## **CTF Report**

**Full Name: Saurav Pundir   
Program: HCS - Penetration Testing 1-Month Internship  
Date: 08-03-2025**

**Category: Web 2.0**

**Description:** Lock Web

**Challenge Overview:** A brief description of the challenge (in 2 sentences)

**Steps for Finding the Flag:**

1. **Initial Reconnaissance:** Started by analyzing the web application and checking available endpoints.
2. **Input Validation Testing:** No visible input fields were found for direct injection testing.
3. **Directory Enumeration:** Used dirb or gobuster and found /index.txt and /robots.txt.
4. **Exploitation:** Visited <https://lock-web-web.hackatronics.com/robots.txt> and found a hidden flag.
5. **Flag Retrieval:** Successfully retrieved and documented the flag.

**Flag:** flag{V13w\_r0b0t5.txt\_c4n\_b3\_u53ful!!!}

**Category: Web 2.0**

**Description:** The World

**Challenge Overview:** Welcome to "The World" challenge! You've landed on a webpage saying "Hello World!" Looks simple, right? But there's more to it than meets the eye. Your mission: dig deep into this website to find hidden paths and uncover the flag.

**Steps for Finding the Flag:**

1. **Initial Reconnaissance:** Observed the structure of the web application for hidden resources.
2. **Input Validation Testing:** No visible input fields were found for direct injection testing.
3. **Directory Enumeration:** Ran gobuster: gobuster dir -u https://the-world-web.hackatronics.com/ -w /usr/share/wordlists /dirb/common.txt -t 50 -x .txt,.php,.html Found **/secret.txt**.
4. **Exploitation:** Visited <https://lock-web-web.hackatronics.com/robots.txt> and found a hidden flag.
5. **Flag Retrieval:** Successfully retrieved and documented the flag.

**Flag:** FLAG{Y0u\_hav3\_4xpl0reD\_th3\_W0rLd!}

**Category: Network Forensics**

**Description:** Corrupted

**Challenge Overview:** This is too EasyPeasyy!

Flag format: flag{!@#$%^&\*()\_+}

**Steps for Finding the Flag:**

1. **Initial Reconnaissance:** Analyzed the given PNG file.
2. **Input Validation Testing:** Used exiftool to examine metadata and found it’s corrupted.
3. **Directory Enumeration:** Not applicable for this challenge.
4. **Exploitation:** Used hexedit to correct the first 8 bytes of the PNG file.
5. **Flag Retrieval:** Opened the corrected PNG file and retrieved the flag.

**Flag:** flag{m3ss3d\_h3ad3r$}

**Category: Network Forensics**

**Description:** Shadow web

**Challenge Overview:** Unravel hidden data within the intricate landscape of protocols. This MULTIverse of packets contains some Form Data which can reveal the secrets of Web. Try to find this secrets that are scattered to get a flag.

**Steps for Finding the Flag:**

1. **Initial Reconnaissance:** Analyzed .pcapng file for anomalies.
2. **Input Validation Testing:** Examined scattered POST data.
3. **Directory Enumeration:** Not applicable for this challenge.
4. **Exploitation:** Extracted single characters hidden in POST requests.

Rearranged them and identified base64-encoded text: “**ZmxhZ3ttdWx0MXBsM3A0cnRzYzBuZnVzM3N9”**

Decoded using:

**echo ZmxhZ3ttdWx0MXBsM3A0cnRzYzBuZnVzM3N9 | base64 -d**

1. **Flag Retrieval:** Successfully retrieved the flag.

**Flag:** flag{mult1pl3p4rtsc0nfus3s}

**Category: Reverse Engg**

**Description:** Lost in the Past

**Challenge Overview:** I enjoyed making small projects when I was at a young age! I used to love hiding random funny texts in my projects that no one else could understand but myself. Coincidentally, I found a project file of something I made at that time. But it’s been so long, I can’t find that text. Can you help me find it?

**Steps for Finding the Flag:**

1. **Initial Reconnaissance:** Extracted all files from the provided folder and analyzed their content in Kali.
2. **Input Validation Testing:** Examined scattered POST data.
3. **Directory Enumeration:** Reviewed “Screen1.scm” and “Scrum.bky”.
4. **Exploitation:** Found an encrypted string in Scrum.bky:

**7=28LE\_\_0>F490C6GbCD?8N**

Decoded using ROT47 decoder and I got the flag.

1. **Flag Retrieval:** Successfully retrieved the flag.

**Flag:** flag{t00\_much\_rev3rs1ng}

**Category: Reverse Engg**

**Description:** Decrypt Quest

**Challenge Overview:** I enjoyed making small projects when I was at a young age! I used to love hiding random funny texts in my projects that no one else could understand but myself. Coincidentally, I found a project file of something I made at that time. But it’s been so long, I can’t find that text. Can you help me find it?

**Steps for Finding the Flag:**

1. **Initial Reconnaissance:** Downloaded and analyzed the provided encrypted file.
2. **Input Validation Testing:** Used CyberChef to extract Java code.
3. **Directory Enumeration:** Found a Google Drive link embedded in the Java code.
4. **Exploitation:** Accessed the Google Drive link, which contained a hint about Unix Epoch year (1970).

Modified the Java code to search for the 1970 epoch value and terminate when found.

1. **Flag Retrieval:** Successfully retrieved the flag.

**Flag:** flag{hjwilj111970djs}

**Category: OSINT**

**Description:** Time Machine

**Challenge Overview:** Mr. TrojanHunt has power to travel time. He is hiding some extremely confidential file from the governemnt. Can you help NIA to get secrets of TrojanHunt?

Flag format: flag{!@#$%^&\*()\_+}

**Steps for Finding the Flag:**

1. **Initial Reconnaissance:** Researched Trojan Hunt CTF for context on google and haved a look on Archive
2. **Input Validation Testing:** No user input required.
3. **Directory Enumeration:** Listed all files and found secret.txt.
4. **Exploitation:** Opened secret.txt and found the flag inside.
5. **Flag Retrieval:** Successfully retrieved the flag.

**Flag:** flag{Tr0j3nHunt\_t1m3\_tr4v3l}

**Category: Crypto**

**Description:** Wh@t7he####

**Challenge Overview:** Change my mind!

Flag format: flag{!@#$%^&\*()\_+}

**Steps for Finding the Flag:**

1. **Initial Reconnaissance:** Analyzed the provided file.
2. **Input Validation Testing:** Tried different decoding techniques.
3. **Directory Enumeration:** Not applicable.
4. **Exploitation: -** Recognized encoding as Reversefuck then Used an interpreter to decode the data.
5. **Flag Retrieval:** Successfully retrieved the flag.

**Flag:** flag{R3vers3ddd\_70\_g3t\_m3}

**Category: Crypto**

**Description:** Success Recipe

**Challenge Overview:** My friend who is a Chef sent me this recipe but i can't understand it He likes to write in weird languages Can you help me?

**Steps for Finding the Flag:**

1. **Initial Reconnaissance:** Analyzed a recipe that appeared to be written in an esoteric programming language.
2. **Input Validation Testing:** Checked the syntax and structure.
3. **Directory Enumeration:** Not applicable.
4. **Exploitation: -** Identified the language as Chef using chatgpt.

- Found an online Chef interpreter and corrected syntax errors

(e.g., until crack→ until cracked).

- Executed the code, which produced Brainfuck-encoded output.

- Decoded the Brainfuck code.

1. **Flag Retrieval:** Successfully obtained the flag.

**Flag:** flag{y0u\_40+\_s3rv3d!}