

Internship Final Report – Cyber Security (Red Teaming)

Student Details

- Name: Mostafa karam
- University: Faculty of Computer and Data Science
- Major: Computer Science / Cybersecurity
- Internship Duration: March 25, 2025 – June 25, 2025
- Company: Hack Secure
- Domain: Cybersecurity Red Teaming & Ethical Hacking
- Mentor: Mr. Nishant Prajapati
- Assistant Mentor: Mr. Aman Pandey
- Coordinator: Mr. Shivam Kapoor

Objectives

The objectives of my internship were to:

1. Strengthen practical cybersecurity skills through hands-on red team tasks.
2. Understand and apply penetration testing techniques.
3. Complete real-world exploit challenges and CTF labs.
4. Develop and deliver 3 functional Python-based security tools.

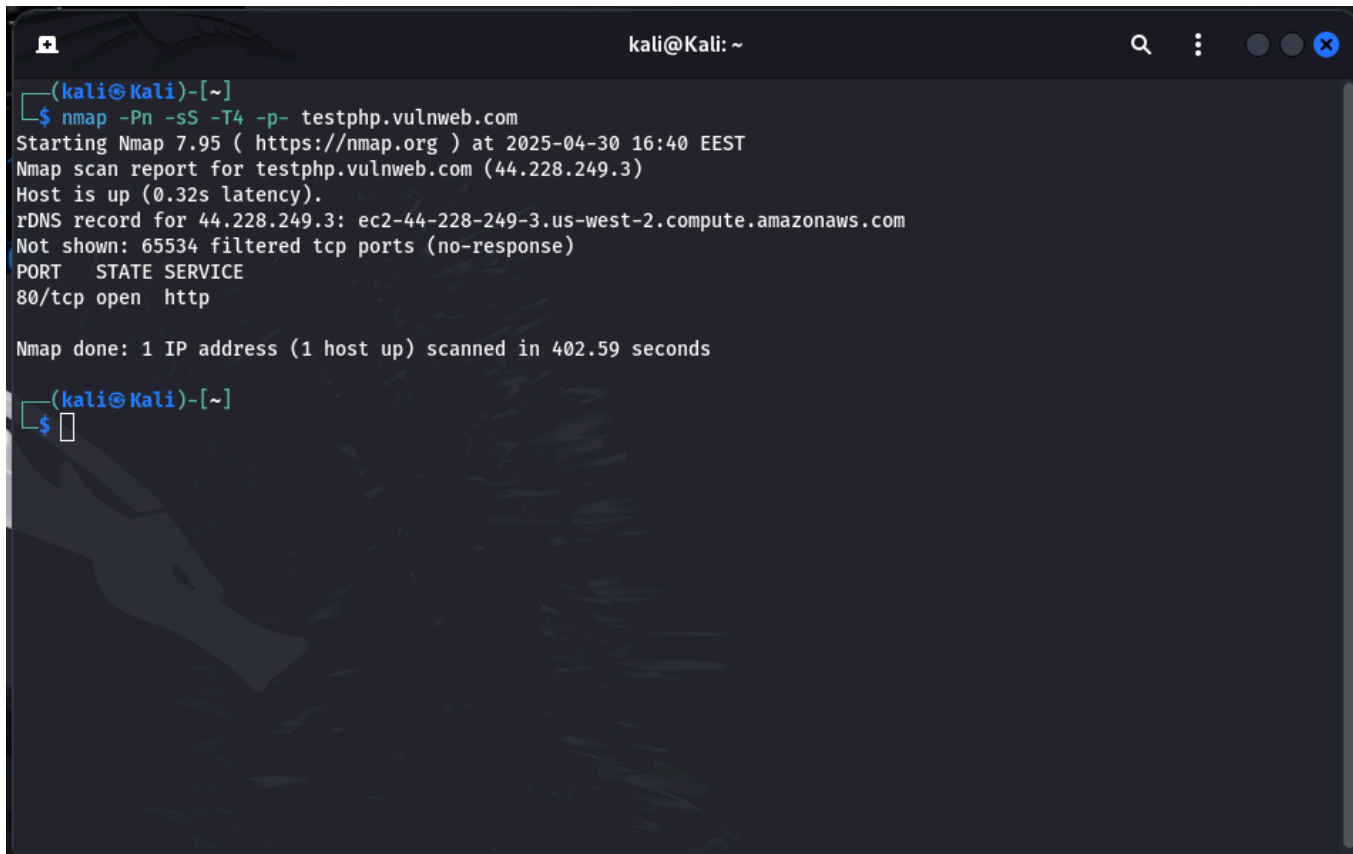
Tasks and Responsibilities:

