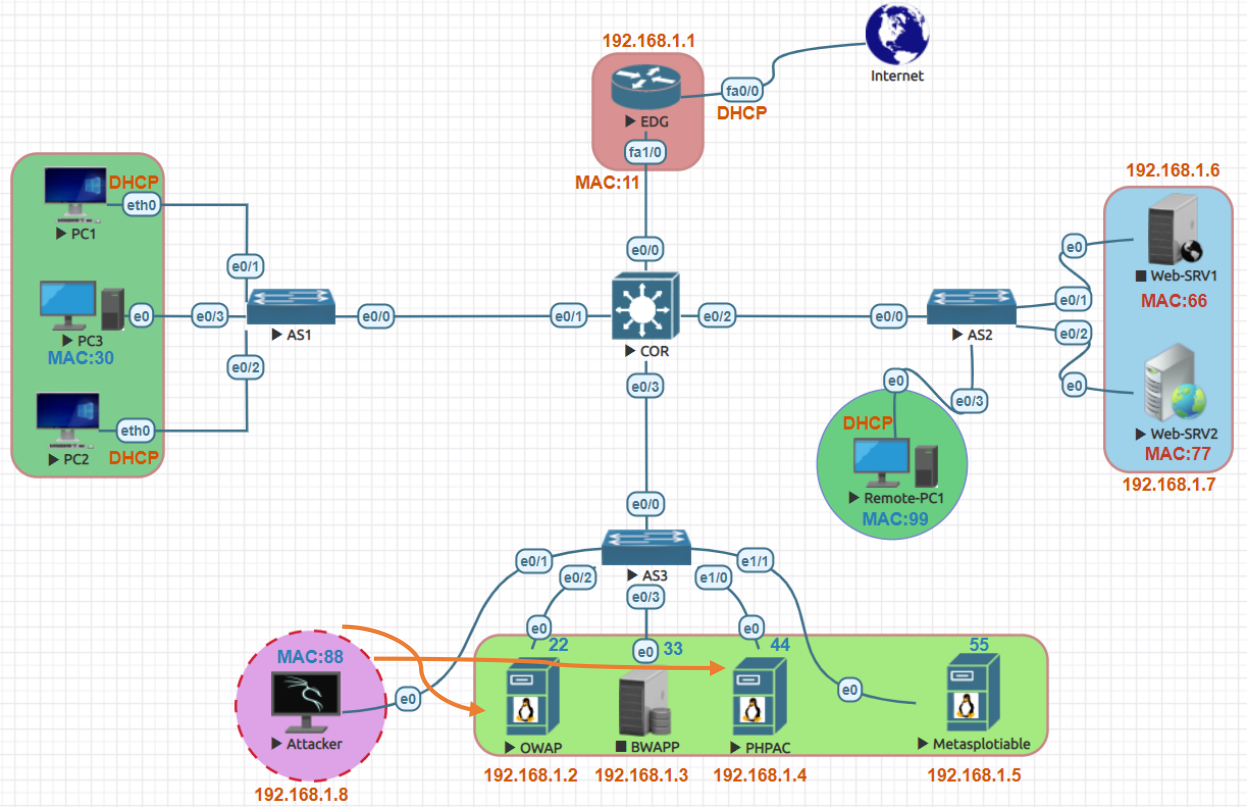
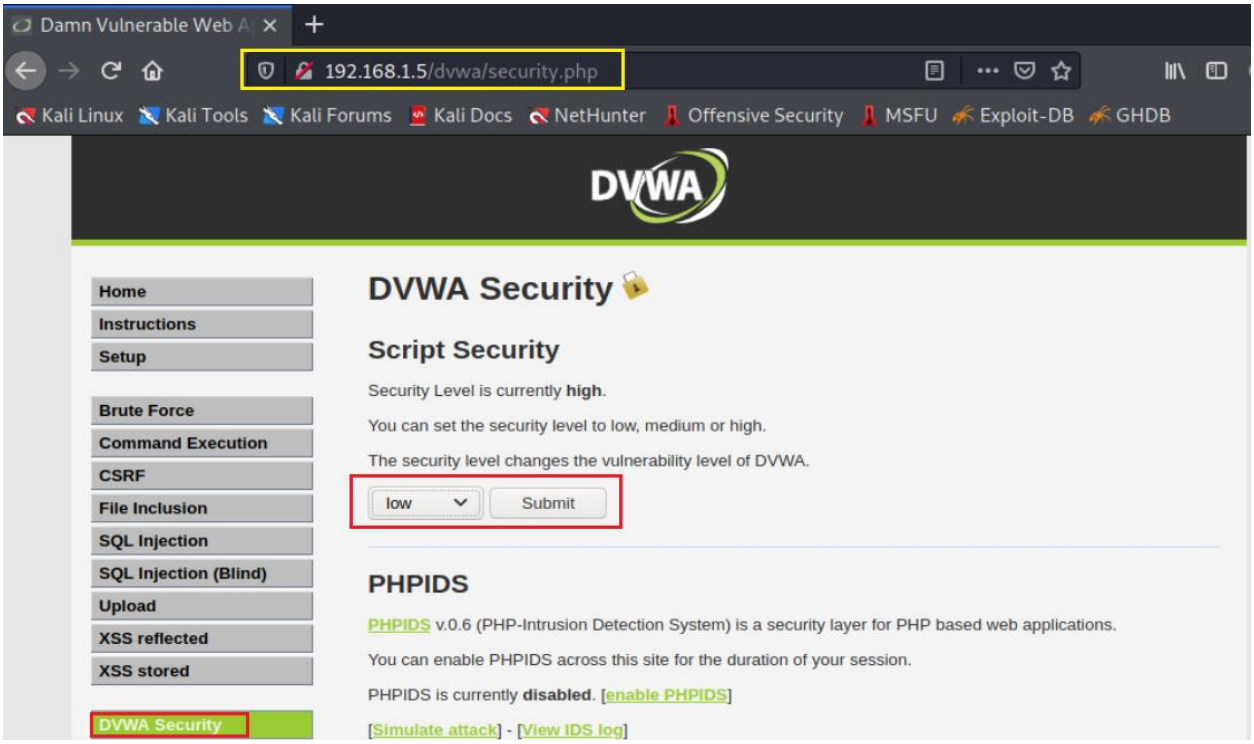
Command Injection Attack:



