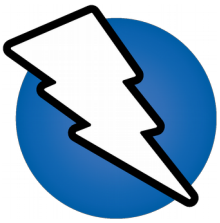
OWASP ZAP 2.7
Guia de Inicio



Resumen

Este documento lo que buscar hacer es servir como una introducción muy básica para poder utilizar la herramienta de Zed Attack Proxy (ZAP) de OWASP para poder realizar pruebas relacionadas a la seguridad, incluso aunque no tenga experiencia en cuanto a pruebas de seguridad. Para ello, se insertan algunos de los conceptos y terminologías relacionadas a las pruebas de seguridad, pero este documeto no busca ser una guía que sea agotadora de ZAP ni de las pruebas de seguridad.

Si usted ya ha terminado con las pruebas de seguridad o penetración, usted quizas pueda comenzar con la introducción ZAP.

ConsultarEnlaces que son útilespara conseguir los recursos e informaciónacerca de ZAP.

Conceptos básicos relacionados a las pruebas de seguridad

La prueba de seguridad del software es el proceso que se encarga de evaluar y probar un sistema para poder descubrir todos los riesgos de seguridad y las vulnerabilidades que tenga el sistema y su datos. No existe una terminología que sea universal, pero para nuestros propósitos, nosotros definimos las evaluaciones que se realizan como el análisis y los descubrimientos de las vulnerabilidades sin intentar explotar dichas vulnerabilidades. Nosotros definimos las pruebas como el descubrimiento y el intento de la explotación de todas las vulnerabilidades.

Con mucha frecuencia, las pruebas de seguridad de separan, de forma arbitraria, de acuerdo a el tipo de vulnerabilidad que se prueba o el tipo de prueba que se vaya a realizar. Una interrupción que es muy comun es:

- **La evaluación de las vulnerabilidades** El sistema se escanea y se analiza para poder detectar todos los problemas relacionados a la seguridad.
- **Las pruebas de penetración**El sistema se impone a un análisis y a los ataques generados por atacantes con malas intenciones de forma simulada.
- **Prueba de tiempo de ejecución** - El sistema se somete a análisis y pruebas de seguridad de parte de un usuario final.
- **Revisión del código**: el código del sistema es sometido a una revisión y a un análisis de forma detallada que busca de forma puntual las vulnerabilidades relacionadas a la seguridad.

Usted tiene que tener en cuenta que la evaluación de los riesgos, que normalmente se incluye como parte de las pruebas de seguridad, nose encuentra incluida en esta lista. Esto se debe a que una evaluación de los riesgos no es realmente una prueba como tal sino que más bien el análisis de la gravedad recibida de los diferentes tipos de riesgos (seguridad del software, seguridad del personal, seguridad del hadware, etc) y cualquier paso de reducción para esos riesgos.

Más acerca de las pruebas de penestración

La prueba relacionada de penetración (pentesting) se realiza como si el probador fuera un tipo de atacante externo y malicioso cuyo objetivo es ingresar al sistema y tratar de robar todos los datos o realizar algún tipo de ataque de denegación del servicio.

La prueba de Penetración tiene la ventaja de ser mucho mas precisa porque tiene menos positivos que son falsos (resultados que se encargan de informar sobre alguna vulnerabilidad que no se encuentra realmente presente), pero puede tomar mucho tiempo realizarla.

Pentesting tambíen se utiliza para poder probar los mecanismos de defensa, para confirmar los planes de respuesta y tambien confirmar que se cumpla la política de seguridad.

El pentesting de forma automática es una pieza muy importante de la validación de la integración que es continua. Eso ayuda a poder descubrir las nuevas vulnerabilidades y regresiones para las vulnerabilidades anteriores en un dominio que cambia de forma rápida y para el cual el desarrollo puede ser que sea muy colaborativo y distribuido.

El conjunto de operaciones de Pentesting

Se utilizan las pruebas manuales y automatizadas, normalmente en grupo, para poder probar todo, desde los servidores, redes, dispositivos hasta los puntos finales. Este documento se enfoca en las aplicaciones web o en pentesting de los sitios web.