Task 1 Report: Port Scanning on testphp.vulnweb.com

- **Objective:**
 - Identify open ports on the target web server <http://testphp.vulnweb.com/> to understand the services exposed to the internet.
- **Tools Used:**
 - Nmap
- **Command Used:**
 - `nmap -Pn -sS -T4 -p- testphp.vulnweb.com`
- **Findings (Scan Results):**
 - Open Port:
 - 80/tcp - HTTP Service

The scan revealed that only port 80 (HTTP) is open. All other ports are filtered, indicating no response or active firewall/security filtering.

Screenshot:



```
(kali㉿kali)-[~]
└─$ nmap -Pn -sS -T4 -p- testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-30 16:40 EEST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.32s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 402.59 seconds

(kali㉿kali)-[~]
└─$
```



Task 2 Report: Directory Brute Forcing on

- **Objective:**
 - Identify hidden or unlisted directories on the target web server, testphp.vulnweb.com, to find potential attack surfaces.
- **Tools Used:**
 - Gobuster
- **Command Used:**
 - `gobuster dir -u http://testphp.vulnweb.com/ -w /usr/share/wordlists/dirb/common.txt -t 50`
- **Findings (Directories Discovered):**
 - `/admin` — Redirects to `/admin/`
 - `/cgi-bin/` — Forbidden (403)
 - `/crossdomain.xml` — Publicly accessible
 - `/CVS` — Redirects to `/CVS/`
 - `/CVS/Root`, `/CVS/Repository`, `/CVS/Entries` — Files found inside the CVS directory
 - `/favicon.ico` — Website's favicon
 - `/index.php` — Main page
 - `/images` — Image directory
 - `/pictures` — Pictures directory
 - `/secured` — Secure area (potentially interesting)
 - `/vendor` — Library/vendor files directory

Screenshot:

```
(kali@kali)-[~]
$ gobuster dir -u http://testphp.vulnweb.com/ -w /usr/share/wordlists/dirb/common.txt -t 50
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://testphp.vulnweb.com/
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/admin (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/admin/]
/cgi-bin/ (Status: 403) [Size: 276]
/cgi-bin (Status: 403) [Size: 276]
/crossdomain.xml (Status: 200) [Size: 224]
/CVS (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/CVS/]
/CVS/Root (Status: 200) [Size: 1]
/CVS/Repository (Status: 200) [Size: 8]
/CVS/Entries (Status: 200) [Size: 1]
/favicon.ico (Status: 200) [Size: 894]
/index.php (Status: 200) [Size: 4958]
/images (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/images/]
/pictures (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/pictures/]
/secured (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/secured/]
/vendor (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/vendor/]
Progress: 4614 / 4615 (99.98%)
=====
Finished
=====
```

Task 3 Report: Capturing Login Credentials Using Wireshark

- Objective:
 - Intercept and analyze network traffic during a login attempt on <http://testphp.vulnweb.com/> to check if credentials are transmitted securely.
- Tools Used:
 - Wireshark
- Steps Followed:
 1. Opened Wireshark and started capturing traffic on the active network interface.
 2. I visited <http://testphp.vulnweb.com/> and attempted to log in by submitting a test username and password.
 3. Applied HTTP filters in Wireshark and identified a POST request directed to </userinfo.php>.
 4. Analyzed the packet payload, revealing the username and password in plain text.
- Findings:
 - Form Fields Captured:
 - Username (`uname`) = `test`
 - Password (`pass`) = `test`
- Data was transmitted unencrypted due to the usage of HTTP rather than HTTPS.

