Internship Final Report

Student Name: Onyekachi Williams Akurunwa

University: N/A

Major: Computer Science

Internship Duration: April 10th, 2025 - May 3rd, 2025

Company: Hack Secure

Domain: Cyber Security

Mentor: Mr. Nishant Prajapati

Assistant Mentor: Mr. Aman Pandey

Coordinator: Mr. Shivam Kapoor

Objectives

Going into this internship, my main goals were to:

1. Really get a solid grasp of cybersecurity principles and how they're applied.
2. Get practical, hands-on experience finding, analyzing, and dealing with security threats.
3. Become more skilled with cybersecurity tools and techniques by using them in actual scenarios.

Tasks and Responsibilities

Throughout my time at Hack Secure, I got involved in a range of cybersecurity tasks, generally covering areas like:

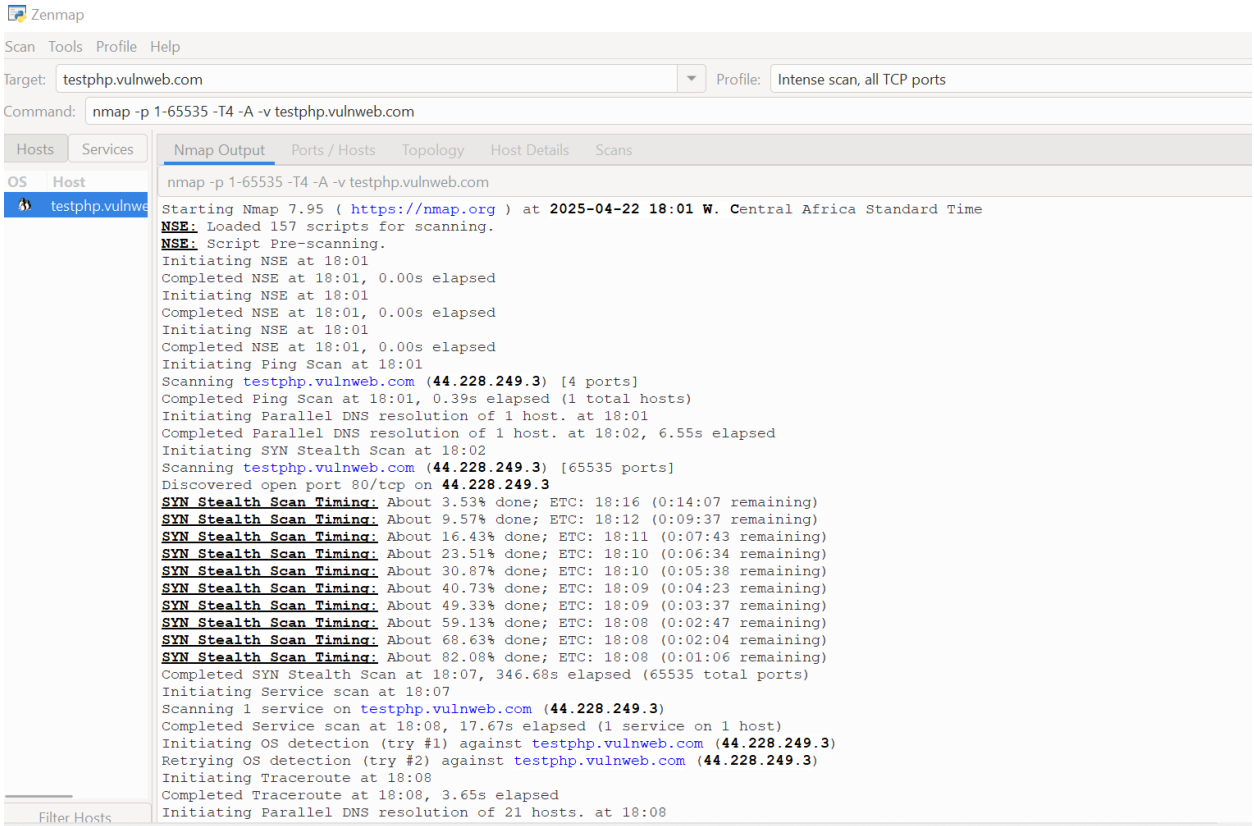
- Vulnerability Assessment
- Penetration Testing
- Traffic Analysis
- Decryption and Cryptanalysis
- Reverse Engineering
- Network Security
- Payload Creation

Here’s a breakdown of the specific tasks and projects I worked on:

