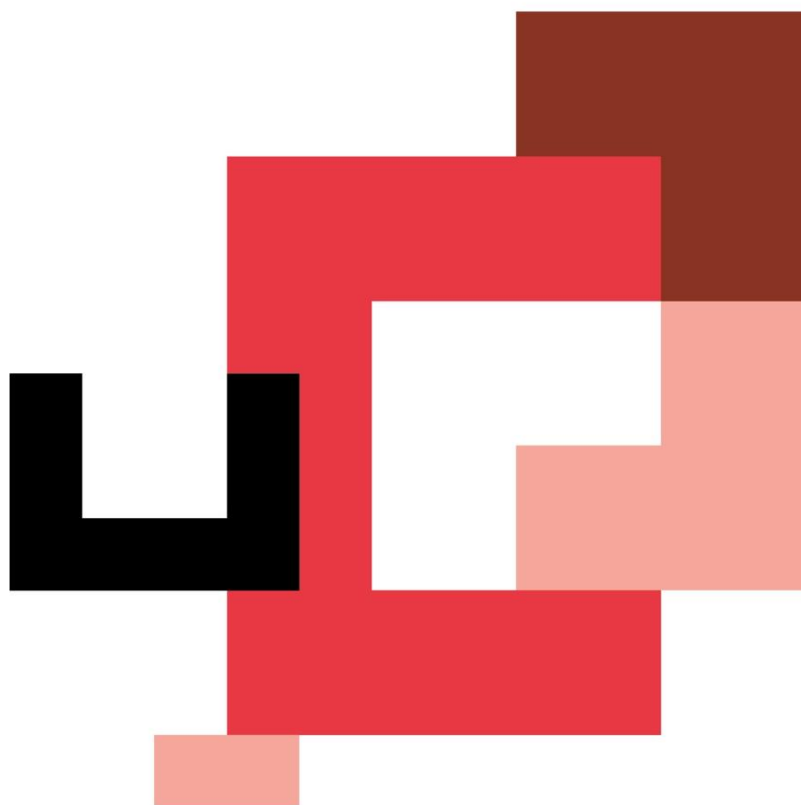




BOOTCAMP

Ciberseguridad en formato online



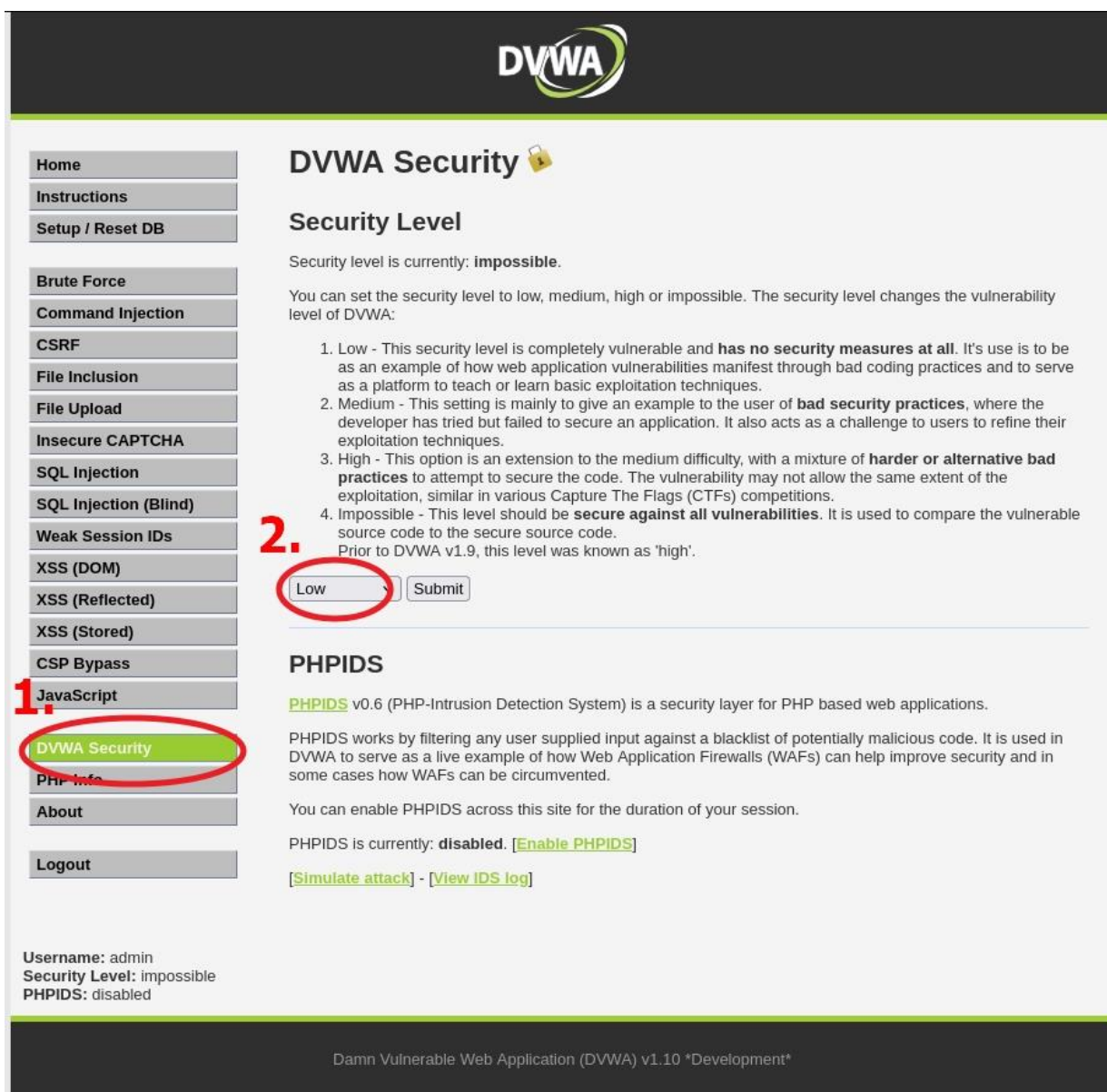
EJERCICIOS SQL Injection

Prerrequisitos

Para esta actividad lo primero que vamos a necesitar es colocar la máquina **vm** y la **Kali** en la misma red, para ello vamos a colocarlas en Red Nat.

Una vez tengamos establecida la configuración de red debemos conectarnos a través de nuestra **Kali** al recurso levantado por la máquina **vm** en el puerto 80.

Una vez accedido al recurso nos dirigimos a cambiar el nivel de la máquina y lo establecemos en **Low**



The screenshot shows the DVWA Security page. On the left is a sidebar menu with various security exercises. 'DVWA Security' is highlighted with a red circle and labeled '1.'. The main content area is titled 'DVWA Security' with a lock icon. Below it is the 'Security Level' section, which states the current level is 'impossible'. It lists four levels: Low, Medium, High, and Impossible. The 'Low' level is selected in a dropdown menu, which is circled in red and labeled '2.'. A 'Submit' button is next to the dropdown. Below the security level section is the 'PHPIDS' section, which states it is currently disabled and provides links to enable it, simulate an attack, or view the IDS log. At the bottom, the footer shows the username 'admin', security level 'impossible', and PHPIDS status 'disabled'.


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
1. JavaScript
2. DVWA Security
PHP Info
About
Logout

Username: admin
Security Level: impossible
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.10 *Development*

Después nos dirigimos al recurso de **SQL Injection**



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

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection

User ID:

More Information

- <http://www.securiteam.com/securityreviews/SDP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-okw/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>

