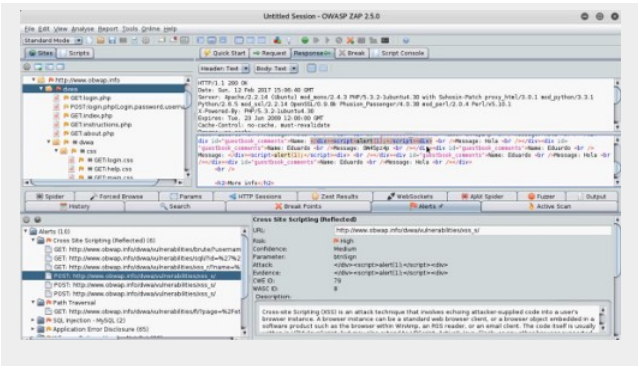
Fundamentos de Hacking Web

Curso Virtual - 2017



Último Curso del Año 2017

Fechas

Sábados 23, 30 de Set, 7 y 14 de Oct del 2017

Horario:

De 9:00 am a 12:15 pm (UTC -05:00)

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

1. Presentación

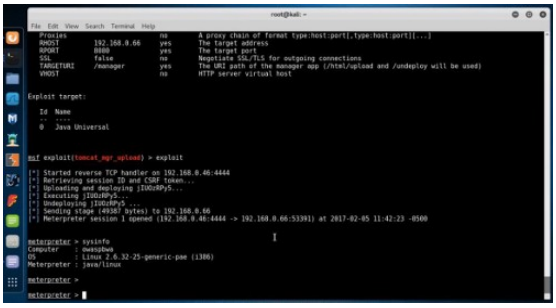
La mayoría de usuarios confían en las aplicaciones web para realizar diversas tareas diarias, ya sea en el trabajo, en casa, o para jugar; siendo posible accederlas muchas veces al día desde laptops, computadoras, tablets, teléfonos y otros dispositivos. Estas aplicaciones web se utilizan para realizar compras, transacciones bancarias, pagos de cuentas, interactuar con redes sociales y otros propósitos. El problema con las aplicaciones web es no ser tan seguras como se piensa, y la mayoría de las veces los ataques utilizados para ganar acceso son relativamente sencillos y simples. De hecho cualquiera puede utilizar herramientas de hacking para realizar ataques devastadores.

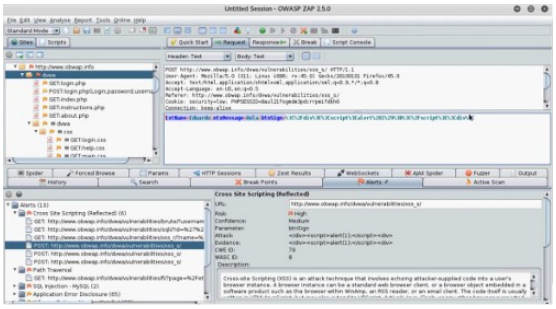
2. Objetivos

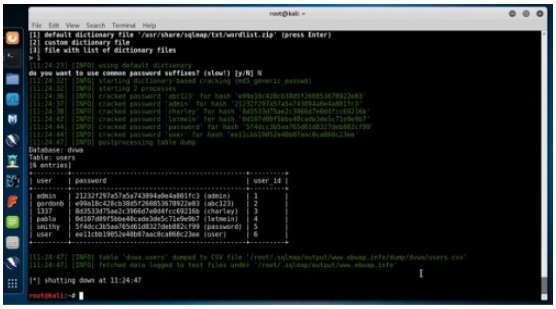
Este curso enseña a los participantes como realizar evaluaciones contra aplicaciones web, de tal manera se pueda también prevenir los ataques. Se abarca la teoría, herramientas y tecnologías utilizadas para identificar y explotar las vulnerabilidades web más dañinas actualmente presentes en las aplicaciones web. Esto significa tener la capacidad de obtener información sensible desde una base de datos, evadir una página de login, o suplantar usuarios. Se aprenderá sobre la selección del objetivo, como realizar los ataques, cuales herramientas son necesarias y como utilizarlas.

