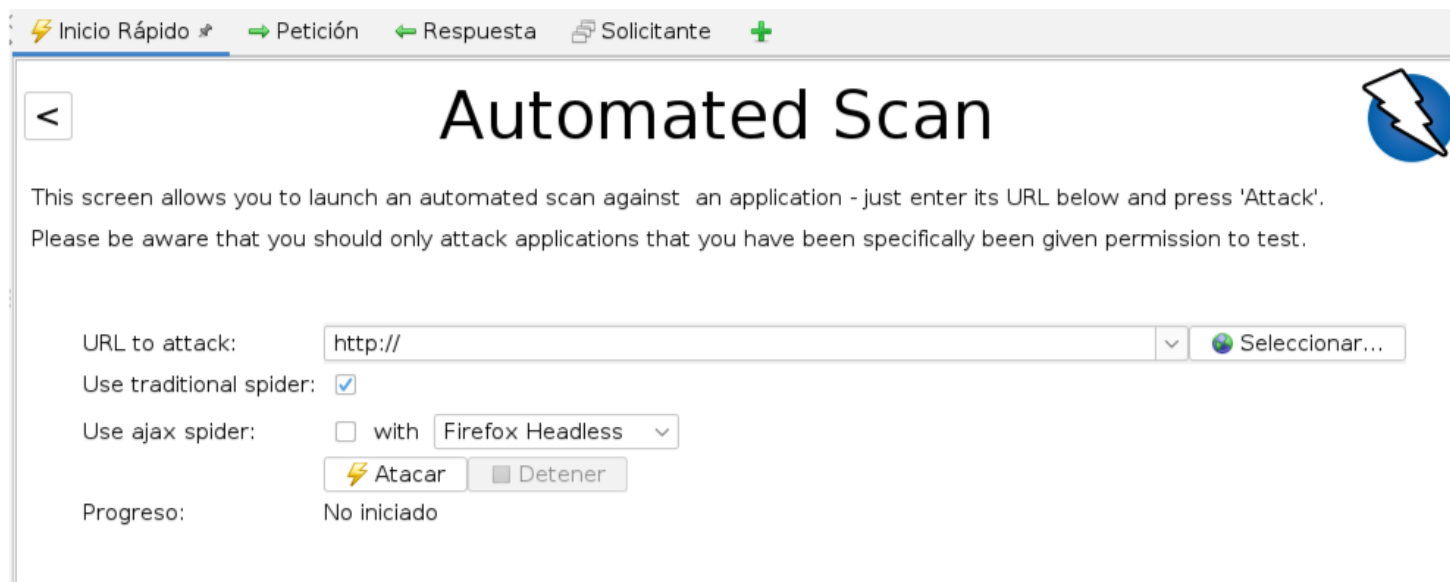
Notas:

La interfaz de usuario de ZAP se compone de los siguientes elementos:

1. **Menú:** brinda acceso a muchas de las herramientas automáticas y manuales.
2. **Barra de herramientas:** incluye botones que facilitan el acceso a las funciones más utilizadas.
3. **Ventana de árbol:** muestra el árbol de Sitios y el árbol de Scripts.
4. **Ventana del área de trabajo:** muestra solicitudes, respuestas y scripts y le permite editarlos.
5. **Ventana de información:** muestra detalles de las herramientas automáticas y manuales.

6. **Pie de página:** muestra un resumen de las alertas encontradas y el estado de las principales herramientas automatizadas.

Escaneo automatizado



Inicio Rápido → Petición ← Respuesta Solicitante +

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'. Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack: Seleccionar...

Use traditional spider: ☒

Use ajax spider: ☐ with Firefox Headless

⚡ Atacar ■ Detener

Progreso: No iniciado

Notas:

Para ejecutar un escaneo automatizado de inicio rápido:

1. Inicie ZAP y haga clic en la pestaña **Inicio rápido** de la ventana del área de trabajo.
2. Haga clic en el botón grande de **Escaneo automatizado**.
3. En el cuadro de texto de **URL para atacar**, ingrese la URL completa de la aplicación web que desea atacar.
4. Haga clic en el botón de **ataque**

ZAP procederá a analizar la aplicación web y realizará un escaneo pasivo con un spider tradicional. Luego, ZAP utilizará el escáner activo para atacar todas las páginas, funcionalidades y parámetros descubiertos.



ZAP proporciona 2 spiders para rastrear aplicaciones web, puede usar una o ambas desde esta pantalla.

