OWASP Top 10 2021

Sábados 16 y 23 de Julio del 2022. De 9:00am a 12:00am (UTC -05:00)

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

Presentación

OWASP Top 10 es un documento estándar para concienciación dirigido hacia los desarrolladores, como también para la seguridad en aplicaciones web. Representa un amplio consenso sobre los riesgos más críticos en seguridad en las aplicaciones web.

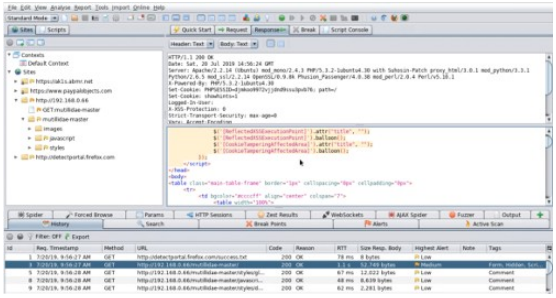
Globalmente reconocido por los desarrolladores como el primer paso hacia una codificación más segura.

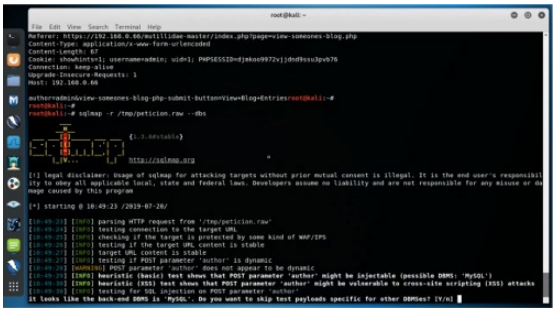
Las empresas deberían adoptar este documento e iniciar el proceso de asegurar sus aplicaciones web para minimizar estos riesgos. Utilizar OWASP Top 10 es quizás el primer paso más efectivo para cambiar la cultura de desarrollo de software en la organización, de tal manera se produzca código más seguro.

Existen tres nuevas categorías, cuatro categorías con cambios en el nombre y su alcance, además de alguna consolidación en el Top 10 2021. Se han cambiado los nombres de ser necesario, para enfocarse en la causa raíz sobre los síntomas.

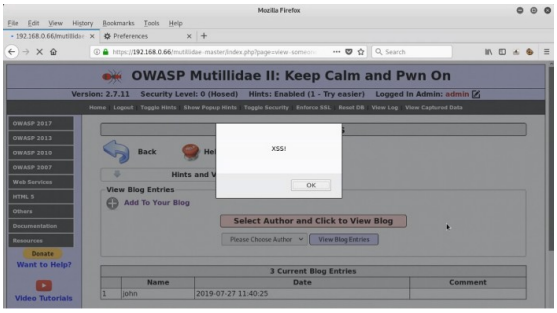
Temario

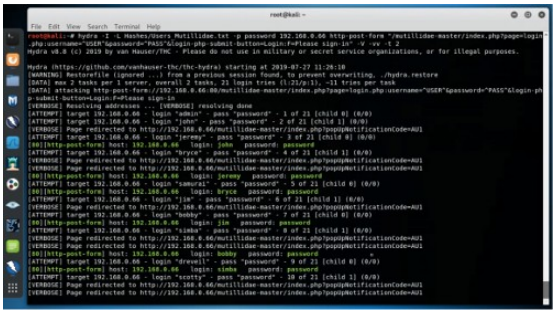
- Introducción
- Bienvenido a OWASP Top 10 2021
- Que ha cambiado en el Top 10 para el 2021
- Metodología
- Como están estructuradas las categorías
- Como son utilizados los datos para seleccionar las categorías
- ¿Porqué no solo datos estadísticos puros?
- ¿Porqué la tasa de incidencia en lugar de la frecuencia?
- ¿Cual es el proceso para la recolección y análisis de datos?
- Factores de datos
- Como utilizar OWASP Top 10 como un estándar
- Como iniciar un programa de seguridad en aplicaciones web con OWASP Top 10
- Etapa 1 Identificar las carencias y metas del programa en seguridad en aplicaciones
- Etapa 2 Planificar una ruta para un ciclo de vida de desarrollo seguro
- Etapa 3 Implementar un ruta con los equipos de desarrollo
- Etapa 4 Migrar toda las aplicaciones existentes y futuras hacia una ruta
- Etapa 5 Probar si la ruta ha mitigado los problemas encontrados





en OWASP Top 10
- Etapa 6 Construir su programa dentro de un programa maduro para seguridad en aplicaciones
- Sobre OWASP
- A01 Control de Acceso Roto
- A02 Fallos Criptográficos
- A03 Inyección
- A04 Diseño Inseguro
- A05 Configuraciones Inadecuadas en Seguridad
- A06 Componentes Vulnerables o Desactualizados
- A07 Fallas en la Identificación y Autenticación
- A08 Fallas en el Software e Integridad de Datos
- A09 Fallas en el Registro de Eventos y Vigilancia
- A10 Falsificación de Peticiones en el Lado del Servidor
- Siguientes Pasos
- Temas sobre calidad de código
- Negación de Servicio
- Errores en la gestión de memoria





Material

Todos los participantes al Curso Virtual de OWASP Top 10 tendrán la posibilidad de descargar los videos de cada sesión, un día después de impartida la misma.

- **Kali Linux:**
  Link de Descarga: https://www.kali.org/get-kali/

- **OWASP Mutillidae II**
  Link de Descarga: https://github.com/webpwnized/mutillidae

- **DVWA**
  Link de Descarga: https://github.com/digininja/DVWA

fechas y Horario

El Curso Virtual de OWASP Top 10 tiene una duración total de seis (6) horas, las cuales se dividen en dos (2) sesiones de tres (3) horas cada una.

- **Fechas:**

  Sábados 16 y 23 de Julio del 2022

- **Horario:**

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

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

Inversión y Forma de Pago:

Acceso a todos los videos y material:

S/. 175 Soles o $ 50 Dólares

Acceso al aula virtual por 30 días, todos los videos, material, evaluaciones, certificado de participación y certificado de aprobación.

S/. 260 Soles o $ 75 Dólares

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

Residentes en Perú	Residentes en Otros Países
Deposito bancario o transferencia interbancaria en la siguiente cuenta: Scotiabank ScotiaBank Cuenta de Ahorros en Soles: 324-0003164 A nombre de: Alonso Eduardo Caballero Quezada CCI: 009-324-203240003164-58	Transferencia de dinero mediante Western Union y MoneyGram o pago por Paypal: MoneyGram. WESTERN UNION WU moving money for better PayPal Escriba por favor un mensaje de correo electrónico a caballero.alonso@gmail.com para proporcionarle los datos requeridos.

Confirmado el pago se enviará al correo electrónico del participante, los datos necesarios para conectarse hacia la plataforma, además de toda la información pertinente para su participación en el curso

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.

INTERMEDIA ANYMEETING

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

Instructor

Alonso Eduardo Caballero Quezada. 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). He sido instructor, expositor y conferencista en el OWASP LATAM Tour, OWASP Perú Chapter Meeting, OWASP LATAM at Home, PERUHACK, PERUHACKNOT, 8.8 Lucky Perú, Ekoparty University Talks Perú. Cuento con más de diecisiete años de experiencia en el área y desde hace trece años laboro como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Pertenecí por muchos años al grupo internacional RareGaZz y grupo Peruano PeruSEC. He dictado cursos para España, Ecuador, México, Bolivia y Perú, presentándome también en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux y Software Libre.