Tipo : Guía de laboratorio
Capítulo : Seguridad de aplicaciones web
Duración : 45 minutos

I. OBJETIVO

Instalar y validar reporte de OWASP Zed Attack Proxy

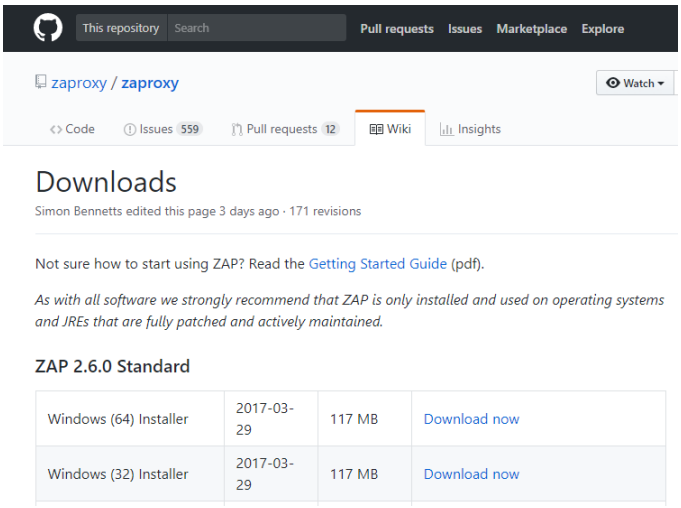
II. REQUISITOS

Los siguientes elementos de software son necesarios para la realización del laboratorio:

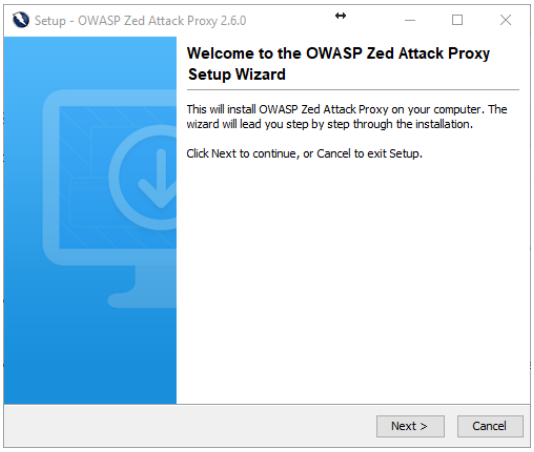
- Windows 10 (como mínimo Windows 8)
- Visual Studio 2017 (como mínimo Visual Studio 2015)

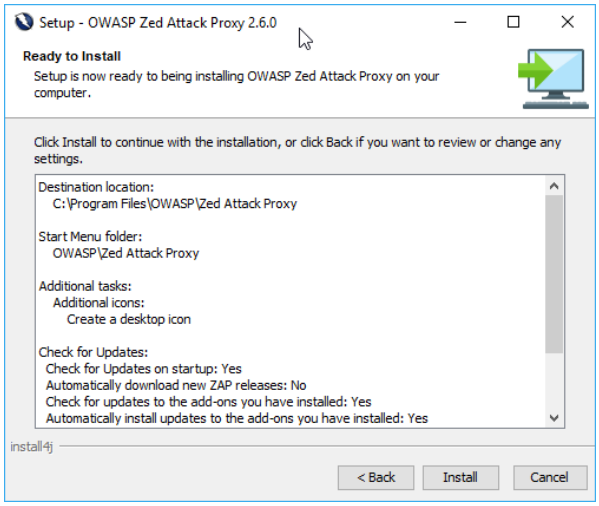
III. EJECUCIÓN DEL LABORATORIO

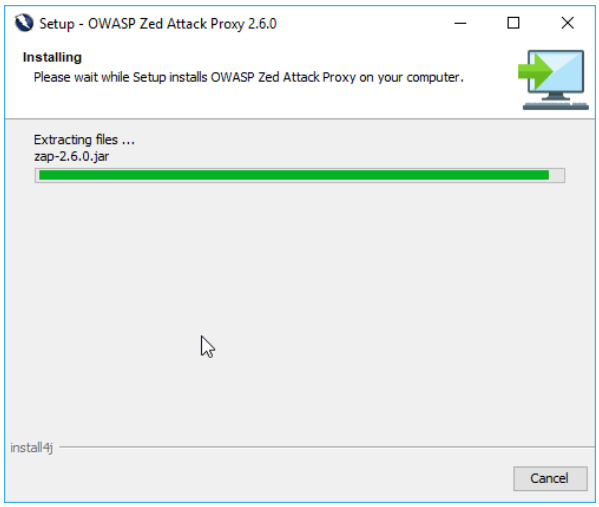
1. Descarga la última versión vigente OWASP Zed Attack Proxy desde la siguiente URL: https://github.com/zaproxy/zaproxy/wiki/Downloads