Screenshot:

| | | | | | | | | |
|------|---------------|--------------|-----------|------|------|---|-----|------------------------------------|
| 1993 | 114.074382684 | 44.228.249.3 | 10.0.2.15 | HTTP | 389 | GET /CVS/pricelist HTTP/1.1 | 764 | HTTP/1.1 404 Not Found (text/html) |
| 1995 | 114.074382684 | 44.228.249.3 | 10.0.2.15 | HTTP | 386 | GET /CVS/prices HTTP/1.1 | 764 | HTTP/1.1 404 Not Found (text/html) |
| 1996 | 114.075113113 | 44.228.249.3 | 10.0.2.15 | HTTP | 387 | GET /CVS/print HTTP/1.1 | 764 | HTTP/1.1 404 Not Found (text/html) |
| 1998 | 114.381039974 | 44.228.249.3 | 10.0.2.15 | HTTP | 387 | GET /CVS/print HTTP/1.1 | 764 | HTTP/1.1 404 Not Found (text/html) |
| 1999 | 114.381759988 | 44.228.249.3 | 10.0.2.15 | HTTP | 387 | GET /CVS/print HTTP/1.1 | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2001 | 114.584527462 | 44.228.249.3 | 10.0.2.15 | HTTP | 387 | GET /CVS/print HTTP/1.1 | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2002 | 114.585193354 | 44.228.249.3 | 10.0.2.15 | HTTP | 385 | GET /CVS/print HTTP/1.1 | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2008 | 114.890510952 | 44.228.249.3 | 10.0.2.15 | HTTP | 387 | GET /CVS/print HTTP/1.1 | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2009 | 114.897342530 | 44.228.249.3 | 10.0.2.15 | HTTP | 391 | GET /CVS/print_order HTTP/1.1 | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2011 | 115.200238928 | 44.228.249.3 | 10.0.2.15 | HTTP | 384 | HTTP/1.1 404 Not Found (text/html) | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2012 | 115.200954742 | 44.228.249.3 | 10.0.2.15 | HTTP | 389 | GET /CVS/printarticle HTTP/1.1 | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2014 | 115.507346244 | 44.228.249.3 | 10.0.2.15 | HTTP | 384 | HTTP/1.1 404 Not Found (text/html) | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2015 | 115.507760850 | 44.228.249.3 | 10.0.2.15 | HTTP | 392 | GET /CVS/printarticle HTTP/1.1 | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2017 | 115.724707263 | 44.228.249.3 | 10.0.2.15 | HTTP | 384 | HTTP/1.1 404 Not Found (text/html) | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2018 | 115.725146280 | 44.228.249.3 | 10.0.2.15 | HTTP | 388 | GET /CVS/printenv HTTP/1.1 | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2020 | 115.943539777 | 44.228.249.3 | 10.0.2.15 | HTTP | 384 | HTTP/1.1 404 Not Found (text/html) | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2021 | 115.944098635 | 44.228.249.3 | 10.0.2.15 | HTTP | 387 | GET /CVS/printenv HTTP/1.1 | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2023 | 116.148981227 | 44.228.249.3 | 10.0.2.15 | HTTP | 387 | GET /CVS/printenv HTTP/1.1 | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2024 | 116.149122919 | 44.228.249.3 | 10.0.2.15 | HTTP | 388 | GET /CVS/printers HTTP/1.1 | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2030 | 116.428945959 | 44.228.249.3 | 10.0.2.15 | HTTP | 570 | POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded) | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2032 | 116.430582275 | 44.228.249.3 | 10.0.2.15 | HTTP | 384 | HTTP/1.1 404 Not Found (text/html) | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2033 | 116.430806708 | 44.228.249.3 | 10.0.2.15 | HTTP | 389 | GET /CVS/printenv HTTP/1.1 | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2035 | 116.738380585 | 44.228.249.3 | 10.0.2.15 | HTTP | 3644 | HTTP/1.1 200 OK (text/html) | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2036 | 116.738381060 | 44.228.249.3 | 10.0.2.15 | HTTP | 384 | HTTP/1.1 404 Not Found (text/html) | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2038 | 116.738381060 | 44.228.249.3 | 10.0.2.15 | HTTP | 388 | GET /CVS/printenv HTTP/1.1 | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2040 | 116.941278928 | 44.228.249.3 | 10.0.2.15 | HTTP | 384 | HTTP/1.1 404 Not Found (text/html) | 764 | HTTP/1.1 404 Not Found (text/html) |
| 2041 | 116.941600916 | 44.228.249.3 | 10.0.2.15 | HTTP | 391 | GET /CVS/printthread HTTP/1.1 | 764 | HTTP/1.1 404 Not Found (text/html) |

