Encontrar Vulnerabilidades con Zed Attack Proxy

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

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

e-mail: ReYDeS@gmail.com

Sábado 25 de Abril del 2015

Presentación

Alonso Eduardo Caballero Quezada es 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 Miembro de Open Web Application Security Project (OWASP).

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 e integra actualmente el Grupo Peruano de Seguridad PeruSEC. Ha dictado cursos en Perú y Ecuador, 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/

¿Qué es Zed Attack Proxy?

Zed Attack Proxy (ZAP) es un herramienta integrada para 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 realizando pruebas funcionales y quiens son nuevos en los temas de pruebas de penetración.

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

Entre las características más sobresalientes de ZAP se pueden enumerar, 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

Funcionalidades 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 puede 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 de “Break”, permitiendo cambiar campos ocultos o deshabilitados, permitiendo evitar o sobrepasar validaciones en el lado del cliente. El 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

Una Prueba de Penetración Básica

Explorar:

Usar el navegador para explorar todas las funcionalidades proporcionadas por la aplicación. Seguir los enlaces, presionar todos los botones, llenar y enviar todos los formularios. Si las aplicaciones soportan varios roles, 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 la “Araña” para encontrar URLs perdidos u ocultos. También se puede utilizar la “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

Una Prueba de Penetración Básica (Cont.)

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. 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

Cursos Virtuales

Todos los Cursos Virtuales dictados están disponibles en Video.

Curso Virtual de Hacking Ético

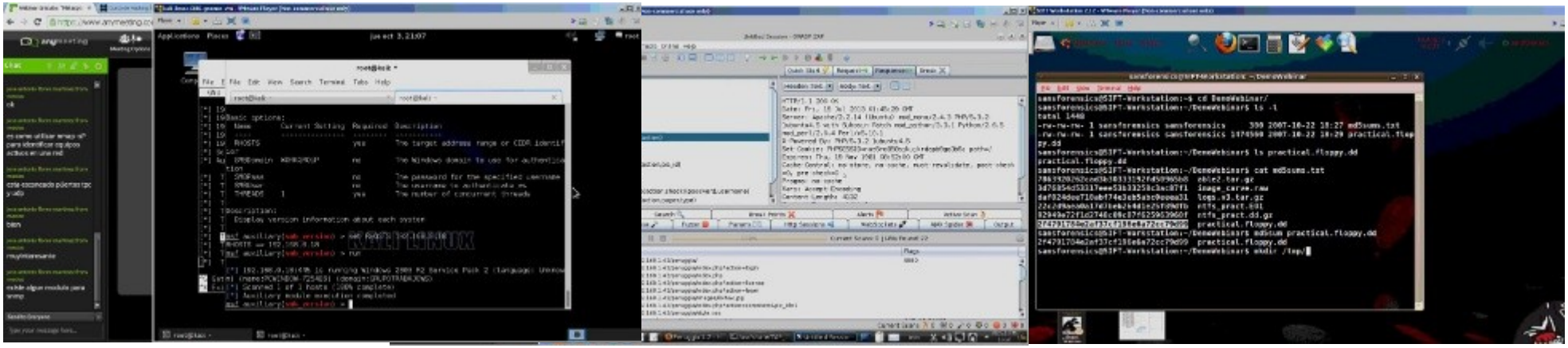
http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

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 25 Webinars Gratuitos sobre Hacking Ético, Hacking Aplicaciones Web e Informática Forense.

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

Diapositivas utilizadas en los Webinars Gratuitos.

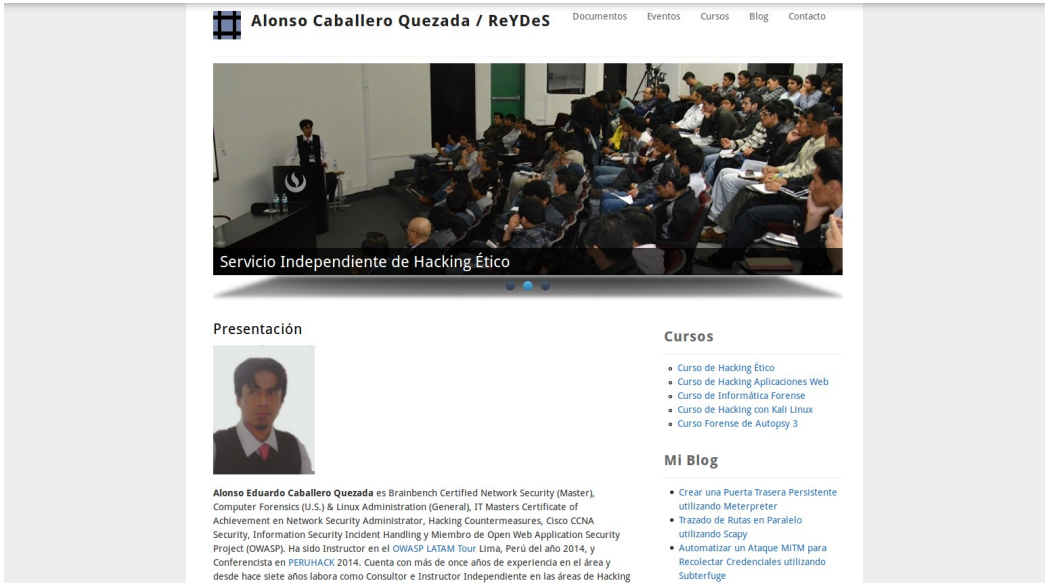
http://www.reydes.com/d/?q=node/3

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



Preguntas, Comentarios, Sugerencias, etc...

.

¡Muchas Gracias!

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

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

e-mail: ReYDeS@gmail.com

Sábado 25 de Abril del 2015