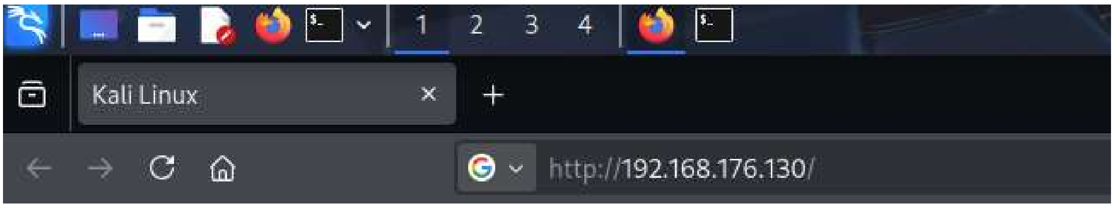
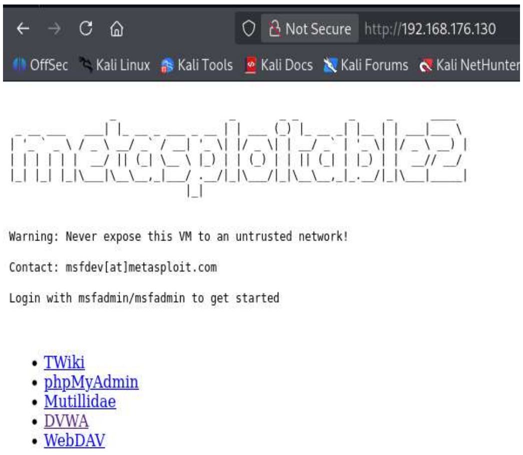
Instructions:-

1.First we should download vmware or virtual box from official websites.
2.Download kali linux and metasploitable 2 (vulnerable machine)
3.Install kali and metasploitable 2 machine one by one on vmware or virtual box
4.run the both kali and metasploitable machine and login the metasploitable machine with default username and password
5.Metasploitable machine Default username and password is msfadmin:msfadmin
6.after login check the metasploitable ip address using "ifconfig" command and note that ip address
7.login the kali linux, then open the terminal and type the command sudo apt update && sudo apt upgrade -y
8.configure foxyproxy with browser, after that run "burp" command in terminal.
9.Now burpsuite will open and run burpsuite
10.open the browser and type http://put your metasploitable ip address



