Webinar Gratuito

Escanear Vulnerabilidades Web con Zed Attack Proxy

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: http://www.ReYDeS.com -:- e-mail: ReYDeS@gmail.com

Jueves 30 de Enero del 2020

Presentación

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator Certified, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures y Pen Testing.

Ha sido instructor y expositor en OWASP Perú, PERUHACK, 8.8 Lucky Perú. Cuenta con más de 17 años de experiencia y desde hace 13 años labora como consultor e instructor independiente en las áreas de Hacking Ético y Forense Digital. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux.

https://twitter.com/Alonso_ReYDeS

https://www.youtube.com/c/AlonsoCaballero

https://www.facebook.com/alonsoreydes/

http://www.reydes.com

https://www.linkedin.com/in/alonsocaballeroquezada/

reydes@gmail.com

Pruebas de Seguridad

Las pruebas de seguridad para el software es el proceso de evaluar y probar un sistema, para descubrir riesgos de seguridad y vulnerabilidades en los sistemas y sus datos. No existe una terminología universal, pero se pueden definir las evaluaciones como el análisis y descubrimiento de vulnerabilidades, sin intentar explotar estas vulnerabilidades. Y se definen las pruebas como el descubrimiento e intento de explotación a estas vulnerabilidades.

Las pruebas de seguridad son algunas veces divididas de alguna manera arbitraría, de acuerdo ya sea el tipo de vulnerabilidad siendo probada, o el tipo de prueba realizada.

- Evaluación de vulnerabilidad
- Prueba de Penetración
- Pruebas en Tiempo de Ejecución
- Revisión de Código

Notar la evaluación de riesgo no está listado.

* https://www.zaproxy.org/getting-started/

Pruebas de Penetración

Un Pentesting es realizado por un profesional simulando a un atacante externo malicioso, con la meta de irrumpir dentro de los sistemas, para robar o realizar algún tipo de negación de servicio.

Tiene la ventaja de ser más preciso porque tiene pocos falsos positivos, pero puede consumir tiempo de ejecución.

También es utilizado para evaluar los mecanismos de defensa, verificar planes de respuesta, y confirmar la adherencia con las políticas de seguridad.

Las pruebas de penetración manuales y automáticas se utilizan juntas para evaluar todo, desde servidores, dispositivos, clientes, etc. Una prueba de penetración generalmente sigue las siguientes etapas:

- Explorar
- Atacar
- Reportar

Zed Attack Proxy

ZAP es un herramienta libre y de fuente abierta para pruebas de penetración, la cual es mantenida bajo el proyecto OWASP. ZAP está específicamente diseñada para pruebas aplicaciones web, siendo flexible y ampliable.

En su núcleo, ZAP es aquello lo cual se conoce como un proxy “Hombre en el Medio”. Se sitúa entre el navegador del profesional en pruebas de penetración y la aplicación web, de tal manera puede interceptar e inspeccionar los mensajes enviados entre el navegador y la aplicación web, modificar el contenido si es necesario, para luego retransmitir los paquetes hacia su destino. Puede ser utilizado como una aplicación autónoma y como un proceso demonio.

ZAP proporciona funcionalidades para un amplio rango de niveles en conocimientos; desde desarrolladores hasta profesionales nuevos en pruebas de seguridad, como también especialistas en el tema.

* https://www.zaproxy.org

Spider

Es utilizado para automáticamente descubrir nuevos recursos (URLs) en un sitio particular. Inicia con una lista de URLs a visitar llamadas semillas, lo cual depende de como el Spider inicia. Luego visita estas URLs, identifica todos los hipervínculos en la página, y luego los añade hacia la lista de URLs a visitar, luego el proceso continúa recursivamente conforme nuevos recursos se encuentren. El Spider puede ser configurado e iniciado utilizando ZAP.