OWAP IP Address
192.168.1.2
Metasplotiable IP Address
192.168.1.5
Attacker IP Address
192.168.1.8

Attacker
Command Injection
DVWA

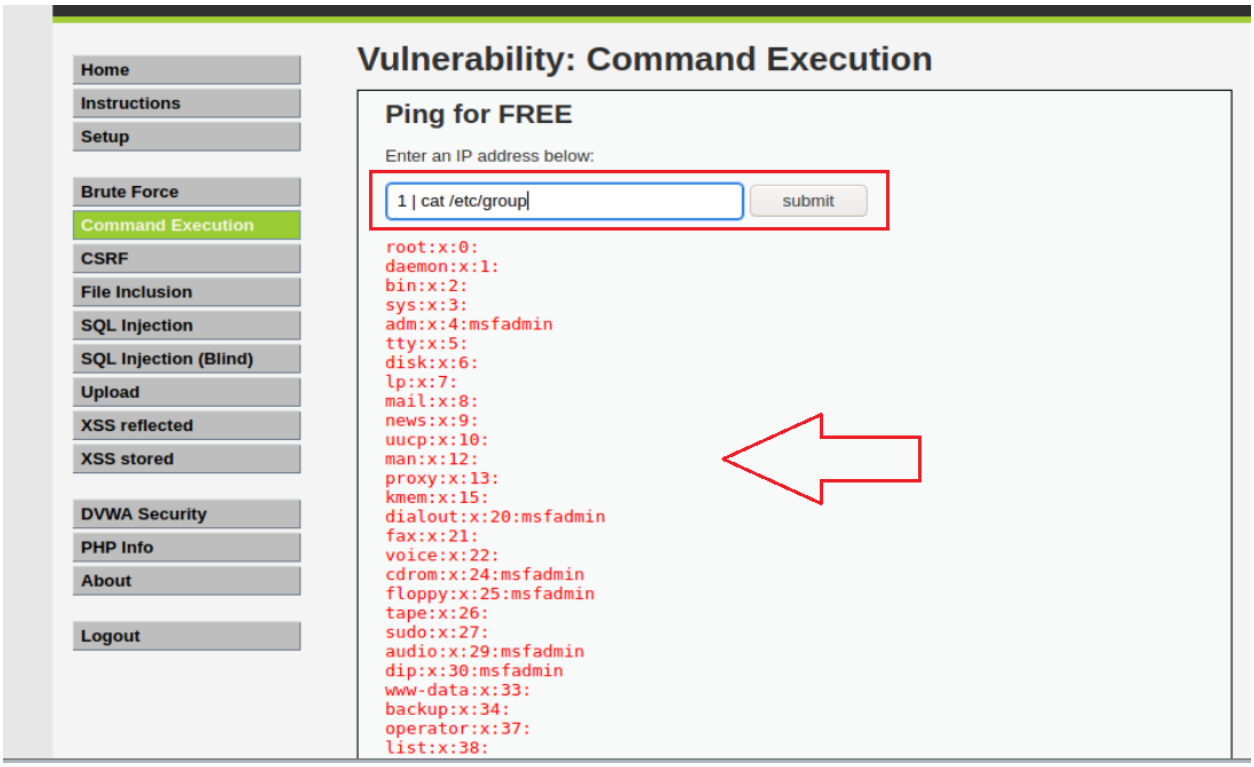
Open Metasplotiable Server. Open your browser and enter the required URL 192.168.1.5/dvwa/login.php Log in using the username “admin” and password as “password”. These are the default DVWA login credentials. After a successful login, set the DVWA security to LOW then click on Command Execution on the left-side menu.



We can also execute multiple commands at one time just by using the & sign. type the command 1 | pwd & whoami & ps which it will give us the following result

We can also use the command 1 | uname -a & users & id & w for discovering the hostname, the users that are logged in.

We can use the 1 | cat /etc/group in order to display information about the user groups and its members on the target system.



Always in Linux-based operating systems we want to display the contents of /etc/passwd file because we can find information about the users.