Pentesting normalmente realiza estas estapas:

- **Explorar**: el ensayador busca poder aprender algo sobre el sistema que se está probando. Esto incluye intentar determinar qué software está en uso, qué puntos finales existen, qué parches están instalados, etc. También incluye la búsqueda en el sitio de contenido oculto, las vulnerabilidades que son conocidas y otras idicaciones sobre alguna debilidad. [cadena vacía]
- **Ataque**: el probador intentar poder explotar las vulerabilidades que son conocidas o que son sospechosas para poder demostrar que estas existen.
- **Reporte**: el probador informa todo sobre los resultados obtenidos en la prueba, incluidas las vulnerabilidades, cómo las lograron explotar, que tan dificil fueron los exploits y que tan grave fue la explotación. [cadena vacía]

Metas de Pentesting

El objetivo final de pentesting es poder conseguir las vulnerabilidades para poder abordar estas vulnerabilidades. También puede verificar que algún sistema no se encuentra vulnerable a un tipo conocido o a algún defecto que sea específico; o en el caso de las vulnerabilidades que se han informado como vulnerabilidades fijas, verifica que el sistema ya no se encuentre vulnerable a dicho efecto.

Presentación de ZAP

Zed Attack Proxy (ZAP) es una herramienta gratuita de una prueba de penetración de código abierto el cual se mantiene bajo la cubierta del Open Web Aplication Security Project (OWASP). ZAP se encuentra diseñado de forma específica para poder probar las aplicaciones web y es tanto flexible como extensible.

En su esencia, ZAP es lo que se conoce comunmente como un "hombre en el medio del proxy". Se encuentra localizado entre el navegador del examinador y la aplicación web para que así pueda interceptar y revisar todos los mensajes que fueron enviados entre el navegador y la aplicación web, y así poder cambiar el contenido si es necesario para luego reenviar esos paquetes al destino. It se pued utilizar como una aplicación la cual es independiente y como un proceso de daemon.

Si ya se encuentra algún otro proxy de red en utso, como en muchos dominios que son corporativos, ZAP se puede modificar para conectarse a dicho proxy.

ZAP otorga una funcionalidad para una gran variedad de niveles de habilidades, desde los desarrolladores, probadores que son nuevo de las pruebas de seguridad, hasta especialistas en la pruebas de seguridad. ZAP posee varias versiones para cada uno de los sistemas operativos principales y Docker, por lo que no se encuentra asociado a un solo sistema operativo. La funcionalidad extra se encuentra disponible de forma gratuita desde una variedad de complementos en el mercado ZAP, muy accesibles desde el cliente ZAP.

Debido a que ZAP es un código abierto, el código fuente se puede revisar para poder observar exactamente cómo se establece la funcionalidad. Cualquiera puede trabajar en ZAP de forma voluntaria, enmendando errores, agregando funciones, creando solicitudes de extracción para poder establecer soluciones en el proyecto e ingresar complemento para poder admitir soluciones de forma especializada.

Para poder conseguir más información, revise la Página de Zed Attack del proxy.

Al igual que mucho de los proyectos de código abierto, las donaciones son muy bien recibidas para poder ayudar o colaborar con los costos que generan los proyectos. Usted puede conseguir un botón para poder realizar una donación en la página de owasp.org para ZAP en https://www.owasp.org/index.php/ZAP.

Colocar y organizar ZAP

ZAP posee varios instaladores para Windows, Linux y Mac OS/X. Hay también Docker images el cual se encuentra disponible en el sitio de las descargas que se especifica a continuación.

Instalar ZAP

Lo primero que se debe realizar es la instalación de ZAP en el sistema en el que usted desea poder realizar la prueba de pentesting. Descargue el instalador que sea apropiado de la localización de descarga de ZAP en la página https://github.com/zaproxy/zaproxy/wiki/Downloads y active el instalador. [cadena vacía]

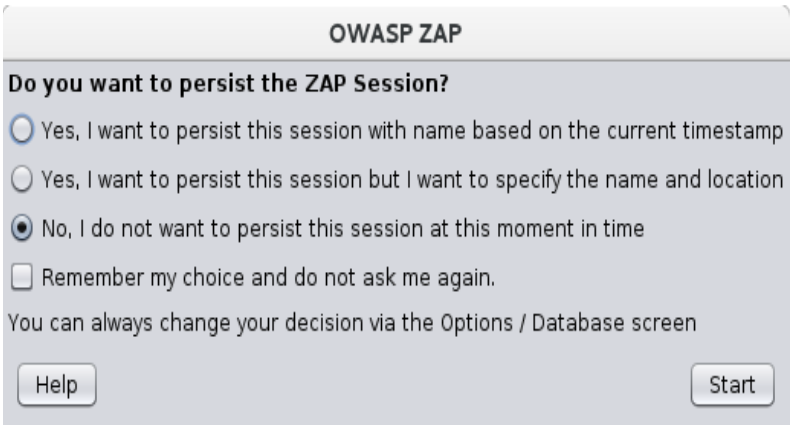
Usted tiene que tener en cuenta que ZAP necesita de Java 8+ para poder ejecutarse. El instalador de Mac OS/X incluye también una versión que es adecuada de Java, pero se debe instalar java 8+ de forma separada para Windows, Linux y las versiones de la multiplataforma. La versión de Docker s no necesita de la instalación de Java.

