# Curso Virtual Hacking Aplicaciones Web 2019

**Domingos 3, 10, 17 y 24 de Febrero del 2019. 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 escaners 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.

## Objetivos:

En este curso se enseña a los participantes a entender las principales fallas en las aplicaciones web y su explotación;y lo más importante; aprender a realizar un proceso repetible y verificado en la realidad, para encontrar de manera consistente estas fallas en sus organizaciones. El participante aprenderá una metodología para pruebas de cuatro fases, además de la configuración y utilización de las herramientas para realizar pruebas satisfactorias. Comprender como 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.

## Fechas & Horarios:

El Curso Virtual de Hacking Aplicaciones Web tiene una duración de doce (12) horas, dividas en cuatro (4) sesiones de tres (3) horas de duración.

**Fechas:**

Domingos 3, 10, 17 y 24 de Febrero del 2019

**Horarios:**

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

**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 y Phishing Countermeasures. Ha sido instructor y expositor en OWASP LATAM Tour Lima, Perú, 0x11 OWASP Perú Chapter Meeting, PERUHACK 2014, PERUHACK2016NOT, y 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 y GNU/Linux. Su correo electrónico es ReYDeS@gmail.com y su página personal es: http://www.ReYDeS.com.

## Más Información:

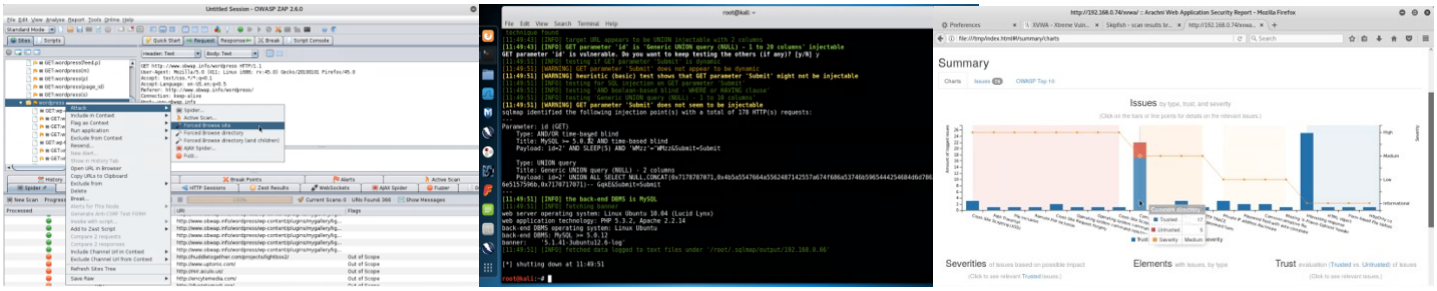
Para obtener más información sobre este curso virtual, tiene a su disposición los siguientes mecanismos de contacto.

**Correo electrónico:**

caballero.alonso@gmail.com

**Teléfono:** (+51) 949304030

**Sitio Web:** http://www.reydes.com



## Temario: (Actualizado)

- Pruebas de Penetración contra Aplicaciones Web
- Métodos y Tipos de Pruebas de Penetración
- Componentes de una Prueba de Penetración Web
- 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 y Navegación de Directorios
- Cosecha de Nombres de usuarios
- Inyección de Comandos
- Inyección SQL y SQL ciega (SQLi)
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Pruebas de Autenticación
- Ajax y Mash-ups
- Mapeo, Descubrimiento y Explotación en Ajax
- Ataques Lógicos, Ataques API, y Ataques a Datos
- JSON, WebServices
- UDDI, SOAP, Entidad
- Inyección XPATH
- Explotación
- Evasión de Autenticación
- Explotación de Inyección SQL e Inyección SQL ciega
- SQLMap y BeFF

## Material:

- Kali Linux
- OWASP BWAP y BeeBox.

***** Si el participante lo requiere se le enviarán dos (2) DVDs conteniendo el material utilizado en el curso, por S/. 75 Soles adicionales. Esto incluye los gastos de envío hacia cualquier lugar del Perú.

## Inversión y Forma de Pago:

El 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
Cuenta de Ahorros en Soles: 324-0003164
A nombre de: Alonso Eduardo Caballero Quezada

**Residentes en Otros Países**

Transferencia de dinero mediante Western Union o MoneyGram.

Western Union moving money for better

MoneyGram

Escribir por favor un mensaje de correo electrónico para enviarle los datos necesarios para realizar la transferencia.

Confirmado el depósito o la transferencia se enviará al correo electrónico del participante, los datos necesarios para conectarse al sistema, además del material 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 de alta calidad para el instructor y los participantes, entre otras características ideales para el dictado de cursos virtuales.