Webinar Gratuito
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

Jueves 24 de Octubre del 2013

¿Quién Soy?

- Consultor e Instructor Independiente en Hacking Ético, Informática Forense y GNU/Linux.
- Ex Integrante de RareGaZz y actual integrante de PeruSEC.
- Ex Redactor en la Revista Linux+ DVD (ES).
- Creador del II Reto Forense Digital Sudamericano - Chavin de Huantar 2012.
- Brainbench Certified Network Security, Brainbench Certified Computer Forensics (U.S.) & Brainbench Certified Linux Administration (General). CNHE, CNCF, CNHAW.
- Más de 11 años de experiencia en el área.
- Twitter: @Alonso_ReYDeS
- LinkedIn: 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 que realizan pruebas funcionales y que 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 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 que se realizan a la aplicación web y todas las respuestas que se reciben 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 que sea enviado a 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” el cual permite 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 y llenar 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 la “Araña” para encontrar URLs que se han perdido o que están ocultas. 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

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

Curso Online de Hacking Aplicaciones Web (Último Curso)

Días:

Sábados 26 de Octubre, 2, 9 y 16 de Noviembre del 2013

Horario:

De 9:00am a 12:30 (UTC -05:00)

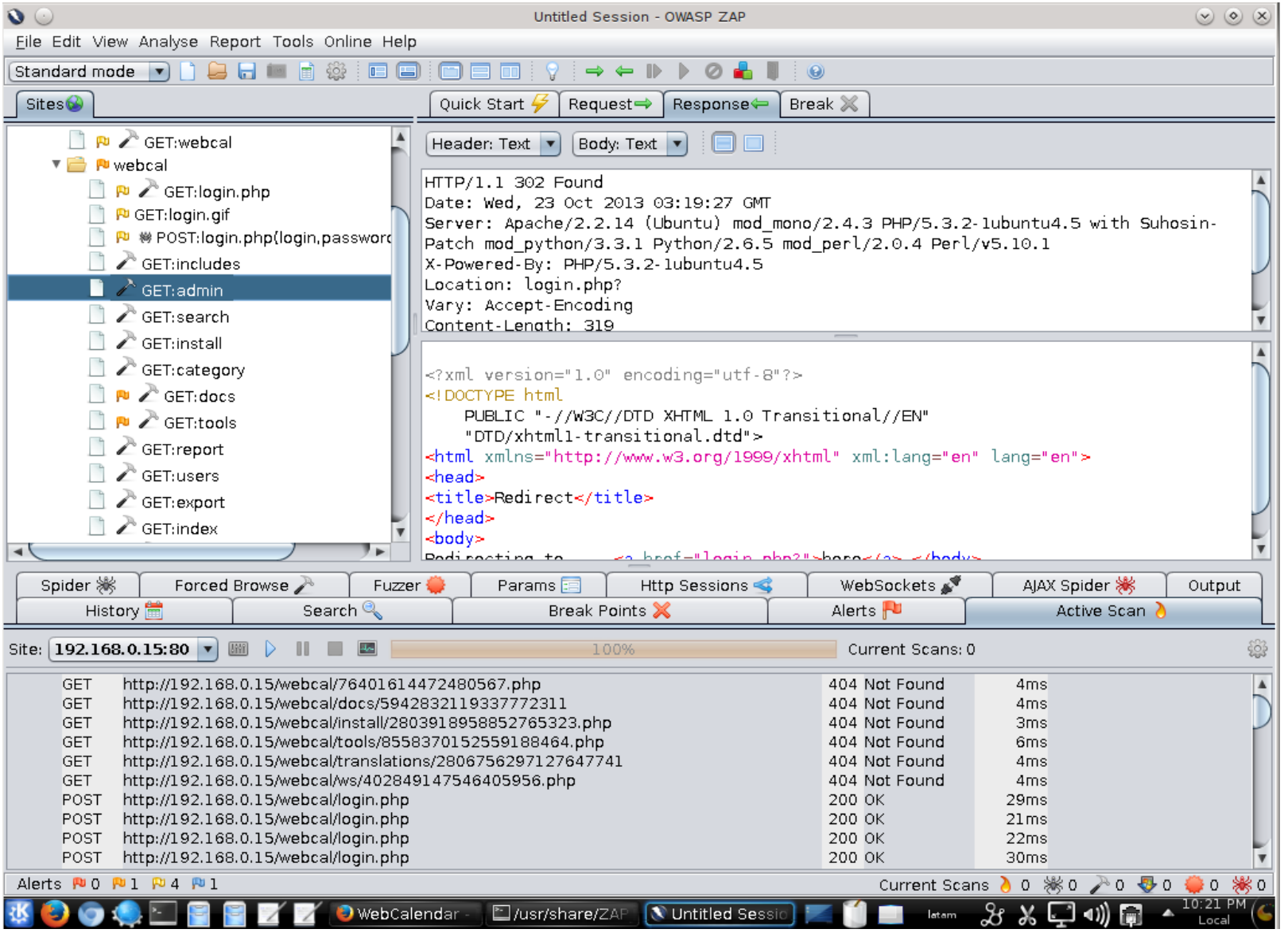
Más Información:

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

Correo electrónico: caballero.alonso@gmail.com
Twitter: https://twitter.com/Alonso_ReYDeS
LinkedIn: http://pe.linkedin.com/in/alonsocaballeroquezada/
Skype: ReYDeS
Sitio Web: http://www.reydes.com

Demos

A continuación se realizarán demostraciones prácticas sobre Zed Attack Proxy (ZAP).



¿Preguntas?



Webinar Gratuito
¡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

Jueves 24 de Octubre del 2013