MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Webinar Gratuito
Hacking Aplicaciones Web

Alonso Eduardo Caballero Quezada

Consultor e Instructor en Hacking Ético y Forense Digital

e-mail: ReYDeS@gmail.com

Marzo 2018

Presentación

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

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 y Cyber Warfare and Terrorism..

Ha sido instructor y expositor en OWASP Perú Chapter, instructor y expositor en PERUHACK, además de expositor en 8.8 Lucky Perú. Cuenta con más de catorce años de experiencia y desde hace diez 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

http://www.reydes.com

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

reydes@gmail.com

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

Agenda

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

- ¿Porqué la Web?
- Las Pruebas contra Aplicaciones Web Frecuentemente son Limitadas
- Funcionalidad con la Web 2.0
- Aplicaciones en la Nube
- Entender la Web
- Metodología para una Prueba de Penetración contra Aplicaciones Web
- Conocer las Herramientas
- Permiso para las Pruebas
- Guía para Pruebas de OWASP
- Herramientas para Pruebas de Penetración
- Escaners de Seguridad para Aplicaciones Web
- Navegadores Web
- Proxys para Interceptación

¿Porqué la Web?

Nuestras vidas diarias utilizan aplicaciones web. Originalmente la web tuvo bases estáticas. Muchos de los sitios web actuales crecen significativamente en cuanto a su complejidad.

- Funcionalidad crítica de la empresa disponible para los empleados y posiblemente al público mediante portales en Internet.
- Suites de oficias completamente funcionales se ofrecen mediante navegadores web.
- Administración basada en web de aplicaciones críticas para la empresa, e incluso infraestructuras de seguridad.

Existe actualmente una mayor superficie de ataque.

- Más complejidad para los atacantes puedan manipular.
- Mayor ganancia para los atacantes buscando realizar fraude, obtener dinero, o causar daño.

Las Pruebas contra Aplicaciones Web Frecuentemente son Limitadas

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Muchas empresas evalúan únicamente la funcionalidad de las aplicaciones desplegadas hacia la web.

- Raramente es evaluada la seguridad.
- Esto se torna obvio cuando se examinan los reportes diarios sobre vulnerabilidades en listas de correo.
- Common Vulnerabilites and Exposures (CVE), incluye un gran número de vulnerabilidades. (La mayoría de los reportes se enfocan en aplicaciones web).
- Las aplicaciones web están muy bien representados también en Exploit Database.

* https://cve.mitre.org/
* https://www.exploit-db.com/

Funcionalidad con la Web 2.0

Los sitios web hacen más a lo aquello percibido por nosotros.

- Las peticiones HTTP se hacen sin la interacción del usuario.
- Mash-ups combinan diversas aplicaciones.

AJAX y otras tecnologías permiten al sitio web realizar peticiones por nosotros.

Se debe entrenar a los usuarios a esperar este tipo de comportamiento desde los clientes web.

Un ejemplo de esto es Google Maps.

* https://www.google.com/maps
* https://en.wikipedia.org/wiki/Mashup_(web_application_hybrid)

Aplicaciones en la Nube

- La computación en la Nube se ha expandido notablemente.

  Recursos bajo demanda se están convirtiendo en algo común.

- Evaluar estas aplicaciones no es diferente.

  Estos tienden a enfocarse sobre la funcionalidad.

- La responsabilidad y restricciones detienen muchos procesos para pruebas de seguridad.

  ¿Se está permitido de realizarlo?

- Los proveedores titubean para permitir pruebas.

  O esto debe ser asumido.

Entender la Web

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Para realizar pruebas de penetración exitosas contra aplicaciones web, se necesita un profundo conocimiento sobre las tecnologías web.

Los profesionales en pruebas de penetración tienen una perspectiva diferente al de los usuarios normales.

- Se debe pensar maliciosamente, pero actuar profesionalmente
- ¿Cómo se pueden evadir las restricciones?
- ¿Cuales errores cometieron los desarrolladores, administradores, y operadores de los sistemas objetivo?

Frecuentemente una mentalidad diferente a la de los desarrolladores y administradores.

- Enfocarse en evadir los controles de las aplicaciones.
- Encontrar problemas en la lógica de la empresa.

Metodología para una Prueba de Penetración contra Aplicaciones Web

Debido a nuestras consideraciones y perspectivas pueden fallar durante una prueba de penetración, se requiere utilizar una metodología.

Una metodología debe ser:

- **Probada.**
  Hacer un seguimiento de su utilización.

- **Repetible.**
  Los desarrolladores (y otros evaluadores) puede reproducir los resultados.

