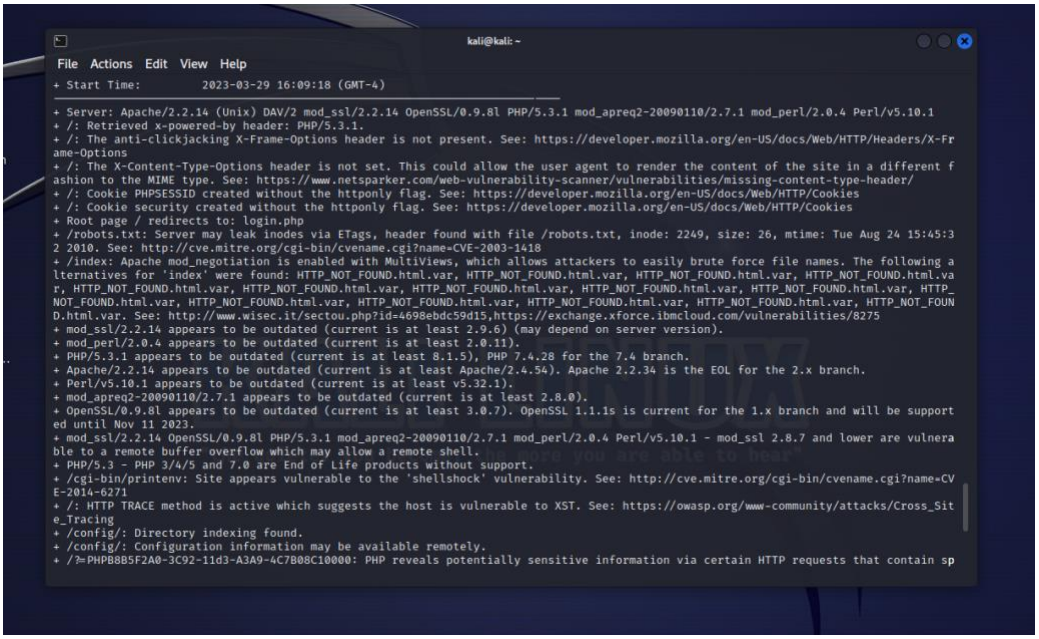
1. **Nmap**

   This tool is relatively easy to use I started up my DVWA for a target and ran nmap -v -A -sV to 10.10.1.11 to see any open ports. I was successful in finding there are 3 open ports ftp, ssh, http. With the other commands I was able to get OS detection, version detection, script scanning, and traceroute. I didn't have to wait that long for the results to come back maybe 15 seconds.

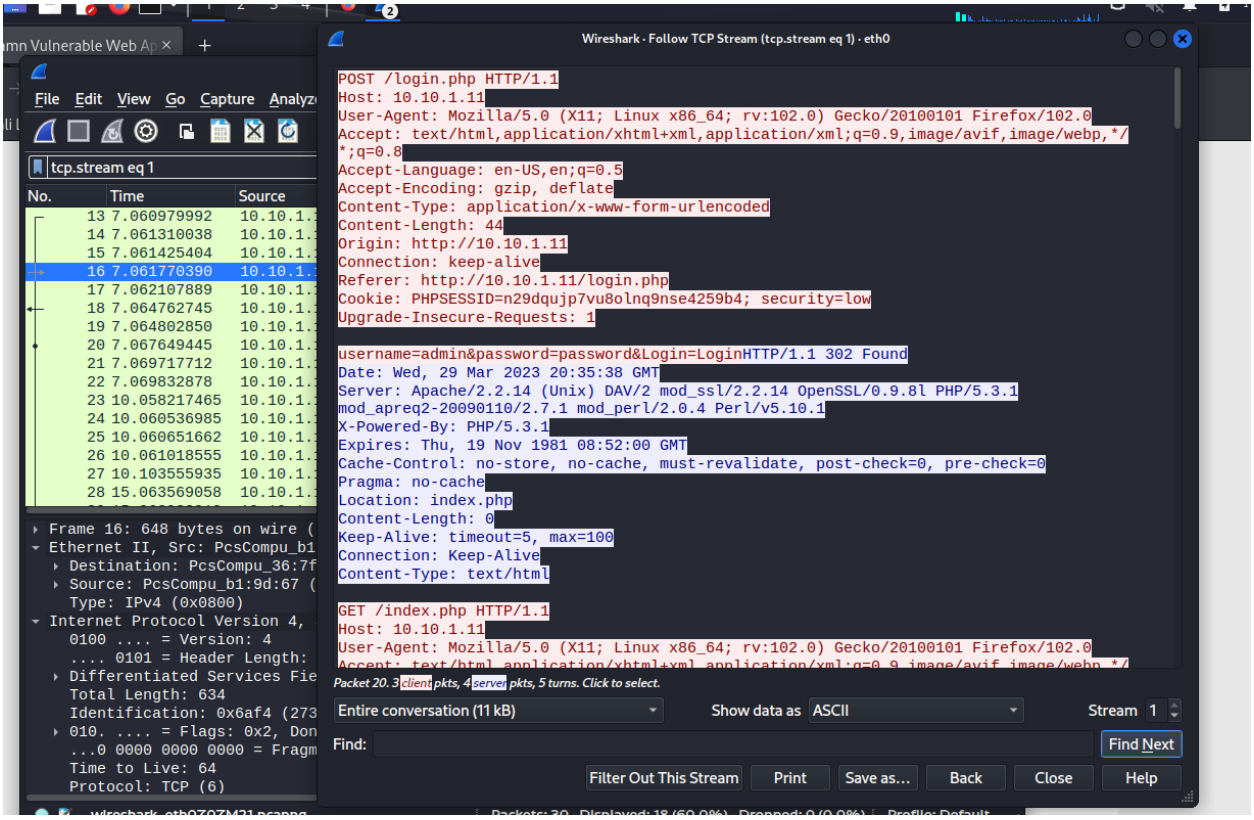
2. **Nikto tool**

   This took a little bit to get the scan but the return showed the target port of 80 (http). I used a simple scan of 10.10.1.11 for vulnerabilities. This scan can show what the website is vulnerable to. For example in my scan it shows the server and the apache mod_negotiation is enabled and can suffer from brute force attacks.



