Instituto Politécnico Nacional

Unidad Profesional Interdisciplinaria en Ingeniería y Tecnologías Avanzadas

Seguridad de Redes

Profesor. Polanco Montelongo Francisco Antonio

Alumno: Hernández Guzmán Bryan Alexis

Grupo: 3TV4

Práctica: OWASP

INTRODUCCION

OWASP (acrónimo de Open Web Application Security Project, en inglés 'Proyecto abierto de seguridad de

aplicaciones web') es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen

que el software sea inseguro. La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona

los proyectos e infraestructura de OWASP. La comunidad OWASP está formada por empresas, organizaciones

educativas y particulares de todo mundo. Juntos constituyen una comunidad de seguridad informática que

trabaja para crear artículos, metodologías, documentación, herramientas y tecnologías que se liberan y pueden

ser usadas gratuitamente por cualquiera.

OWASP es un nuevo tipo de entidad en el mercado de seguridad informática. Estar libre de presiones

corporativas facilita que OWASP proporcione información imparcial, práctica y redituable sobre seguridad de

aplicaciones informáticas. OWASP no está afiliado a ninguna compañía tecnológica, si bien apoya el uso

informado de tecnologías de seguridad. OWASP recomienda enfocar la seguridad de aplicaciones informáticas

considerando todas sus dimensiones: personas, procesos y tecnologías.

Los documentos con más éxito de OWASP incluyen la Guía OWASP y el ampliamente adoptado documento de

autoevaluación OWASP Top 10. Las herramientas OWASP más usadas incluyen el entorno de formación

WebGoat, la herramienta de pruebas de penetración WebScarab y las utilidades de seguridad para entornos

.NET OWASP DotNet. OWASP cuenta con unos 50 capítulos locales por todo el mundo y miles de participantes

en las listas de correo del proyecto. OWASP ha organizado la serie de conferencias AppSec para mejorar la

construcción de la comunidad de seguridad de aplicaciones web.

El más famoso de los proyectos de esta metodología es conocido con el nombre OWASP TOP 10, que no es

más que un listado de los problemas de seguridad más comunes en las aplicaciones web y ordenados de más

a menos críticos.

A1: Inyección

A2: Pérdida de autenticación y gestión de sesiones

A3: Datos sensibles accesibles

A4: Entidad externa de XML (XXE)

A5: Control de acceso inseguro

A6: Configuración de seguridad incorrecta

A7: Cross site scripting (XSS)

A8: Decodificación insegura

A9: Componentes con vulnerabilidades

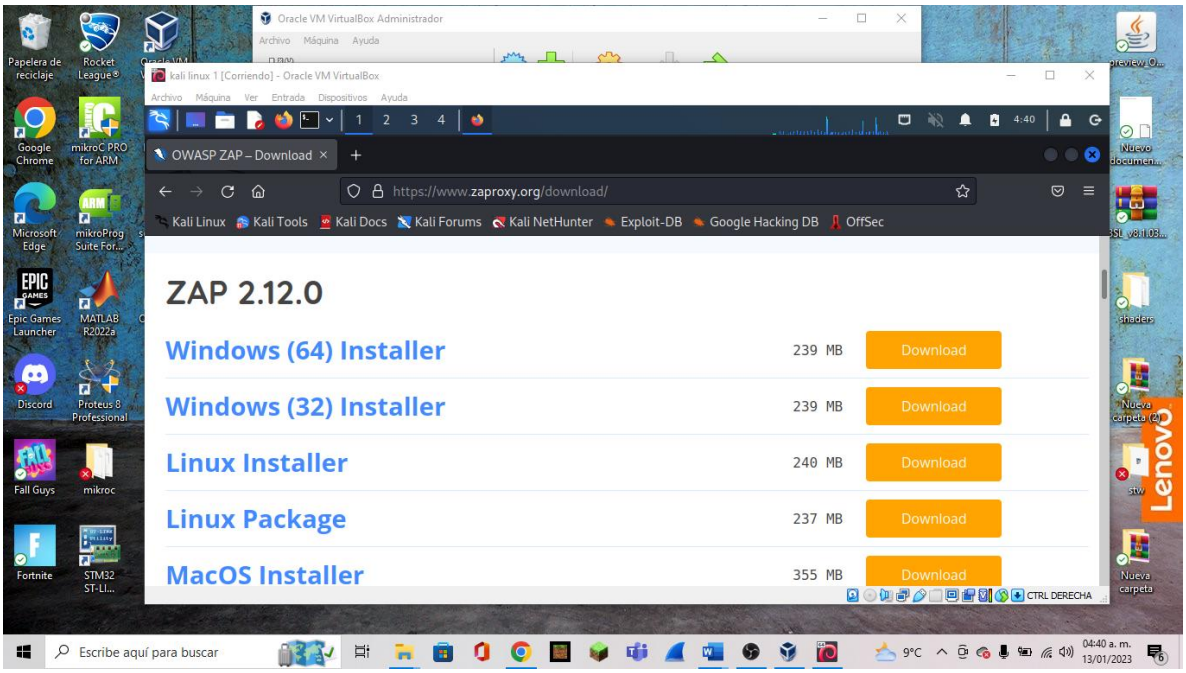
A10: Insuficiente monitorización y registro