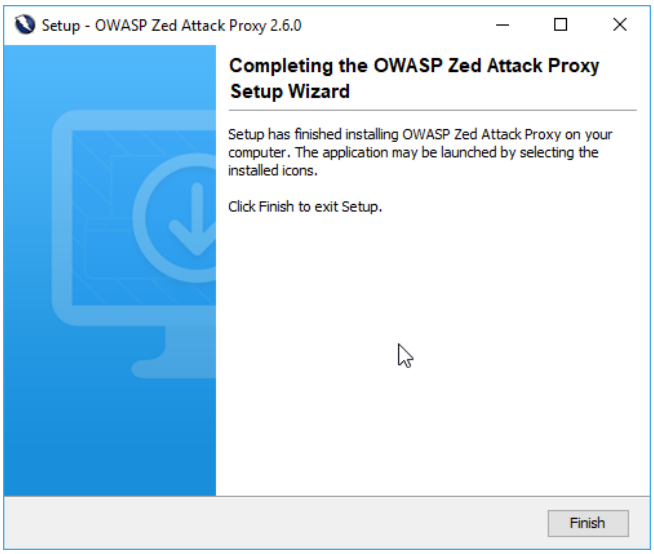


2. Una vez finalizada la descarga, iniciar la instalación:

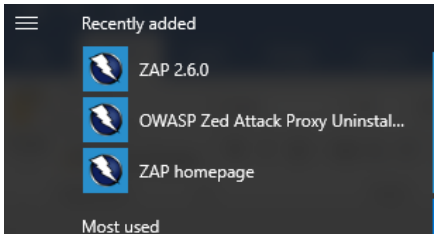



Setup - OWASP Zed Attack Proxy 2.6.0
Ready to Install
Setup is now ready to being installing OWASP Zed Attack Proxy on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files\OWASP\Zed Attack Proxy
Start Menu folder:
OWASP\Zed Attack Proxy
Additional tasks:
Additional icons:
Create a desktop icon
Check for Updates:
Check for Updates on startup: Yes
Automatically download new ZAP releases: No
Check for updates to the add-ons you have installed: Yes
Automatically install updates to the add-ons you have installed: Yes
install4j
< Back
Install
Cancel

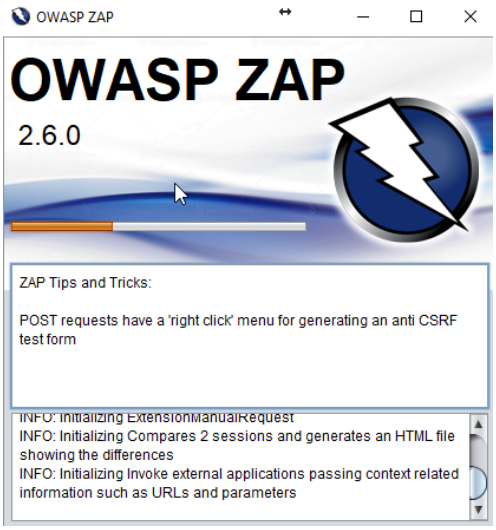

Setup - OWASP Zed Attack Proxy 2.6.0
Installing
Please wait while Setup installs OWASP Zed Attack Proxy on your computer.
Extracting files ...
zap-2.6.0.jar
install4j
Cancel

