Webinar Gratuito

Inyección SQL

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 4 de Febrero 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

SQL

SQL (Structured Query Language) es un lenguaje estándar para acceder y manipular bases de datos.

SQL puede ejecutar consultas contra una base de datos, obtener datos, insertar registros, actualizar registros, borrar registros, crear nuevas bases de datos, crear nuevas tablas, crear procedimientos almacenados en una base de datos, crear vistas, y ajustar permisos en tablas, procedimientos y vistas.

Para construir un sitio web el cual muestre datos desde una base de datos se necesita; un programa de base de datos, un lenguaje para scripting en el lado del servidor, utilizar SQL para obtener datos, y utilizar HTML / CSS en la página.

* https://www.w3schools.com/sql/sql_intro.asp

Inyección SQL

Implica la inserción o “inyección” de una consulta SQL mediante la entrada de datos desde un cliente hacia la aplicación.

La explotación exitosa de una inyección SQL puede leer datos sensibles desde una base de datos, modificar los datos de la base de datos, ejecutar operaciones de administración sobre la base de datos, recuperar contenido de un archivo presente en el sistema de archivos, y en algunos casos ejecutar comandos a nivel del sistema operativo.

Los ataques de inyección SQL son un tipo de ataque para inyección, en el cual comandos SQL son inyectados dentro de una entrada plana de datos, para poder efectuar la ejecución de comandos SQL predefinidos.

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

Inyección SQL (Cont.)

Los ataques de inyección SQL pueden ser divididos en las siguientes tres clases:

- **Inband:** Los datos se extraen utilizando el mismo canal utilizado para inyectar el código SQL. Es el tipo de ataque más sencillo, en el cual los datos obtenidos son presentados directamente en la página de la aplicación web.

- **Out-of-band:** Los datos son obtenidos utilizando un canal diferente (se genera un correo electrónico con los resultados de la consulta y se envían al profesional)

- **Inferential o Blind:** No existe una transferencia de datos, pero se está en la capacidad de reconstruir la información enviando peticiones particulares y observando el comportamiento resultante del servidor de base de datos.

Técnicas para Detectar Inyecciones SQL

Entender como la aplicación interactúa con el servidor de bases de datos para acceder hacia los datos. Ejemplos típicos donde una aplicación necesita hablar con una base de datos son:

- Formularios para autenticación
- Motores de búsqueda
- Sitios de comercio electrónico

La primera prueba usualmente consiste en añadir una ‘ (comillas simple) o ; (punto y coma). Otra manera es insertar una cadena donde se espera un número.

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05-Testing_for_SQL_Injection

SQLMap

SQLMap es una herramienta para pruebas de penetración, la cual automatiza el proceso de detectar y explotar fallas de inyección SQL, para consecuentemente tomar control de los servidores de bases de datos.

Incorpora un poderoso motor para la detección, ademas de muchas características importantes para los profesionales en pruebas de penetración, como también una amplio espectro de opciones, las cuales permiten desde obtener una huella de la base de datos, obtener datos desde la base de datos, acceder al sistema de archivos subyacente y ejecutar comandos sobre el sistema operativo, mediante conexiones fuera de banda.

* http://sqlmap.org/
* https://github.com/sqlmapproject/sqlmap/wiki

Curso

Curso Virtual Hacking Aplicaciones Web 2021

Domingos 7, 14, 21 y 28 de Febrero del 2021. 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