Durante el procesamiento de una URL, el Spider hace una petición para capturar el recurso, luego interpretar la respuesta identificando hipervínculos. Tiene diferentes comportamientos cuando procesa ciertos tipos de respuestas:

- HTML
- Archivos robots.txt
- Formato OData Atom
- Respuesta de texto No HTML
- Respuesta No texto

* https://www.zaproxy.org/docs/desktop/start/features/spider/

Active Scan

Intenta encontrar potenciales vulnerabilidades utilizando ataques conocidos contra los sistemas seleccionados.

El escaneo activo es un ataque a estos sistemas. No debe ser utilizado en aplicaciones web sin autorización.

Para facilitar la identificación del tráfico de ZAP y hacer excepciones en un Firewall de Aplicación Web, ZAP es acompañado por un script “AddZapHeader.js”, el cual puede ser utilizado para añadir una cabecera específica a todo el tráfico pasando a través u originándose desde ZAP.

Resaltar el escaneo activo únicamente puede encontrar ciertos tipos de vulnerabilidades. Las vulnerabilidades lógicas, como control de acceso inadecuado, no serán encontrados por ningún escaneo activo o de vulnerabilidades automática.

Una prueba de penetración manual debe ser siempre realizada además del escaneo activo para encontrar todos los tipos de vulnerabilidades.

* https://www.zaproxy.org/docs/desktop/start/features/ascan/

Cross Site Scripting

XSS es una técnica de ataque, la cual involucra hacer un eco del código proporcionado por el atacante dentro de un instancia del navegador del usuario. Una instancia del navegador puede ser un cliente estándar de navegación web, o un objeto navegador incorporado en un producto de software, como un navegador dentro de WinAmp, un lector RSS, o un cliente de correo electrónico. El código usualmente está escrito en HTML/JavaScript, pero puede también extenderse hacia VBScript, ActiveX, Java, Flash, o cualquier otra tecnología soportando navegación.

Cuando un atacante captura el navegador del usuario para ejecutar su código, el código se ejecutará dentro del contexto de seguridad (o zona) del sitio web anfitrión. Con este nivel de privilegio, el código tiene la capacidad de leer, modificar, y transmitir cualquier dato sensible accedible por el navegador. Con esto se puede secuestrar la cuenta de un usuario (robar cookies), redirigir el navegador hacia otra ubicación, o posiblemente mostrar contenido fraudulento entregado por un sitio web siendo visitado.

* https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A7-Cross-Site_Scripting_(XSS).html

Cross Site Scripting (Cont.)

Los ataques de XSS esencialmente comprometen las relaciones de confianza entre el usuario y el sitio web. Las aplicaciones utilizando instancias de un objeto navegador, el cual carga contenido desde el sistema de archivos, puede ejecutar código bajo la zona de la máquina local, permitiendo el compromiso del sistema.

Existen tres tipos de ataques de XSS:

- XSS No persistente (Reflejado)
- XSS Persistente (Almacenado)
- XSS basado en DOM

* https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

Inclusión Remota de Archivos

La inclusión remota de archivos (RFI) es una técnica de ataque utilizada para “explotar” mecanismos para la “inclusión dinámica de archivos”, en las aplicaciones web.

Cuando las aplicaciones web toman una entrada del usuario (URL, valor de parámetro, etc.) y los pasa dentro de comandos para incluir archivos, la aplicación web podría ser engañada para incluir archivos remotos con código malicioso.

* https://wiki.owasp.org/index.php/Testing_for_Local_File_Inclusion

Inyección SQL

Un ataque de inyección SQL consiste en la inserción o “inyección” de una consulta SQL mediante una entrada de datos desde el cliente hacia la aplicación.

Una explotación exitosa de inyección SQL puede leer datos sensibles desde la base de datos, modificar los datos de la base de datos (Insertar, actualizar, borrar), ejecutar operaciones de administración sobre la base de datos (como apagar el DBMS), recuperar contenido de un archivo presente en el sistema de archivos del DBMS, y en algunos casos entregar comandos hacia el sistema operativo.