Una vez que se logre completar toda la instalación, inicie ZAP y lea todos los términos de la licencia. Haga clic en **Acepto** si usted esta de acuerdo con todos los términos, y ZAP finalizará la instalación, luego ZAP se iniciará de forma automática.

Mantener una sesión

Cuando usted inicia por primera vez ZAP, se le va a preguntar si usted desea continuar la sesión de ZAP. Por defecto, todas las sesiones de ZAP siempre son grabadas en el disco de una de las bases de datos de HSQLDB con un nombre y una localización que es predeterminada. Si usted no mantiene la sesión, esos archivos se van a eliminar cuando usted salga de ZAP.

Si usted elige mantener una sesión, la información que se encuentra en la sesión se va a guardar en la base de datos local para que usted pueda ingresar a ella más adelante, y usted podrá seleccionar los nombres y las localizaciones personalizadas para poder guardar dichos archivos.

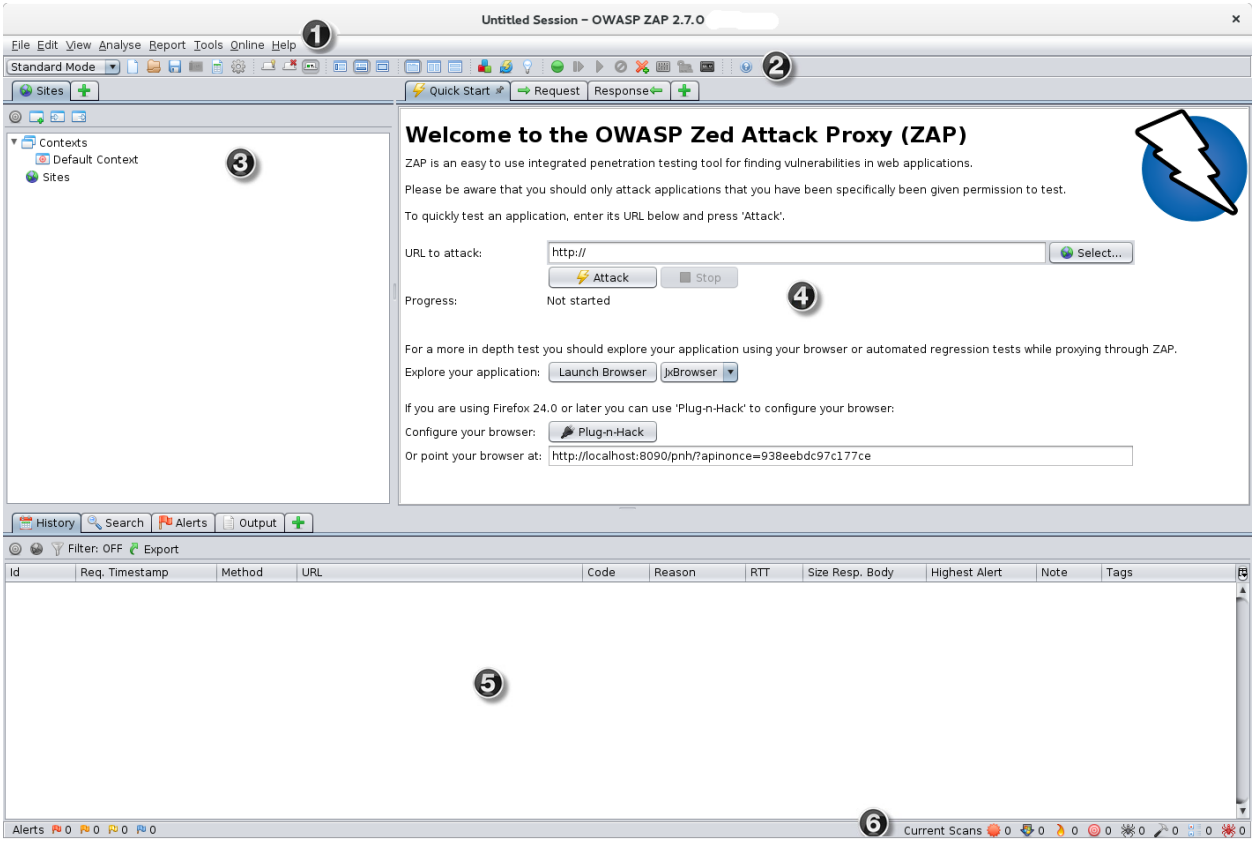


Por ahora, elija**No, no deseo continuar en esta sesión en este preciso momento**, luego haga clic en **Comenzar**. Las sesiones de ZAP no se podrán mantener por ahora.

UI ZAP

La interfaz del usuario de ZAP esta compuesta por los siguientes elementos:

1. **Barra de menús**: otorga el acceso a muchas de las herramientas las cuales son automática y manuales
2. **Barra de herramienta**: esta incluye los botones que otorgar un acceso fácil a las funciones más utilizadas de forma habitual.
3. **Ventana de Árbol** - Muestra el árbol de sitios y el árbol de secuencias de comando.
4. **Ventana de espacio de trabajo** - Muestra de solicitudes, respuestas, y secuencias de comando y le permite editarlos.
5. **Ventana de información** - Muestra los detalles de las herramientas manuales y automatizadas.
6. **Pie de página** - muestra un resumen de las alertas encontradas y el estado de las principales herramientas automatizadas.



Mientras usa ZAP, puede hacer clic en **Ayuda** en la barra de menú o presionar F1 para acceder a la ayuda contextual desde la Guía del usuario de ZAP.

Para obtener más información acerca de la interfaz de usuario, consulte la descripción general de la interfaz de usuario de ZAP en la documentación en línea de ZAP.

ZAP también es muy compatible con una API de mucha potencia y funcionalidad en línea de los comandos, las cuales se encuentran más allá del alcance de esta guía.

Lanzamiento de navegadores