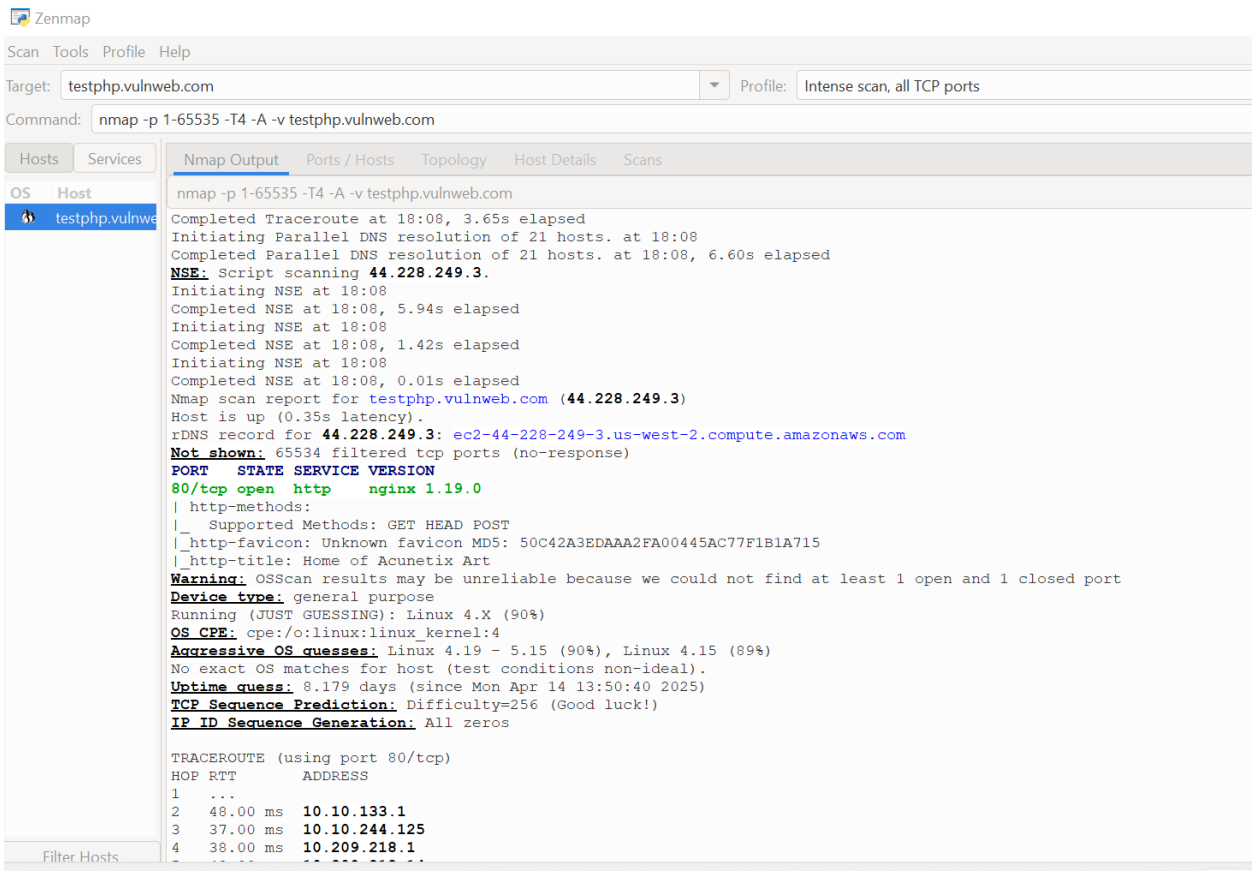
TASK LEVEL INTERMEDIATE

1). Finding open ports on http://testphp.vulnweb.com/

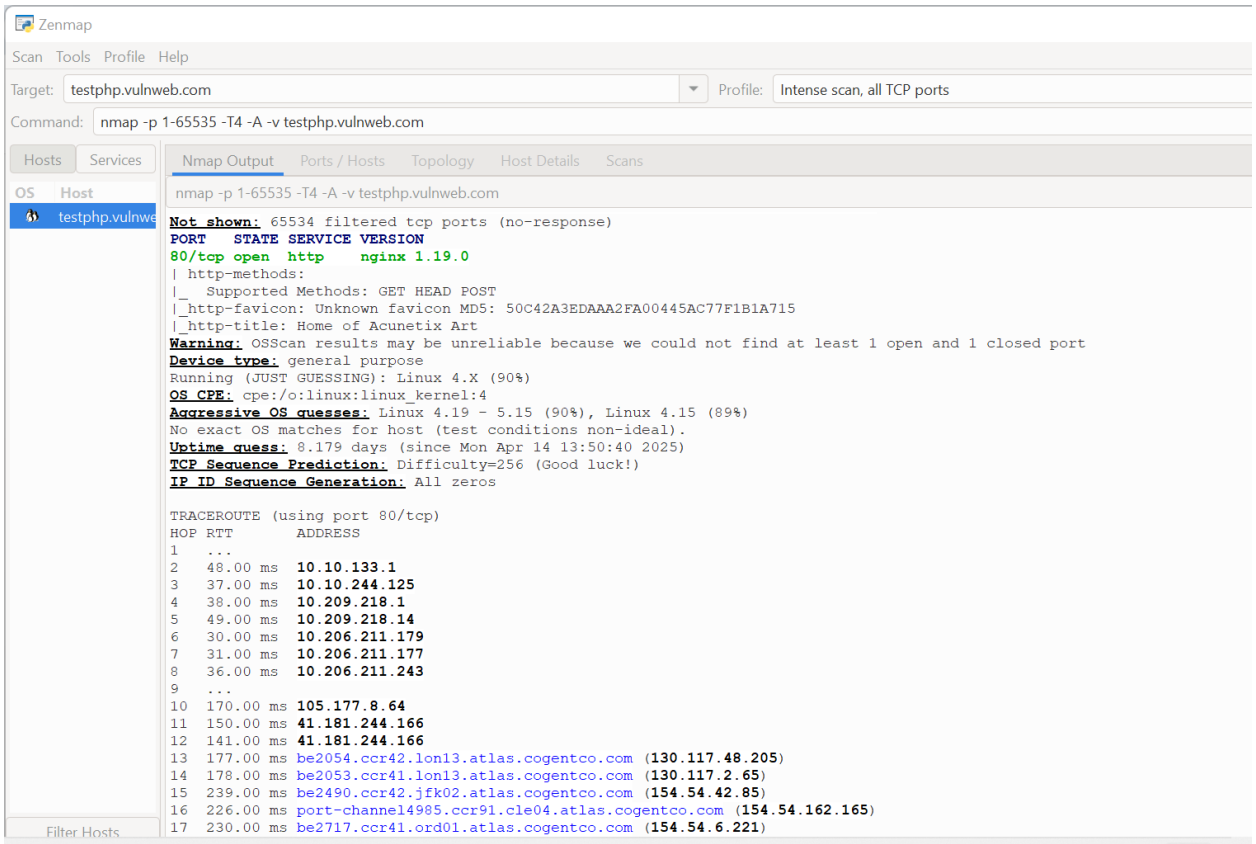
- What I Did and Found: My first step was to map out the target website, testphp.vulnweb.com (IP 44.228.249.3). I used Zenmap to run Nmap with the command nmap -p 1-65535 -T4 -A -v testphp.vulnweb.com. I set it for an intense scan across all TCP ports, making sure to include service/version detection, faster timing, and verbose output so I wouldn't miss anything. The scan clearly showed port 80/tcp was open and running an nginx 1.19.0 web server. Nmap's OS detection guessed it was Linux. I didn't find any other open TCP ports in the results I gathered.
- What I Learned: Running this scan and digging through the output really helped me get comfortable with using Nmap from the command line and understanding what the results mean. It pinpointed the web server as the main thing to look at on this target.
- My Screenshots:
  - Hacksecure internship- task level intermediate- task 1- screenshot 1.png