Desarrollo:

Para el desarrollo de esta práctica se realizaron los siguientes pasos.

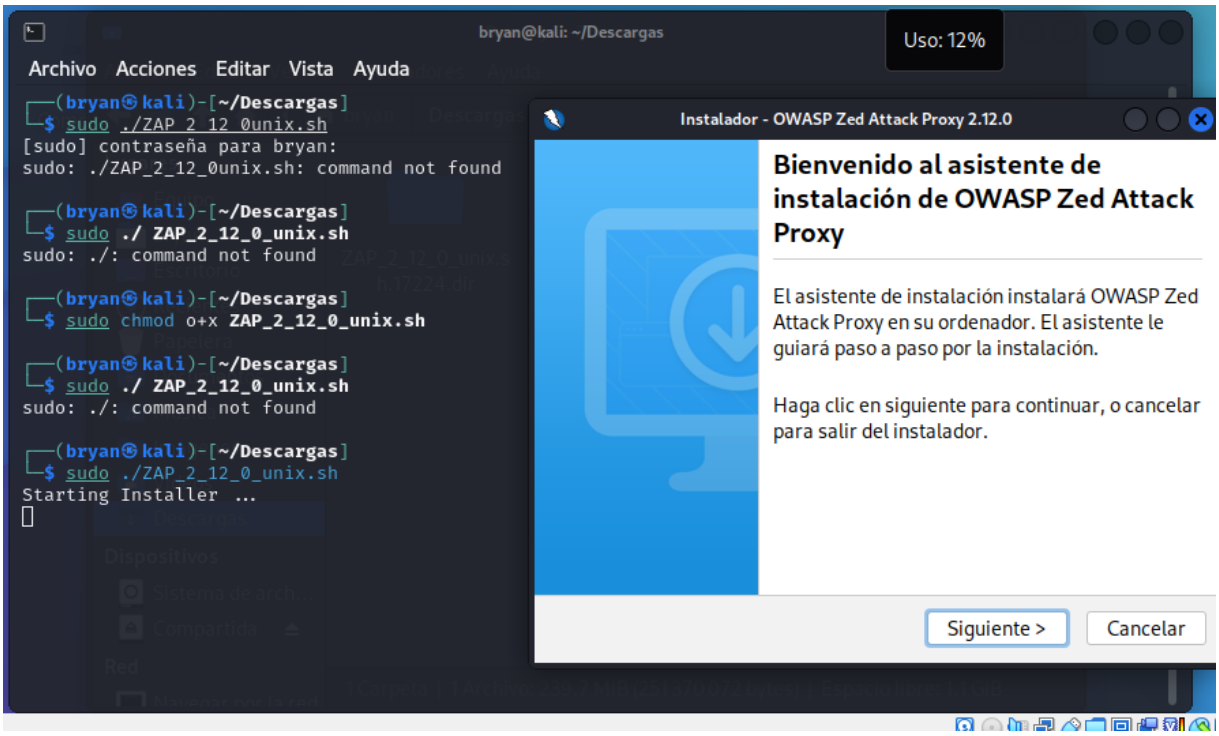
Se debera descargar el instalador desde el siguiente link