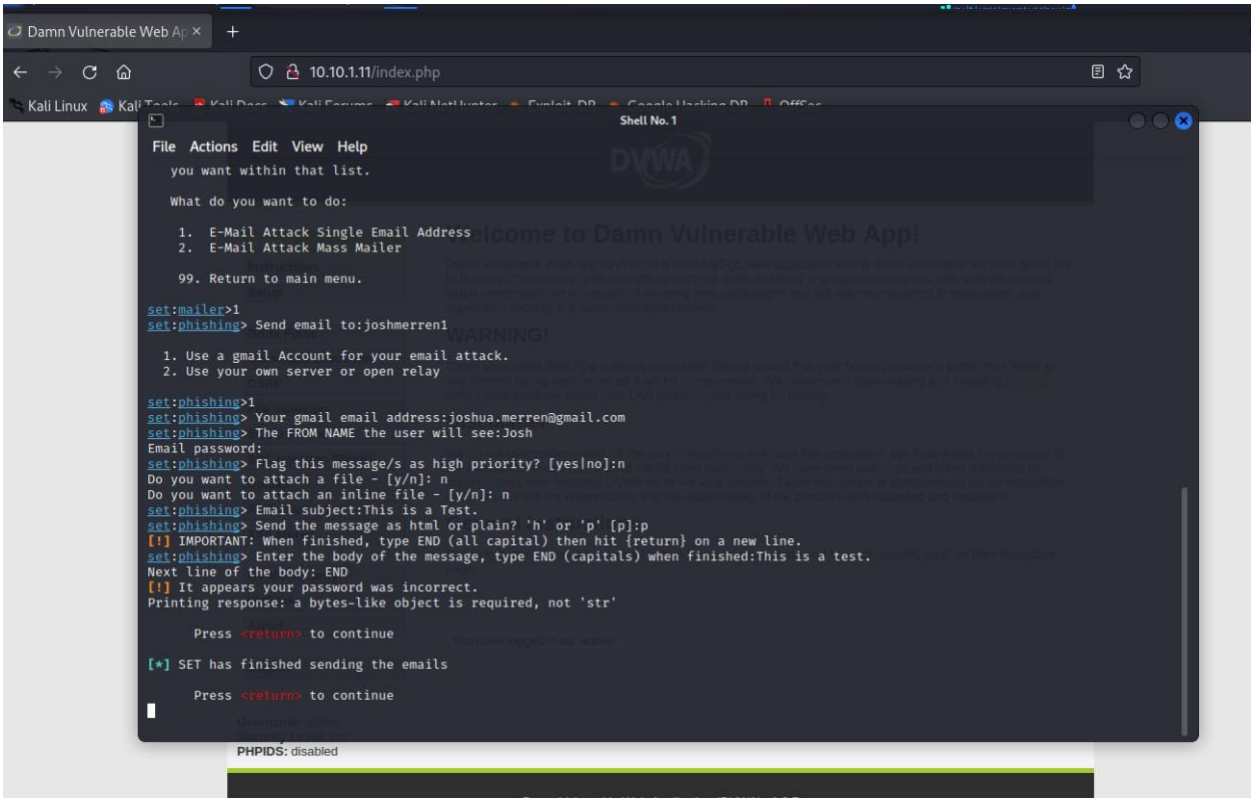
3. **Wireshark**

This took me a little time to remember to find and sort packets. I went to the DVWA and logged in and used Wireshark for packet capture. I was able to get the login credentials. It took a little bit since I normally used the other Wireshark and not the one on kali Linux. But I was able to filter packets and find the login of admin and password of password. I think the hardest thing for Wireshark is knowing how to filter and what to look for to try and find the information you are looking for.



4. **Social engineering toolkit.**

I tried to get an email to send through, but it didn't work. I did though get through all the steps to send it and what it would say. I was kind of hoping this would work so I could take a screen shot of the email after I got it. This is easy to use as well, it has step-by-step instructions for what you need to do. It can make it simple for a common person that isn't tech savvy to be able to send a phishing email. I could get through doing a phishing email in a matter of a couple of minutes.


Damn Vulnerable Web Ap
10.10.1.11/index.php
Kali Linux
Shell No. 1
File Actions Edit View Help
you want within that list.
What do you want to do:
1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
99. Return to main menu.
set:mailer>1
set:phishing> Send email to:joshmerren1
1. Use a gmail Account for your email attack.
2. Use your own server or open relay
set:phishing>1
set:phishing> Your gmail email address:joshua.merren@gmail.com
set:phishing> The FROM NAME the user will see:Josh
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:n
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:This is a Test.
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:This is a test.
Next line of the body: END
[!] It appears your password was incorrect.
Printing response: a bytes-like object is required, not 'str'
Press <return> to continue
[*] SET has finished sending the emails
Press <return> to continue
PHPIDS: disabled