http://192.168.176.130/

11. click dvwa, now it will show dvwa login page



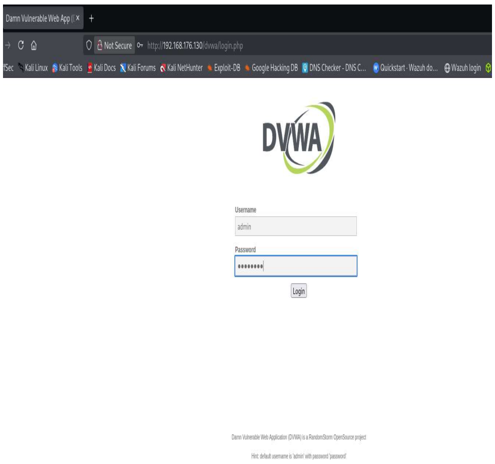
http://192.168.176.130

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV



http://192.168.176.130/dvwa/login.php

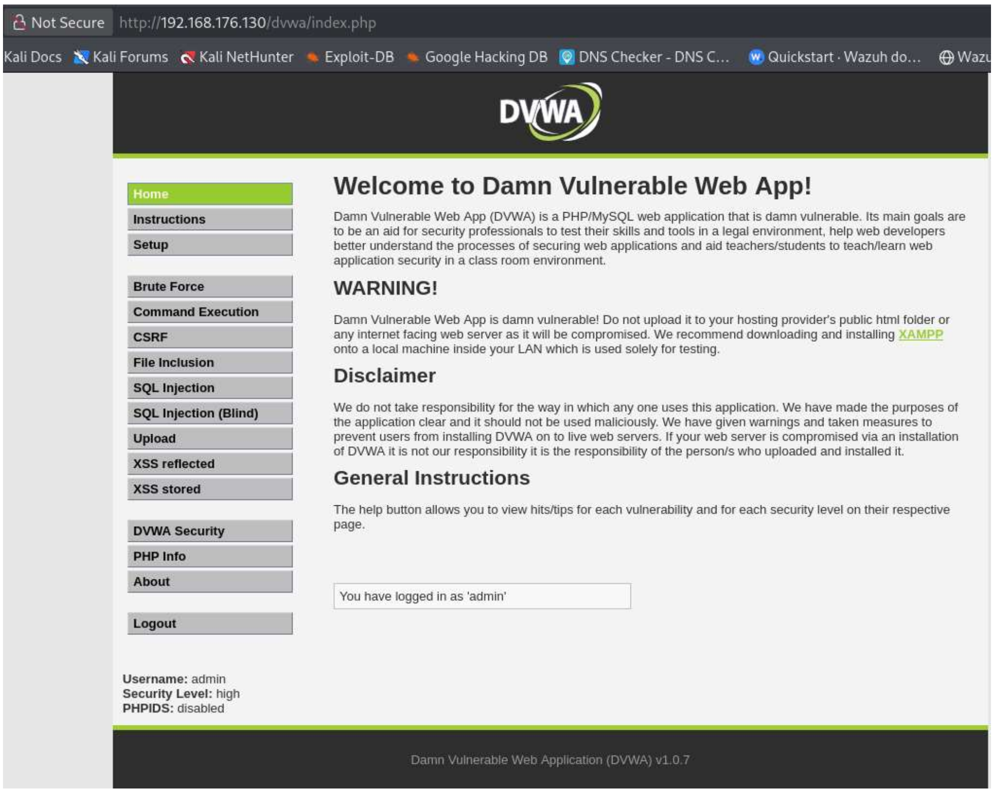
Username: admin

Password: ••••••••

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'

12.login with default username and password. Default username and password is admin:password
13.Now it shows more vulnerablity names like brute force, command execution, sqlinjection, fileinclusion and more…



Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are 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 aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

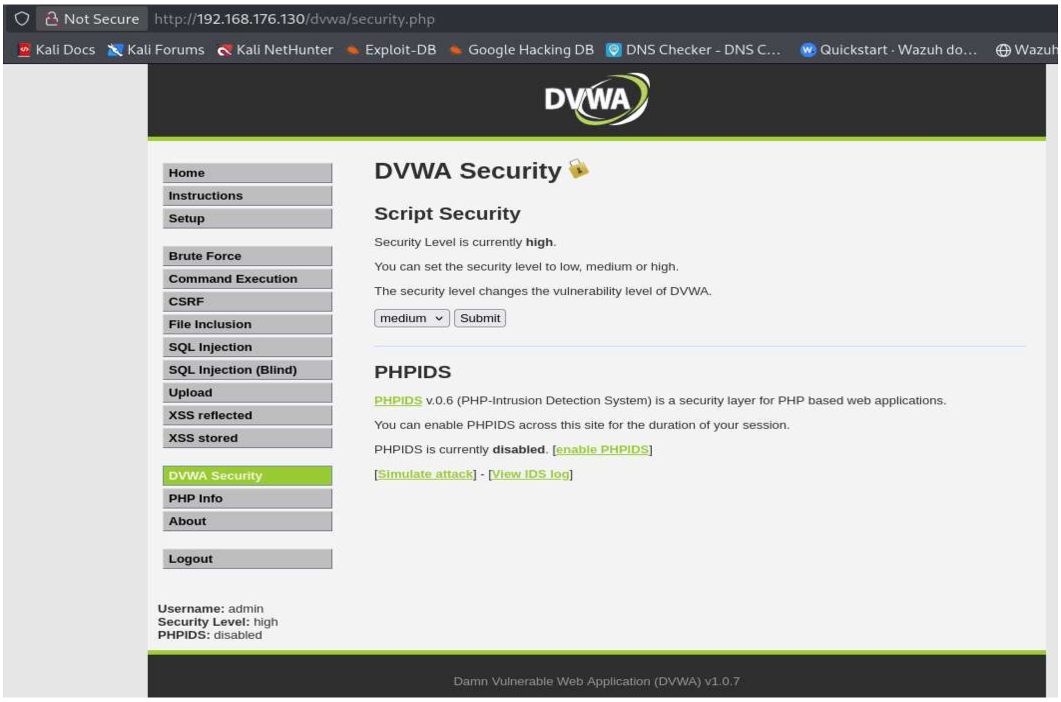
The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

Username: admin
Security Level: high
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

14. Before we do vulnerability analysis, we should set DVWA Security level, so click DVWA Security icon



DVWA Security

Script Security

Security Level is currently **high**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]

Username: admin
Security Level: high
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

15. We can choose security level low, medium, high whatever you want.
16. Before you implement security testing, you should search and download some payloads and files like sql injection cheatsheet, command injection cheatsheet using browser
17. I just showed some payloads into the DVWA Report pdf file. Check it