Webinar Gratuito

Guía para Pruebas de Seguridad Web de OWASP

Alonso Eduardo Caballero Quezada

Instructor y Consultor Independiente en Ciberseguridad

Sitio Web: www.ReYDeS.com -:- Correo: ReYDeS@gmail.com

Jueves 15 de Febrero 2024

Alonso Eduardo Caballero Quezada

ISC2 Certified in Cybersecurity (CC), LPI Security Essentials Certificate, EXIN Ethical Hacking Foundation Certificate, 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, Ransomware Techniques, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS), OPEN-SEC Ethical Hacker (OSEH), Codered Certificate of Achievement: Digital Forensics Essentials (DFE) y Ethical Hacking Essentials (EHE).

Más de 20 años de experiencia como consultor e instructor independiente en las áreas de Hacking Ético, Forense Digital, GNU/Linux, y áreas relacionadas.

Redes Sociales

https://www.linkedin.com/in/alonsocaballeroquezada/

https://twitter.com/Alonso_ReYDeS

https://www.youtube.com/c/AlonsoCaballero

https://www.facebook.com/alonsoreydes/

https://www.instagram.com/alonso_reydes/

reydes@gmail.com

www.reydes.com

+51 949 304 030

@ReYDeS

Proyecto para Pruebas de OWASP

Su propósito es ayudar a comprender el que, por que, cuando, donde, y como de las pruebas a aplicaciones web.

El proyecto ha entregado un marco de trabajo completo para pruebas, no meramente una simple lista de verificación o prescripción de problemas a abordarse.

Puede utilizarse este marco de trabajo como plantilla para construir programas propios de pruebas, o para cualificar los procesos de otros.

La guía de pruebas describe en detalle tanto el marco general para pruebas, cuanto las técnicas requeridas para implementar el marco de trabajo en práctica.

https://owasp.org/www-project-web-security-testing-guide/latest/2-Introduction/

¿Porqué Pruebas de Penetración?

El documento está diseñado para ayudar a las organizaciones a entender aquello comprendido en un programa de pruebas, y para ayudar a identificar los pasos a realizarse para construir y operar un programa moderno para pruebas de aplicaciones web.

Esta guía ofrece una visión amplia de los elementos requeridos para crear un programa completo de seguridad en aplicaciones web.

Puede utilizarse como referencia y como metodología para ayudar a determinar la brecha entre las prácticas existentes y las mejores prácticas de la industria. Permite a las organizaciones compararse con sus homólogos de la industria, para entender la magnitud de los recursos requeridos para probar y mantener el software, o prepararse para una auditoría.

¿Qué es Metodología para Pruebas de OWASP?

Las pruebas de seguridad nunca serán una ciencia exacta, donde una lista completa de todos los posibles problemas a evaluar puedan ser definidas. De hecho las pruebas de seguridad son sólo una de las muchas técnicas confortables para probar la seguridad de las aplicaciones web bajo ciertas circunstancias. El propósito del proyecto es recopilar todas las técnicas posibles de evaluación, explicar técnicas, y mantener la guía actualizada. La metodología para pruebas de seguridad de aplicaciones web de OWASP, se basa en el enfoque de caja negra. Donde se tiene poca o ninguna información sobre la aplicación a evaluar

El modelo de prueba consiste en:

- Profesional: Quién realiza las actividades de prueba
- Herramientas y metodología: El núcleo de este proyecto de guía para pruebas
- Aplicación: La caja negra a evaluar

Pruebas de Seguridad de Aplicaciones Web

- Recolección de Información
- Pruebas sobre la Gestión de Configuración y Despliegue
- Pruebas sobre la Gestión de Identidad
- Pruebas de Autenticación
- Pruebas de Autorización
- Pruebas sobre la Gestión de la Sesión
- Pruebas de Validación de Entradas
- Pruebas sobre el Manejo de Error
- Pruebas sobre Debilidad Criptográfica
- Pruebas sobre la Lógica del Negocio
- Pruebas para el Lado del Cliente
- Pruebas API

https://owasp.org/www-project-web-security-testing-guide/latest/

Captura de Información

- Realizar Reconocimiento de Descubrimiento en Motores de Búsqueda por Fuga de Información
- Obtener una Huella del Servidor Web
- Revisar Metaarchivos del Servidor Web por Fuga de Información
- Enumerar Aplicaciones sobre el Servidor Web
- Revisar el Contenido de la Página Web por Fuga de Información
- Identificar Puntos de Entrada hacia la Aplicación
- Mapear Rutas de Ejecución a través de la Aplicación
- Obtener una Huella del Framework de la Aplicación Web
- Obtener una Huella de la Aplicación Web
- Mapear la Arquitectura de la Aplicación

