Curso Virtual Hacking Aplicaciones Web 2021

Domingos 7, 14, 21 y 28 de Febrero del 2021. 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 modernas tienen un rol muy importante en todas las organizaciones. Pero si la organización no tiene la capacidad de evaluar y asegurar adecuadamente sus aplicaciones web, los atacantes maliciosos podrían comprometer estas aplicaciones, afectar el funcionamiento normal de la empresa, como también robar datos sensibles. Desafortunadamente muchas organizaciones operan bajo la errada percepción, de confiar el descubrimiento de las fallas en sus sistemas, únicamente a la ejecución de escáneres automáticos de seguridad para aplicaciones web. Consecuentemente se debe entender; no existe un parche o solución total para las aplicaciones web creadas a medida o personalizadas; por lo tanto los atacantes maliciosos se están enfocando cada vez más en este tipo de infraestructura, la cual tiene un gran valor.

Objetivos

Este curso enseña a los participantes a entender las principales fallas encontradas en las aplicaciones web, además de como es factible explotarlas. Siendo lo más importante aprender a realizar un proceso factible de ser repetido y verificado en el mundo real, para consecuentemente encontrar de manera consistente estas fallas en sus organizaciones. El participante aprenderá una metodología para realizar una prueba de penetración constituida de cuatro etapas, además de la configuración y utilización de las herramientas para realizar pruebas satisfactorias. Comprendercomo se realiza la comunicación entre todas las partes involucradas en una aplicación web. Seleccionar y utilizar los diferentes métodos, además de técnicas para realizar los ataques más relevantes, como por ejemplo; Inyección de Comandos, Recorrido de Directorios, Inyección SQL, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), entre muchas vulnerabilidades más.

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, Phishing Countermeasures, Pen Testing, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS) y OPEN-SEC Ethical Hacker (OSEH). Ha sido instructor en el OWASP LATAM Tour, expositor en OWASP Perú Chapter Meeting y OWASP LATAM at Home , además de Conferencista en PERUHACK, instructor en PERUHACKNOT, y conferencista en 8.8 Lucky Perú. Cuenta con más de dieciséis años de experiencia en el área y desde hace doce años labora como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Perteneció por muchos años al grupo internacional RareGaZz y PeruSEC. Ha dictado cursos 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: **https://www.ReYDeS.com**

Fechas & Horarios

Duración: Catorce (14) horas. Una (1) sesión previamente grabada de dos (2) horas, y cuatro (4) sesiones en vivo de tres (3) horas de duración cada una.

Fechas:

Domingos 7, 14, 23 y 28 de Febrero del 2021

Horarios:

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

Más Información

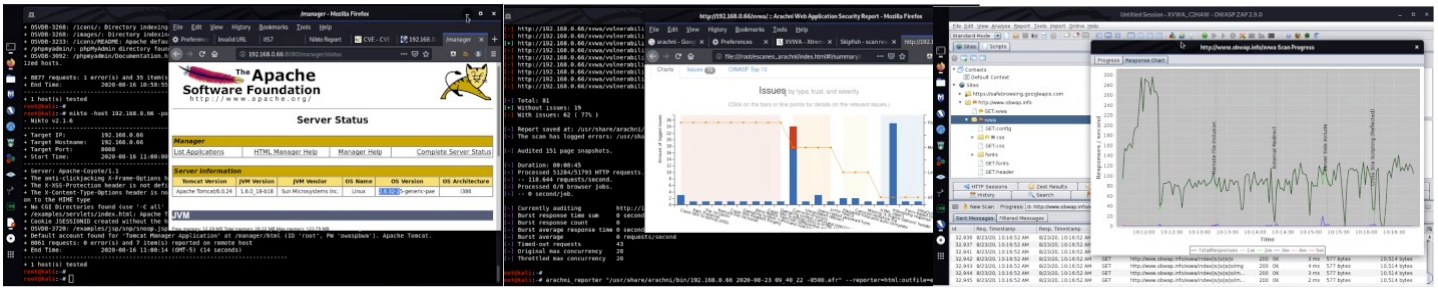
Para obtener más información sobre este curso virtual, tiene a su disposición los siguientes mecanismos de contacto.

Correo electrónico:

caballero.alonso@gmail.com

Teléfono: (+51) 949 304 030

Sitio Web: https://www.reydes.com



Temario (Actualizado)

- Pruebas de Penetración contra Aplicaciones Web
- Métodos, Tipos y Componentes de Pruebas de Penetración
- Reporte y Presentación de los Hallazgos
- Metodología de Ataque
- Tipos de Fallas
- Reconocimiento
- Consultas Whois y DNS
- Fuentes de Información Externa
- Google Hacking
- Mapeo
- Escaneo de Puertos
- Huella del SO
- Escaneo de Versiones.
- Analisis del Soporte SSL
- Hosting Virtual y Balanceo de Carga
- Analizar la Configuración del Software
- Spidering al Sitio Web
- Gráfica del flujo de la Aplicación
- Descubrimiento
- Escaners Automáticos de Vulnerabilidades en Aplicaciones Web
- Vulnerabilidades en Aplicaciones Web y Técnicas manuales
- Skipfish, Arachni
- Zed Attack Proxy
- Exposición de Información
- Navegación de Directorios
- Recolectar Nombres de usuarios
- Inyección de Comandos
- Inyección SQL y SQL ciega (SQLi)
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Pruebas de Autenticación
- Subida Irrestricta de Archivos
- Inyección de Formula
- XSS DOM
- Referencia Directa a Objetos Inseguros
- Control Inadecuado para Acceso de Nivel Funcional
- Criptografía
- Redirecciones
- Reenvios No Válidos
- Explotación
- Evasión de Autenticación
- Explotación de Inyección SQL
- Inyección SQL ciega
- SQLMap
- BeFF

Material

- Kali Linux
- OBWAP
- Metasploitable 2
- Herramientas Windows

Inversión y Forma de Pago

Este curso tiene un costo de:

S/. 350 Soles o $ 110 Dólares

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

Residentes en Perú

Depósito bancario en la siguiente cuenta:

Scotiabank

Scotiabank Perú SAA
Cuenta de Ahorros en Soles: 324-0003164
A nombre de: Alonso Eduardo Caballero Quezada
Código de Cuenta Interbancario (CCI): 009-324-203240003164-58

Residentes en otros países

Transferencia de dinero mediante Western Union y MoneyGram o pago por Paypal

Escribir por favor un mensaje de correo electrónico caballero.alonso@gmail.com para indicarle los datos necesarios para realizar el pago.

Confirmado el depósito o la transferencia se enviará al correo electrónico del participante, los datos necesarios para conectarse a la plataforma, además de la información pertinente para su participación en el curso.

INTERMEDIA ANYMEETING

El curso se realiza utilizando el sistema para video conferencias de nombre **Anymeeting.** El cual proporciona transmisión de audio y video HD en alta calidad, tanto para el instructor y los participantes, entre otras características ideales para el dictado de cursos virtuales o en línea.