Webinar Gratuito

Cross-Site Scripting (XSS)

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 12 de Agosto del 2021

Alonso Eduardo Caballero Quezada

EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator Certified, 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.reydes.com

reydes@gmail.com

+51 949 304 030

JavaScript

Es un lenguaje de programación ligero, interpretado, o compilado en tiempo de ejecución, con funciones de primera clase.

Aunque es más conocido como un lenguaje de guiones (scripts) para páginas web, muchos entornos los cuales no son para navegación lo utilizan, como Node.js, Apache CouchDB, o Adobe Acrobat.

JavaScript es un lenguaje basado en prototipos, multi paradigma, imperativo, y declarativo (por ejemplo, programación funcional).

No confundir JavaScript con el lenguaje de programación Java. Los dos lenguajes de programación tienen muy diferente sintaxis, semántica y utilización.

* https://developer.mozilla.org/en-US/docs/Web/JavaScript

Cross-Site Scripting (XSS)

Los ataques de XSS son un tipo de inyección, en el cual guiones (scripts) maliciosos son inyectados dentro de sitios web benigno y confiable.

Ocurren cuando un atacante utiliza una aplicación web para enviar código malicioso, generalmente en la forma de un guion (script) para el lado del navegador, hacia un usuario final diferente.

Las fallas permitiendo estos ataques sean exitosos están ampliamente diseminadas, y ocurren en cualquier aplicación web la cual utilice las entradas de los usuarios dentro de la salida, la cual genera sin validarla o codificarla.

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

Cross-Site Scripting (XSS) (Cont.)

Un atacante puede utilizar un XSS para enviar un guion (script) malicioso hacia un usuario desprevenido.

El navegador del usuario no tiene manera de conocer el guion (script) no es fiable, y ejecutará el guion (script).

Debido al navegador cree el guion (script) proviene desde una fuente fiable, el guion (script) malicioso puede acceder hacia las cookies, tokens de sesión, u otra información sensible retenida por el navegador, y utilizado con este sitio.

Estos guiones (scripts) pueden incluso escribir nuevamente el contenido de una página HTML.

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

Tipos de Cross-Site Scripting

- **XSS Almacenado** (Persistente o Tipo I). Ocurren cuando la entrada de un usuario el almacenada en el servidor, como en una base de datos, en un foro de mensajes, log de visitantes, campo de comentario, etc.

- **XSS Reflejado** (No persistente o Tipo II). Ocurren cuando la entrada de un usuario es retornada inmediatamente por la aplicación web, en un mensaje de error, resultado de búsqueda, o cualquier otra respuesta la cual incluya alguna o toda la entrada proporcionada por el usuario como parte de una petición.

- **XSS basado en DOM** (Tipo 0). Es una forma de XSS en la cual el flujo de datos contaminado, desde la fuente hasta el receptor ocurre en el navegador, es decir la fuente de datos está en el DOM, el receptor también, y el flujo de datos nunca sale del navegador

* https://owasp.org/www-community/Types_of_Cross-Site_Scripting

Técnicas para Detectar XSS

Objetivos de la prueba

- Identificar variables las cuales sean reflejadas en las respuestas
- Evaluar la entrada aceptada, además de la codificación aplicada sobre aquello devuelto (si lo hubiese)

Como Probar

- Detectar vectores de entrada / Formularios de entrada
- Analizar los vectores de entrada / Analizar código HTML
- Verificar el impacto

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/01-Testing_for_Reflected_Cross_Site_Scripting

Curso

Curso Virtual Hacking Aplicaciones Web 2021

Sábados 14, 21, 28 Agosto y 4 Setiembre. 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

