# DVWA Penetration Testing Report

Conducted by: **Riddhi Bagri**

Under the guidance of: **Vansh Damania**

## Introduction:

License: DVWA is a free software coded in PHP and has MySQL backend database

Warning: DVWA is damn vulnerable web application, run it in an isolated environment/network

Scope: Training and Security testing (penetration testing)

## Accessing DVWA:

-Install Oracle VM VirtualBox

-Install Kali Linux machine on VM VirtualBox

By Default: Username=kali, Password=kali

-Install Docker on Kali machine and accessing DVWA using command following commands in command prompt :

1. sudo apt update
2. sudo apt install –y docker.io
3. sudo systemctl enable docker --now
4. sudo usermod –aG docker $USER
   Logout and Re-login kali linux
5. newgrp docker
6. docker run –rm –it –p 80:80 vulnerables/web-dvwa
   Go to Firefox and open local host 127.0.0.1
   By Default: Username=admin, Password=password
   Create a new database and login again

## Vulnerabilities found:

By setting the difficulty to low, following vulnerabilities were detected.

### <u>**Vulnerability 1**</u>: <u>File Inclusion</u>

-Level: Easy.

-Steps:

- Click on File Inclusion and go to search tab, change the localhost/dvwa/vulnerabilities/fi/?page=include.php to localhost/dvwa/vulnerabilities/fi/?page=../../../../../../proc/version localhost/dvwa/vulnerabilities/fi/?page=../../../../../../etc/passwd
- Required codes will be displayed on top of DVWA page

-Learning: There are two types of file inclusion-Local File Inclusion, Remote file Inclusion. Remote File inclusion (RFI) and Local File Inclusion (LFI) are vulnerabilities that are often found in poorly-written web applications. These vulnerabilities occur when a web application allows the user to submit input into files or upload files to the server and exploit the information.

-Possible ways to mitigate can be to prevent users from passing input into the file systems and make a whitelist of acceptable inputs and allowable file extensions.

## **Vulnerability 2**: SQL Injection

-Level: Easy.

-Steps:

- Click on SQL Injection and type 1' which shows error in SQL database which implies it can be injected.
- Type this command will extract database version and database name:
  1 and 1=1 union all select @@version,database() from information_schema.tables# ,
- Hash passwords will be displayed, Un-hash the password corresponding to admin using John the Ripper.

-Learning: Allows an attacker to provide an input containing SQL statements to modify the output in a way to retrieve desired data from the database. This vulnerability in the application is termed as SQL injection. With this vulnerability, an attacker can dump entire data from the database accessible to the user.

-Possible ways to mitigate can be to use parameterised queries in SQL.

## **Vulnerability 3:** XSS (cross-site)

-Level: Easy.

-Steps: Click on XSS Reflected and type following:

- <script>alert("xss")</script>
  A message will be appread "xss", click OK to continue
- <script>alert("Hack by Riddhi")</script>
  A message will be appread "Hack by Riddhi", click OK to continue

-Learning: If a website allows users to input data like comment, username field and email address field then attacker can insert their own malicious code and exploit it. XSS is executed only on the victim side. In, reflected cross-site scripting an attacker sends input script website that is then reflected back to the victim’s browser and all the information is exploited.

-Possible ways to mitigate can be to make users aware of such attacks stopping them to click on unwanted links.

**Note:** Also learnt to use BurpSuite and explored **BruteForce vulnerability** (which is hit and trial method in a list of usernames and passwords which reflects whose length is huge that is correct information) in DVWA using it on Kali Linux.