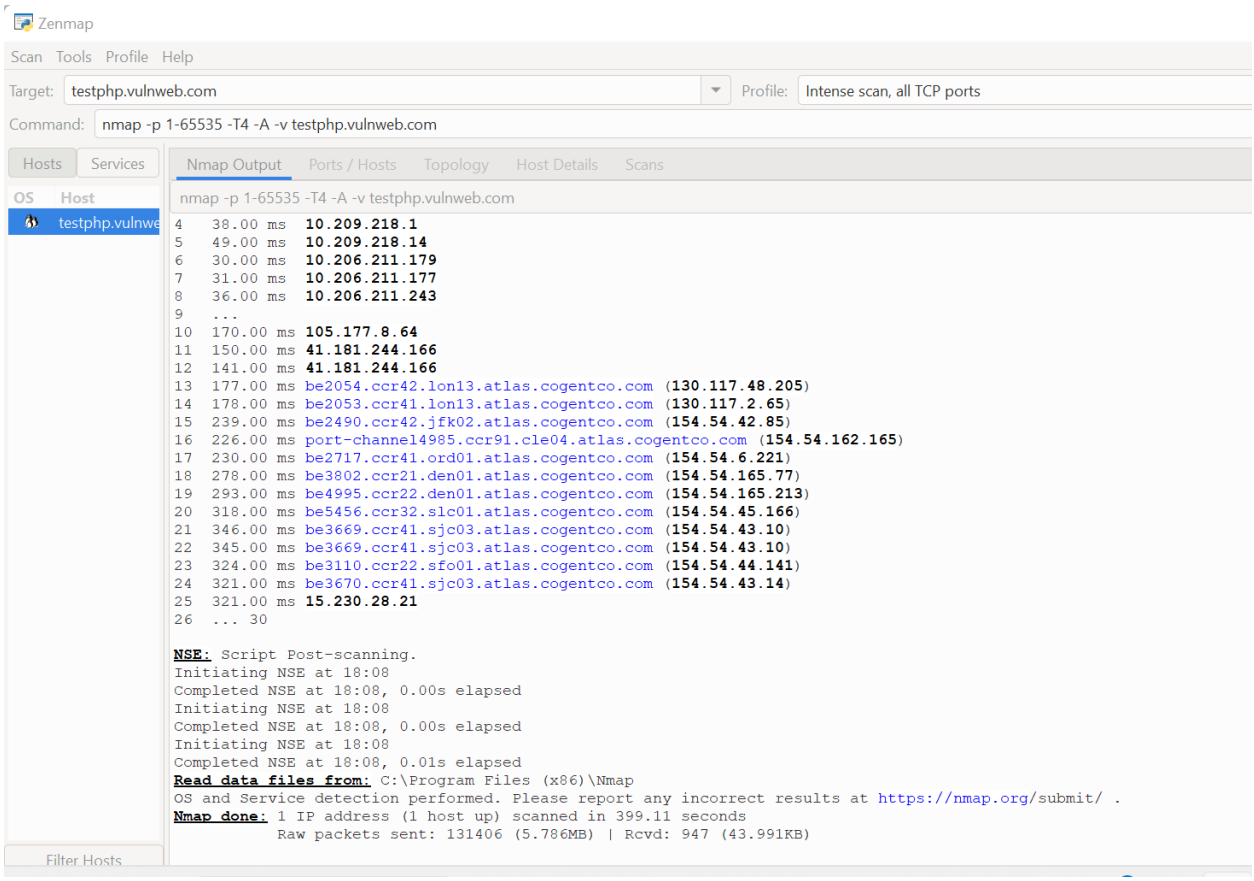
  - intern-task intermediate- task 1- screenshot 2.png



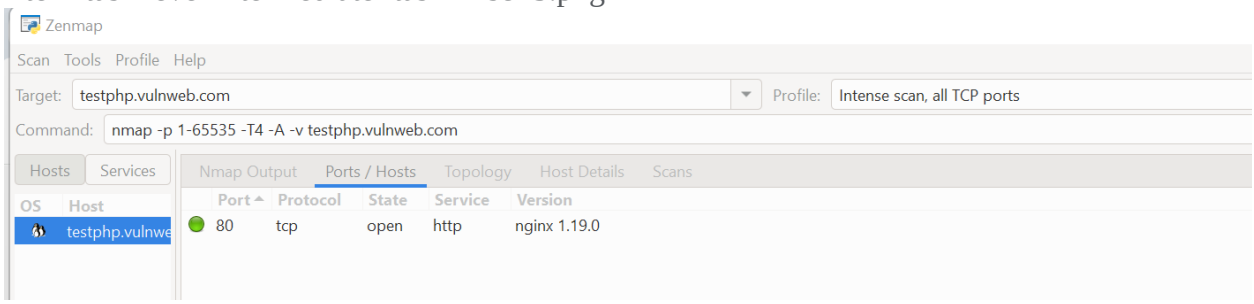
- intern-task level intermediate- task 1-scr 3.png



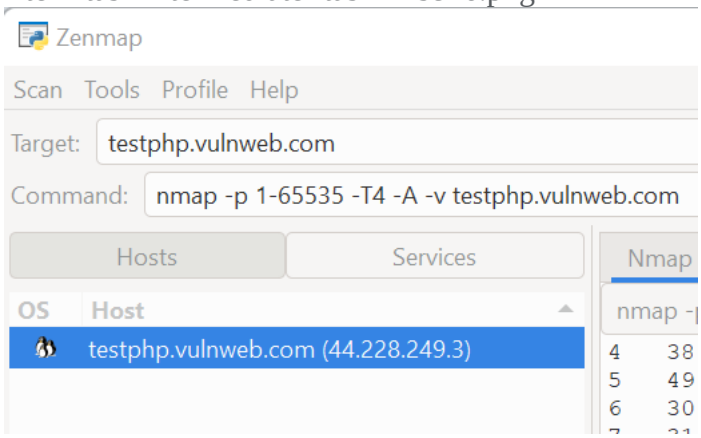
- intern-task level intermediate- task 1- scr 4.png



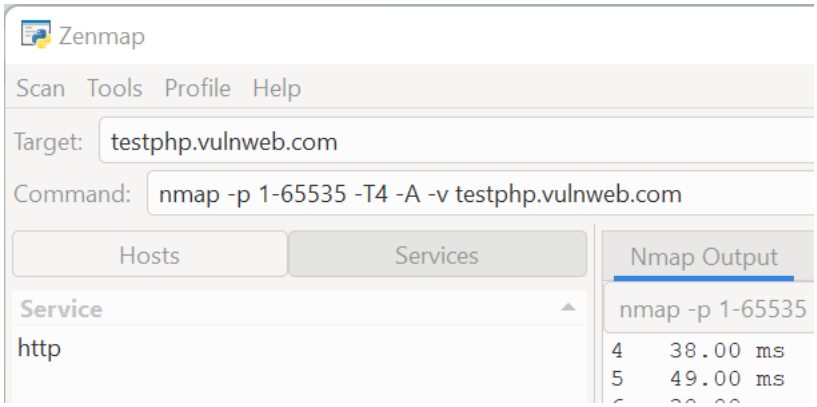
- intern-task level intermediate- task 1- scr 5.png



