Webinar Gratuito

Damn Vulnerable Web Application (DVWA)

Alonso Eduardo Caballero Quezada

| Hacking | Forense | Linux | OSINT | Ciberseguridad |

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

Jueves 31 de Julio 2025

Alonso Eduardo Caballero Quezada

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). 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.

Redes Sociales

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

https://x.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

Damn Vulnerable Web Application

DVWA es una aplicación web PHP/MariaDB extremadamente vulnerable. Su meta principal es ayudar a los profesionales en ciberseguridad a probar sus habilidades y herramientas en un entorno legal, ayudar a los desarrolladores web a comprender mejor los procesos de ciberseguridad en aplicaciones web, además de ayudar tanto a estudiantes cuanto a profesores para aprender sobre ciberseguridad de aplicaciones web en un entorno controlado de clase.

El objetivo de DVWA es practicar algunas de las vulnerabilidades web más comunes con diferentes niveles de dificultad, mediante una interfaz sencilla y directa. Tener en consideración este software contiene vulnerabilidades tanto documentadas cuanto no documentadas. Esto es intencional. Se anima a intentar descubrir tantos problemas como sea posible.

* DVWA: https://github.com/digininja/DVWA

¡Advertencia!

¡DVWA es extremadamente vulnerable!. No subirla en una carpeta HTML pública de su proveedor de hosting, ni en ningún servidor con conexión hacia internet, pues serán comprometidos. Se recomienda utilizar una máquina virtual (como VirtualBox o VMware) configurada en modo de red NAT. Dentro de una máquina invitada, también se puede descargar e instalar XAMPP para el servidor web y la base de datos.

Descargo de responsabilidad

Lo creadores no se responsabilizan del uso dado a esta aplicación (DVWA). Se han aclarado los propósitos de la aplicación y no debe utilizarse con fines maliciosos. Se han emitido advertencias y tomado medidas para evitar los usuarios instalen DVWA en servidores web activos. Si el servidor web se compromete debido a la instalación de DVWA, NO es su responsabilidad.

Instalación

El procedimiento de instalación es relativamente sencillo, existiendo la documentación oficial, como también una gran cantidad de videos explicando detalladamente la instalación en diferentes escenarios.

- Instalación Automática (No es un script oficial)
- Windows + XAMPP
- Docker
- Linux (Versiones de PHP, Paquetes de Linux, Módulos de Apache).

* Installation:
https://github.com/digininja/DVWA?tab=readme-ov-file#installation

Configuración

Después de realizar la instalación se requieren realizar algunas configuraciones, para aprovechar todas las funcionalidades y características de DVWA.

- Archivo de configuración
- Configuración con variables de entorno
- Configuración de la base de datos
- Deshabilitar la autenticación (opcional)
- Permisos de carpetas
- Configuración de PHP
- reCAPTCHA
- Credenciales por defecto

* Configurations:
https://github.com/digininja/DVWA?tab=readme-ov-file#configurations

Curso Hacking Aplicaciones Web

Curso Hacking Aplicaciones Web 2025

Domingos 3, 10, 17, y 24 de Agosto 2025. De 9:00 am a 12:00 pm (UTC -05:00)

Las clases en vivo se quedan grabadas en el aula virtual

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.

Objetivos

Este curso enseña a los participantes a entender las principales fallas encontradas en las aplicaciones web, como también a identificar y explotarlas con el propósito de demostrar el potencial impacto hacia la empresa. Los profesionales en seguridad de la información frecuentemente se esfuerzan en ayudar a las organizaciones a entender su riesgo en términos de la empresa. Ejecutar elaborados e impresionantes ataques tiene poco valor si la organización no toma en serio su riesgo, y despliega las medidas correctivas adecuadas. El propósito de este curso es mejorar la seguridad de las organizaciones a través de una prueba de penetración, y no solo demostrar las habilidades de Hacking. Este curso ayuda a los participantes a demostrar el verdadero impacto de las fallas en las aplicaciones web, no únicamente a través de la explotación, sino también a través de una adecuada documentación y reporte.

Fechas y Horarios

Duración:

Catorce (14) horas. Una (1) sesión grabada de dos (2) horas, y cuatro (4) sesiones en vivo de tres (3) horas de duración cada una.

