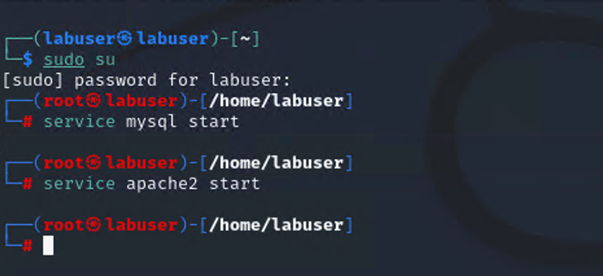
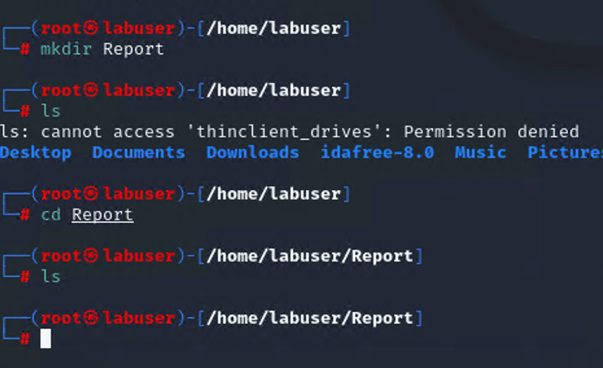
**Step1: To scanning DVWA using NMAP**

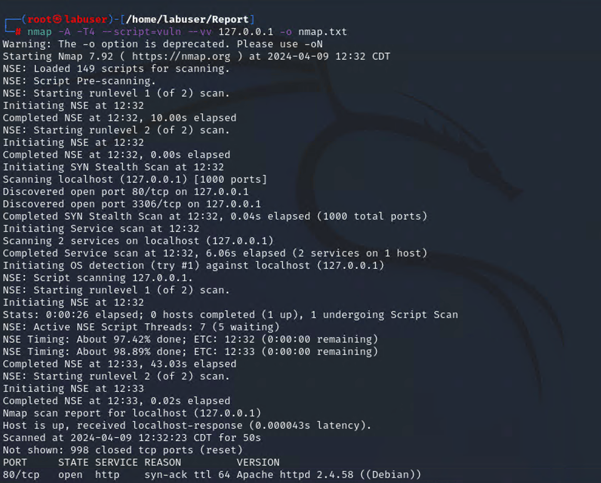
Step 1: Scan DVWA using NMAP:



Make directory to perform tasks:



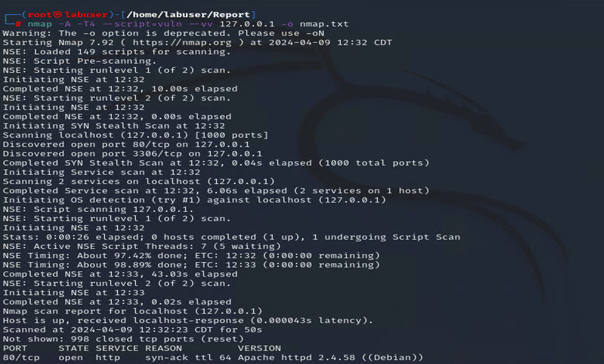
Step 2: Run the nmap scan on dvwa website using nmap, this will act as a scanning phase for any vulnerability assessment:



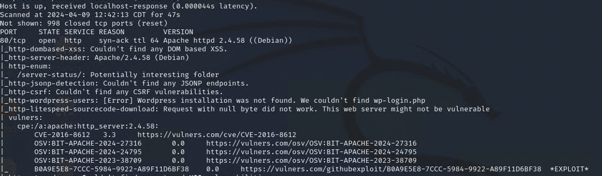
We have stored the results in nmap.txt file.

