OWASP Zed Attack Proxy

Webinar Gratuito

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Jueves 5 de Mayo del 2016

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 del año 2014, y Conferencista en PERUHACK 2014. 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 al grupo internacional de Seguridad RareGaZz y al Grupo Peruano de Seguridad 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/

OWASP Zed Attack Proxy

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

Está diseñada para ser utilizada por personas con un amplio espectro de experiencia en seguridad, siendo también ideal para desarrolladores y personas quienes realizan pruebas funcionales y son nuevos en los temas de pruebas de penetración.

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

Entre las características más resaltantes de ZAP se enumeran; es Open Source, Multiplataforma, fácil de instalar, completamente libre, facilidad de uso, páginas ayuda completas, traducido a 20 lenguajes, basado en la comunidad y que está e desarrollo activo.

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

Características de ZAP

- Proxy de Interceptación.
- Escaner Automático
- Escaner Pasivo
- Navegación Forzada
- Fuzzer
- Certificados SSL Dinámicos
- Soporte para “Web Sockets”
- Soporte para un amplio rango de lenguajes de scripting
- Soporte Plug-n-Hack

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

Proxy de Interceptación

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”, los cuales permiten cambiar las solicitudes y respuestas al vuelo.

Break Points

Permiten interceptar una solicitud desde el navegador y cambiarlo antes de ser enviado hacia la aplicación en evaluación. También se pueden cambiar las respuestas recibidas desde la aplicación. 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. La cual 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

Prueba de Penetración 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 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 explorar cualquier enlace encontrado.

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

Prueba de Penetración Básica

Navegación Forzada

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

Escaneo Activo

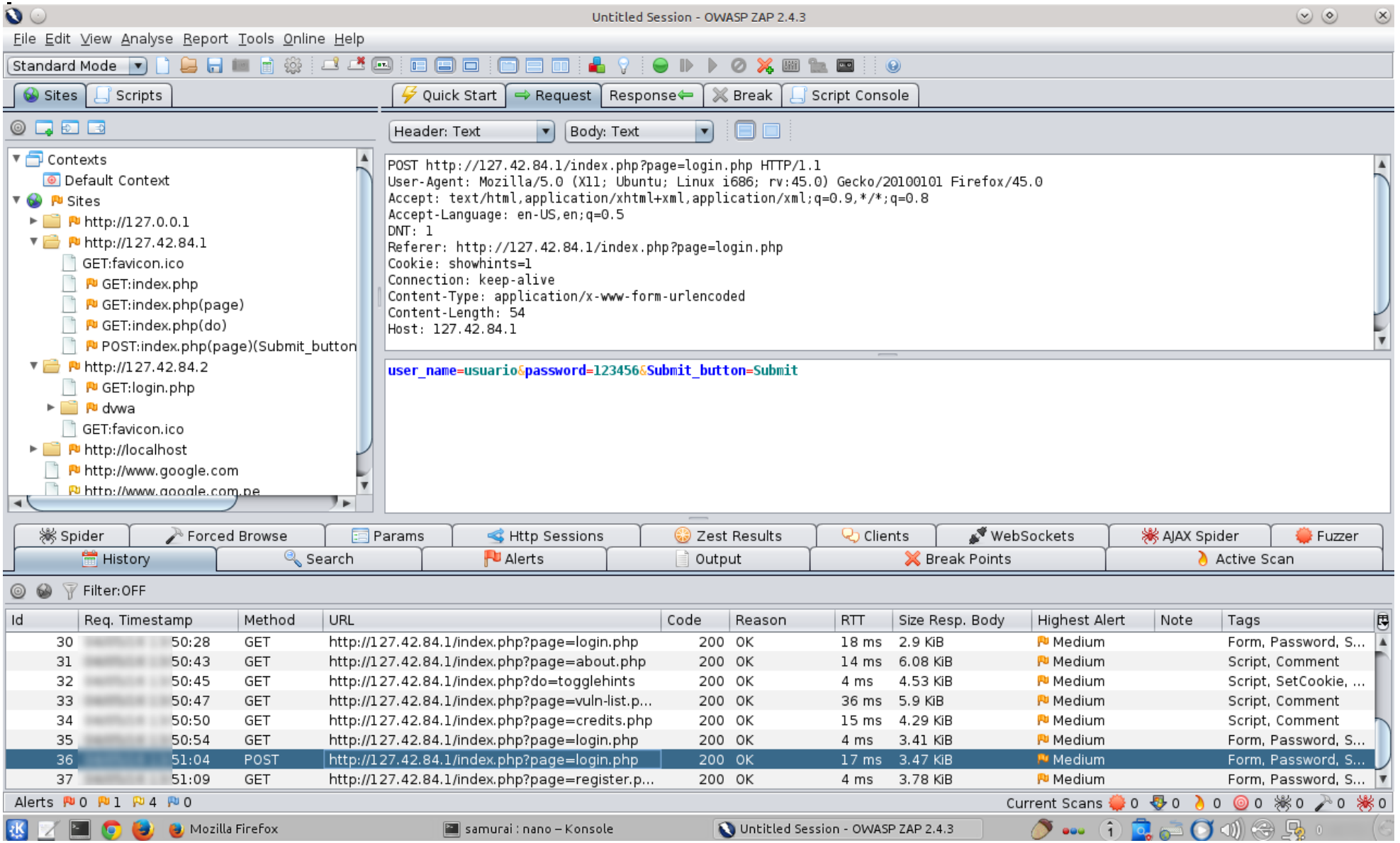
Utilizar el escaner activo para encontrar vulnerabilidades sencillas.

