OWASP
Open Web Application Security Project

Pruebas de Penetración con Zed Attack Proxy

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético e Informática Forense
reydes@gmail.com -:- www.reydes.com

Miércoles 23 de Noviembre del 2016. Lima, Perú.

Presentación

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPI Linux Essentials Certificate, Brainbench Certified Network Security (Master), Computer Forensics (U.S.) & Linux Administration (General), IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling y Digital Forensics.

Ha sido Instructor en el OWASP LATAM Tour Lima, Perú, y Conferencista en PERUHACK. Cuenta con más de doce años de experiencia en el área y desde hace ocho años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético & Informática Forense. Perteneció por muchos años a los grupos de seguridad RareGaZz y PeruSEC. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Informática Forense, GNU/Linux y Software Libre.

@Alonso_ReYDeS www.facebook.com/alonsoreydes
pe.linkedin.com/in/alonsocaballeroquezada/

ZAP

OWASP
Open Web Application Security Project

OWASP Zed Attack Proxy es una herramienta integrada para realizar pruebas de penetración, la cual permite encontrar vulnerabilidades en las aplicaciones web.

Ha sido diseñada para ser utilizada por personas con diversa experiencia en seguridad, siendo también ideal para desarrolladores y personas quienes realizan pruebas funcionales, y nuevos en temas de pruebas de penetración.

ZAP proporciona escaners automáticos como también un conjunto de herramientas para encontrar de manera manual vulnerabilidades en seguridad.

Entre sus características más resaltantes se enumeran; es open source, multiplataforma, fácil de instalar, completamente libre, fácil de utilizar, incluye completas páginas de ayuda, está traducido a 20 lenguajes, se basa en una comunidad con desarrollo muy activo.

* ZAP: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Características

OWASP
Open Web Application Security Project

- Proxy de Interceptación
- Escaner Automático
- Escaner Pasivo
- Navegación Forzada
- Fuzzer
- Puntos de Interrupción
- Spider
- Add-ons

* https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project#tab=Functionality

Proxy

ZAP es un proxy de interceptación. El cual permite observar todas las solicitudes realizadas hacia la aplicación web y todas las respuestas recibidas desde esta.

Se pueden definir además “Break Points” o puntos de interrupción, los cuales permiten cambiar las solicitudes y respuestas al vuelo.

Break Points (Puntos de Interrupción)

Permiten interceptar una solicitud del navegador y cambiarlo antes de ser enviado hacia la aplicación web en evaluación. También se pueden cambiar las respuestas recibidas desde la aplicación web. La solicitud o respuesta será mostrada en la pestaña “Break”, la cual permite cambiar campos ocultos o deshabilitados, permitiendo evitar o sobrepasar validaciones en el lado del cliente. Esta es una técnica esencial en las pruebas de penetración.

* http://code.google.com/p/zaproxy/wiki/HelpStartConceptsIntercept
* http://code.google.com/p/zaproxy/wiki/HelpStartConceptsBreakpoints

PdP Básica

Explorar

Usar el navegador para explorar todas las funcionalidades proporcionadas por la aplicación web. Seguir los enlaces, presionar todos los botones, además de completar y enviar todos los formularios. Si las aplicaciones soportan varios roles, además se debe hacer esto con cada rol. Para cada rol se debe guardar una sesión diferente de ZAP en un archivo e iniciar una nueva sesión antes de empezar a utilizar el siguiente rol.

Spider

Utilizar una “Araña” para encontrar URLs perdidas u ocultas. También se puede utilizar una “Araña AJAX” para mejorar los resultados y capturar los enlaces construidos de manera dinámica. Y así explorar cualquier enlace encontrado.

* http://code.google.com/p/zaproxy/wiki/HelpPentestPentest

PdP Básica

OWASP
Open Web Application Security Project

Navegación Forzada

Utilizar el escaner de navegación forzada para encontrar nombres de archivos y directorios sin ninguna referencia.