- **Explicable.**
  Se debe expresar los problemas descubiertos y los arreglos de una manera comprensible.

Conocer las Herramientas

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Entender cuales herramientas están disponibles, y como estas se integran dentro una régimen completo de pruebas.

Obtener profundos conocimientos sobre la utilización de cada herramienta.

- Conocer sus fortalezas y debilidades.
- Entender fallas comunes y tácticas para evitarlos.
- Determinar como el conocimiento capturado desde una herramienta puede ser alimentado dentro de otra, en una prueba integrada.

Como ampliar y mejorar las herramientas.

- Como mínimo, desarrollar scripts para automatización.
- Desarrollar partes para mejorar las herramientas existentes.
- Identificas diferencias y crear nuevas herramientas. Existe mucho por innovar en las herramientas para pruebas contra aplicaciones web.

Permiso para las Pruebas

Obtener el permiso del personal relacionado con el objetivo de evaluación, es absolutamente vital.

- No será muy agradable terminar con una acusación legal, o peor aún, enfrentar una sentencia para ir a prisión.

  Obtener un memo escrito firmado por alguien con autoridad.

- En la parte final está un ejemplo.

  El permiso debe estar por escrito, y esta debe estar firmada.

- No se debe confiar en meros acuerdos verbales o simples mensajes de correo electrónico. Pues luego se podría estar en problemas.

* http://www.counterhack.net/permission_memo.html

Guía para Pruebas de OWASP

La guía para pruebas de OWASP, puede servir como una lista de verificación o pruebas de sanidad para procesos de pruebas de penetración contra aplicaciones web.

Una prueba de penetración contra aplicaciones web, no necesariamente se adhiere perfectamente con la guía para pruebas de OWASP, pero este ayuda a determinar pruebas relevantes mientras se realizan las diversas evaluaciones.

- Es una simple identificador para permitir ver información adicional sobre las fallas.

Lo más importante, las pruebas proporcionan un punto para la investigación sobre como la organización vulnerable puede empezar a remediar sus fallas.

* https://www.owasp.org/index.php/OWASP_Testing_Project

Herramientas para Pruebas de Penetración

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Se debe planificar cuidadosamente la construcción de un conjunto de herramientas para realizar pruebas de penetración contra aplicaciones web.

Algunas consideraciones clave son:

- Plataforma para el ataque
- Escaners de seguridad automáticos para aplicaciones web
- Navegadores web
- Proxys para interceptación

* https://www.owasp.org/index.php/Appendix_A:_Testing_Tools

Escaners de Seguridad a Aplicaciones Web

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Los escaners de vulnerabilidades altamente automatizados son una bendición para los profesionales en pruebas de penetración.

Estos típicamente tienen la capacidad de escanear rápidamente un vasto número de aplicaciones web de gran magnitud.

Su alta automatización y capacidad rápida para el escaneo, son un gran activo, pero también una gran debilidad. (La velocidad frecuentemente tiene el costo de la profundidad).

Necesariamente se emplea un escaner de seguridad para aplicaciones web, pero no es la única herramienta la cual se necesita utilizar. (Burp Suite Pro, ZAP, Acunetix, Qualys, etc).

¿Cual es el mejor?. Se aprecia la automatización, pero frecuentemente falla en encontrar problemas más sutiles. Se debe determinar cual es el mejor, basándose en las aplicaciones web de la empresa.

Navegadores Web

No es una obligación, pero se podrían realizar muchos aspectos de una prueba de penetración contra una aplicación web, utilizando un navegador web.

No se intenta iniciar una guerra entre los navegadores web, pero el navegador necesita considerar.

- No se debe basar el navegador por vanidad o por referencia de alguien.
- La selección y configuración del navegador web, podría tener implicaciones en la prueba.

Algunas consideraciones

- Se necesita un navegador el cual no impacte en las pruebas de seguridad a realizar (en particular XSS).
- Ampliar las capacidades de un navegador mediante extensiones y add-ons podría también ser ventajoso.

Proxys para Interceptación

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Sobre un lado del espectro se tienen a los escaners automáticos, y sobre el otro lado se tienen a los navegadores web.

Los proxys para interceptación son la última pieza en el conjunto de herramientas, los cuales proporcionan un punto intermedio entre lo completamente automático y abiertamente manual.

El proxy para interceptación ocupa un rol primordial en el arsenal del profesional en pruebas de penetración.

Zed Attack Proxy y Burp Suite son dos muy buenas elecciones, y son herramientas fundamentales para realizar diversas evaluaciones.

