CTF Report

Full Name: Sahil Naik

Program: HCS - Penetration Testing 1-Month Internship

Date: 08/03/2025

---

1. Lock Web

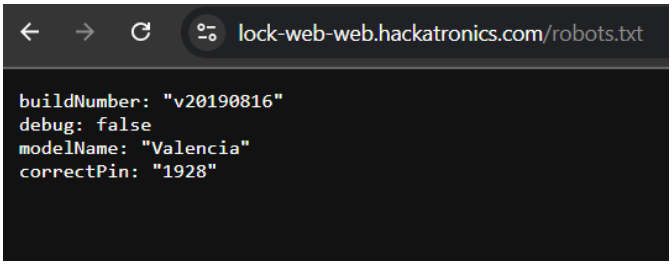
Category: Web 2.0

Description: This category focuses on modern web technologies and interactive web applications, testing players' skills in exploiting web-based functionalities.

Challenge Overview: Players used fuzzing tools to discover hidden directories and files on a web server, revealing critical information to solve the challenge.

Steps for Finding the Flag:

1. **Initial Reconnaissance:** Started by analyzing the web application's functionality and structure. Found some buttons and one input field
2. **Input Validation Testing:** Attempted to enter random numbers to see its behaviour and also tried triggering xss.
3. **Directory Enumeration:** Explored directories and endpoints within the web application to uncover hidden pages or functionalities that may lead to the flag using dirbuster and a seclist to fuzz.
4. **Exploitation:** Found a subdomain/directory called robots.txt, checked it on the browser and got the correct pin.



5. **Flag Retrieval:** Entered the pin and got the flag.

Flag: flag{V13w_r0b0t5.txt_c4n_b3_u53ful!!!}

Points : 100

---

2. The World

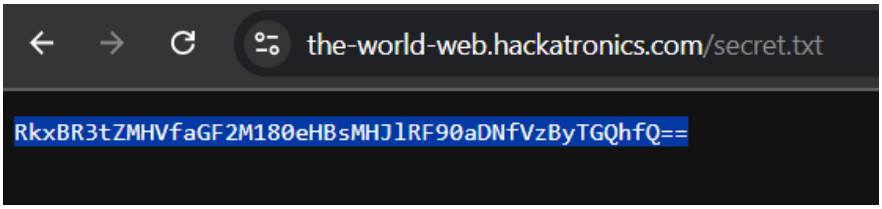
Category: Web 2.0

Description: This category focuses on modern web technologies and interactive web applications, testing players' skills in exploiting web-based functionalities.

Challenge Overview: Players used fuzzing tools to discover hidden directories and files on a web server, revealing critical information to solve the challenge.

Steps for Finding the Flag:

1. **Initial Reconnaissance:** Started by analyzing the web application's functionality and structure. Didn't find any interactive elements.
2. **Directory Enumeration:** Explored directories and endpoints within the web application to uncover hidden pages or functionalities that may lead to the flag using dirbuster and a seclist to fuzz.
3. **Exploitation:** Found a subdomain/directory called secret.txt, checked it on the browser and got an encoded string.



4. **Decoding :** decoded the above string using CyberChef base64 decode tool
5. **Flag Retrieval:** Got the flag on CyberChef after decoding

Flag: FLAG{Y0u_hav3_4xpl0reD_th3_W0rLd!}

Points : 150

---

3. Shadow Web

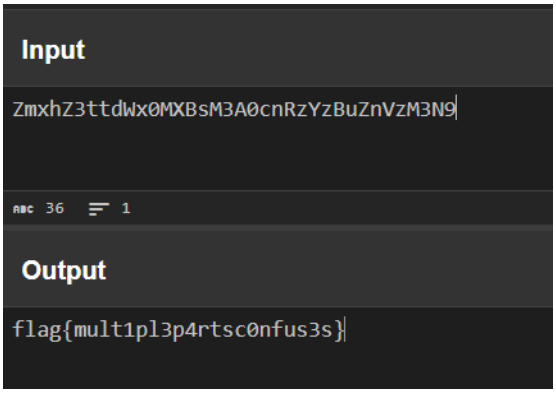
Category: Network Forensics

Description: This category focuses on analyzing network traffic captures to uncover hidden data, testing players' ability to extract meaningful information from packet captures.

