Único Curso del Año 2018

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

Domingos 20 y 27 de Mayo del 2018

De 9:00 am a 12:15 pm (UTC -05:00) - 6 horas en Total

1. Presentación:

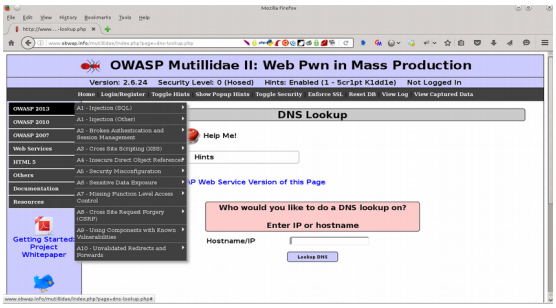
El software inseguro está minando las infraestructuras críticas financieras, de salud, defensa, energía y otras. Conforme el software incrementa su complejidad y capacidad de conexión, la dificultad para alcanzar la seguridad en las aplicaciones se incrementa de manera exponencial. El veloz ritmo de los procesos modernos para el desarrollo del software, hacen los riesgos más comunes sean esenciales de descubrir y resolver rápidamente de manera precisa. Ya no es permisible tolerar problemas de seguridad relativamente simples como los presentados en este OWASP TOP 10.

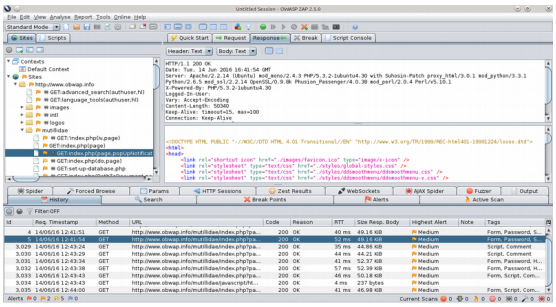
Aunque el objetivo original del proyecto OWASP TOP 10 fue simplemente crear conciencia entre los desarrolladores y gerentes, se ha convertido en un estándar de facto para seguridad en aplicaciones.

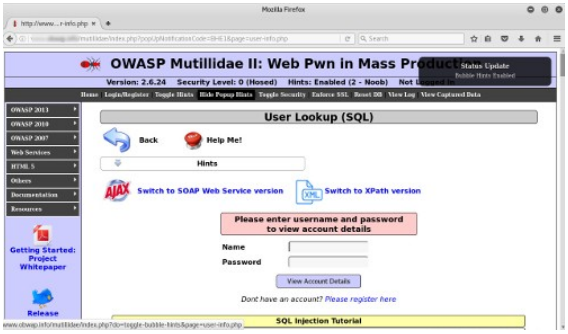
En esta nueva versión del OWASP TOP 10 2017, los problemas y recomendaciones están escritas de una forma concisa y de manera comprobable, para ayudar con la adopción del OWASP TOP 10 en los programas de seguridad en aplicaciones. Se alienta a las organizaciones a utilizar el Estándar de Verificación para la Seguridad de Aplicaciones (ASVS) de OWASP si se requiere un verdadero estándar, pero para la mayoría el OWASP TOP 10 es un gran inicio en el camino de la seguridad en aplicaciones.

2. Temario:

- Introducción a OWASP TOP 10 2017
- Anotaciones sobre la Publicación
- OWASP Mutillidae II
- OWASP Zed Attack Proxy (ZAP)
- Riesgos de Seguridad en Aplicaciones
- A1:2017-Injection (Inyección)
- A2:2017-Broken Authentication (Autenticación Rota)
- A3:2017-Sensitive Data Exposure (Exposición de Datos Sensibles)
- A4:2017-XML External Entities (XXE) (Entidades Externas XML)
- A5:2017-Broken Access Control (Control de Acceso Roto)
- A6:2017-Security Misconfiguration (Malas Configuraciones en Seguridad)
- A7:2017-Cross-Site Scripting (XSS)
- A8:2017-Insecure Deserialization (Deserialización Insegura)
- A9:2017-Using Components with Known Vulnerabilities (Componentes con Vulnerabilidades Conocidas)
- A10:2017-Insufficient Logging&Monitoring (Insuficiente Registro de Sucesos y Vigilancia)
- Lo Siguiente para los Desarrollares
- Lo Siguiente para los Evaluadores de Seguridad
- Lo Siguiente para las Organizaciones
- Lo Siguiente para los Gerentes de Aplicaciones
- Anotaciones sobre el Riesgo
- Detalles Sobre los Factores de Riesgo
- Metodología y Datos







3. Material:

Se sugiere al participante descargar como mínimo la siguiente máquina virtual en su sistema para desarrollar el curso.

- **Kali Linux 2018.1**
  Enlace de Descarga (32 Bit)
  https://images.offensive-security.com/virtual-images/kali-linux-2018.1-vm-i386.7z

  Enlace de Descarga (64 Bit)
  https://images.offensive-security.com/virtual-images/kali-linux-2018.1-vm-amd64.7z

- **OWASP Mutillidae II**
  Enlace de Descarga:
  https://sourceforge.net/projects/mutillidae/files/

[*] Si el participante lo requiere se le puede enviar 1 DVD con las máquinas virtuales añadiendo S/. 75 Soles por el concepto de gastos de envío a cualquier lugar del Perú.

4. Día y Horario:

La duración total del Curso es de 6 (seis) horas. El Curso se dictará en los siguientes días y horarios.

Domingos 20 y 27 de Mayo del 2018
De 9:00 am a 12:15 pm (UTC -05:00) - 6 Horas en Total

[*] No habrá reprogramaciones. El Curso se dictará **sin** ningún requisito mínimo de participantes.

5. Inversión y Forma de Pago:

El Curso tiene un costo de:

S/. 165 Soles o $ 50 Dólares

El pago del Curso se realiza mediante un depósito bancario en la siguiente cuenta:

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

Una vez realizado el depósito, enviar por favor el comprobante escaneado a la siguiente dirección de correo electrónico: **caballero.alonso@gmail.com**.

Otros Países

Para residentes en otros países el pago se realiza mediante una transferencia de dinero utilizando Western Union o MoneyGram. Por favor escribir un mensaje de correo electrónico a **caballero.alonso@gmail.com**. para coordinarlos datos para realizar la transferencia.

Confirmado el depósito o transferencia, se enviará al correo electrónico del participante, los datos necesarios para conectarse hacia el sistema y poder participar en el curso.

6. Más Información:

Si desea mayor información sobre el Curso Virtual OWASP TOP 10 2017, tiene a su disposición los siguientes mecanismos de contacto:

Correo electrónico: caballero.alonso@gmail.com

Vía Web: http://www.reydes.com

Celular: +51 949304030

7. Sobre el 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, Cybersecurity Management, Cyber Warfare and Terrorism y Enterprise Cyber Security Fundamentals. Ha sido instructor en el OWASP LATAM Tour Lima, Perú del año 2014 y expositor en el 0x11 OWASP Perú Chapter Meeting 2016, además de Conferencista en PERUHACK 2014, instructor en PERUHACK2016NOT, y conferencista en 8.8 Lucky Perú 2017. Cuenta con más de catorce años de experiencia en el área y desde hace diez 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, GNU/Linux y Software Libre. Su correo electrónico es ReYDeS@gmail.com y su página personal es: http://www.ReYDeS.com.