Webinar Gratuito

Vulnerabilidades en Aplicaciones Web

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: https://www.ReYDeS.com -:- e-mail: ReYDeS@gmail.com

Jueves 3 de Noviembre 2022

Alonso Eduardo Caballero Quezada

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, Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist y OSEH.

Más de 18 años de experiencia como consultor e instructor independiente en las áreas de Hacking Ético y Forense Digital. 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.

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

https://www.reydes.com

+51 949 304 030

@ReYDeS

¿Qué es una Vulnerabilidad?

Las vulnerabilidades en las aplicaciones web implican un fallo del sistema o una debilidad en una aplicación basada en la web. Existen desde hace años, en gran parte debido a la falta de validación o sanitización de las entradas en los formularios, servidores web mal configurados, y defectos en el diseño de las aplicaciones, pudiendo ser explotadas para comprometer la seguridad de la aplicación.

Estas vulnerabilidades no son iguales a otros tipos comunes de vulnerabilidades, como las vulnerabilidades relacionadas a la red o las vulnerabilidades de activos.

Surgen porque las aplicaciones web necesitan interactuar con múltiples usuarios a través de múltiples redes, y este nivel de accesibilidad es fácilmente aprovechado por los ciberatacantes.

Ejemplos de Vulnerabilidades

Algunas de las vulnerabilidades presentadas a continuación se basa en el CWE Top 25

- Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
- Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
- Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
- Cross-Site Request Forgery (CSRF)
- Improper Authentication
- Missing Authorization
- Server-Side Request Forgery (SSRF)

Cross-Site Scripting

Son un tipo de inyección, en el cual se inyectan scripts maliciosos en sitios web. Se producen cuando un atacante utiliza una aplicación web para enviar código malicioso, generalmente en forma de script para el lado del navegador, hacia otro usuario. Se producen en cualquier lugar en el cual una aplicación web utiliza la entrada de un usuario en la salida generada sin validarla o codificarla.

Se puede utilizar XSS para enviar un script malicioso hacia un usuario desprevenido. El navegador no tiene forma de saber el script no es de confianza, y lo ejecutará. Como cree el script proviene de una fuente de confianza, el script malicioso puede acceder hacia cualquier cookie, token de sesión, u otra información sensible retenida por el navegador, y utilizada con ese sitio. Estos scripts pueden incluso reescribir el contenido de la página HTML.

* https://owasp.org/www-community/attacks/xss/

Inyección SQL

Un ataque de inyección SQL consiste en la inserción o "inyección" de una consulta SQL a través de los datos de entrada del cliente hacia la aplicación.

Un ataque de inyección SQL exitoso puede leer datos sensibles desde la base de datos, modificar los datos desde la base de datos (Insertar/Actualizar/Borrar), ejecutar operaciones de administración en la base de datos (como apagar el SGBD), recuperar el contenido de un archivo determinado presente en el sistema de archivos del SGBD y; en algunos casos; enviar comandos hacia el sistema operativo.

Son un tipo de ataque de inyección, en el cual se inyectan comandos SQL en la entrada de datos, para afectar a la ejecución de comandos SQL predefinidos.

* https://owasp.org/www-community/attacks/SQL_Injection

Inyección de Comandos en el S.O.

Es un ataque cuyo propósito es la ejecución de comandos arbitrarios en el sistema operativo anfitrión, a través de una aplicación vulnerable. Son posibles cuando una aplicación envía datos no seguros suministrados por el usuario (formularios, cookies, cabeceras HTTP, etc.) hacia una shell del sistema. En este ataque los comandos del sistema operativo suministrados por el atacante, suelen ejecutarse con los privilegios de la aplicación vulnerable. Son posibles en gran medida debido a la insuficiente validación de entradas.

Este ataque se diferencia de la inyección de código, donde se permite al atacante añadir su código, el cual luego es ejecutado por la aplicación. En este ataque el atacante amplía la funcionalidad por defecto de la aplicación, el cual ejecuta comandos del sistema, sin necesidad de inyectar código.