Frame 2030: 570 bytes on wire (4624 bits), 570 bytes captured (4624 bits) on interface eth0, id 0

Ethernet II, Src: PCSysntec f5:8a:a9 (08:00:27:f5:8a:a9), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 44.228.249.3

Transmission Control Protocol, Src Port: 42872, Dst Port: 80, Seq: 2582, Ack: 21548, Len: 524

Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

Form item: "uname" = "test"

Form item: "pass" = "test"

0000

52 55 0a 00 02 02 00 00

27 f5 8a a9 00 00 45 00

RU

00 00 00 00 00 00 00 00

E

0010

82 34 bd 8f 40 00 40 00

49 3e 0a 00 02 0f 2c e4

4

0 0 0 0 0 0 0 0

I

0020

f9 03 a7 70 00 50 75 7f

1f a6 1e b5 a8 2d 50 1b

x

Pu

P

0030

1f ff 34 10 00 00 50 4f

53 54 20 2f 75 73 05 72

4

PO

ST /user

0040

69 6e 66 6f 2e 70 68 70

20 48 54 54 50 2f 31 2e

info.php

HTTP/1.

0050

31 0d 0a 48 6f 73 74 3a

20 74 65 73 74 70 68 70

1

Host: testphp

0060

2e 70 75 6c 6e 77 65 62

2e 63 6f 65 6d 0a 55 73

vulnweb.com

Us

0070

65 72 2d 41 67 65 6e 74

3a 20 4d 6f 7a 69 6c 6c

er-Agent

: Mozilla



Task 4 Report: SQL Injection

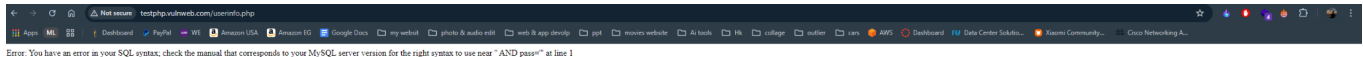
- Objective:
 - Test whether the login or search functionalities on the website are vulnerable to SQL Injection, and attempt to extract information from the backend database.
- Tools Used:
 - Manual SQLi Testing via Browser Input Field
- Steps Followed:
 1. Navigated to the login form on <http://testphp.vulnweb.com/>.
 2. Entered the following SQL payload in the username field: ' OR 1=1 –
 3. Left the password field blank or with any value.Upon form submission, the following error message was displayed:

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' AND pass='' at line 1

Analysis:

- The error message confirms the input is directly injected into the SQL query without proper sanitization.
- This indicates the website is vulnerable to SQL Injection.
- An attacker could potentially exploit this vulnerability to:
 - Bypass login
 - Enumerate users or databases
 - Dump sensitive data