- intern-task intermediate- task 1- scr 6.png



- intern- task level intermediate- task 1- scr 7.png

- 

---

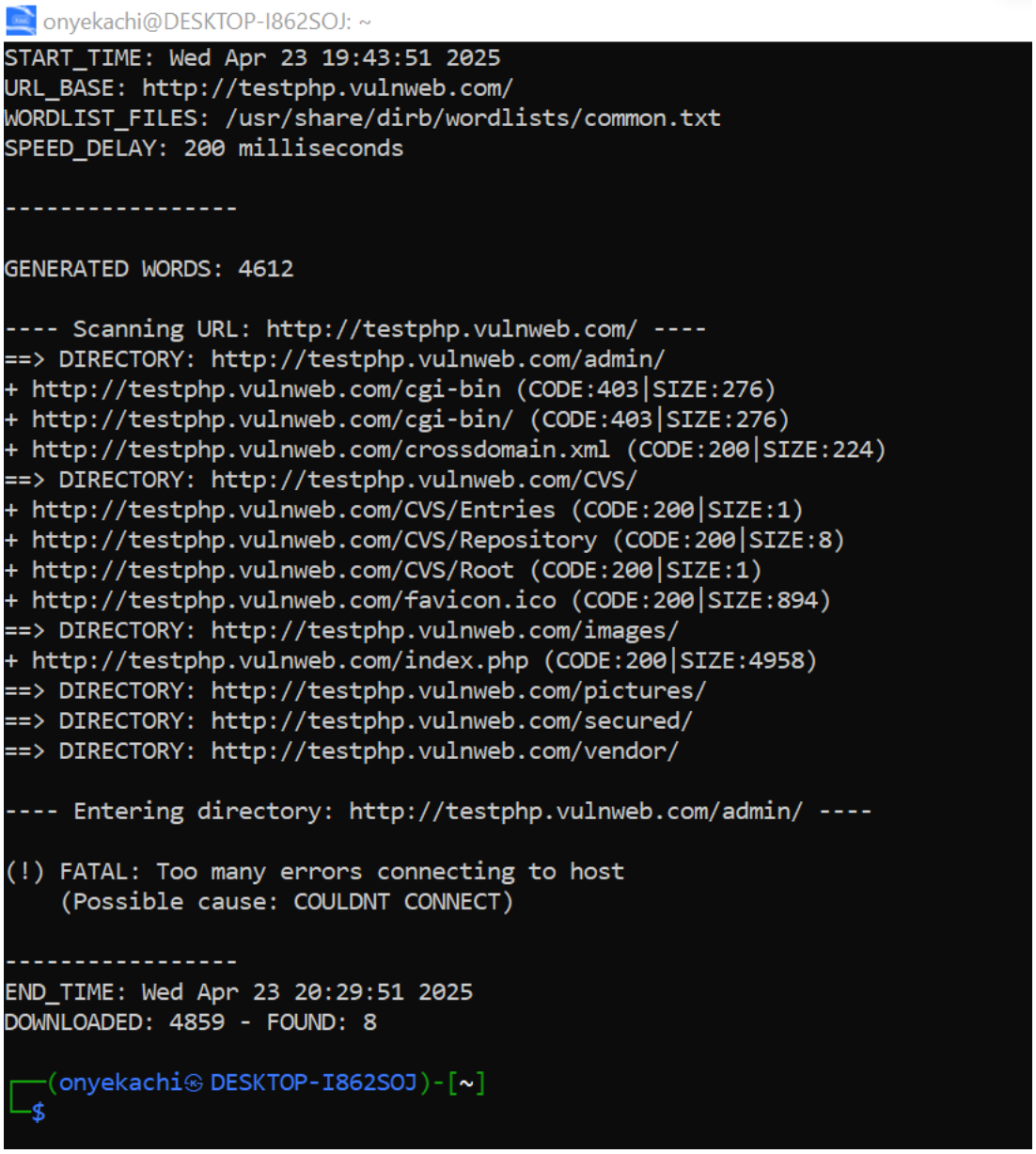
2). Brute forcing directories on http://testphp.vulnweb.com/

- What I Did and Found: Next, I wanted to see what directories might be hiding on the web server. I used the Dirb tool (dirb http://testphp.vulnweb.com/) with the common.txt wordlist to brute-force directory names. This uncovered several interesting finds like /admin/ and /cgi-bin/ (both gave a 403 Forbidden, but good to know they exist), plus accessible locations like /CVS/, /images/, /pictures/, /secured/, /vendor/, and the index.php file itself.
- What I Learned: This exercise showed me how effective Dirb is for discovering web content that isn't directly linked. Finding these directories helped me understand the site structure better and identify potential areas that might need more investigation. It hammered home how important content discovery is in pen testing.
- My Screenshots:
  - intern- task level intermediate- task 2- scr 1.png

onyekachi@DESKTOP-I862SOJ: ~

```
┌──(onyekachi㉿DESKTOP-I862SOJ)-[~]
└─$ dirb http://testphp.vulnweb.com/ -z 200

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Apr 23 19:43:51 2025
URL_BASE: http://testphp.vulnweb.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
SPEED_DELAY: 200 milliseconds

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://testphp.vulnweb.com/ ----
==> DIRECTORY: http://testphp.vulnweb.com/admin/
+ http://testphp.vulnweb.com/cgi-bin (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/crossdomain.xml (CODE:200|SIZE:224)
==> DIRECTORY: http://testphp.vulnweb.com/CVS/
+ http://testphp.vulnweb.com/CVS/Entries (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/CVS/Repository (CODE:200|SIZE:8)
+ http://testphp.vulnweb.com/CVS/Root (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/favicon.ico (CODE:200|SIZE:894)
==> DIRECTORY: http://testphp.vulnweb.com/images/
+ http://testphp.vulnweb.com/index.php (CODE:200|SIZE:4958)
==> DIRECTORY: http://testphp.vulnweb.com/pictures/
==> DIRECTORY: http://testphp.vulnweb.com/secured/
==> DIRECTORY: http://testphp.vulnweb.com/vendor/

---- Entering directory: http://testphp.vulnweb.com/admin/ ----

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT CONNECT)

-----------------
```