Username: admin

Security Level: impossible

PHPIDS: disabled

View Source

View Help

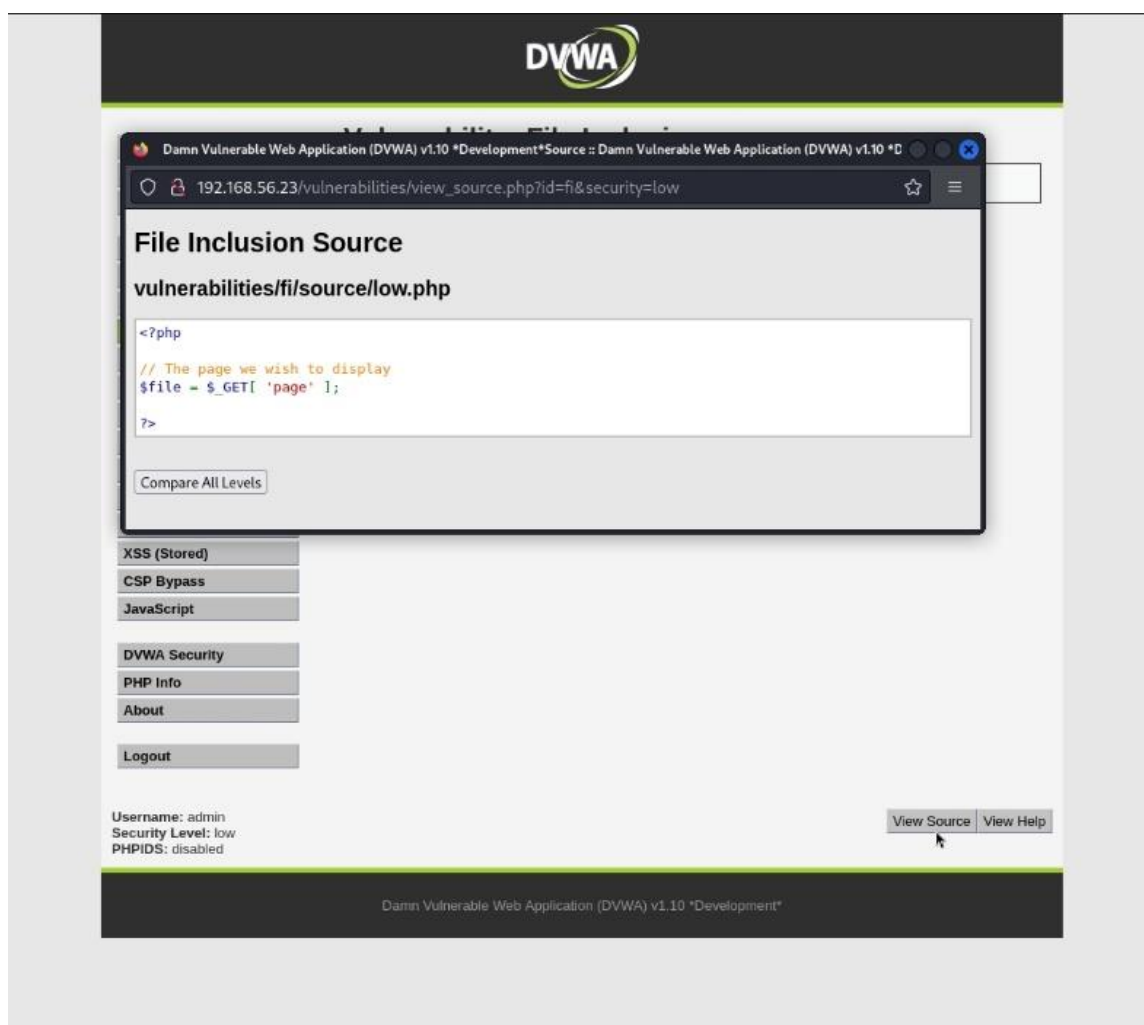
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

Y ya estaríamos listos para comenzar el challenge.

Ejercicio

Para esta actividad debes conseguir vulnerar la aplicación web en el nivel **Low y Medium**, obteniendo las credenciales de los 5 usuarios que hay en la base de datos de la DVWA.

Como pista recordarte que puedes ver el código que hay por detrás de la aplicación y así analizar la vulnerabilidad en particular pulsando, como se muestra en la imagen, en el botón **View Source**.



El informe a presentar debe constar; a parte de la explicación y subsanación de la vulnerabilidad, de aportaciones visuales que permitan revelar la explotación de dicha vulnerabilidad.



THE BRIDGE