Challenge Overview: Players examined a **PCAP** file to analyze HTTP traffic, identifying crucial requests that contained fragments of the flag.

Steps for Finding the Flag:

1. **Packet Analysis:** Loaded the **PCAP** file into Wireshark and filtered HTTP traffic to inspect request and response data.
2. **Flag Extraction:** Found multiple HTTP responses containing encoded fragments of the flag within the payload.
3. **Decoding:** Combined the extracted parts and decoded the final string using **CyberChef's Base64 decode** tool.



4. **Flag Retrieval:** Successfully reconstructed and retrieved the full flag after decoding.

Flag: Flag{mult1pl3p4rtsc0nfus3s}

Points : 150

---

4. Lost in the Past

Category: Reverse Engg

Description: This category involves analyzing and deconstructing files or applications to uncover hidden data, encryption methods, or encoded messages.

Challenge Overview: Players explored a given project folder, searching for clues and hidden information that could lead to the flag.

Steps for Finding the Flag:

1. **File Investigation:** Scanned through the project folder, checking for unusual or hidden files.
2. **Discovery:** Found an **XML** file containing a `<cipher>` tag with an encoded string.
3. **Decryption Analysis:** Used **dCode.fr** to identify the encryption method, which was detected as **ROT47**.
4. **Decoding:** Applied **ROT47 decoding** to reveal the hidden flag.
5. **Flag Retrieval:** Successfully obtained the flag after decoding.

Flag: flag{t00_much_rev3rs1ng}

Points : 150

---

5. Time Machine

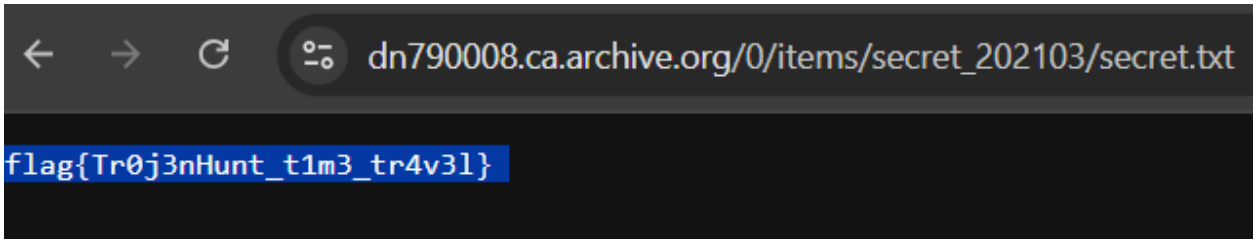
Category: OSINT

Description: This category focuses on gathering publicly available information using open-source intelligence techniques to uncover hidden data.

Challenge Overview: Players had to track down confidential files hidden by TrojanHunt using OSINT techniques and search engine dorking.

Steps for Finding the Flag:

1. **Analysis:** After reading the challenge description I focused on the 'time machine' and the wayback machine came to my mind.
2. **Search Dorking:** Used the Google dork to directly get the url:
   `intitle:"TrojanHunt" OR intext:"TrojanHunt"`
3. **Discovery:** Found a link on Archive.org leading to a hidden file:
   https://archive.org/details/secret_202103
4. **Flag Retrieval:** Accessed the archived file and extracted the flag.