El spider tradicional de ZAP descubre enlaces examinando el HTML en las respuestas de la aplicación web. Es rápida, pero no siempre es efectiva cuando se explora una aplicación web AJAX que genera enlaces usando JavaScript.

Para las aplicaciones AJAX, es probable que el spider AJAX de ZAP sea más eficaz. Es más lenta que el spider tradicional.

ZAP primero escaneará pasivamente todas las solicitudes y respuestas enviadas a través de él, luego se realiza un análisis activo que intenta encontrar otras vulnerabilidades mediante ataques conocidos.

Alertas

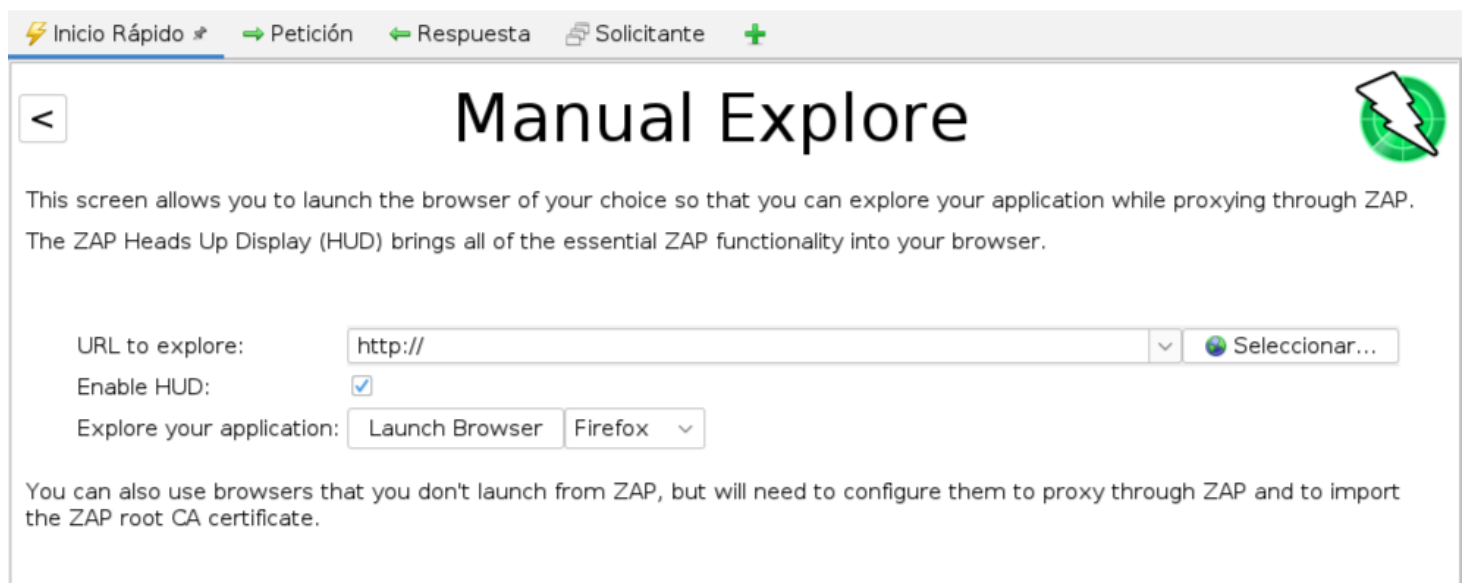
-  Alto
-  Medio
-  Bajo
-  Informativo
-  Falso positivo

Notas:

Para ver las alertas creadas durante su prueba:

1. Haga clic en la pestaña Alertas en la ventana de información.
2. Haga clic en cada alerta que se muestra en esa ventana para mostrar la URL y la vulnerabilidad detectada en el lado derecho de la Ventana de información.
3. En las ventanas del área de trabajo, haga clic en la pestaña Respuesta para ver el contenido del encabezado y el cuerpo de la respuesta. Se resaltará la parte de la respuesta que generó la alerta.

Exploración manual



The screenshot shows the 'Manual Explore' interface in ZAP. At the top, there's a navigation bar with tabs: 'Inicio Rápido' (selected), 'Petición', 'Respuesta', 'Solicitante', and a '+' icon. Below the tabs, the title 'Manual Explore' is centered, with a back arrow on the left and a ZAP logo on the right. The main text explains that this screen allows launching a browser to explore an application while proxying through ZAP, and that the ZAP Heads Up Display (HUD) brings essential ZAP functionality into the browser. Below this, there are input fields for 'URL to explore:' (containing 'http://') and a dropdown menu labeled 'Seleccionar...'. There's also a checkbox for 'Enable HUD:' which is checked. At the bottom, there's a section for 'Explore your application:' with a 'Launch Browser' button and a dropdown menu showing 'Firefox'. A note at the very bottom states: 'You can also use browsers that you don't launch from ZAP, but will need to configure them to proxy through ZAP and to import the ZAP root CA certificate.'