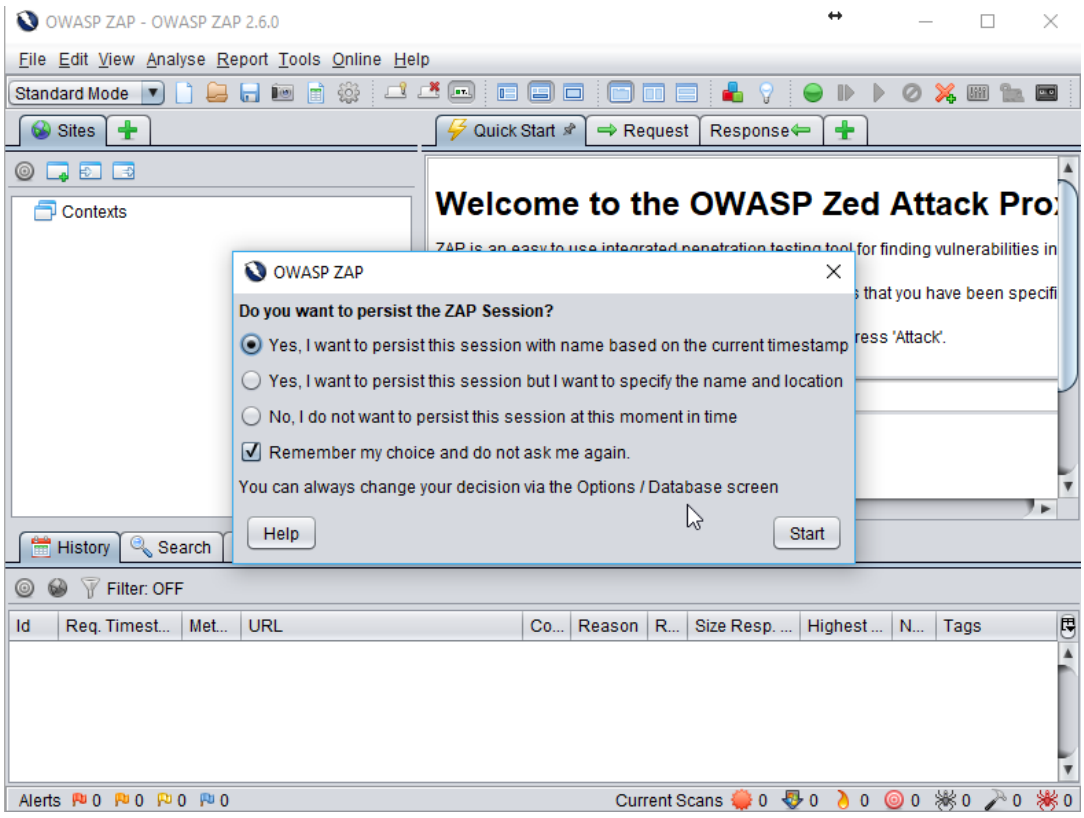

Setup - OWASP Zed Attack Proxy 2.6.0
Completing the OWASP Zed Attack Proxy Setup Wizard
Setup has finished installing OWASP Zed Attack Proxy on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Finish

3. Finalizada la instalación, procedemos con la ejecución del ejecutable:



Al momento de elaborar el presente material la versión vigente es: 2.6.0; al abrir dicho ejecutable visualizaremos la siguiente pantalla:



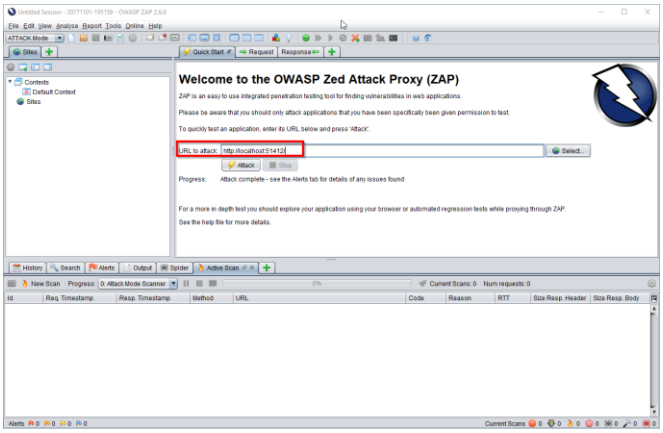


Marcamos las opciones como en la imagen y hacemos clic en Start.

4. Para poder iniciar el escaneo, primero debemos de ejecutar nuestra aplicación.

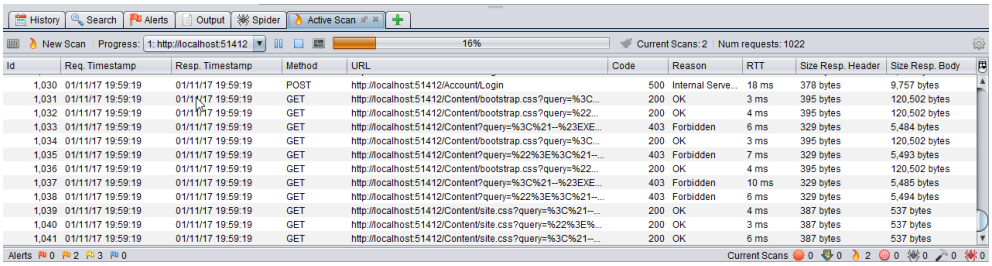
5. Una vez la compilación y ejecución se encuentra en marcha, copiamos la URL en mi caso es: **http://localhost:51412/** , recordemos que por ser IISExpress el puerto puede variar por cada ordenador.

6. Ahora iniciamos el análisis de nuestra aplicación web con los siguientes pasos:
   (1) En la ventana pegamos la URL de la aplicación web.