Fechas:

Domingos 3, 10, 17 y 24 de Agosto del 2025

Horarios:

De 9:00 am a 12:00 pm (UTC -05:00)

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), y Codered Certificate of Achievement: Digital Forensics Essentials (DFE) y Ethical Hacking Essentials (EHE). Cuento con más de veintiún años de experiencia en el área, y desde hace diecisiete años laboro como consultor e instructor en 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. Mi correo electrónico es ReYDeS@gmail.com y mi página personal está en: www.ReYDeS.com

Más Información

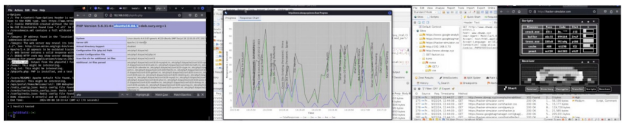
Para obtener más información sobre este curso, tiene a su disposición los siguientes mecanismos de contacto.

Correo electrónico:

reydes@gmail.com

WhatsApp: https://wa.me/51949304030

Sitio Web: www.reydes.com



Temario

- Pruebas Actuales de Seguridad contra Aplicaciones Web
- Pruebas Estáticas y Dinámicas de Seguridad (SAST) y (DAST)
- Metodologías para Prueba de Penetración contra Aplicaciones
- Guía de Pruebas para Seguridad Web
- OWASP Zed Attack Proxy
- DNSRecon
- OSINT
- Google Dorks
- Shodan para Pruebas de Penetración
- Metadatos
- Maltego, TheHarvester
- Encriptar HTTP en Tránsito
- SSL / TLS
- Perfilar el Servidor y Versión del Servidor
- Configuración del Software
- Nikto
- Spidering al Sitio Web
- Páginas por Defecto
- Detección de Tecnologías utilizando ZAP
- Navegación Forzada con ZAP
- Fuzzing con Zed Attack Proxy
- Fuga de Información
- Diferentes tipos de Autenticación
- Recolectar Nombres de Usuario
- Escáneres de Vulnerabilidades
- Tipos de Vulnerabilidades en Aplicaciones Web
- Descubrimiento y Explotación
- Escaneo Activo con Zed Attack Proxy
- Rastreo de Sesión
- Fallas o Defectos de Sesión
- Inyección de Comandos
- Inclusión de Archivo Local y Archivo Remoto
- Recorrido de Directorios
- Inyección SQL
- Meta Información de Base de Datos
- Explotación In-band /Inline
- SQLMap
- XML External Entity (XXE)
- Server Side Request Forgery (SSRF)
- DOM
- Cross Site Scripting (XSS)
- XSS Reflejado, Almacenado y DOM
- Descubrir XSS
- Inyección HTML
- BeEF
- Cross-Site Request Forgery (CSRF)
- Fallas Lógicas

Material

- Kali Linux
- Metasploitable3 (ub1404)
- Hackazon

Beneficios e Inversión

- Acceso al aula virtual por 60 días
- Acceso a las sesiones en vivo
- Video de las cuatro (4) sesiones
- Acceso libre a las sesiones en vivo del siguiente curso a dictarse
- Material utilizado durante el desarrollo del curso
- Dos (2) horas de asesoría en vivo personalizada por videoconferencia
- Libro "Fundamentos de Hacking Web" escrito por el instructor
- Certificado digital de participación
- Certificado digital de aprobación por una duración total de 24 horas

S/. 450 Soles o $ 140 Dólares

El pago del curso se realiza:

Residentes en Perú

Depósito bancario Scotiabank

Cuenta de Ahorros en Soles: 324-0003164
A nombre de: Alonso Eduardo Caballero Quezada

O también pagos con Yape o Plin. Escriba un mensaje a https://wa.me/51949304030 para proporcionarle los datos pertinentes.

Residentes en otros países

Pago a través de Paypal PayPal

O también transferencia de dinero mediante Western Union y MoneyGram

Escriba un mensaje a reydes@gmail.com para proporcionarle los datos.

Confirmado el pago se enviará los datos para conectar su participación en el curso.

Certificados

Certificados; constancias de participación y aprobación; expedidos a nombre de la empresa Peruana MILESEC EIRL.