Tú puedes comenzar de forma rápida y fácil los navegadores que están preconfigurados para el proxy por medio de ZAP a través de la pestaña de inicio rápido. Los navegadores que son iniciados de esta manera también van a ignorar las advertencias de validación de los certificados que, de lo contrario, se podrían informar.

Esta opción iniciará cualquiera de los navegadores más comunes que haya instalado con nuevos perfiles.

Si usted desea poder utilizar cualquiera de sus navegadores con un perfil que ya existe, por ejemplo, con otros complementos del navegador que ya estan instalados, usted deberá modificar su navegador de manera manual por medio de ZAP e importar y también confiar en el certificado ZAP Roor CA. Consulte laGuía del usuario de ZAP para obtener más detalles.

Intente conectar su aplicación web

Una vez que haya configurado correctamente su navegador para usar ZAP como su proxy, intente conectarse a la aplicación web que va a probar.

Si usted no puede ingresar a su aplicación web, revise lo siguiente:

1. Revise la configuración del proxy que utiliza el navegador para poder conectarse a ZAP.
2. Verifique que la configuración del proxy en ZAP sea la que se utiliza en el navegador para poder intentar conectarse a ZAP.
3. Verifique que la aplicación web que usted necesita probar se esté ejecutando.
4. Revise si su red necesita un proxy para poder llegar a su aplicación web. Si es así, puede que usted necesite modificar ZAP para poder utilizar un proxy.

Para poder modificar ZAP para lograr utilizar un proxy saliente:

1. Inicie ZAP y en la barra de menú, haga clic en **Herramientas** -> **Opciones**.
2. Seleccione**Conexión** en el panel izquierdo.
3. En la **utilizar la extensión de proxy** de la sección **Conexión** comprobar ajustes **Utilizar una casilla de verificación del servidor proxy de salida** . [cadena vacía]
4. Ingrese la **Dirección/Nombre de dominio** y **Puerto** para su proxy de red.
5. Haga clic en **Aceptar** para guardar la configuración y verificar que ahora puede conectarse a su aplicación web.

Una vez que su navegador esté conectado de forma exitosa a su aplicación web, entonces estará lista para poder ejecutar una prueba.

Start Pentesting with ZAP

La manera más fácil de poder comenzar a utilizar ZAP es ejecutando una prueba de inicio rápido. Quick Start es un complemento de ZAP que se instaló de forma automática cuando usted instaló ZAP.