* https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
* https://portswigger.net/burp/

Más Información

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Sitio Web

http://www.mile-sec.com

Correo Electrónico

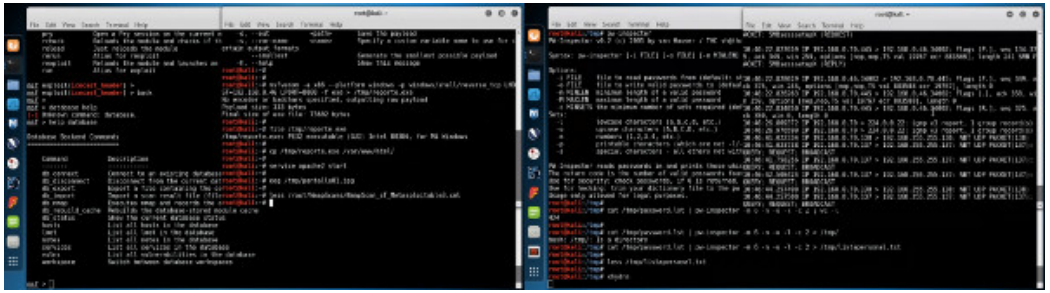
informes@mile-sec.com

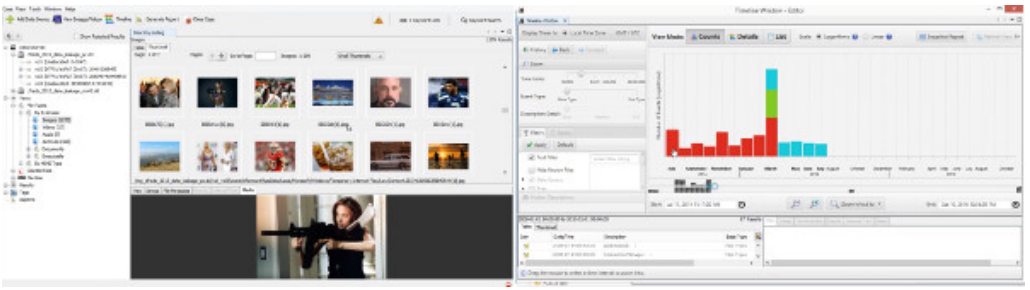
Redes Sociales

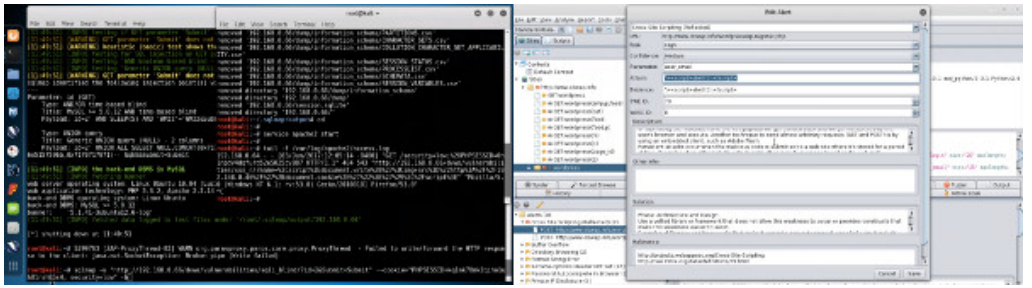
https://www.facebook.com/mileseceirl

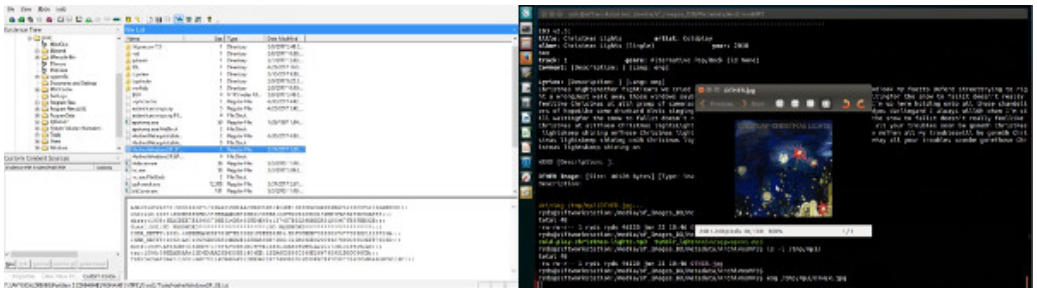
https://twitter.com/mileseceirl

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









¡Muchas Gracias!

Webinar Gratuito
Hacking Aplicaciones Web

Alonso Eduardo Caballero Quezada

Consultor e Instructor en Hacking Ético y Forense Digital

e-mail: ReYDeS@gmail.com

Marzo 2018