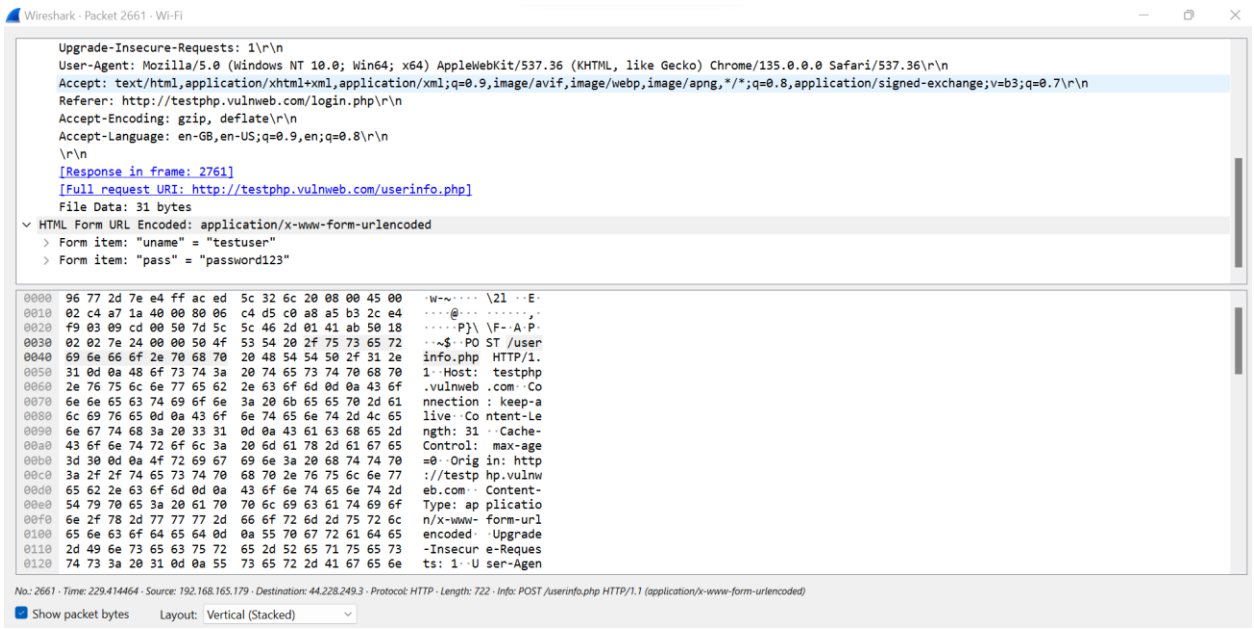
- intern- task level intermediate- task 2- scr 2.png



---

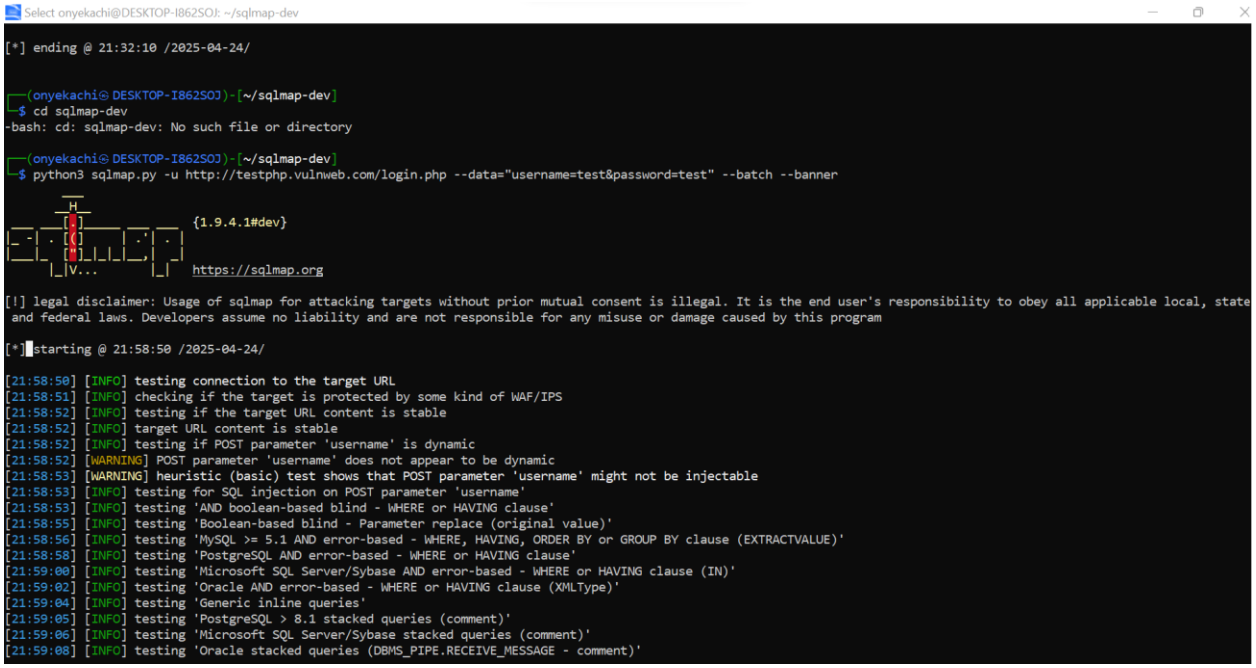
3). Intercepting login credentials with Wireshark on http://testphp.vulnweb.com/

- What I Did and Found: To see how login data was handled, I set up Wireshark to capture traffic while I logged into the site (specifically targeting the /userinfo.php page). I easily captured the HTTP POST request and saw the login credentials – uname=testuser and pass=password123 – being sent completely in the clear (plaintext).
- What I Learned: It was eye-opening to see just how exposed those credentials were. This exercise was a practical demonstration of capturing traffic with Wireshark and really highlighted the risks of using unencrypted HTTP for sensitive information.
- My Screenshot:
  - intern- task level intermediate- task 3- scr.png

