



Materia: Tecnologías para la Web.

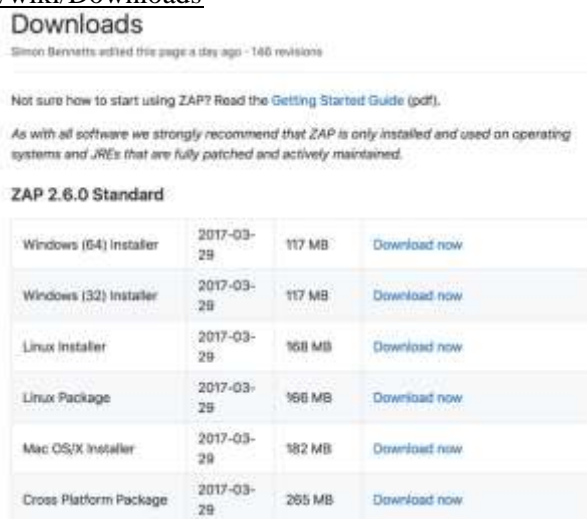
Tema: Instalación y Configuración de la herramienta Proxy Zed Attack de OWASP.

Al estar desarrollando un nuevo sitio web o una aplicación móvil, ver qué sucede detrás de la escena y verificar si existe alguna vulnerabilidad, es parte de tener una aplicación segura. OWASP ZAP es una herramienta de prueba de penetración integrada de código abierto que se utiliza para encontrar vulnerabilidades en aplicaciones web. La herramienta es utilizada por desarrolladores y evaluadores funcionales y es muy fácil de usar. Hay otras herramientas de proxy disponibles, como Charles Proxy, MITM Proxy y Burp Suite.

Descargar e instalar ZAP.

- Descargar ZAP desde GitHub. Elegir el instalador según el sistema operativo.

<https://github.com/zaproxy/zaproxy/wiki/Downloads>

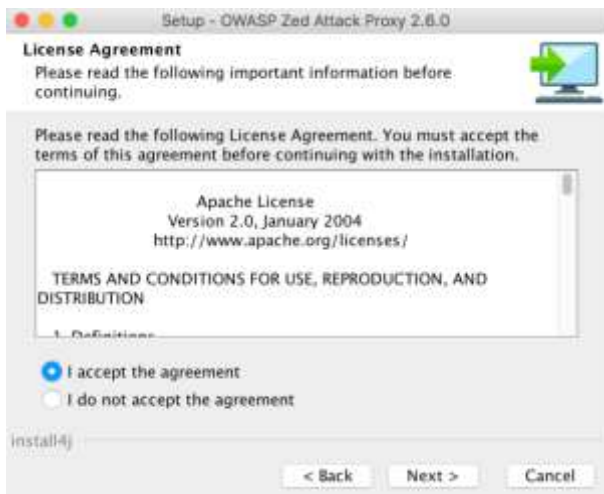


Downloads			
Simon Bennetts edited this page a day ago · 146 revisions			
Not sure how to start using ZAP? Read the Getting Started Guide (pdf).			
As with all software we strongly recommend that ZAP is only installed and used on operating systems and JREs that are fully patched and actively maintained.			
ZAP 2.6.0 Standard			
Windows (64) Installer	2017-03-29	117 MB	Download now
Windows (32) Installer	2017-03-29	117 MB	Download now
Linux Installer	2017-03-29	168 MB	Download now
Linux Package	2017-03-29	166 MB	Download now
Mac OS/X Installer	2017-03-29	182 MB	Download now
Cross Platform Package	2017-03-29	265 MB	Download now

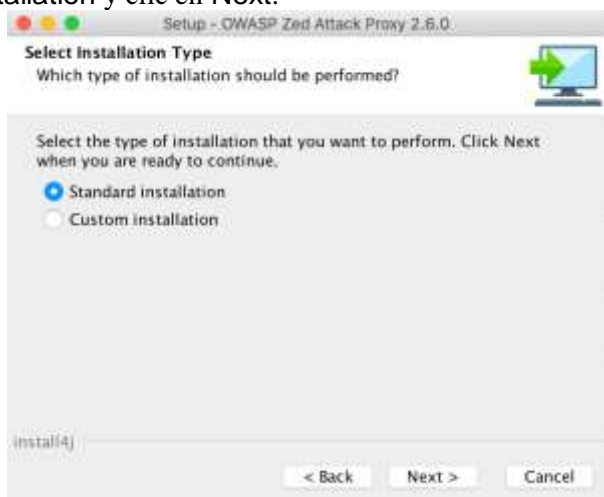
- Una vez iniciado el archivo ejecutable, aparecerá la siguiente pantalla de instalación. En este punto, clic en el botón Next.