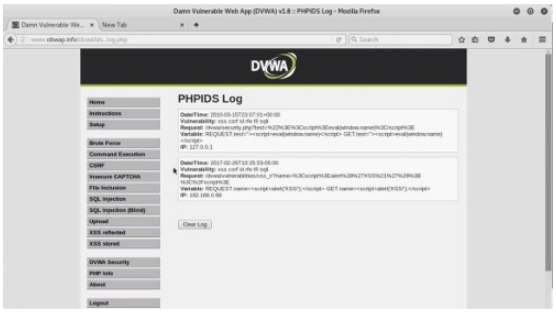
3. Temario

- Fundamentos del Hacking Web
- ¿Qué es una Aplicación Web?
- Servidores Web y HTTP
- Metodologías Existentes
- Vulnerabilidades Web Comunes
- Hacking a Servidores Web
- Reconocimiento
- Escaneo de Puertos y Escaneo de Vulnerabilidades
- Explotación
- Mantener el Acceso
- Reconocimiento y Escaneo de la Aplicación Web
- Explotación con Inyección
- Vulnerabilidades y Ataques de Inyección SQL
- Vulnerabilidades y Ataques de Inyección de Comandos
- Shells Web
- Autenticación Inadecuada y Recorrido de Ruta
- Vulnerabilidades de Autenticación y Sesión
- Vulnerabilidades de Recorrido de Ruta
- Ataques por Fuerza Bruta contra la Autenticación
- Ataques de Sesión
- Ataques de Recorrido de Ruta
- Hacking a Usuarios Web
- Vulnerabilidades Cross Site Scripting
- Vulnerabilidades Cross Site Request Forgery
- Vulnerabilidades Técnicas de Ingeniería Social
- Reconocimiento, Escaneo y Explotación del Usuario Web
- Ataques XSS Reflejados y Almacenados
- Ataques CSRF
- Framework de Ataque
- Medidas Correctivas
- Arreglos en el Servidor Web
- Arreglos en la Aplicación Web
- Arreglos para el Usuario Web









4. Material

Todos los participantes al Curso Virtual Fundamentos de Hacking Web tendrán la posibilidad de descargar los videos de cada sesión, un día después de impartida la misma.

Adicionalmente el participante tiene la opción de adquirir por S/. 75 Soles adicionales, 2 (dos) DVD conteniendo el material y las máquinas virtuales utilizadas durante el desarrollo del curso. Este costo incluye los gastos de envío a cualquier lugar del Perú.

En caso el participante no adquiera los DVDs, se le sugiere descargar y configurar las siguientes máquinas virtuales.

- **Kali Linux 2.0**
  Enlace de Descarga (32 bit VM PAE)
  https://images.offensive-security.com/virtual-images/Kali-Linux-2016.2-vm-i686.7z

- **OWASP Broken Web Applications Project**
  Enlace de Descarga:
  https://sourceforge.net/projects/owaspbwa/files/1.2/OWASP_Broken_Web_Apps_VM_1.2.7z/download

5. Fechas y Horarios

El Curso Virtual Fundamentos de Hacking Web tiene una duración total de doce (12) horas, las cuales se dividen en cuatro (4) sesiones de tres (3) horas cada una.

- **Fechas:**
  Sábados 23, 30 de Setiembre, 7 y 14 de Octubre del 2017

- **Horario:**
  De 9:00 am a 12:15 pm (UTC -05:00). 12 Horas en total.

[*] El Curso se dicta sin ningún requisito mínimo en el número de participantes.

6. Inversión y Forma de Pago

El Curso Virtual de Fundamentos de Hacking Web tiene un costo de:

S/. 330 Soles o $ 100 Dólares

El pago del curso se realiza mediante alguno de los siguientes mecanismos:

Residentes en Perú	Residentes en Otros Países
Deposito Bancario en la siguiente cuenta: Scotiabank ScotiaBank Cuenta de Ahorros en Soles: 324-0003164 A nombre de: Alonso Eduardo Caballero Quezada	Transferencia de dinero mediante alguna de las siguientes empresas: Western Union: http://www.westernunion.com WESTERN UNION WU moving money for better

También puede realizar el depósito en un Agente Scotiabank. Encuentre el más cercano utilizando la siguiente página: http://intl.scotiabank.com/es-pe/locator/Default.aspx Una vez realizado el depósito, enviar por favor el voucher escaneado o sencillamente detallar los datos al siguiente correo: **caballero.alonso@gmail.com**	MoneyGram: https://www.moneygram.com Escribame por favor un mensaje de correo electrónico para detallarle los datos necesarios para realizar la transferencia. Una vez realizada la transferencia, enviar por favor el documento escaneado al siguiente correo: **caballero.alonso@gmail.com**

Confirmado el depósito o la transferencia se le enviará al correo electrónico del participante los datos necesarios para conectarse al sistema, además del material utilizado durante el desarrollo del curso.

El curso se realiza utilizando el sistema de video conferencias Anymeeting. El cual proporciona la transmisión de audio y video en tiempo real de alta calidad, tanto para el instructor como también para los participantes, entre otras características ideales para impartir cursos de manera virtual.

http://www.anymeeting.com

7. Más Información

Si requiere más información sobre el Curso Virtual Fundamentos de Hacking Web, tiene a su disposición los siguientes mecanismos de contacto:

- **Correo electrónico:** caballero.alonso@gmail.com
- **Vía Web:** http://www.reydes.com/d/?q=contact
- **Teléfono:** (+51) 949304030

8. Instructor

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. 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.