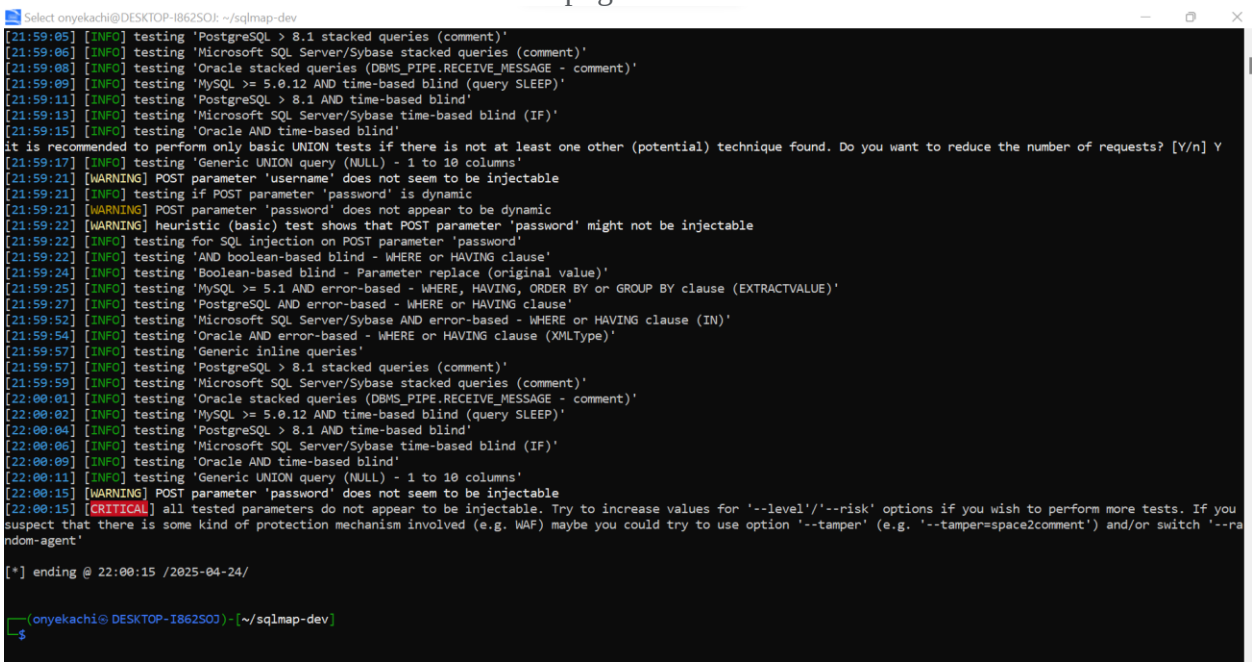
- 

4.) Testing for SQL injection on http://testphp.vulnweb.com/

- What I Did and Found: I then tested the login page (http://testphp.vulnweb.com/login.php) for SQL injection vulnerabilities using sqlmap. I fed it the login parameters (uname=test, passwd=test) and let it run through its tests (boolean-based, error-based, time-based, UNION query). While sqlmap started testing and flagged potential issues, it eventually gave a critical warning suggesting the parameters might not be injectable, or maybe a WAF was blocking the attempts. So, I couldn't confirm an exploitable SQLi based on the tests I ran and captured.
- What I Learned: Using sqlmap gave me hands-on experience with automated SQLi testing. I learned how it probes parameters but also saw that it's not always straightforward – protections like WAFs can get in the way. This was a good reminder that real-world testing often involves overcoming obstacles.
- My Screenshots:
  - intern- task level intermediate- task 4- scr 1.png