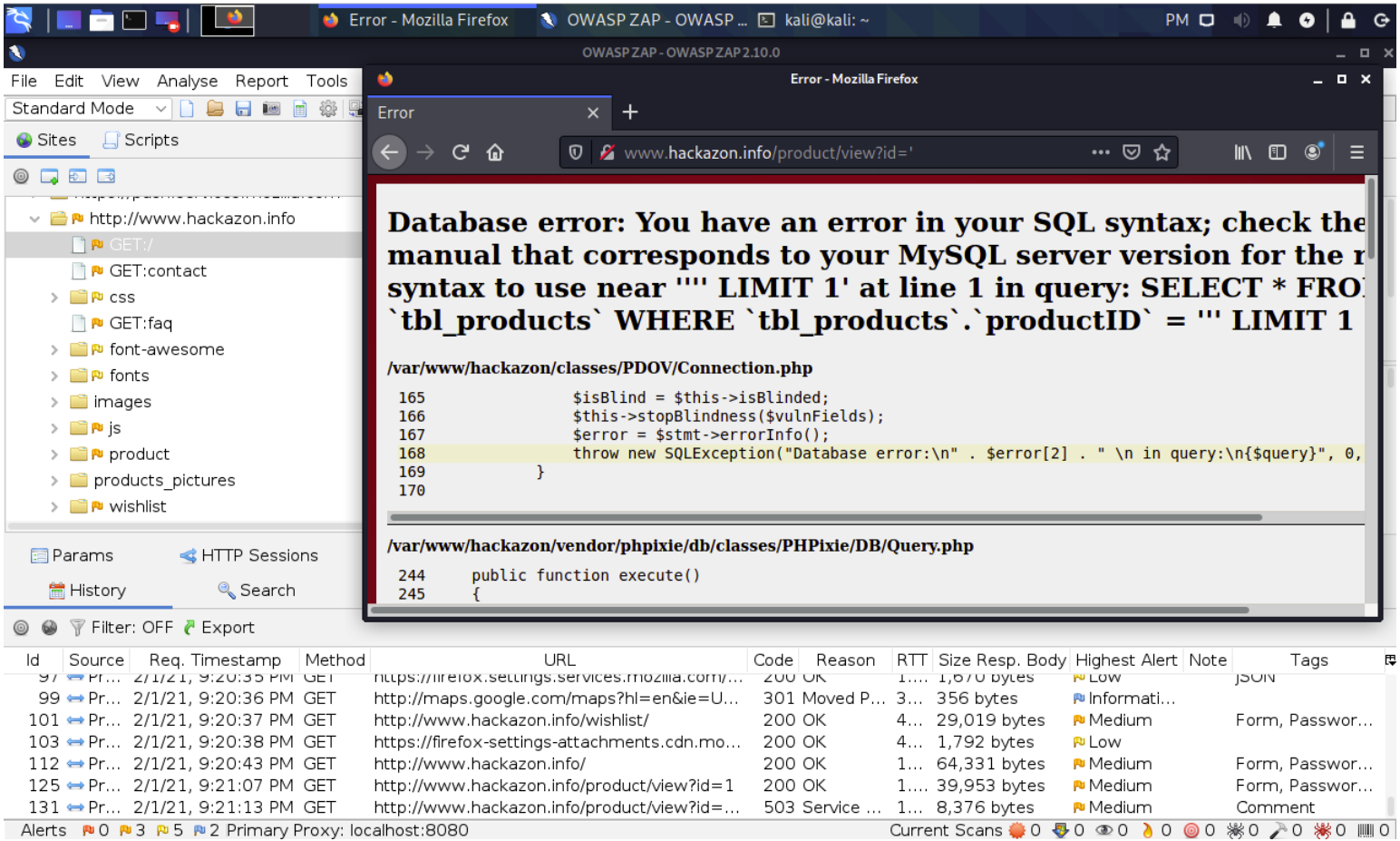
Las aplicaciones web modernas tienen un rol muy importante en todas las organizaciones. Pero si la organización no tiene la capacidad de evaluar y asegurar adecuadamente sus aplicaciones web, los atacantes maliciosos podrían comprometer estas aplicaciones, afectar el funcionamiento normal de la empresa, 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

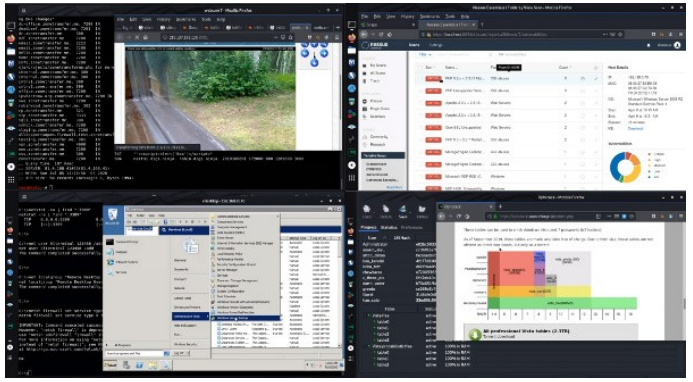
Curso Virtual Hacking con Kali Linux
https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

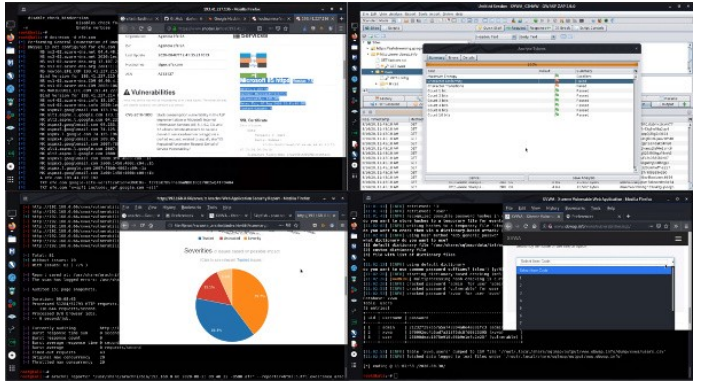
Curso Virtual OSINT - Open Source Intelligence
https://www.reydes.com/d/?q=Curso_de_OSINT

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 63 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

Inyección SQL

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 4 de Febrero del 2021