



# **BOOTCAMP**

## **Ciberseguridad en formato online**



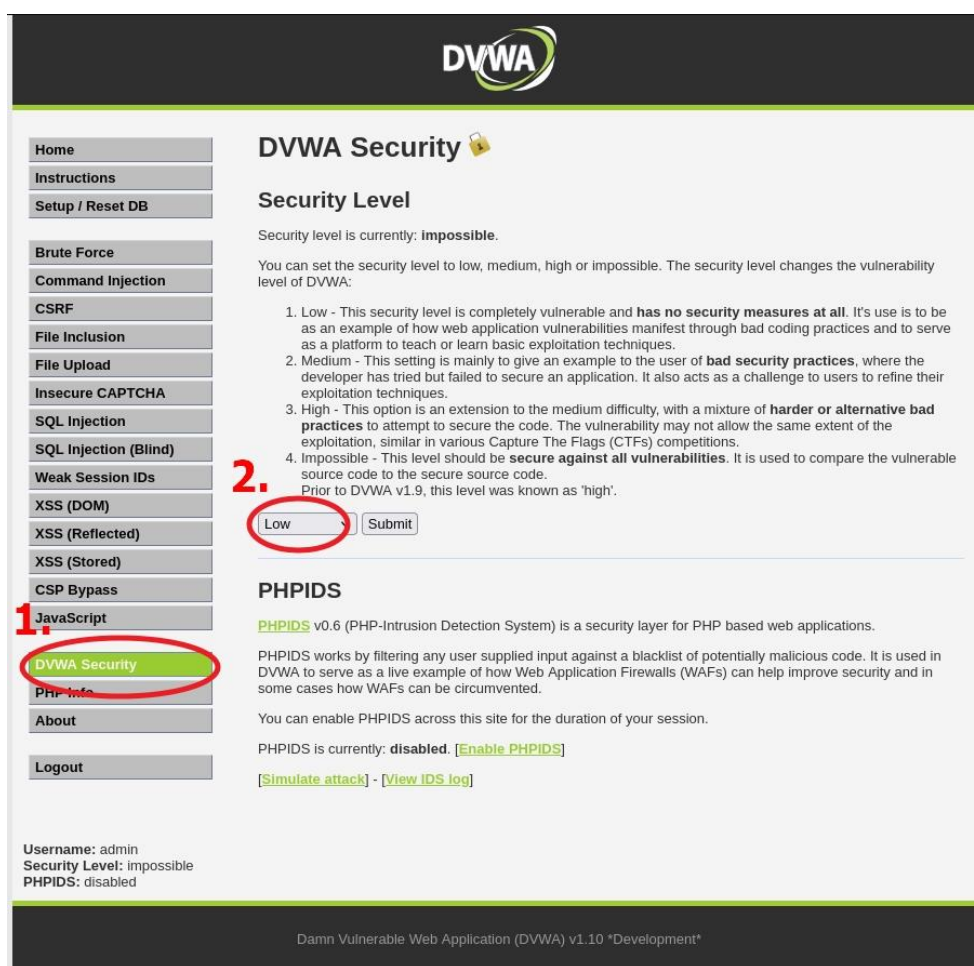
# EJERCICIOS LOCAL FILE INCLUSION Y REMOTE FILE INCLUSION

## Prerrequisitos

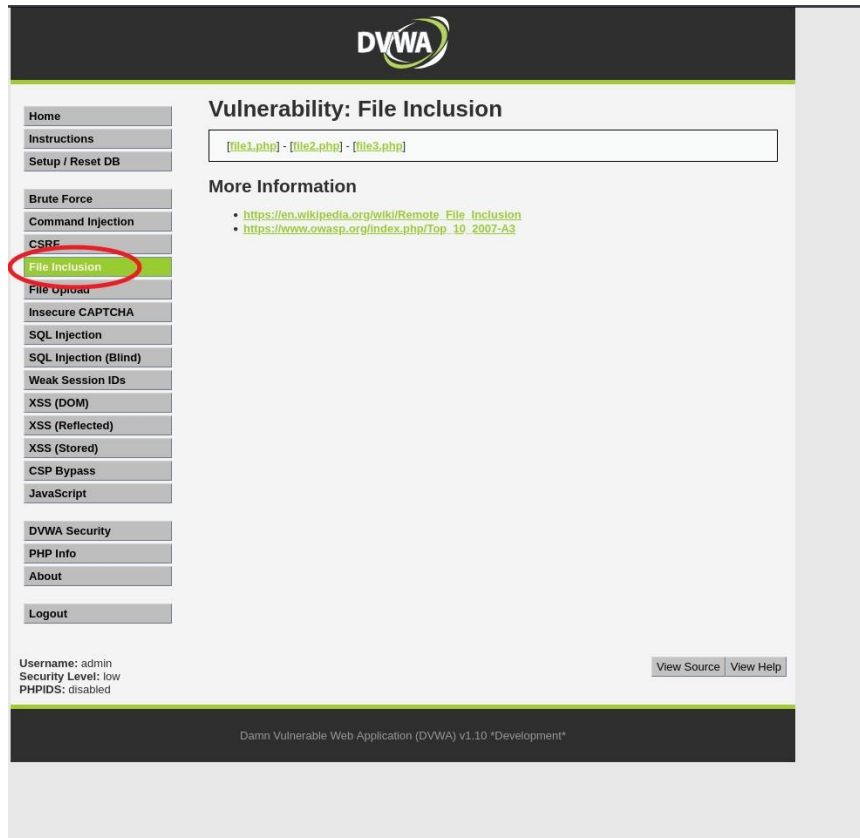
Para esta actividad lo primero que vamos a necesitar es colocar la máquina **vm** y la **Kali** en la misma red, para ello vamos a colocarlas en Red Nat.