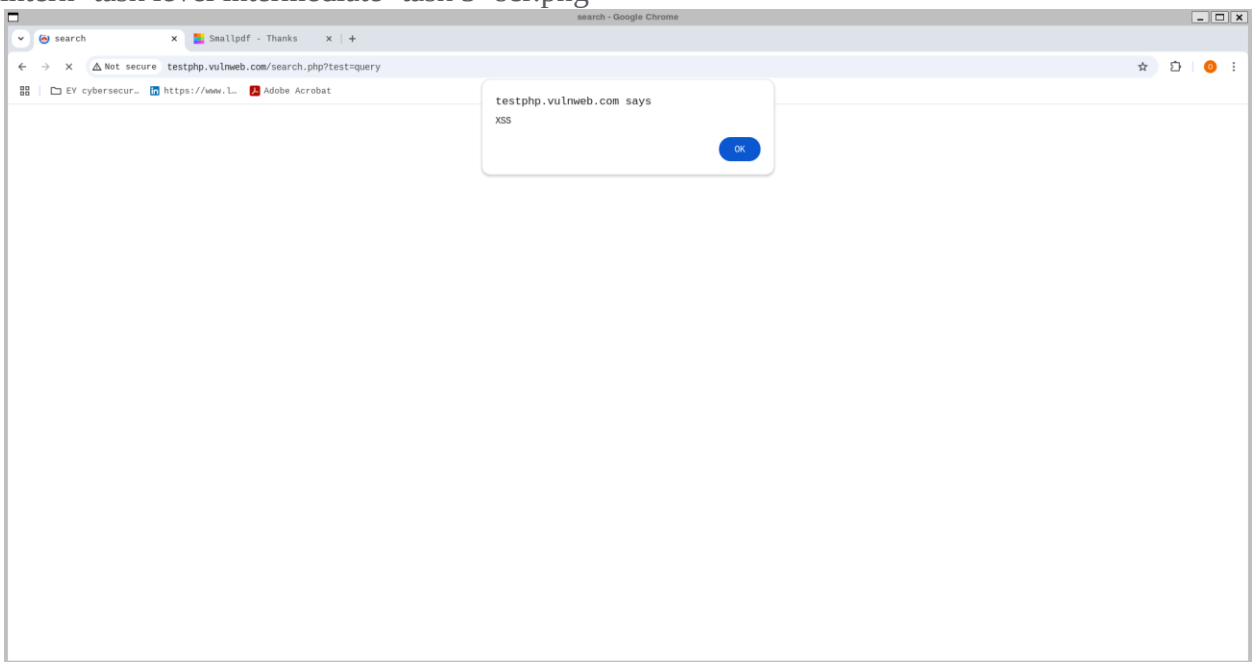


- intern- task level intermediate- task 4- scr 2.png



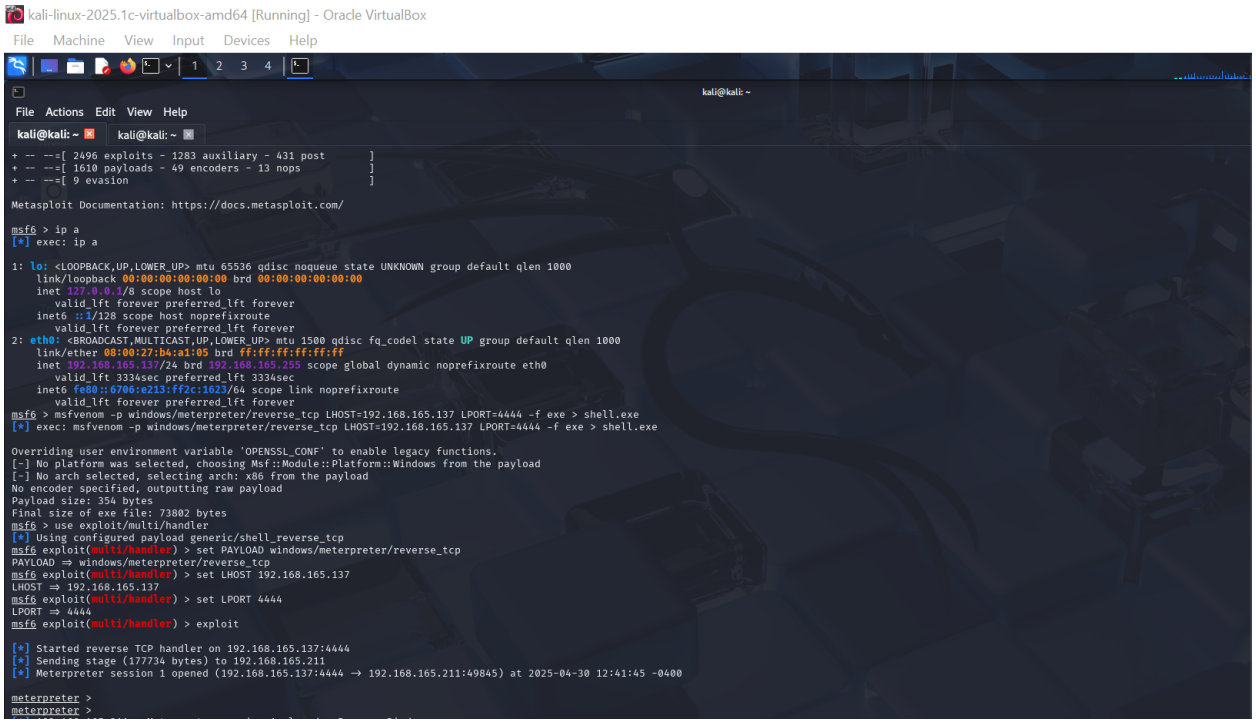
5.) Testing for XSS on http://testphp.vulnweb.com/

- What I Did and Found: I also tested input fields for Cross-Site Scripting (XSS). I focused on the search function (/search.php) and injected a simple JavaScript payload. It worked – the script executed, and I got an alert box with "XSS" to pop up in the browser, confirming a reflected XSS vulnerability.

- What I Learned: Successfully executing this XSS attack helped me understand how these vulnerabilities work in practice. I learned how to craft a basic payload and use input fields to test if a site is vulnerable. Seeing the alert box confirm the vulnerability was a clear success.
- My Screenshot:
  - intern- task level intermediate- task 5- scr.png
  - 

Task (CTF)- Initial access with Metasploit

- What I Did and Found: For the CTF challenge, my objective was to get initial access to the target machine. I used msfvenom to create a Windows Meterpreter reverse TCP payload (shell.exe), setting the LHOST to my machine's IP (192.168.185.137) and LPORT to 4444. Then, I configured the exploit/multi/handler in msfconsole to listen for the incoming connection using the same payload settings. Once the payload (shell.exe) was executed on the target machine (192.168.185.211), it connected back to my listener, and I successfully got a Meterpreter session.
- What I Learned: This task was great practice for using Metasploit. I got comfortable generating payloads with msfvenom and setting up listeners in msfconsole. Successfully catching the reverse shell and getting that Meterpreter prompt felt like a significant achievement and really demonstrated a key phase of penetration testing.
- My Screenshot:
  - CTF Tasks- Initial access with metasploit screenshot.jpg

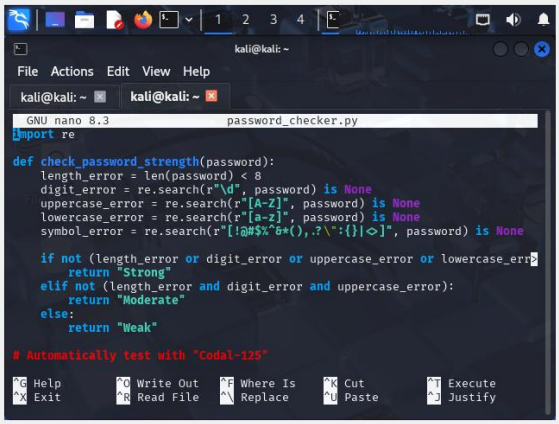
- 

Ethical Hacking Project- Password Strength Checker

- What I Did and Found: For my project, I decided to build a password strength checker using Python. I wrote a script (password_checker.py) that uses regular expressions (the re module) to check if a password includes digits, uppercase letters, lowercase letters, and special symbols. Based on these factors and the password's length, my script outputs whether the password is "Weak," "Moderate," or "Strong." I tested it with Codel-125, and it correctly identified it as "Moderate."
- What I Learned: Building this tool was a good way to apply programming skills to a security concept. It helped me practice using Python and regular expressions, and it was rewarding to create a functional script that evaluates password complexity based on standard criteria. Hyperlink to github project: https://github.com/Onyekachi-537/Ethical-Hacking-Project-Onyekachi-Akurunwa
- My Screenshots:
  - ethical hacking project- scr 1.jpg