https://www.zaproxy.org/download/

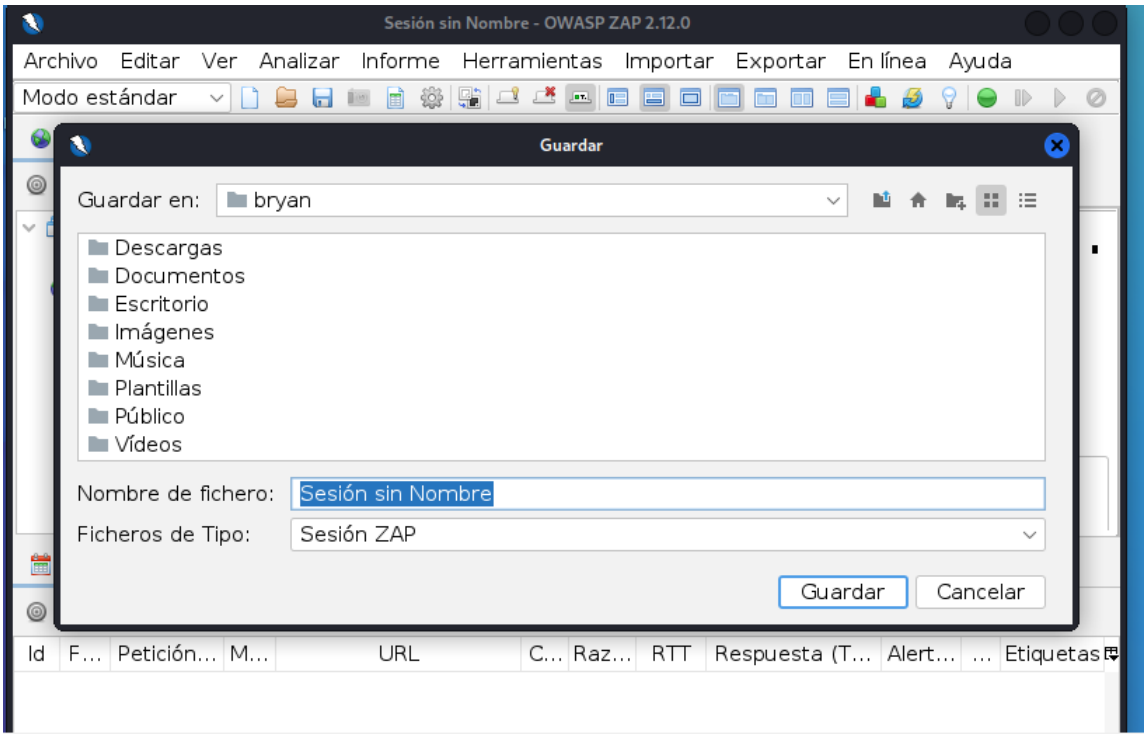


Se ejecutara el comando sudo chmod o+x ZAP_2_12_0unix.sh

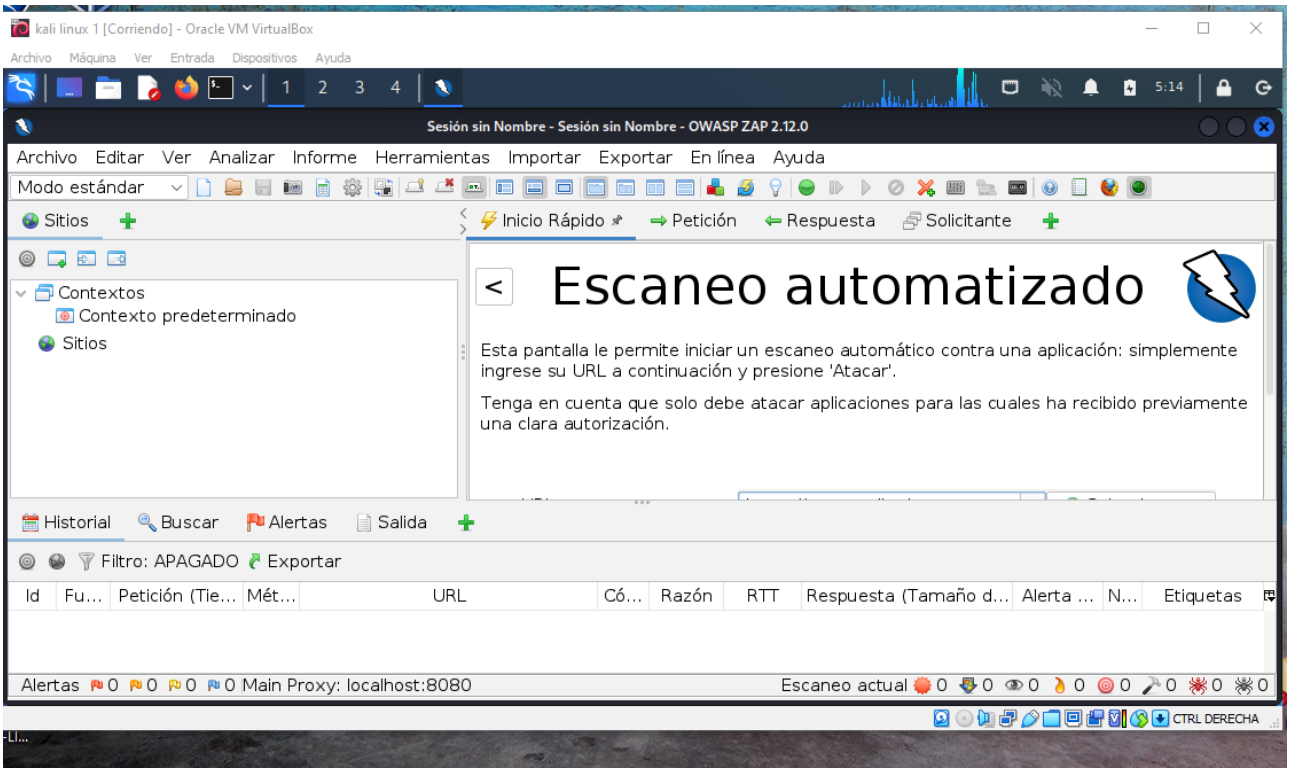