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**



Después nos dirigimos al recurso de **File Inclusion**



**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

DVWA Security  
PHP Info  
About  
Logout

Username: admin  
Security Level: low  
PHPIDS: disabled

**Vulnerability: File Inclusion**

[file1.php] - [file2.php] - [file3.php]

**More Information**

- [https://en.wikipedia.org/wiki/Remote\\_File\\_Inclusion](https://en.wikipedia.org/wiki/Remote_File_Inclusion)
- [https://www.owasp.org/index.php/Top\\_10\\_2007-A3](https://www.owasp.org/index.php/Top_10_2007-A3)

View Source View Help

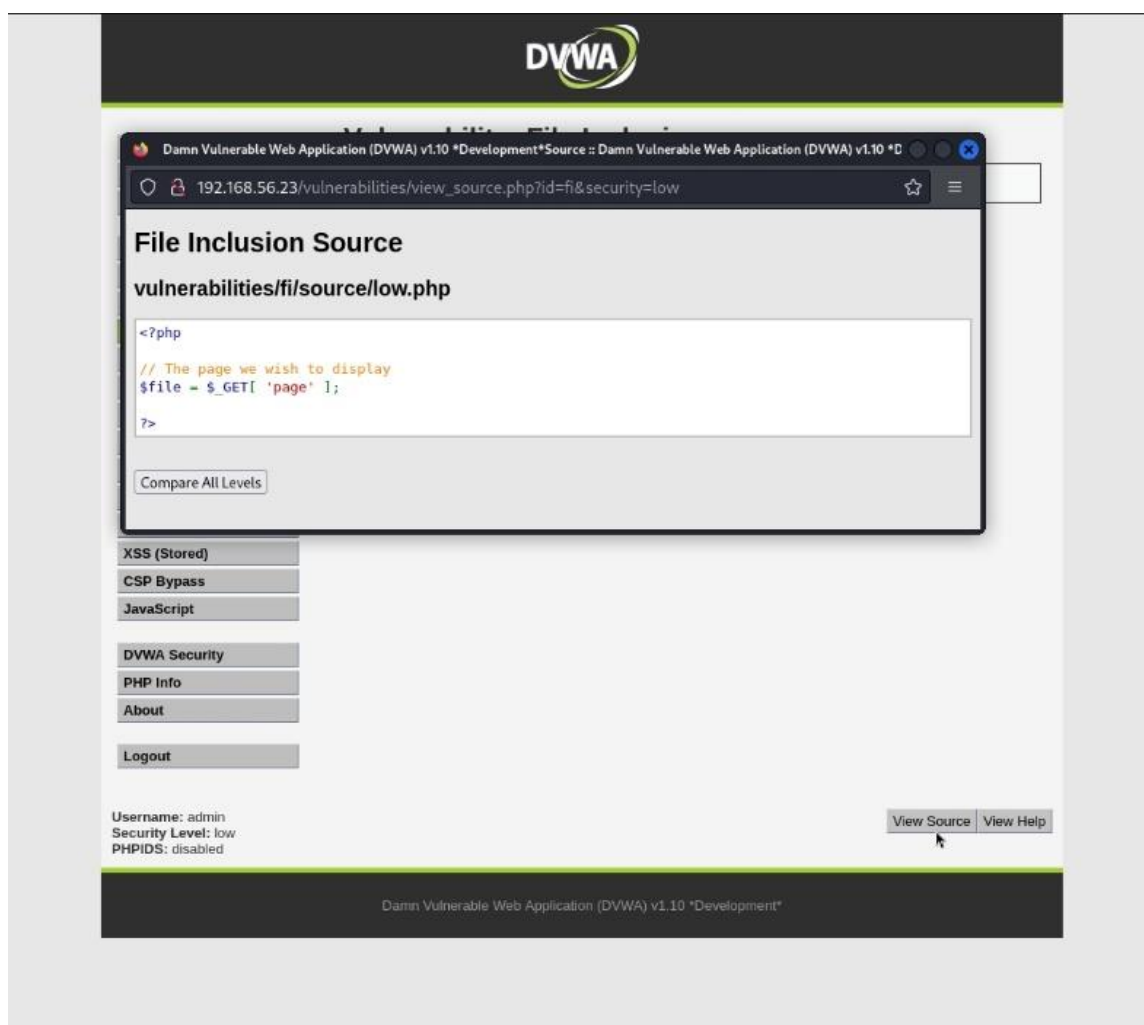
Damn Vulnerable Web Application (DVWA) v1.10 "Development"

Y ya estaríamos listos para comenzar el challenge.

## Ejercicio

Para esta actividad debes realizar un informe explicando la vulnerabilidad presentada en el nivel **Low y Medium**, explicando cómo es que se produce la vulnerabilidad y las recomendaciones pertinentes para solucionar la vulnerabilidad.

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**