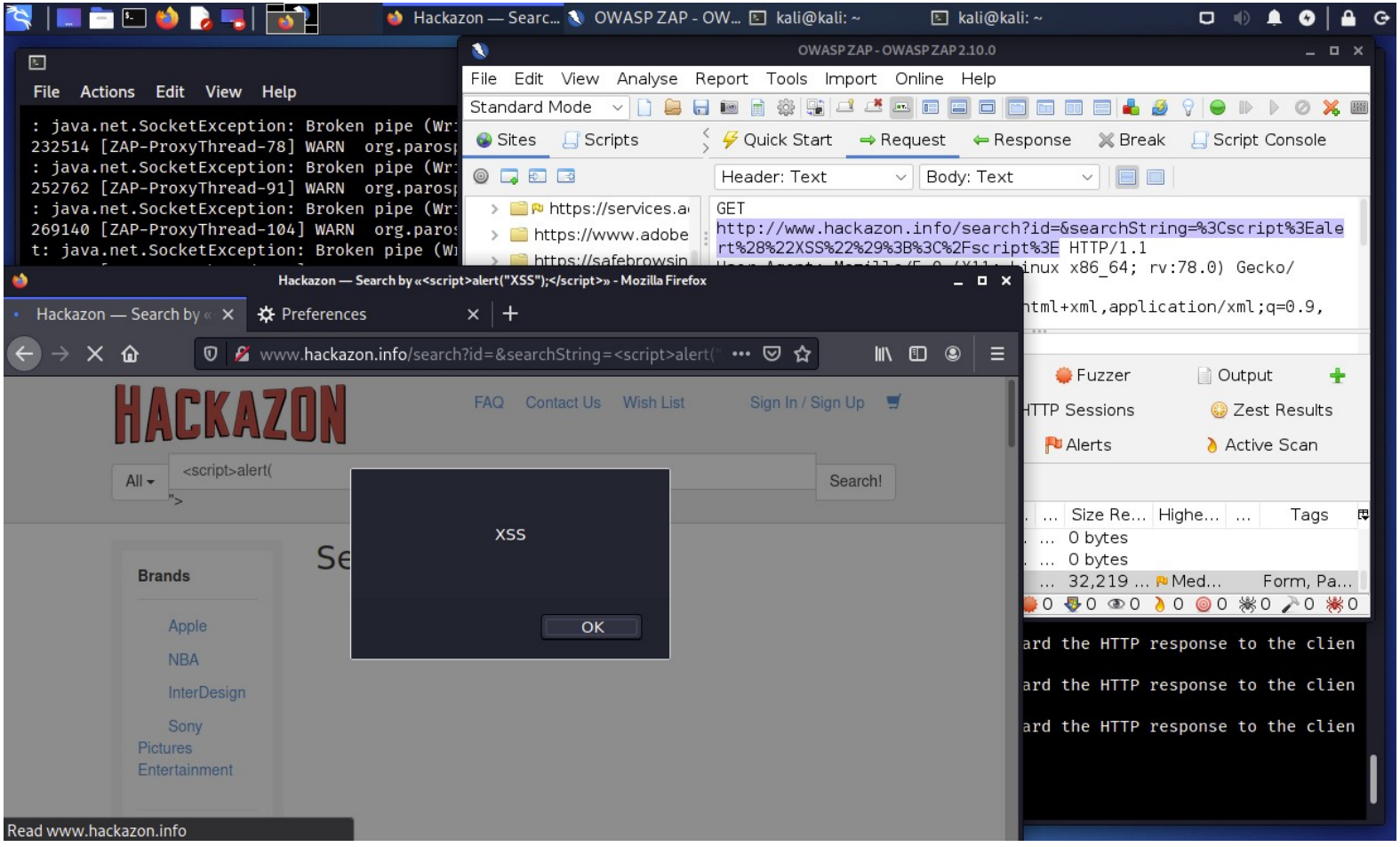
Las aplicaciones web modernas tienen un rol muy importante en todas las organizaciones. Pero si la organización no tiene la capacidad de evaluar y asegurar adecuadamente sus aplicaciones web, los atacantes maliciosos podrían comprometer estas aplicaciones, afectar el funcionamiento normal de la empresa, como también robar datos sensibles. Desafortunadamente muchas organizaciones operan bajo la errada percepción, de confiar el descubrimiento de las fallas en sus sistemas, únicamente a la ejecución de escáneres automáticos de seguridad para aplicaciones web. Consecuentemente se debe entender; no existe un parche o solución total para las aplicaciones web creadas a medida o personalizadas; por lo tanto los atacantes maliciosos se están enfocando cada vez más en este tipo de infraestructura, la cual tiene un gran valor.