Sitio Web:

www.reydes.com

Correo:

reydes@gmail.com

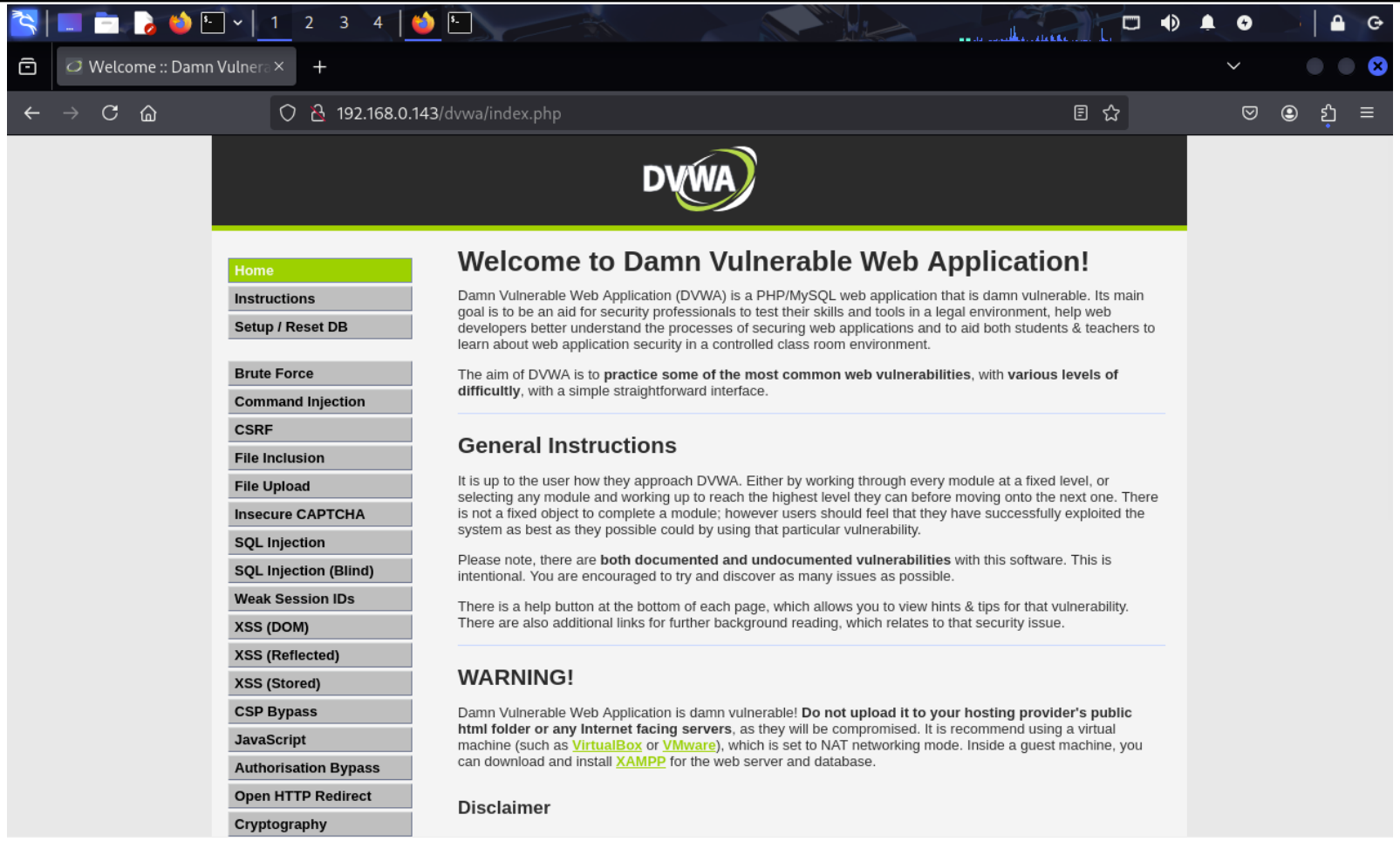
WhatsApp:

https://wa.me/51949304030

Más Información:

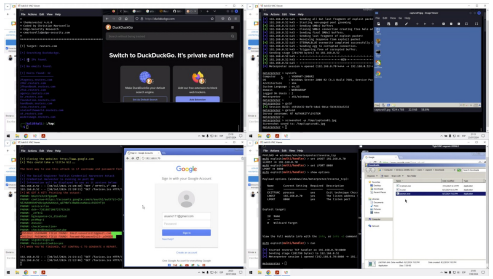
https://www.reydes.com/e/Curso_de_Hacking_Aplicaciones_Web

