Hacking Web

La cantidad de aplicaciones web crece de manera considerable cada día, diversos tipos de tecnologías son utilizados para un desarrollo ágil y de esta manera poder optimizar los tiempos del desarrollador, sin embargo, ¿Cuántas de estas aplicaciones web pasan por un proceso de revisión de Seguridad?

Si bien es cierto, en el mercado existen diversas herramientas automatizadas para la búsqueda, detección y análisis de vulnerabilidades en aplicaciones webs, sin embargo, lo más importante en el proceso de Hacking Web son las pruebas manuales, ya que son éstas las que le dan un valor agregado al servicio.

En este curso se aprenderá a detectar vulnerabilidades en entornos webs de manera manual. Donde alumno podrá tener la capacidad de detectar y comprender diversas vulnerabilidades y de esta manera poder descartar falsos positivos.

Introducción a las tecnologías de Aplicaciones Web

- Introducción a las tecnologías en aplicaciones web
- Arquitecturas en Aplicaciones Web
- Tipos de auditoría Web
- OSINT en Aplicaciones Web
- Reconocimiento Pasivo de Aplicaciones Web

Detección de Vulnerabilidades del lado del cliente

- Reconocimiento Activo de Aplicaciones Web
- Addons en Firefox para Escaneo Manual de Vulnerabilidades
- Ataques del Lado del cliente.
- Cross Site Scripting
  - o Reflected XSS
  - o Comprendiendo el impacto de la vulnerabilidad
  - o Diversas técnicas de detección y explotación
  - o Client Side Template Injection
  - o Stored XSS
  - o Dom XSS
- Cross Site Request Forgery
  - o Desarrollo manual de exploit para explotar un CSRF.

Equipamiento de Nuestro Laboratorio

- DELL INSPIRON 14-3467 i5-7200U 14" 8GB

Escaneo manual con BurpSuite

- Introducción a Burp Suite
- Evaluación de vulnerabilidades mediante Burp Suite
- Sql Injection
  - o Error Based
  - o Union Based
  - o Boolean Based
  - o Time Based
- Integrando Sqlmap con Burp Suite
- Técnicas para explotar un RCE
  - o Local File Inclusion
  - o Remote File Inclusion
  - o Server Side Template Injection
  - o PhP CGI Argument Injection
  - o Apache Struts 2
  - o Diversas técnicas para Bypasear un Uploader
  - o Plugins Vulnerables en WordPress

Lógica de la Aplicación y Web Services

- Referencia Directa Insegura a Objetos Vulnerabilidades de Autenticación
  - o Bypass Login con Sql Injection
  - o Técnicas de Brute Force (Basado en Longitud de Request, Código HTTP, Expresión regular)
- Vulnerabilidades en Web Services
  - o Xml External Entity
  - o SQL Injection en Web Services
  - o Server Side Request Forgery /XSPA

Lógica del Pentester Web

- Pensando como Pentester Web. ¿Qué y como explotar?
- Análisis Dinámico en Aplicaciones Móviles con Burp Suite
- Capture The Flag

Información General:

- **Lugar:** Apoquindo 4775, oficina 302, Las Condes, Santiago
- **Horas:** 40 hrs
- **Valor:** 20 UF

Medio de Pago
Depósito o Transferencia

Cybertrust SPA
Rut: 76.536.515-5
Cta. Cte.70156520
Banco Santander
Email: contacto@cybertrust.cl

cybertrust
INSPIRANDO CONFIANZA

www.cybertrust.cl

Teléfono: +562 3224 3551 | +562 3224 3552 Email: contacto@cybertrust.cl

Experiencia

Ingeniero Civil en Computación e informática con más de 4 años de experiencia en Seguridad Ofensiva, principal fundador de una de las comunidades más grandes de seguridad informática de Chile. "Seguridad Informática Chile" con más de 8.000 miembros activos.

Posee amplia experiencia encontrando fallos de seguridad de empresas internacionales y esta en el muro de la fama de varias compañías incluyendo:

Oracle http://bit.ly/2ffWd1N

Google https://bughunter.withgoogle.com/characterlist/15

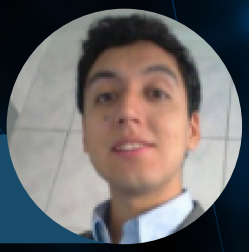
Ha sido instructor de cursos de:

Hacking Web

Hacking Ético con Kali Linux

Certificaciones:

- EC-Council, Ethical Hacking and Countermeasures
- Introduction to Software Vulnerability Exploitation
- The Web Application Hacker's Handbook - BlackHat USA 2017



Samuel Orellana
Consultor Senior
CyberTrust