Escaneo Activo

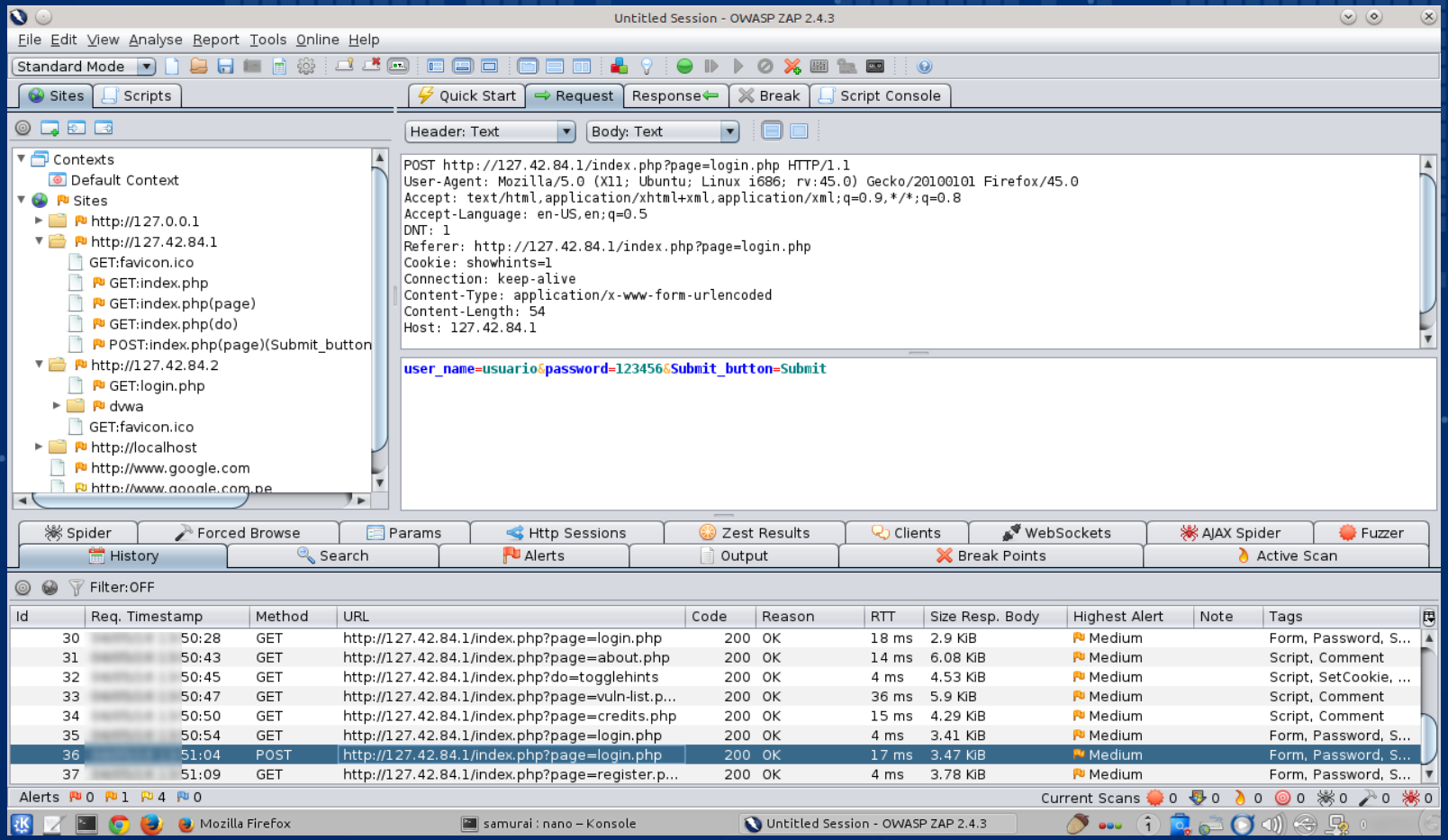
Utilizar el escaner activo para encontrar vulnerabilidades sencillas.

Prueba Manual

Las anteriores pruebas pueden encontrar vulnerabilidades sencillas. Sin embargo, para encontrar más vulnerabilidades se hace necesario evaluar manualmente la aplicación web. Se puede utilizar para este propósito la Guía de Pruebas de OWASP.

* http://code.google.com/p/zaproxy/wiki/HelpPentestPentest
* https://www.owasp.org/index.php/OWASP_Testing_Project

Demostración



+ Información

OWASP
Open Web Application Security Project

Cursos Virtuales en Video

http://www.reydes.com/d/?q=cursos

Videos de Webinars Gratuitos

http://www.reydes.com/d/?q=videos

Mi Blog

http://www.reydes.com/d/?q=blog/1

Mi Sitio web

https://www.reydes.com

OWASP
Open Web Application Security Project

¡Muchas Gracias!

Pruebas de Penetración con Zed Attack Proxy

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético e Informática Forense
reydes@gmail.com -:- www.reydes.com