* https://owasp.org/www-community/attacks/Command_Injection

Curso Virtual Hacking Aplicaciones Web

Domingos 6, 13, 20 y 27 de Noviembre del 2022 De 9:00 am a 12:00 pm (UTC -05:00)

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

Presentación

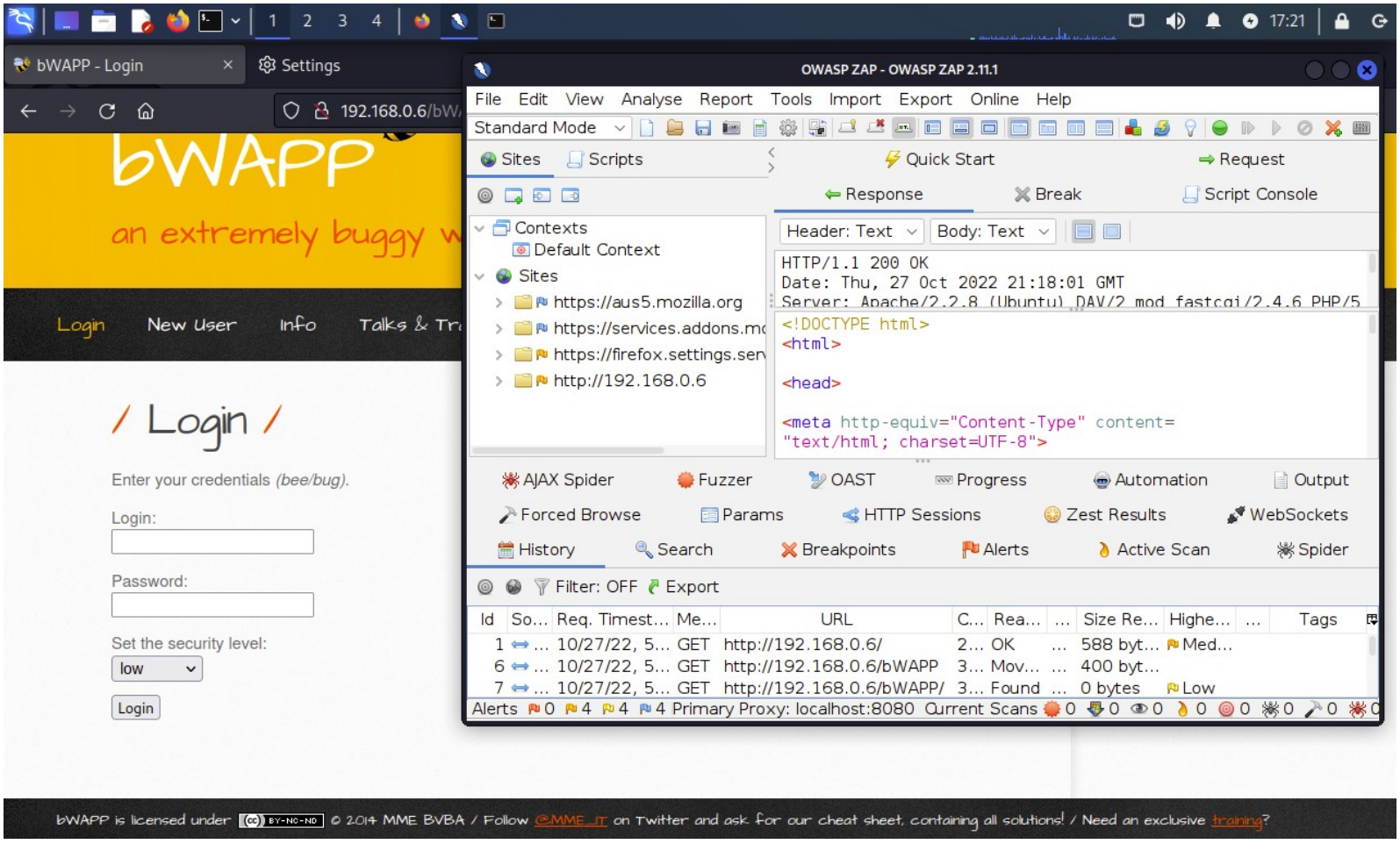
Las aplicaciones web modernas tienen un rol muy importante en todas las organizaciones. Pero si la organización no tiene la capacidad de evaluar y asegurar adecuadamente sus aplicaciones web, los ciberatacantes podrían comprometer estas aplicaciones, afectando el funcionamiento normal de la empresa, como también robar datos sensibles. Desafortunadamente muchas organizaciones operan bajo la errónea percepción, de un escáner de seguridad para aplicaciones web es la manera más fiable de descubrir fallas en sus sistemas. Las ciberdefensas modernas requieren una comprensión realista y profunda de los problemas de seguridad relacionadas con la aplicación web. Cualquiera puede aprender a realizar algunos tipos de ataques contra la web, pero una prueba de penetración efectiva contra aplicaciones web requiere un conocimiento más profundo.