- Aceptar la licencia y clic en Next >:



- Seleccionar Standard Installation y clic en Next:

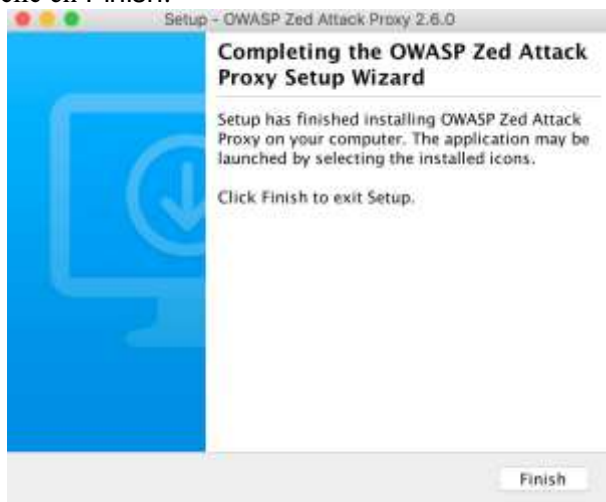


- Para iniciar la instalación clic en Install:





- Al terminar la instalación, clic en Finish:

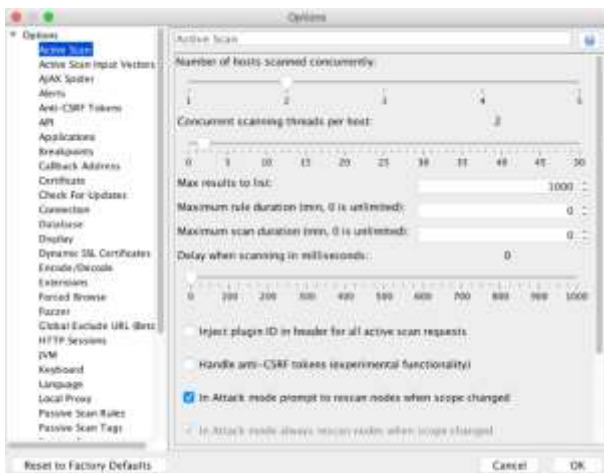


Configuración de ZAP:

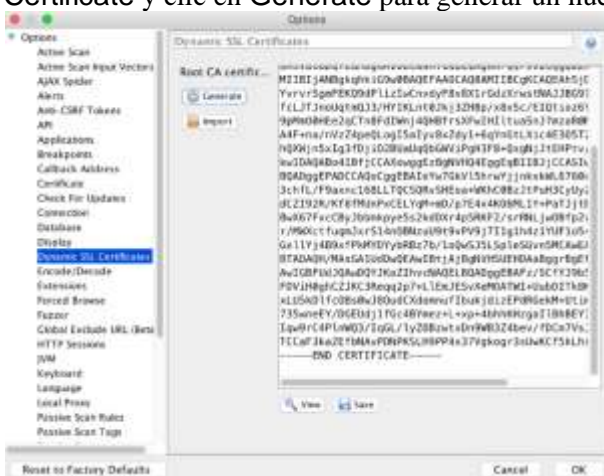
- Abrir ZAP y se deben ver las siguientes opciones. Si se desea que ZAP guarde la sesión en la ubicación predeterminada, se puede elegir la primera opción. Si se desea que la sesión se guarde en una ubicación específica, elegir la segunda opción. Para la última opción, la sesión no se guardará después de salir de una sesión. Para efectos de demostración, elegir la primera opción:



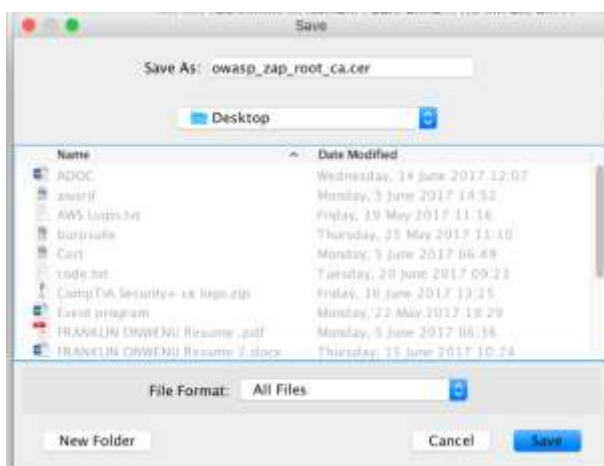
- Ahora, para comenzar a ver el tráfico de una aplicación web en ZAP, tendremos que configurar el navegador para comunicarse con ZAP. Pero antes de hacerlo, se instala el certificado SSL de ZAP para que el navegador no insista con las constantes solicitudes de error de excepción SSL. Es necesario tener un certificado SSL cuando se procesa mediante proxy de sitios https. Si se navega en Tools > Options, se mostrarán las opciones siguientes:



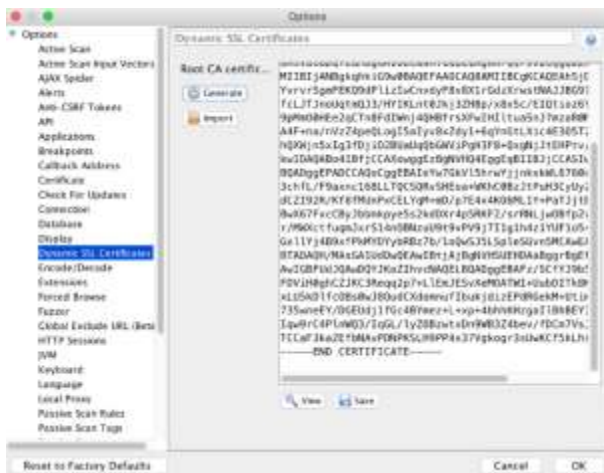
- Dirigirse a Dynamic SSL Certificate y clic en Generate para generar un nuevo certificado:



- Ahora, clic en Save para guardar el certificado en la ubicación que se desee. También, el certificado se puede renombrar:



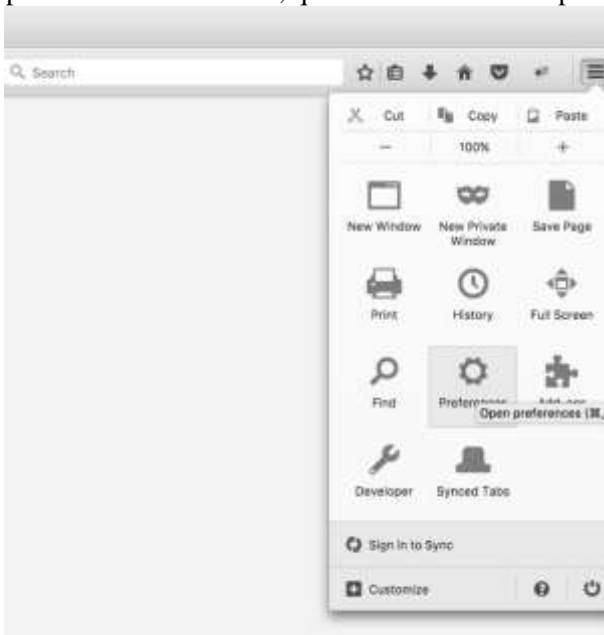
- Clic en Ok para salir de ventana de opciones:



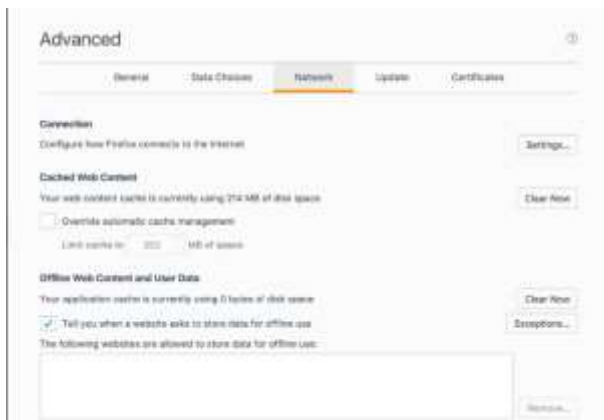
Configuración del navegador web.