**Task 2: To perform vulnerability script scan from Nmap to catch CVE on the website;**

Step 1: Run the nmap scan on dvwa website using nmap, this will act as a scanning phase for any vulnerability assessment:



Step2: The result is shown below, which shows CVE of vulnerabilities available:

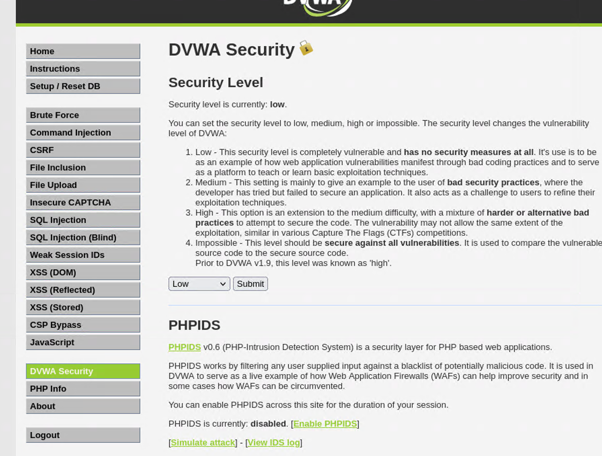


**Step 3: To perform Brute-Force attack on website**

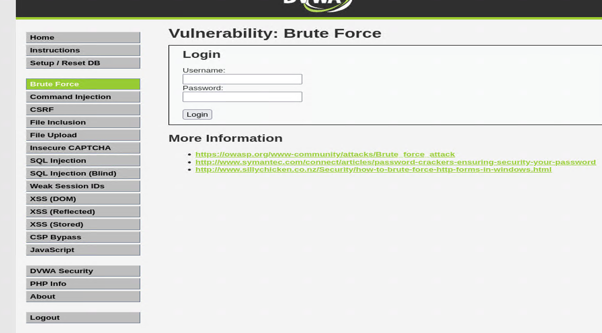
Step1: Login to dvwa website using admin and password credentions:



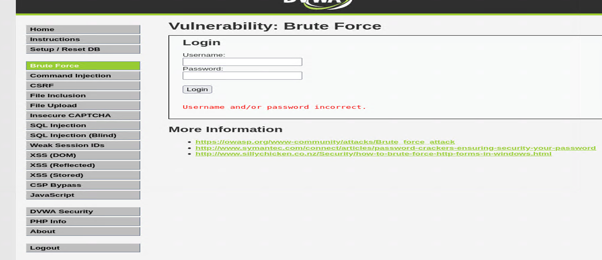
Step2: Set the DVWA security to low:



Step3: Switch to brute force tab:



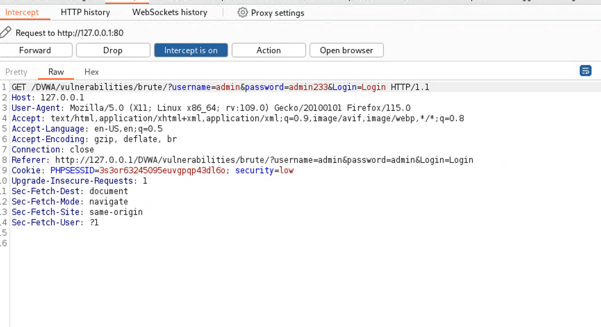
Step4: Try to login using admin and admin:



Step5: Start foxy proxy extension:



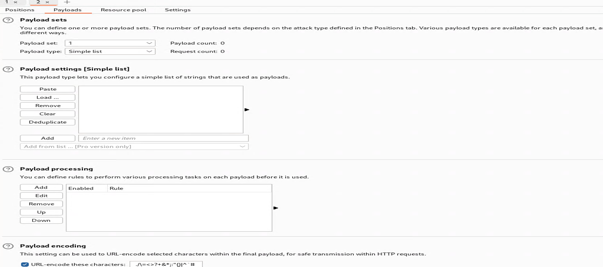
Step6: Turn on proxy in burpsuite and enter username password and check the intercepted data in burpsuite and send it to intruder:



Intruder tab:



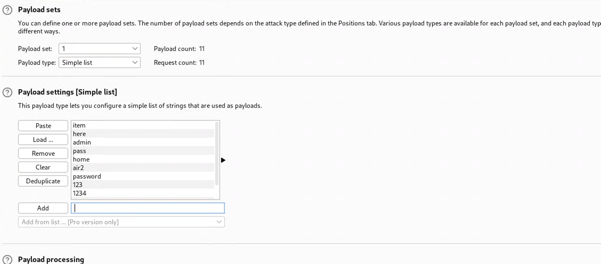
Step7: Open payload tab to bruteforce the password:

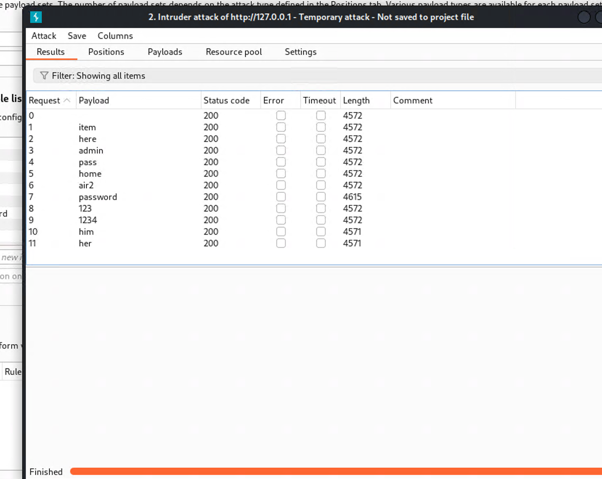


Step8: Extract password list:



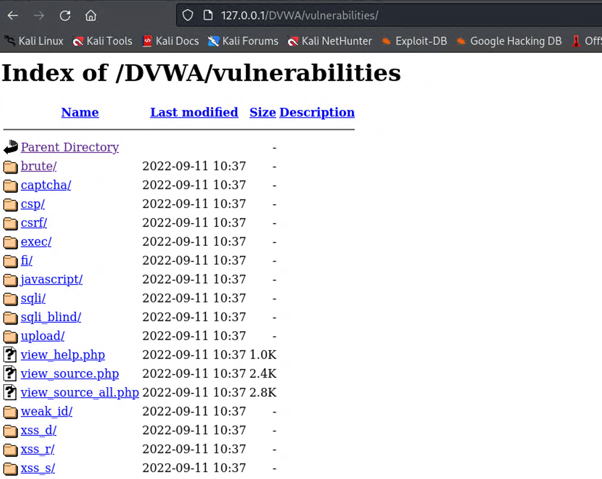
Step9: Load the wordlist in burpsuite:



Step10: Click on Start attack:  


**Step 4: To File Upload vulnerability**

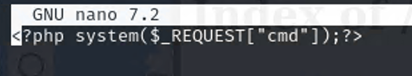
Step1: Type the url: localhost/vulnerabilities to list all files:

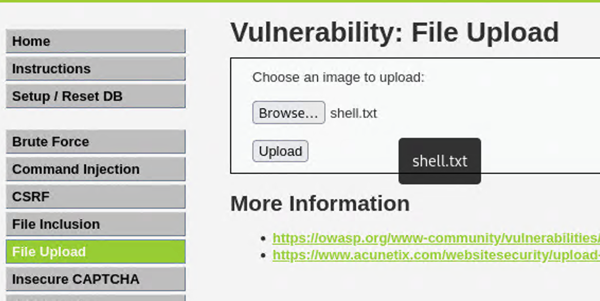


Step2: Generate a shell .txt file:



Step3: Display some text:



Step4: Upload the shell.txt file:  


Step5: Now upload it and open the url:  
  
  
  
Step6: It should automatically redirect to :



Step7: You can also list files using the below command:  