Los ataques de inyección SQL son un tipo de ataque de inyección, en el cual comandos SQL son inyectados dentro de una entrada de datos planos, para efectuar la ejecución de comandos SQL previamente definidos.

* https://owasp.org/www-community/attacks/SQL_Injection

Curso

Curso Virtual Hacking Aplicaciones Web 2020

Domingos 2, 9, 16 y 23 de Febrero del 2020. 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 maliciosos pueden comprometer estas aplicaciones, dañar la funcionalidad de la empresa, y robar datos. Desafortunadamente muchas organizaciones operan bajo la errada percepción, de confiar el descubrimiento de las fallas en sus sistemas a escáneres automáticos de seguridad en aplicaciones web. No existe un parche o solución total para las aplicaciones web personalizadas, por lo tanto los atacantes maliciosos se orientan cada vez más en estos objetivos de alto valor.

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics y Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures y

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

e-mail: reydes@gmail.com Sitio web: http://www.reydes.com

Demostraciones

Activities Applications Places OWASP ZAP

Hackazon - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Hackazon

HACKAZON

All Search products...

A staple of Thai, Indian and Caribbean cuisines, Native...

$30

Etester

about Crest 3D White Luxe Whitestrips Supreme FlexFit-Teeth Whitening Kit 14 treatments

good value...no problems with the phone. Works well with the service. More

Best Choice

Untitled Session - OWASP ZAP 2.8.1

File Edit View Analyse Report Tools Import Online Help

Standard Mode

Sites Scripts

Quick Start Request Response Break Script Console

Header: Text Body: Text

http://www.hackazon.info
- css
- font-awesome
- fonts
- images
  - GET:Hackazon.png
- js
- products_pictures
  - GET:Bed_Head_Men_Bed_Head_
  - GET:Black_Decker_PPRH5B_Profe

```
HTTP/1.1 200 OK
Date: Mon, 20 Jan 2020 11:01:50 GMT
Server: Apache/2.4.18 (Ubuntu)
Set-Cookie: PHPSESSID=feqi910s4cg206phsoru59qg61; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 65501
```