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

Demostraciones



Curso Virtual de Hacking Aplicaciones Web

Curso Virtual de Hacking Aplicaciones Web 2016

Domingos 8, 15, 22 y 29 de Mayo del 2016. De 9:00 am a 12:15 pm (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:

Presentación:

Las aplicaciones web tienen un rol importante en todas las organizaciones modernas. Pero si la organización no evalúa y asegura adecuadamente sus aplicaciones web, los atacantes pueden comprometer estas aplicaciones, dañar la funcionalidad de la empresa, y robar datos. Desafortunadamente, muchas organizaciones operan bajo la errada impresión de la confiabilidad para descubrir fallas en sus sistemas por parte de escaners de seguridad de aplicaciones web. Este curso enseña a los participantes a ir más allá de únicamente presionar un botón para realizar un escaneo, yendo a un nivel profesional para hacer una valiosa prueba de penetración contra aplicaciones web.

Objetivos:

En este curso enseña a los participantes a entender las principales fallas y su explotación, y más importante aún, aprender a realizar un proceso repetible y de prueba real para encontrar de manera consistente estas fallas, para transmitir lo aprendido en sus organizaciones. El participante aprenderá una metodología de evaluación, como configurar y utilizar las herramientas para realizar pruebas de seguridad web satisfactorias. Comprender como se realiza la comunicación entre todas las partes involucradas en una Aplicación Web. Seleccionar y utilizar los diferentes métodos y técnicas para realizar los ataques más relevantes, como por ejemplo SQL Injection (SQLi), Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), entre otros.

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, Digital Forensics y Cybersecurity Management. Ha sido Instructor en el OWASP LATAM Tour Lima, Perú y Conferencista en PERUHACK. Cuenta con más de trece años de experiencia en el área y desde hace nueve años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético & Informática Forense. Perteneció por muchos años al grupo internacional de Seguridad RareGaZz y al Grupo Peruano de Seguridad 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. Su correo electrónico es ReYDeS@gmail.com y su página personal está en: http://www.ReYDeS.com.

Más Información: http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web
E-mail: **caballero.alonso@gmail.com** / Sitio Web: http://www.reydes.com

Cursos Virtuales

Todos los Cursos Virtuales dictados están disponibles en Video.

Curso Virtual de Hacking Ético

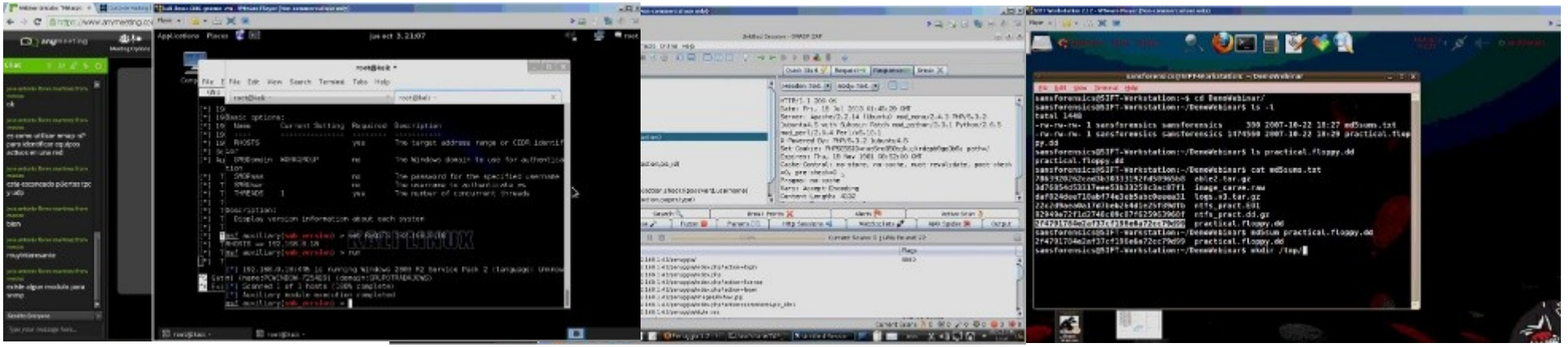
http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web

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

Curso Virtual de Informática Forense

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



Más Contenidos

Videos de 30 Webinars Gratuitos sobre temas de Hacking Ético, Hacking Aplicaciones Web e Informática Forense.

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

Diapositivas utilizadas en los Webinars Gratuitos.

http://www.reydes.com/d/?q=node/3

Artículos y documentos publicados

http://www.reydes.com/d/?q=node/2

Mi Blog sobre temas de mi interés.

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

OWASP Zed Attack Proxy

Webinar Gratuito

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Jueves 5 de Mayo del 2016