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, 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). Ha sido instructor en el OWASP LATAM Tour, expositor en

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

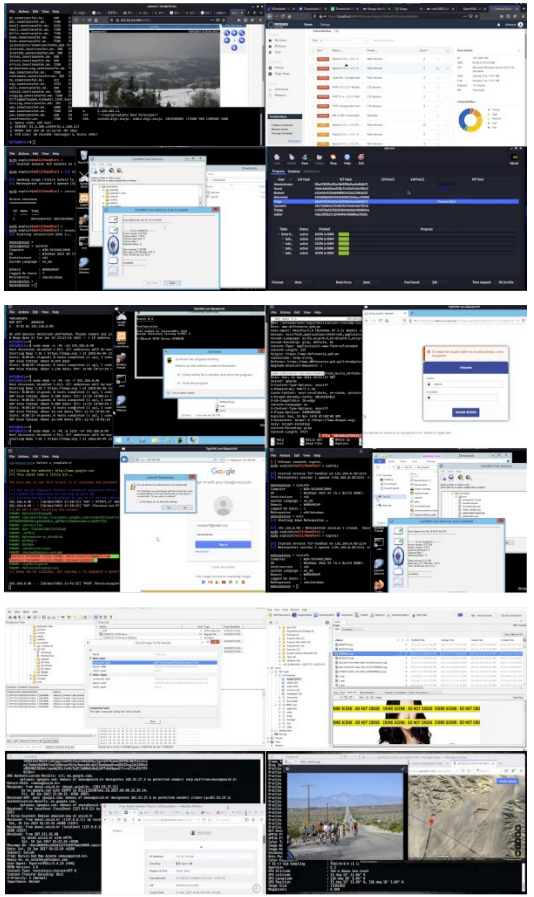
Curso Virtual Hacking con Kali Linux
https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

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 68 webinars gratuitos

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

Diapositivas de los webinars gratuitos

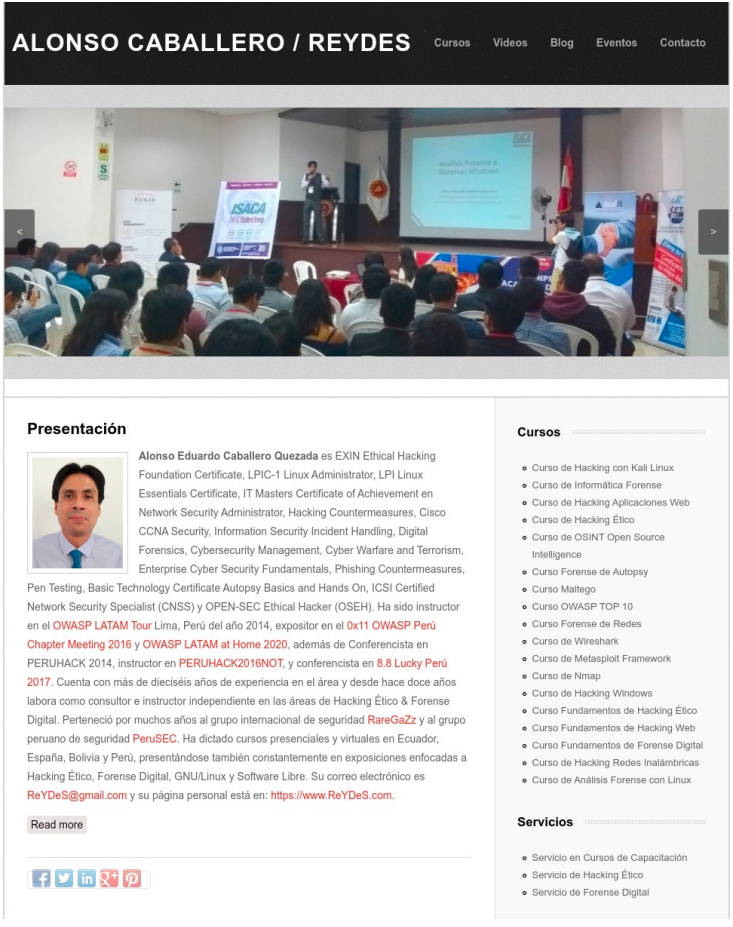
https://www.reydes.com/d/?q=eventos

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

Cross-Site Scripting (XSS)

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 12 de Agosto del 2021