Screenshot:

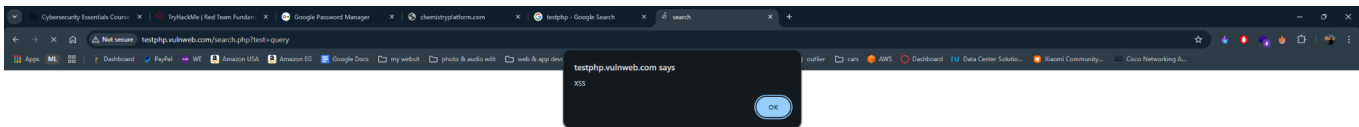


Task 5 Report: Cross-Site Scripting (XSS)

- Objective:

- Test for Cross-Site Scripting (XSS) vulnerabilities by injecting malicious scripts into input fields to evaluate input sanitization on the website.
- Tools Used:
 - Web Browser (Manual Testing)
- Steps Followed:
 1. Navigated to the search page at:
`http://testphp.vulnweb.com/search.php?test=query`
 2. Injected the following JavaScript payload directly into the URL:
`<script>alert('XSS')</script>`
 3. Reloaded the page and observed the result.
- Findings:
 - The browser immediately rendered an alert box with the message **XSS**.
 - This confirms that the input was reflected and executed as code on the page, demonstrating a Reflected XSS vulnerability.

Screenshot:



 **CTF Task – TryHackMe: PickleRick**

Set up your virtual environment

To successfully complete this room, you'll need to set up your virtual environment. This involves starting both your AttackBox and Task Machines, ensuring you're equipped with the necessary tools and access to tackle the challenges ahead.



Attacker machine ⓘ

Status: ● Off

Start AttackBox ▼



Target machine ⓘ

Status: ● Off

Start Machine



This Rick and Morty-themed challenge requires you to exploit a web server and find three ingredients to help Rick make his potion and transform himself back into a human from a pickle.

Deploy the virtual machine on this task and explore the web application: MACHINE_IP

Answer the questions below

What is the first ingredient that Rick needs?

mr. meeseek hair

✓ Correct Answer

What is the second ingredient in Rick's potion?

1 jerry tear


✓ Correct Answer

What is the last and final ingredient?

fleeb juice

✓ Correct Answer

📜 CTF Task – TryHackMe: Red Team Fundamentals



Red Team Fundamentals

Learn about the basics of a red engagement, the main components and stakeholders involved, and how red teaming differs from other cyber security engagements.

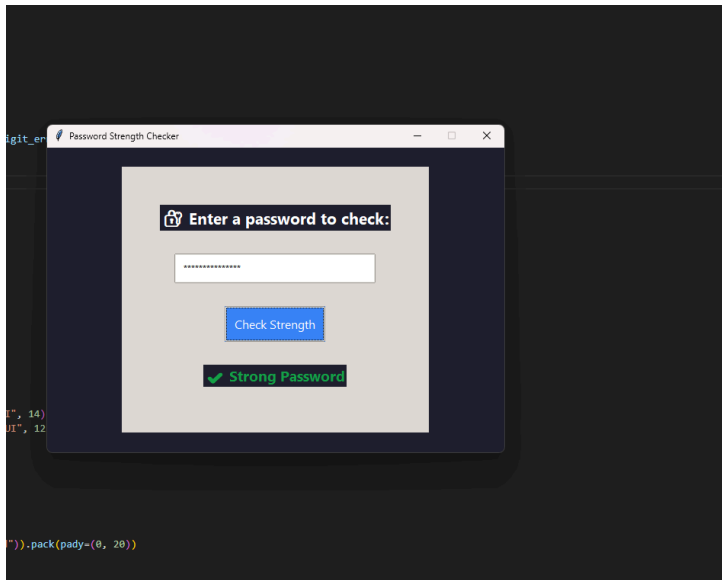
🟢 Easy ⌚ 20 min

[Share your achievement](#) [Help](#) [Save Room](#) [7620](#) [Options](#)