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/01-Information_Gathering/README

Curso OWASP Top 10

OWASP Top 10

Sábados 17 y 24 de Febrero del 2024. De 9:00am a 12:00am (UTC -05:00)

Este curso 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.

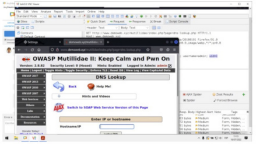
Globalmente reconocido por los desarrolladores como el primer paso hacia una codificación más segura.

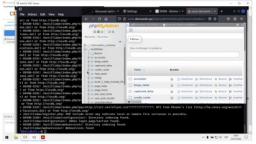
Las empresas deberían adoptar este documento e iniciar el proceso de asegurar sus aplicaciones web para minimizar estos riesgos. Utilizar OWASP Top 10 es quizás el primer paso más efectivo para cambiar la cultura de desarrollo de software en la organización, de tal manera se produzca código más seguro.

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
- Que ha cambiado en el Top 10 actual
- 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

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 17 y 24 de Febrero del 2024

- **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.

Beneficios e Inversión:

- Acceso a las sesiones en vivo
- Acceso al aula virtual por 45 días
- Video de las dos (2) sesiones
- Material utilizado durante el desarrollo del curso
- Asesoría personalizada
- Libro "Fundamentos de Hacking Web" escrito por el Instructor
- Certificado digital de participación
- Certificado digital de aprobación. Puntuación mínima 70/100. Por una duración total de 16 horas

S/. 225 Soles o $ 70 Dólares

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

Residentes en Perú	Residentes en Otros Paises
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	Pago a través de PayPal. O también transferencia de dinero mediante Western Union y MoneyGram PayPal Escriba por favor un mensaje de correo electrónico a reydes@gmail.com para proporcionarle los datos pertinente para realizar el pago.

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

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

ISC2 Certified in Cybersecurity (CC), LPI Security Essentials Certificate, EXIN Ethical Hacking Foundation Certificate, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hardning Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Ransomware Techniques, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS), OPEN-SEC Ethical Hacker (OSEH), Codered Certificate of Achievement: Digital Forensics Essentials (DFE) y Ethical Hacking Essentials (EHE). He sido instructor, expositor y conferencista en el OWASP LATAM Tour, OWASP Perú Chapter Meeting, OWASP LATAM at Home, PERUHACK, PERUHACKNOT, B.B Lucky Perú, Eloquenty University Talks Perú. Cuento con más de dieciocho años de experiencia en el área y desde hace catorce 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. Mi correo electrónico es ReYDes@gmail.com y mi página personal está en: https://www.ReYDes.com

Sitio Web:

www.reydes.com

Correo:

reydes@gmail.com

Más Información:

https://www.reydes.com/d/?q=Curso_OWASP_TOP_10

Prácticas

```
┌──(kali㉿kali)-[~]
└─$ echo -ne "HEAD / HTTP/1.1\r\nHost: afpnews.com\r\
HTTP/1.1 404 Not Found
Date: Thu, 08 Feb 2024 21:41:40 GMT
Content-Length: 74
Content-Type: text/plain; charset=utf-8
Via: 1.1 google
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=25920

┌──(kali㉿kali)-[~]
└─$ echo -ne "HEAD / HTTP/1.1\r\nHost: apnews.com\r\n
HTTP/1.1 200 OK
server: istio-envoy
strict-transport-security: max-age=31536000; includeS
x-powered-by: Brightspot
x-envoy-upstream-service-time: 2770
x-envoy-decorator-operation: brightspot-frontend-veri
Via: 1.1 google
Date: Thu, 08 Feb 2024 21:34:29 GMT
Cache-Control: max-age=120
Age: 461
Content-Type: text/html;charset=UTF-8
Vary: Accept-Encoding
cdn_cache_id: SCL-22372366
cdn_cache_status: stale
origin_request_header:
Transfer-Encoding: chunked
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

┌──(kali㉿kali)-[~]
└─$
```

webcache.googleusercontent.com/search?q=cac

Esta es la memoria caché de Google de https://apnews.com/. Es una instantánea de la página según apareció el 8 Feb. 2024 21:27:18 GMT. Se puede haber cambiado la página actual mientras tanto. Más información.