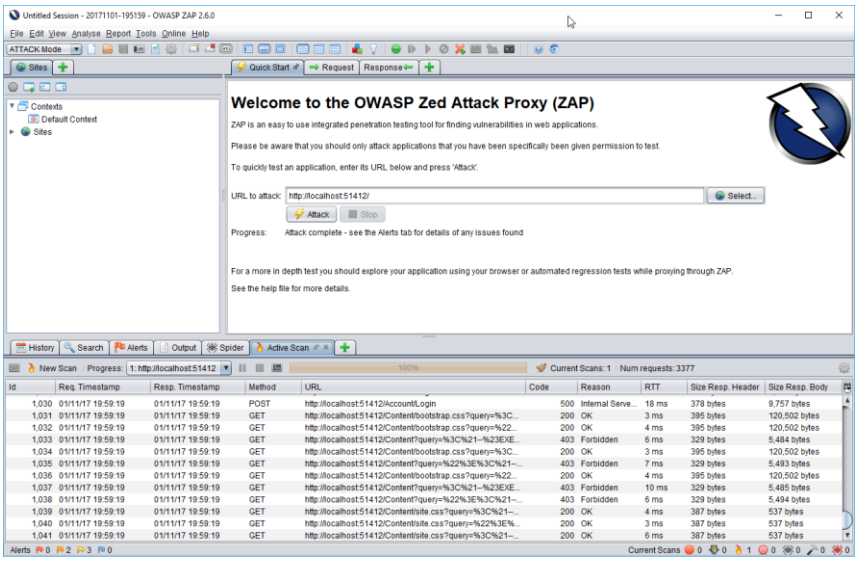


Hacemos clic en Attack

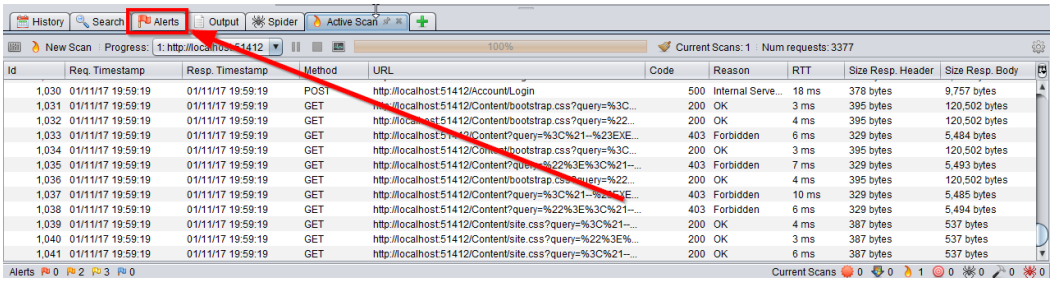
   (2) En la misma ventana podremos notar el avance:



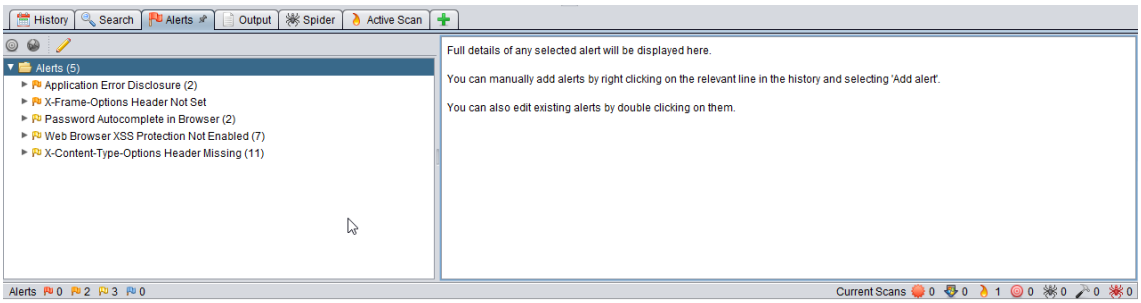
   (3) Esperamos para ver cuáles son las vulnerabilidades detectadas.



(4) Una vez finalizado el escaneo, hacemos clic en Alerts.



(5) Procedemos a revisar nuestras vulnerabilidades:



(6) Tenemos que tener en cuenta que los resultados pueden variar por ordenador.

7. Con ayuda del docente procede a aplicar técnicas para evitar las vulnerabilidades encontradas.

IV. EVALUACIÓN

1. ¿Cuáles son las carpetas principales en una aplicación MVC?

   Las carpetas principales son: Controllers, Views y Models

2. ¿Qué pasa si al nombre del controlador no se le coloca el prefijo Controller?

   Por convención todos los archivos que van a ser controladores deben tener el prefijo Controller al final del nombre para que puedan ser reconocidos por Asp.NET como tales.

3. ¿Cuál es el tipo de datos de los métodos del controller?

   El tipo base de todos los controladores es ActionResult.

4. ¿Qué es una vista Layout?

   Es la vista maestra, en ella se establece la estructura base (html) de todas las vistas que tendrá la aplicación web. Algunas vistas pueden no utilizar la vista base.

5. Los modelos, ¿pueden ser librería de clases?

   Sí, los modelos son un concepto que involucra entidades, acceso a datos, reglas de negocio y pueden ser implementadas en librería de clases (dll).

6. ¿Qué son las vistas parciales?

   Al igual que las vistas normales, estas permiten ser reutilizadas en ciertas partes de la aplicación.