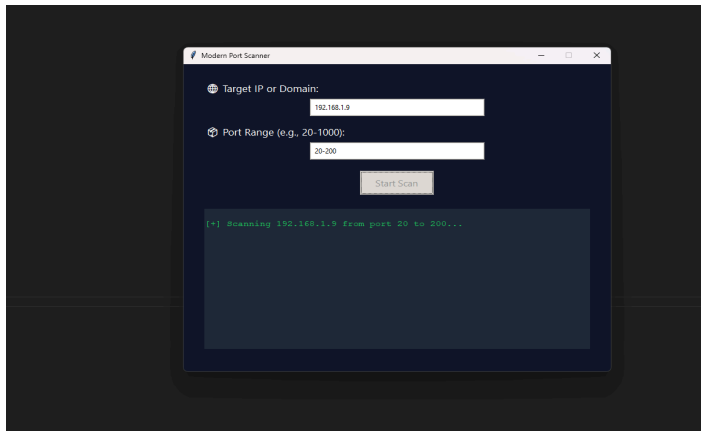
Room completed (100%)

- Task 1 ✓ Introduction
- Task 2 ✓ Vulnerability Assessment and Penetration Tests Limitations
- Task 3 ✓ Red Team Engagements
- Task 4 ✓ Teams and Functions of an Engagement
- Task 5 ✓ Engagement Structure
- Task 6 ✓ Overview of a Red Team Engagement
- Task 7 ✓ Conclusion

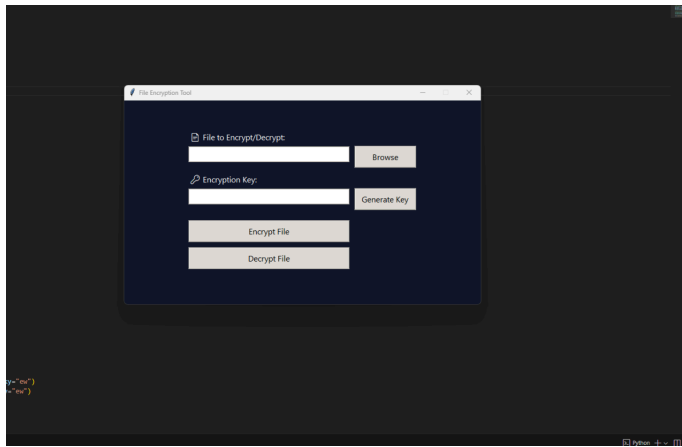
📜 Python Project 1: Password Strength Checker



Python Project 2: Basic Port Scanner



Python Project 3: File Encryption/Decryption Too



Learning Outcomes

- Enhanced practical understanding of web-based vulnerabilities.
- Gained experience using security tools (Nmap, Gobuster, Wireshark, Metasploit, etc.)
- Understood red team methodology and adversarial simulation.
- Built modern Python GUI tools using `tkinter`, threading, and libraries like `socket` and `cryptography`.

Challenges & Solutions

- XSS & SQLi Debugging: Initially struggled to detect injection points, solved by analyzing source and error responses.
- GUI Design: Creating a modern look with `tkinter` required styling with `ttk` and layout improvements.
- Decryption Errors: Fixed key mismatch bugs by adding input validation and error messages.

Conclusion

This internship helped me bridge academic knowledge with professional-level cybersecurity experience. I gained a deeper interest in ethical hacking and hands-on red teaming, which I aim to pursue further in my career.

Acknowledgments

I sincerely thank Hack Secure and my mentors, Mr. Aman Pandey and Mr. Prabhat Raj for guiding me throughout the internship. Their support helped me grow technically and professionally.

Appendix

- GitHub Repo: [<https://github.com/mostafa-karam/HackSecure-Internship>]