Versión completa Versión de sólo texto Ver código fuente

Consejo: para encontrar tu término de búsqueda rápido en esta página, presiona **Ctrl+F** o **⌘-F** (Mac) y usa la barra de búsqueda.

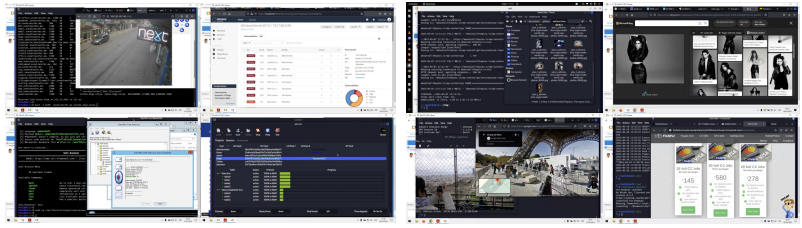
ADVERTISEMENT

AP

Israel-Hamas war | Supreme Court Trump case | Five Marines confirmed dead | Iceland volca

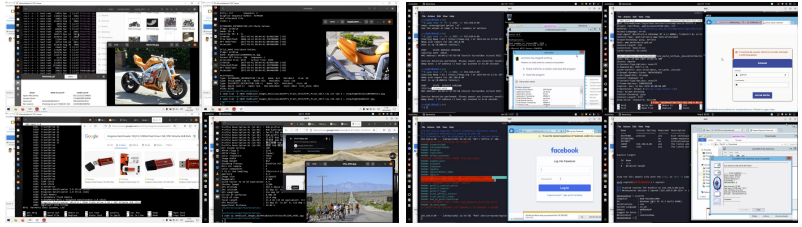
Cursos Disponibles en Video

Curso Hacking Ético
https://www.reydes.com/d/?q=Curso_de_Hacking_Etico



Curso Hacking Aplicaciones Web
https://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

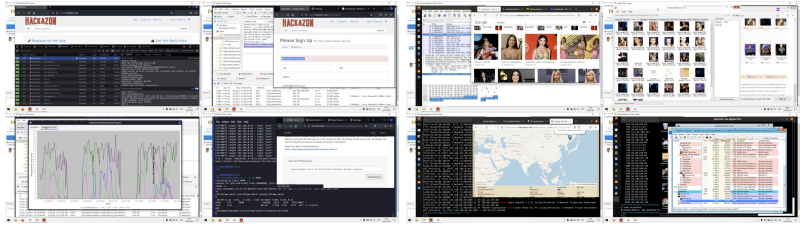
Curso Informática Forense
https://www.reydes.com/d/?q=Curso_de_Informatica_Forense



Curso Hacking con Kali Linux
https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

Curso OSINT - Open Source Intelligence
https://www.reydes.com/d/?q=Curso_de_OSINT

Curso Forense de Redes
https://www.reydes.com/d/?q=Curso_Forense_de_Redes



Y todos los cursos virtuales:

https://www.reydes.com/d/?q=cursos

Más Contenidos

Videos de webinars

https://www.reydes.com/d/?q=videos

Diapositivas de webinars

https://www.reydes.com/d/?q=eventos

Libros y artículos

https://www.reydes.com/d/?q=documentos

Blog

https://www.reydes.com/d/?q=blog/1

Webinar Gratuito

Guía para Pruebas de Seguridad Web de OWASP

Alonso Eduardo Caballero Quezada

Instructor y Consultor Independiente en Ciberseguridad

Sitio Web: www.ReYDeS.com -:- Correo: ReYDeS@gmail.com

Jueves 15 de Febrero 2024