Posteriormente se ejecutará el comando siguiente para su instalación:



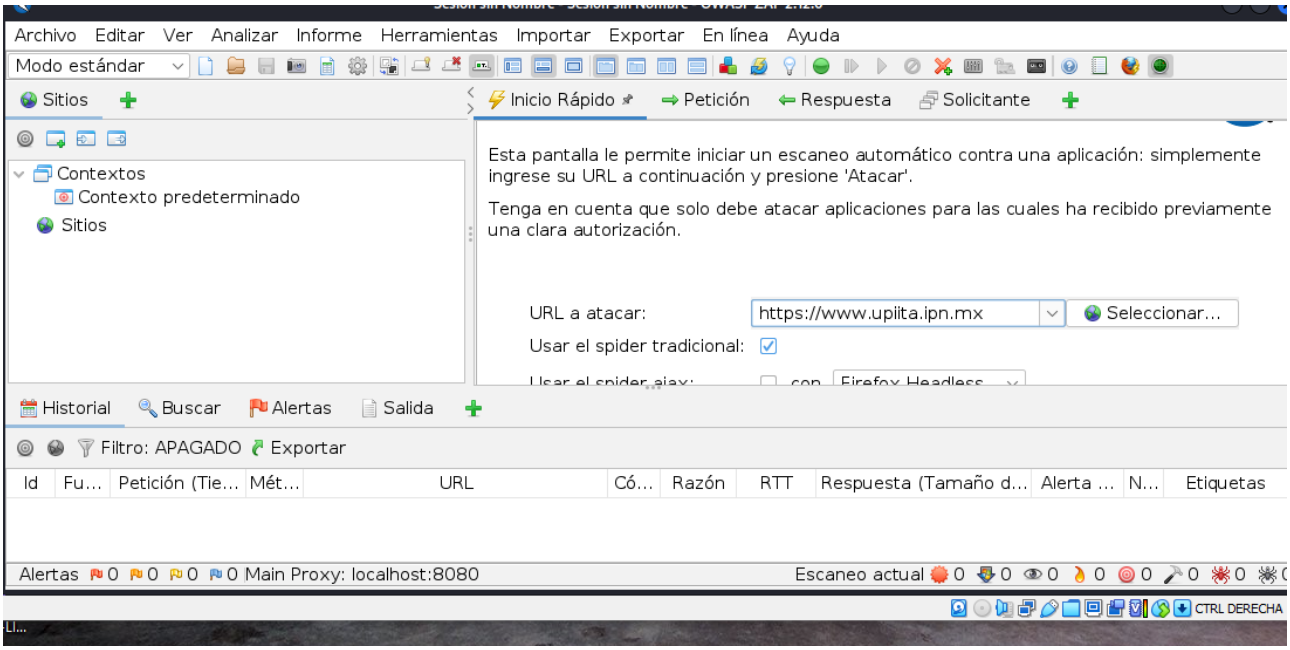
Guardaremos nuestro proyecto:



Seleccionaremos Escaneo automatizado:

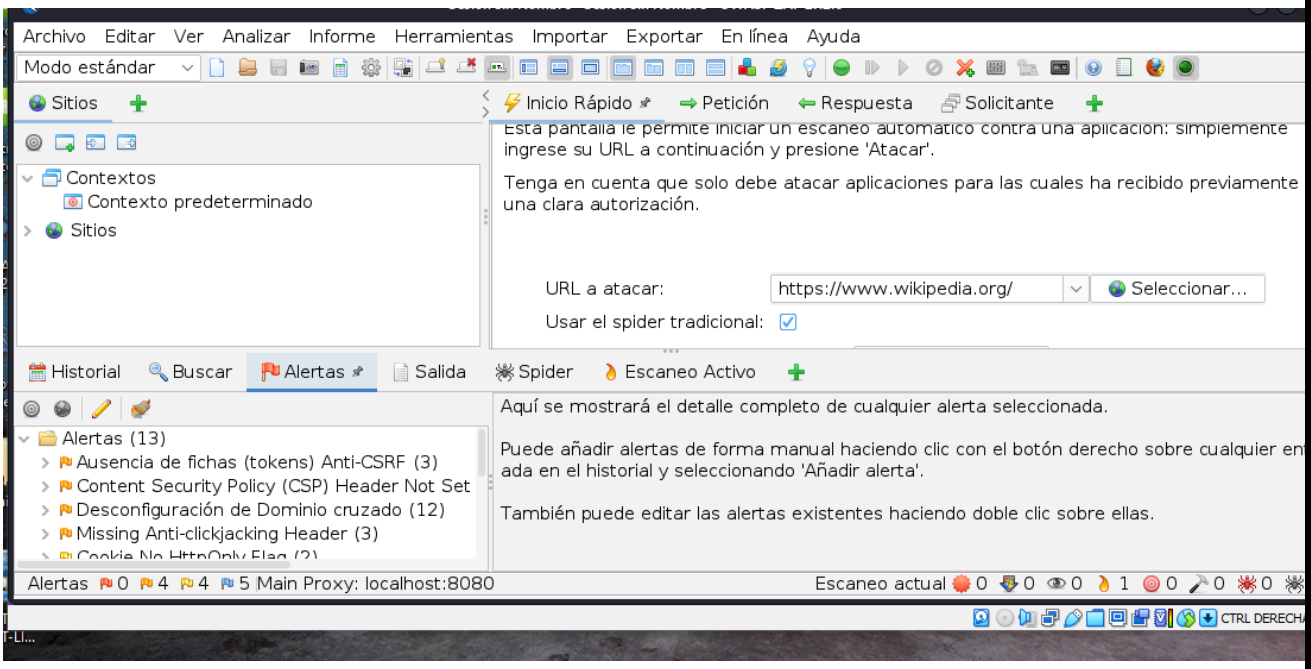


Procederemos a meter nuestra URL que queremos analizar:



Aquí metí la URL de Wikipedia porque otras paginas no me dejaban analizar:

Se puede observar todas las alertas que van llegando:



Conclusión:

Sin duda a la hora de laborar en este ámbito nos hace preguntarnos de todas las exigencias que tendremos, por ejemplo saber que una pagina es lo suficientemente fuerte en el caso si es atacada, no se diga de un banco o de una escuela que puede ser usada para malos fines, sin duda una muy buena practica para entender las vulnerabilidades que a veces ciertas paginas están expuestas, más si es de dominio privado.