IMPORTANTE : solo debe utilizar ZAP para atacar una aplicación que tenga permiso para probar con un ataque activo. Gracias a que esta es una simulación que actúa como un ataque real, el daño real se puede realizar a la funcionalidad, datos, etc, que se encuentran en el sitio. Si a usted le preocupa poder utilizar ZAP, usted puede prevenir que cause muchos daños (aunque la funcionalidad de ZAP se verá reducida de forma significativa) al cambiar al modo seguro.

Para cambiar ZAP a modo seguro, haga clic en la flecha del menú desplegable en la modalidad de la barra de herramientas principal para expandir la lista desplegable y seleccione **Modo seguro** .

Ejecutar una prueba de inicio rápido

Para poder activar una prueba de inicio rápido:

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

ZAP va a proceder a localizar la aplicación web con su araña, y después escaneará de forma pasiva cada una de las páginas que consiga. Después ZAP, utilizará el escáner activo para poder atacar todas las páginas, funcionalidades y los parámetros que fueron descubiertos.

Interpretar los resultados de la prueba

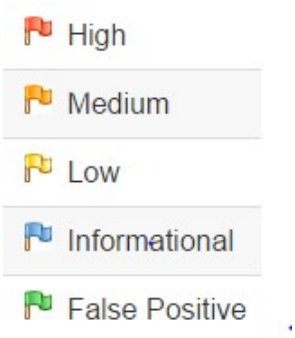
Como ZAP araña es una aplicación web, contruye un mapa de todas las páginas de sus aplicaciones web y de todos los recursos que fueron utilizados para poder representar dichas páginas. Luego registra todas las solicitudes y las respuestas enviadas a cada una de las páginas y crea unas alertas si hay algo que sea incorrecto de forma potencial con una solicitud o respuesta.

Ver páginas exploradas

To examine a tree view of the explored pages, click the **Sites** tab in the Tree Window. Tu puedes expandir todos los nodos para poder observar la URL que son individuales a las que se ingrese. [cadena vacía]

Ver alertas y detalles de alerta

El lado izquierdo del pie de página posee un recuento de todas las alertas conseguidas durante el momento de la prueba, separadas en categorías de riesgo. Estas categorías de riesgo son:



Para poder observar las alertas que fueron creadas durante su prueba:

1. Haga clic **Alertas** en la ventana de información.
2. Haga clic en cada una de las alertas que se muestran en esa ventana para poder mostrar la URL y la vulnerabilidad que fue detectada en el lado derecho de la ventana de información.
3. En el espacio de trabajo de Windows, haga clic en la pestaña **Respuesta** para ver el contenido del encabezado y el cuerpo de la respuesta. La zona de la respuesta que originó la alerta se va a resaltar. [cadena vacía]

Expand Your Pentesting with ZAP

La funcionalidad de el escaneo pasivo y el ataque automático es una gran forma de iniciar una evaluación de una vulnerabilidad de su aplicación web, pero esta posee algunas limitaciones. Entre estas están:

- Las paginas que están protegidas por una página de inicio de sesión no pueden ser detectadas durante una exploración que es pasiva porque, a menos de que se haya modificado la funcionalidad de la autenticación de ZAP, ZAP no va a poder manejar la autenticación que es necesitada.
- Las páginas que no se pueden conseguir con la araña predeterinada de ZAP no se pueden probar durante el momento de un escaneo pasivo. ZAP otorga unas opciones adicionales para el descubrimiento y la cobertura que se encuentra fuera del escaneo pasivo.
- No posee mucho control sobre la secuencia de la exploración en un análisis que es pasivo o a los tipos de ataques que se realizan durante un ataque de forma automática. ZAP otorga un gran variedad de opciones extras para la exploración y los ataques que se encuentran fuera del escaneo pasivo.

Configure and Run a Spider with ZAP

Una forma de poder agrandar y mejorar sus pruebas es modificando la araña que ZAP está utilizando para poder explorar su aplicación. El análisis rápido utiliza la araña tradicional de ZAP, que cosigue los enlaces al revisar el HTML en las respuestas de la aplicación web. Esta araña es muy rápida, pero no siempre es muy efectiva cuando se trata de explorar una aplicación web AJAX que origina unos elances utilizando JavaScript.

Para las aplicaciones que son JAX, es muy posible que la araña de ZAP sea mucho mas eficiente. Esta araña puede explorar la aplicación web invocando los navegadores que después continuan los enlaces que se han generado. La araña AJAX es mucho más lenta que la araña tradicional y necesita una configuración extra para su utilización en un dominio "sin cabeza".