Alonso Eduardo Caballero Quezada 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, 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

Más Información: https://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

e-mail: reydes@gmail.com Sitio Web: https://www.reydes.com

Demostraciones



Cursos Virtuales Disponibles en Video

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

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

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

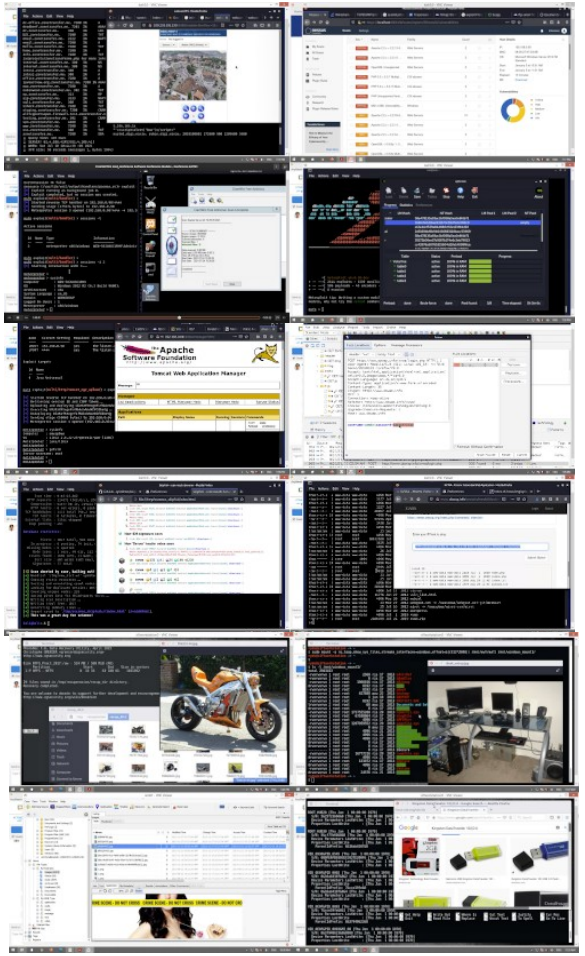
Curso Virtual Hacking con Kali Linux
https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

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

Curso Virtual 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 77 webinars gratuitos

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

Diapositivas de los webinars gratuitos

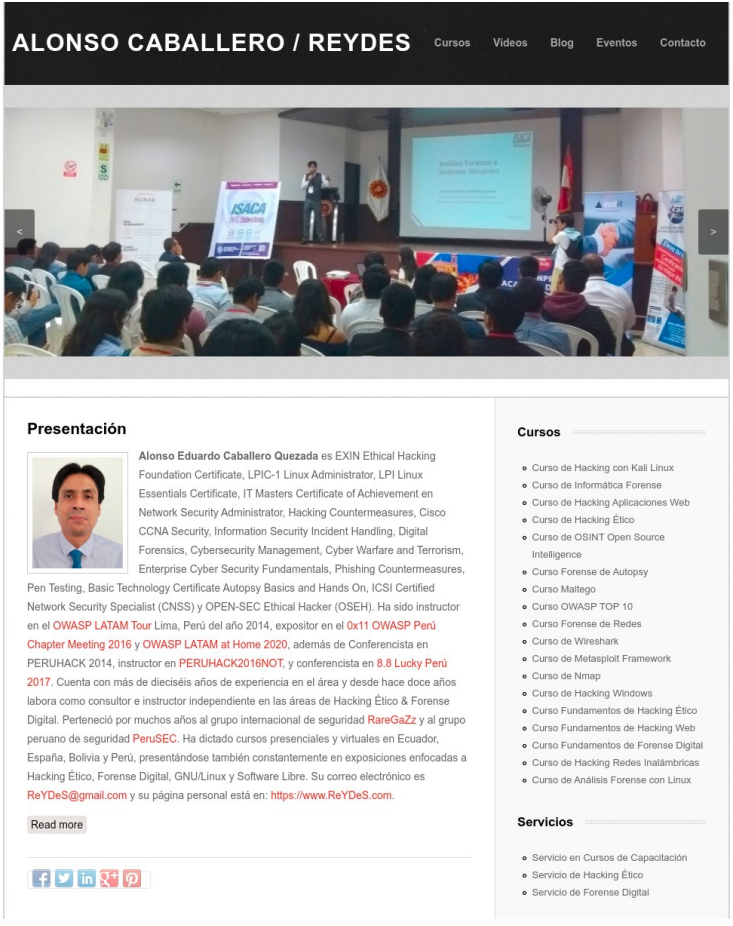
https://www.reydes.com/d/?q=eventos

Artículos y documentos publicados

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

Blog sobre temas de mi interés

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



Webinar Gratuito

Vulnerabilidades en Aplicaciones Web

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: https://www.ReYDeS.com -:- e-mail: ReYDeS@gmail.com

Jueves 3 de Noviembre 2022