El navegador Firefox es un navegador popular cuando se trabaja con herramientas proxy. Sin embargo, se puede usar cualquier otro navegador.

- Abrir FireFox y clic en la opción de Preferencias, que se encuentra en la parte superior derecha de la pantalla.



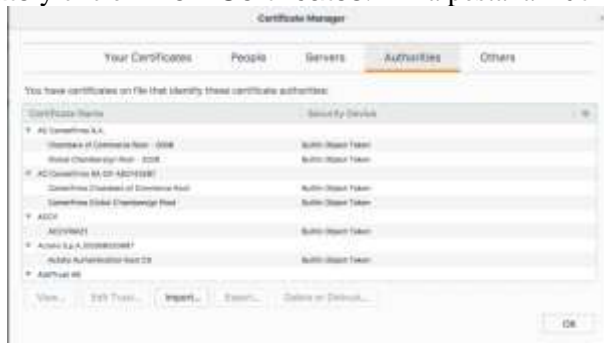
- Clic en la pestaña Advanced y luego clic en la pestaña Network. Enseguida, clic en el botón Settings:



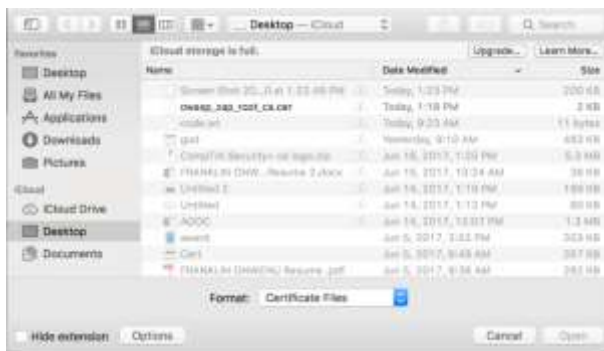
- Configurar el navegador con los siguientes parámetros. Al terminar, clic en OK:



- Clic en la pestaña Certificate y clic en View Certificates. En la pestaña Authorities, clic en el botón Import:



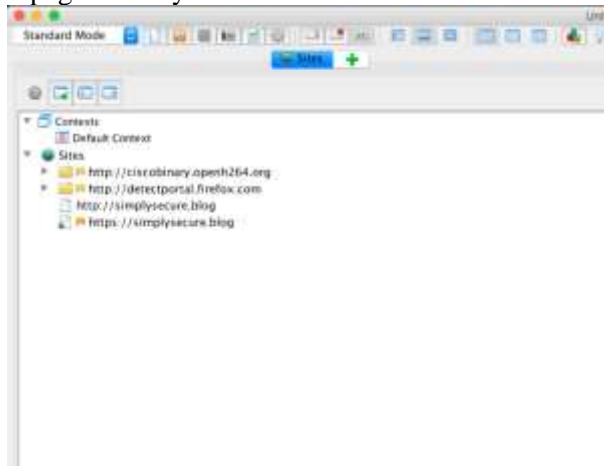
- Localizar y seleccionar el certificado que se guardó anteriormente y clic en Open:



- Seleccionar las tres opciones y clic en OK. Enseguida clic en OK para salir del Administrador de Certificados:



- Ahora, se puede navegar a la página web y observar el tráfico de red en ZAP:



Si hubiera algún problema al configurar ZAP, reiniciar el navegador y ZAP. Si ello no resuelve el problema, visitar Github para obtener sugerencias de solución de problemas. También se puede consultar el video para configurar el navegador con ZAP: <https://www.youtube.com/watch?v=ntUSFP0Af1k>.