Una manera sencilla de modificar entre las arañas es habilitar una pestaña para cada una de las arañas en la ventana de información y utilizar esa misma pestaña para poder comenzar las exploraciones.

1. En la ventana de información, haga clic en el signo más verde(**+**).
2. Click **Spider** to create a Spider tab.
3. Repeat step 1, then click **AJAX Spider** to create an **AJAX Spider** tab.
4. Click the push-pin symbol on both the **Spider** and **AJAX Spider** tabs to pin them to the Information Window. [cadena vacía]

Tenga en cuenta que estas dos pestañas incluyen un **Nueva exploración** botón.

Explor su sitio

Las arañas que son una forma excelente para poder explorar tu sitio básico, pero se tienen que combinar con la exploración manual para poder ser mas eficiente. Las arañas, por ejemplo, solo pueden realizar el ingreso de datos básicos que son predeterminados en los formularios de su aplicación web, pero un usuario puede ingresar información más notable que, a su vez, puede exponer más de la aplicación web a ZAP. Esto es verdadero con cierto tipos de cosas como formularios de registros donde se necesitan las direcciones de correos que sean válidas. La araña puede incorporar una cadena de forma aleatoria, lo cual

producirá un error. Un usuario podrá reaccionar a ese error y otorgar una cadena con el formato que sea correcto, lo que puede ocasionar que más de la aplicación se encuentre expuesta cuando se realice el envío y acepta el formulario.

Como usted ha modificado su navegador para poder utilizar ZAP como su proxy, usted necesita explorar toda su aplicación web con ese navegador. Al hacer esto, ZAP analiza pasivamente todas las solicitudes y respuestas realizadas durante su exploración en busca de vulnerabilidades, continúa construyendo el árbol del sitio y registra las alertas de posibles vulnerabilidades encontradas durante la exploración.

Es importante que ZAP explore cada página de su aplicación web, ya sea vinculada a otra página o no, en busca de vulnerabilidades. La oscuridad no es seguridad, y las páginas ocultas a veces se activan sin previo aviso. Así que sea lo más cuidadoso posible cuando explores su sitio.

Ejecutar un escaneo activo con ZAP

Hasta ahora, ZAP solo ha realizado escaneos pasivos de su aplicación web. El escaneo pasivo no cambia las respuestas de ninguna manera y se considera seguro. El escaneo también se realiza en un hilo de fondo para no ralentizar la exploración. El escaneo pasivo es bueno para encontrar algunas vulnerabilidades y como una forma de familiarizarse con el estado de seguridad básico de una aplicación web y localizar dónde se puede requerir más investigación.

El escaneo activo, sin embargo, intenta encontrar otras vulnerabilidades mediante el uso de ataques conocidos contra los objetivos seleccionados. El escaneo activo es un ataque real contra esos objetivos y puede poner en riesgo a los objetivos, por lo que no utilice el escaneo activo contra los objetivos que no tiene permiso para probar.

Para comenzar un escaneo activo:

1. In the Tree View, in the **Sites** tab, select the sites you want to perform an active scan on.
2. Haga clic con el botón derecho en los sitios seleccionados y seleccione **Active Scan** .

o

1. En la ventana de información, seleccione la pestaña **Active Scan** tab.
2. Click **New Scan**.

To review and modify your settings, then begin an active scan:

1. In the Menu Bar, click **Tools** -> **Active Scan**.
2. Review the settings and make any changes you wish to.
3. Click **Start Scan** to start the Active Scan with these settings.

You can review the results of your active scan the same way you reviewed the results of your passive scan, as shown in Interpret Your Test Results.

Learn More About ZAP

Ahora que está familiarizado con algunas capacidades básicas de ZAP, puede aprender más acerca de las capacidades de ZAP y cómo usarlas desde la Guía del usuario de ZAP. La Guía del Usuario proporciona instrucciones paso a paso, referencias para el API, programación en líneas de comandos, vídeos instructivos y consejos y trucos para usar ZAP. [cadena vacía]

Enlaces Útiles

OWASP Zed Attack Proxy Project – ZAP's main project page

OWASP ZAP Wiki – The ZAP Wiki

OWASP ZAP User Guide - The ZAP User Guide

OWASP ZAP Hot Keys - The list of ZAP hotkeys

ZAP Users Group – Google group for ZAP users

ZAP Developers Group – Google group for developers and contributors to ZAP