kali-linux-2025.1c-virtualbox-amd64 [Running] - Oracle VirtualBox

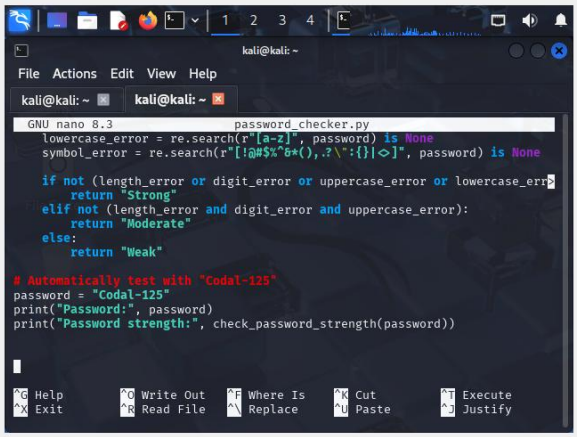
File Machine View Input Devices Help



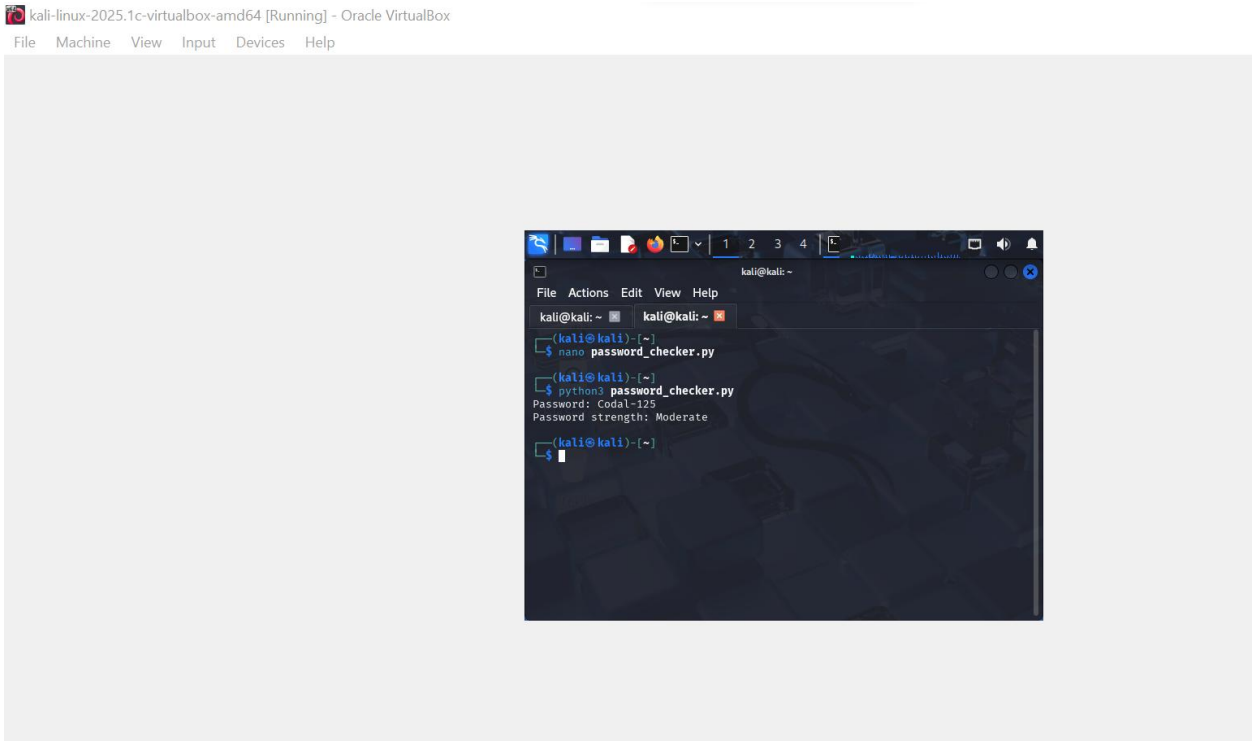
- ethical hacking project - scr 2.jpg

kali-linux-2025.1c-virtualbox-amd64 [Running] - Oracle VirtualBox

File Machine View Input Devices Help



- ethical hacking project- scr 3.png

- 

Learning Outcomes

This internship was a fantastic learning experience for me. Here's what I gained:

- Hands-on Tool Proficiency: I didn't just learn *about* cybersecurity tools; I actually *used* them extensively. I got hands-on practice with Nmap (scanning), Dirb (web discovery), Wireshark (traffic analysis), sqlmap (SQLi testing), Metasploit (payloads & handlers), and even applied secure coding ideas in my Python project.
- Understanding the Security Process: I developed a much clearer picture of how security assessments work, from the initial information gathering and scanning stages all the way through trying to gain access and exploit vulnerabilities.
- Sharpened Problem-Solving Skills: Facing challenges like figuring out open ports, discovering hidden site sections, extracting credentials, and dealing with potential WAFs definitely pushed my analytical thinking and forced me to figure out how to apply the tools effectively to solve problems.
- Personal & Professional Growth: Beyond the technical skills, this internship improved my ability to tackle specific tasks methodically, document what I found using screenshots as proof, and manage my time to meet the goals set for me.

Challenges and Solutions

It wasn't all smooth sailing; I definitely hit some challenges:

- Getting Comfortable with Complex Tools: Tools like Nmap, sqlmap, and Metasploit have a lot of options and can be intimidating at first. Getting the hang of them took focused effort. I overcame this by hitting the documentation hard, watching tutorials, and spending extra time practicing in the lab environment until I felt more confident.
- Making Sense of Tool Output: Sometimes, the output from tools like Nmap or sqlmap wasn't immediately clear. Figuring out what the scan results *really* meant, or why sqlmap might be getting blocked, required me to slow down, analyze the details, and look things up in documentation or online security resources.

Conclusion

Overall, my internship experience at Hack Secure was incredibly valuable and really boosted my knowledge and practical skills in cybersecurity. Getting to use industry-standard tools on realistic targets taught me so much about vulnerability assessment, penetration testing, and how exploits actually work. Completing all the intermediate tasks, tackling the CTF challenge, and building my password checker project has definitely solidified my interest in cybersecurity as a career path. I feel much more prepared now for the kinds of challenges I'll encounter in this field.

Acknowledgments

I really want to thank Hack Secure for giving me this internship opportunity. I owe a special thanks to my mentor, Mr. Aman Pandey, and assistant mentor Mr. Prabhat Raj – their guidance and support were incredibly helpful throughout my time here. I also thank Amrita Vishwa Vidyapeetham for making this internship possible; it's been a huge part of my growth. I hope this report gives a good sense of my experience and shows how I was able to connect what I learned in my studies with practical, hands-on skills in a professional cybersecurity setting.