Flag: flag{Tr0j3nHunt_t1m3_tr4v3l}

Points : 100

---

6. Wh@t7he####

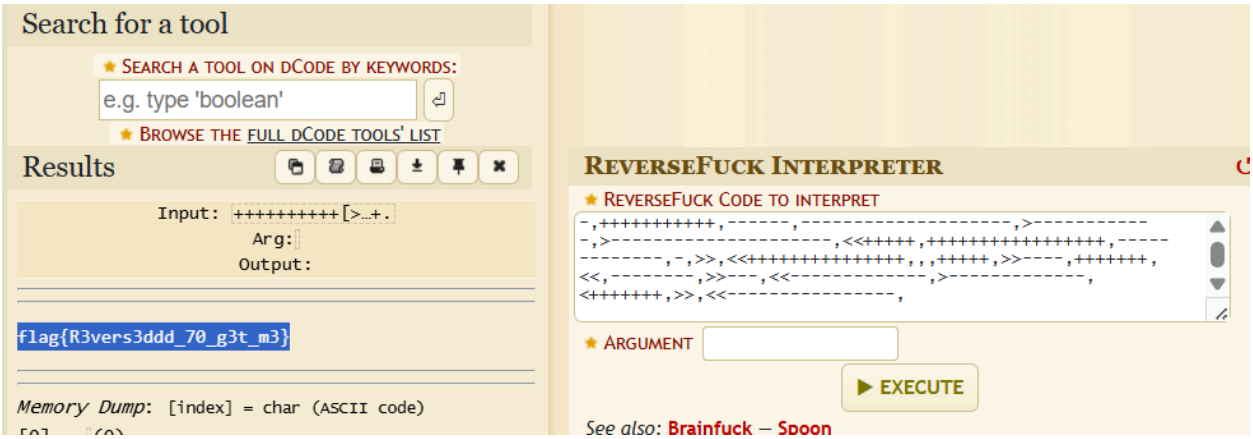
Category: Crypto

Description: This category challenges players to identify and decode encrypted messages using various cryptographic techniques.

Challenge Overview: Players had to analyze an encrypted file, determine the cipher used, and decrypt it to reveal the flag.

Steps for Finding the Flag:

1. **File Analysis:** Downloaded and opened the given file to inspect its contents.
2. **Cipher Identification:** Copied the content and used dCode.fr to analyze the encryption method.
3. **Decryption:** Identified the cipher as ReverseFuck and used the appropriate tool to decode it.
4. **Flag Retrieval:** Successfully obtained the flag after decryption.



Flag: flag{R3vers3ddd_70_g3t_m3}

Points : 100

---

7. Success Recipe

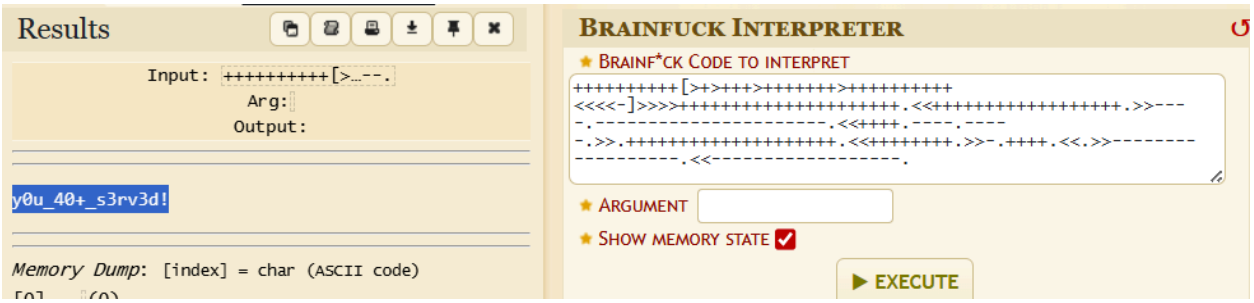
Category: Crypto

Description: This category tests players' ability to recognize and decode obscure or esoteric encryption methods.

Challenge Overview: Players had to interpret and decode an encrypted message hidden within an esoteric programming language.

Steps for Finding the Flag:

1. **Initial Analysis:** Copied the given recipe-like text and identified it as an esoteric language (Chef).
2. **Decoding Step 1:** Used an online Chef esolang interpreter to convert it into another code format.
3. **Decoding Step 2:** The output was Brainfuck code, which was then decoded using a Brainfuck interpreter.
4. **Flag Retrieval:** Successfully obtained the flag after decoding.



Flag: flag{y0u_40+_s3rv3d!}

Points : 150

Score :

1.	Lock Web	:	100
2.	The World	:	150
3.	Shadow web	:	150
4.	Lost in the Past	:	150
5.	Time Machine	:	100
6.	Wh@t7he####	:	100
7.	Success Recipe	:	150
	Total	**:**	**900**