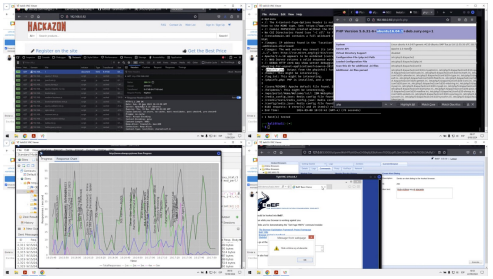
Prácticas

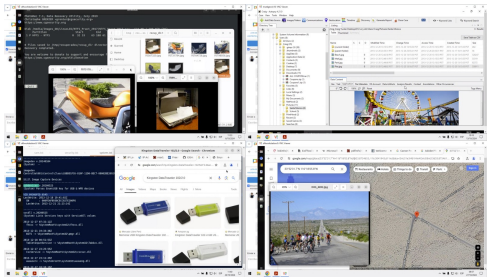

1 2 3 4
Welcome :: Damn Vulner
192.168.0.143/dvwa/index.php
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
Cryptography
Welcome to Damn Vulnerable Web Application!
Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.
The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficultly, with a simple straightforward interface.
General Instructions
It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.
Please note, there are both documented and undocumented vulnerabilities with this software. This is intentional. You are encouraged to try and discover as many issues as possible.
There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.
WARNING!
Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public html folder or any Internet facing servers, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.
Disclaimer

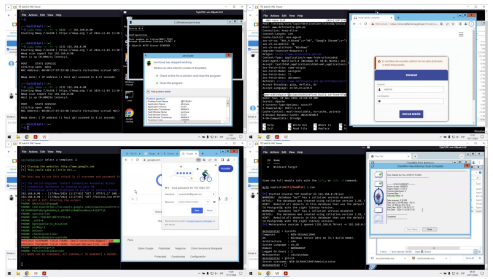
Cursos (Aula Virtual)

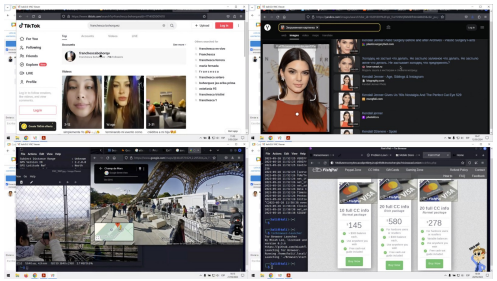
- Curso Hacking Ético
- Curso Hacking Aplicaciones Web
- Curso Informática Forense
- Curso Hacking con Kali Linux
- Curso OSINT - Open Source Intelligence
- Curso Forense de Redes
- Curso CiberSeguridad
- Curso Bug Bounty
- Curso OWASP Top 10
- Curso Análisis de Malware
- Curso Hacking OT
- Curso Maltego CE
- Y más...

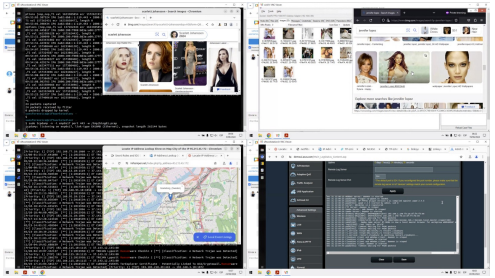












Alonso Eduardo Caballero Quezada :|: Sitio web: www.reydes.com :|: Correo: reydes@gmail.com

Más Contenidos

Videos de webinars

https://www.reydes.com/e/videos

Diapositivas de webinars

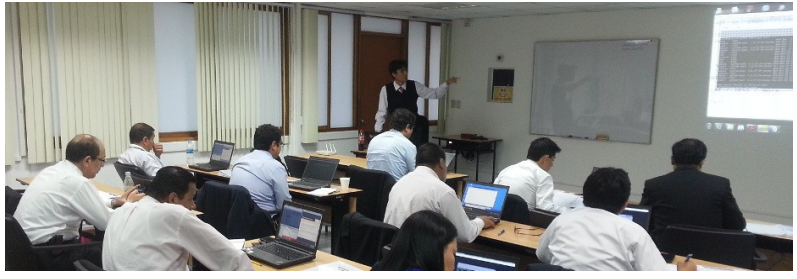
https://www.reydes.com/e/eventos

Libros y artículos

https://www.reydes.com/e/documentos

Blog

https://www.reydes.com/e/blog



Webinar Gratuito

Damn Vulnerable Web Application (DVWA)

Alonso Eduardo Caballero Quezada

| Hacking | Forense | Linux | OSINT | Ciberseguridad |

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

Jueves 31 de Julio 2025