Notas:

Para explorar manualmente una aplicación:

1. Inicie ZAP y haga clic en la pestaña Inicio rápido de la ventana del área de trabajo.

2. Haga clic en el botón grande Exploración manual.
3. En el cuadro de texto URL para explorar, ingrese la URL completa de la aplicación web que desea explorar.
4. Seleccione el navegador que le gustaría usar
5. Haga clic en Iniciar navegador

ZAP HUD



Notas:

El Heads Up Display (HUD) es una nueva interfaz que brinda acceso a la funcionalidad ZAP directamente en el navegador. Es ideal para personas nuevas en la seguridad web y también permite que los probadores de penetración experimentados se centren en la funcionalidad de una aplicación.

Reporte

ZAP Scanning Report - Mozilla Firefox

ZAP Scanning Report

file:///home/kali/informe.html

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

ZAP Scanning Report

Summary of Alerts Generated on vie., 13 ago. 2021 19:11:38

Risk Level	Number of Alerts
High	0
Medium	5
Low	3
Informational	2

Alerts

Name	Risk Level	Number of Instances
Cross-Domain Misconfiguration	Medium	54
CSP: style-src unsafe-inline	Medium	4
CSP: Wildcard Directive	Medium	4
Vulnerable JS Library	Medium	2
X-Frame-Options Header Not Set	Medium	1
Cross-Domain JavaScript Source File Inclusion	Low	2
Incomplete or No Cache-control Header Set	Low	1
X-Content-Type-Options Header Missing	Low	53
Information Disclosure - Suspicious Comments	Informational	6
Timestamp Disclosure - Unix	Informational	23

Alert Detail

Notas:

Para generar un reporte:

1. Abrir el menú Reporte
2. Escoger el tipo de informe a generar

Las opciones que maneja este menú son:

- **Generar informe HTML:** genera un nuevo informe HTML que contiene las alertas generadas.
- **Generar informe XML:** genera un nuevo informe XML que contiene las alertas generadas.
- **Generar informe Markdown:** genera un nuevo informe de Markdown que contiene las alertas generadas.
- **Exportar mensajes a archivo:** permite guardar solicitudes y respuestas en un archivo de texto. Seleccione los mensajes para guardar en la pestaña Historial; use la tecla Mayús para seleccionar varios mensajes.
- **Exportar respuesta a archivo:** Esto le permite guardar una respuesta específica en un archivo. Seleccione el mensaje relevante en la pestaña Historial; tenga en cuenta que las respuestas binarias (como imágenes) se pueden guardar, así como las respuestas de prueba.
- **Exportar todas las URL a archivo:** Esto le permite guardar todas las URL a las que se accede en un archivo de texto o HTML. Esto se puede utilizar, entre otras cosas, para comparar las URL disponibles para usuarios con diferentes roles o permisos en el mismo sistema.

- **Exportar las URL seleccionadas a un archivo:** Según la selección (incluida la selección múltiple) en el árbol de Sitios, se exportan todas las URL y las URL secundarias de los nodos seleccionados.
- **Exportar URL para contexto:** Se exportan todas las URL del árbol Sitios que se encuentran dentro del contexto seleccionado. Esta funcionalidad también está disponible en el menú contextual cuando se usa en un nodo Contexto en el panel del árbol Sitios.
- **Comparar con otra sesión:** Esto le solicita una sesión ZAP que haya guardado previamente. Luego le solicita un archivo de salida en el que se escriben todas las URL a las que accede la sesión actual y la sesión que ha seleccionado para compararla. El archivo contendrá una tabla que enumera las URL y las respuestas HTTP para las URL en las 2 sesiones. Los botones de JavaScript le permiten mostrar todas las URL, solo aquellas a las que se accede en la primera sesión, la segunda sesión y aquellas a las que se accede por ambas sesiones. Esto es particularmente útil para comparar 2 sesiones que acceden a la misma aplicación utilizando diferentes usuarios. Podrá ver qué URL son visibles para los usuarios y podrá intentar acceder a todas las URL cuando inicie sesión como cualquiera de los usuarios.

Recursos

- [Sitio oficial](#)
- [Documentación oficial](#)
- [OWASP Latam](#)