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <title>Hackazon </title>

    <meta name="viewport" content="width=device-width, initial-scale=1.0">
```

Zest Results | Clients | WebSockets | AJAX Spider | Callbacks | Fuzzer | Token Gen | Output

History | Search | Break Points | Alerts | Active Scan | Spider | Forced Browse | Params | HTTP Sessions

Filter: OFF Export

Id	Req. Timestamp	Met...	URL	Co...	Reason	...	Size Resp. ...	Highest ...	N...	Tags
48	1/20/20, 11:02:...	GET	http://www.hackazon.info/js/amf/ser...	200	OK	...	827 bytes	Low		Comment
47	1/20/20, 11:02:...	GET	http://www.hackazon.info/js/site.js	200	OK	...	17,020 bytes	Low		Hidden, Com...
46	1/20/20, 11:02:...	GET	http://www.hackazon.info/js/swfobje...	200	OK	...	26,351 bytes	Low		Object, Com...
66	1/20/20, 11:02:...	GET	http://www.hackazon.info/fonts/glyp...	200	OK	...	23,292 bytes	Low		
68	1/20/20, 11:02:...	GET	http://www.hackazon.info/font-awes...	200	OK	...	83,760 bytes	Low		

Alerts 0 1 5 2 Current Scans 0 0 0 0 0 0 0 0 0

Cursos Virtuales 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

Curso Virtual Hacking con Kali Linux
http://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

Curso Virtual OSINT - Open Source Intelligence
http://www.reydes.com/d/?q=Curso_de_OSINT

Curso Virtual Forense de Redes
http://www.reydes.com/d/?q=Curso_Forense_de_Redes

Y todos los cursos virtuales:

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

Más Contenidos

Videos de 52 webinars gratuitos

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

Diapositivas de los webinars gratuitos

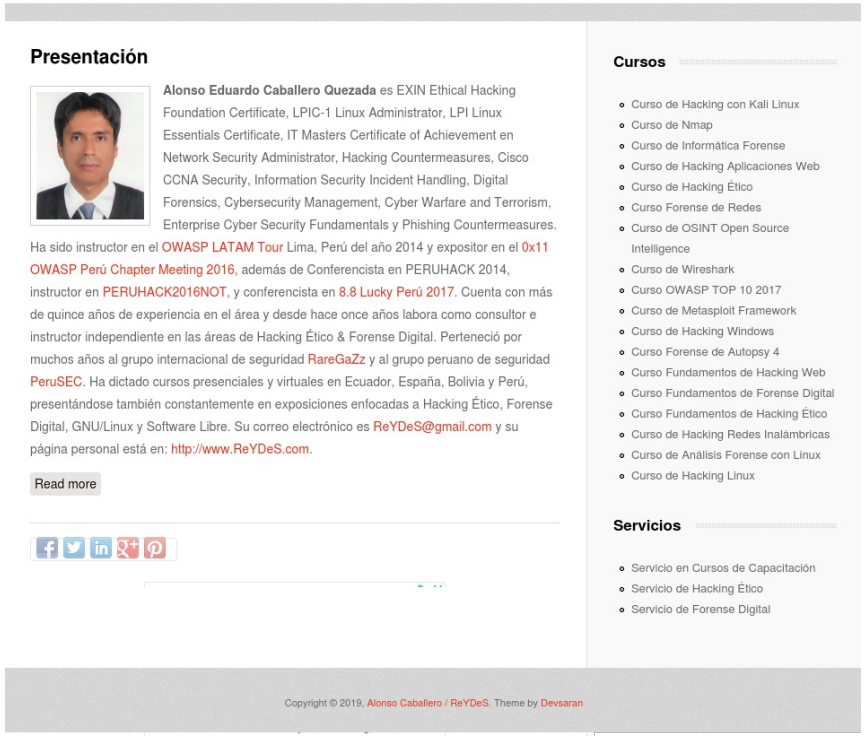
http://www.reydes.com/d/?q=node/3

Artículos y documentos publicados

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

Blog sobre temas de mi interés.

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



Presentación

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals y Phishing Countermeasures. Ha sido instructor en el OWASP LATAM Tour Lima, Perú del año 2014 y expositor en el 0x11 OWASP Perú Chapter Meeting 2016, además de Conferencista en PERUHACK 2014, instructor en PERUHACK2016NOT, y conferencista en 8.8 Lucky Perú 2017. Cuenta con más de quince años de experiencia en el área y desde hace once años labora como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. 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, Forense Digital, GNU/Linux y Software Libre. Su correo electrónico es ReYDeS@gmail.com y su página personal está en: http://www.ReYDeS.com.

Read more

Cursos

- Curso de Hacking con Kali Linux
- Curso de Nmap
- Curso de Informática Forense
- Curso de Hacking Aplicaciones Web
- Curso de Hacking Ético
- Curso Forense de Redes
- Curso de OSINT Open Source Intelligence
- Curso de Wireshark
- Curso OWASP TOP 10 2017
- Curso de Metasploit Framework
- Curso de Hacking Windows
- Curso Forense de Autopsy 4
- Curso Fundamentos de Hacking Web
- Curso Fundamentos de Forense Digital
- Curso Fundamentos de Hacking Ético
- Curso de Hacking Redes Inalámbricas
- Curso de Análisis Forense con Linux
- Curso de Hacking Linux

Servicios

- Servicio en Cursos de Capacitación
- Servicio de Hacking Ético
- Servicio de Forense Digital

Copyright © 2019, Alonso Caballero / ReYDeS. Theme by Devsaran

Webinar Gratuito

Escanear Vulnerabilidades Web con Zed Attack Proxy

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: http://www.ReYDeS.com -:- e-mail: ReYDeS@gmail.com

Jueves 30 de Enero del 2020