**Instal·lació i Explotació de Vulnerabilitats a DVWA**

**1. Objectius de la Pràctica**

* Aprendre a instal·lar i configurar DVWA (Damn Vulnerable Web Application) en un entorn Kali Linux.
* Entendre els diferents nivells de seguretat de DVWA i com afecten la dificultat d’explotació de vulnerabilitats.
* Practicar l’explotació de vulnerabilitats típiques (SQL Injection, XSS, Command Injection, Brute Force).
* Reflexionar sobre els mecanismes de mitigació i les millors pràctiques de seguretat per aplicacions web.

**2. Preparació de l’entorn**

1. Actualitzar el sistema:

**sudo apt update**

1. Instal·lar el paquet LAMP (Linux, Apache, MySQL, PHP):

**sudo apt install apache2 mariadb-server php php-mysql libapache2-mod-php -y**

1. Iniciar i habilitar els serveis per arrencar amb el sistema:

**sudo systemctl start apache2**

**sudo systemctl start mariadb**

**sudo systemctl enable apache2**

**sudo systemctl enable mariadb**

**3. Instal·lació de DVWA**

1. Descarregar DVWA:

**cd /var/www/html**

**sudo git clone https://github.com/digininja/DVWA.git**

1. Configurar permisos i fitxer de configuració:

**cd DVWA**

**sudo cp config/config.inc.php.dist config/config.inc.php**

**sudo chown -R www-data:www-data /var/www/html/DVWA/**

**sudo chmod -R 755 /var/www/html/DVWA/**

1. Configurar la base de dades:

**sudo mysql**

**CREATE DATABASE dvwa;**

**CREATE USER 'dvwauser'@'localhost' IDENTIFIED BY 'password';**

**GRANT ALL PRIVILEGES ON dvwa.\* TO 'dvwauser'@'localhost';**

**FLUSH PRIVILEGES;**

**EXIT;**

Copieu l’arxiu de configuració

**cd /var/www/html/DVWA/config**

**sudo cp config.inc.php.dist config.inc.php**

Assegureu-vos de tenir:

**$\_DVWA[ 'db\_database' ] = getenv('DB\_DATABASE') ?: 'dvwa';**

**$\_DVWA[ 'db\_user' ] = getenv('DB\_USER') ?: 'dvwauser';**

**$\_DVWA[ 'db\_password' ] = getenv('DB\_PASSWORD') ?: 'password';**

1. Inicialitzar DVWA a través del navegador:
	* Obriu: <http://localhost/DVWA/setup.php>
	* Feu clic a “Create/Reset Database”.
	* Un cop fet, accediu a <http://localhost/DVWA/>

Credencials per defecte:
**Usuari: admin
Contrasenya: password**

**4. Explotació de Vulnerabilitats**

A DVWA trobareu diferents seccions, cadascuna amb una vulnerabilitat:

* SQL Injection: Proveu a fer consultes manipulades, per exemple: **' OR '1'='1**
* XSS (Reflected/Stored): Introduïu **<script>alert('XSS')</script>** en un camp d’entrada i observeu el resultat.
* Command Injection: Proveu **8.8.8.8; ls** per executar comandes al servidor.
* Brute Force: Utilitzeu eines com **hydra** per atacar la pàgina d’inici de sessió.

Canvi de nivell de seguretat: Aneu a “DVWA Security” i canvieu el nivell a Low, Medium, High per veure com la dificultat i les proteccions varien.

**5. Anàlisi i Reflexió**

* Documenteu les vulnerabilitats trobades i les tècniques d’explotació utilitzades.
* Compareu el comportament de DVWA en diferents nivells de seguretat.
* Proposeu mesures de seguretat per a cada vulnerabilitat (prepared statements, filtratge d’entrada, tokens CSRF, etc.).

**6. Lliurament**

* Un document on es detallin:
	+ Les passes d’instal·lació i configuració.
	+ Les vulnerabilitats explotades i resultats obtinguts.
	+ Les mesures de mitigació proposades.