CTF Report

Full Name: Krish Gupta Program: HCS - Penetration Testing 1-Month Internship

Date: 08 March 2025

Category: Web 2.0

Description: This challenge focused on identifying hidden directories and understanding backend request handling to discover the flag.

Challenge Overview: The Web Lock lab required us to bypass a PIN-based lock by applying good content discovery methodologies and understanding backend request behavior.

Steps for Finding the Flag:

1. Initial Reconnaissance:
    - Opened the web application and inspected the source code using browser developer tools.
    - No useful information was found in the source code.
2. Capturing Requests:
    - Used Burp Suite to capture the HTTP requests made by the web application.
    - Observed that the entered PIN is sent to the backend via the endpoint /check-pin?pin=1234.
    - Response from the server indicated whether the PIN was correct using the success parameter (true for correct, false for incorrect).
3. Content Discovery:
    - Revisited the challenge description, which hinted at avoiding brute force and suggested the possibility of hidden directories.
    - Tried common hidden directories and accessed the URL /robots.txt.
    - Discovered the correct PIN mentioned in the robots.txt file.
4. Exploitation:
    - Used the discovered PIN to successfully unlock the web application.
5. Flag Retrieval:(points-100)
    - After entering the correct PIN, the following flag was revealed:
    - flag {V13w_r0b0t5.txt_c4n_b3_u53ful!!!}

Flag: flag{V13w_r0b0t5.txt_c4n_b3_u53ful!!!}

CTF Report

Full Name: Krish Gupta Program: HCS - Penetration Testing 1-Month Internship

Date: 08 March 2025

Category: Web 2.0

Description: This challenge involved uncovering hidden files and decoding encoded data to retrieve the final flag.

Challenge Overview: The "The World" lab required careful content discovery, request analysis, and decoding techniques to successfully obtain the flag.

Steps for Finding the Flag:

1. Initial Reconnaissance:
    - Used directory brute forcing tools like Dirbuster to check for hidden files and extensions.
    - Inspected the source code and checked various files through Burp Suite.
2. Capturing Requests:
    - Captured HTTP requests using Burp Suite to analyze communication between the client and server.
    - Explored different paths and parameters to find any hidden directories or files.
3. Content Discovery:
    - Finally discovered a hidden file named secret.txt.
    - Accessed the file through the URL and retrieved an encoded string.
4. Decoding the Data:
    - The contents of secret.txt were Base64 encoded.
    - Used an online Base64 decoder to decode the string and obtain the final flag.
5. Flag Retrieval:(points-150)
    - After decoding, the following flag was revealed: FLAG{Y0u_hav3_4xpl0reD_th3_W0rLd!}

Flag: FLAG{Y0u_hav3_4xpl0reD_th3_W0rLd!}

CTF Report

Full Name: Krish Gupta Program: HCS - Penetration Testing 1-Month Internship

Date: 08 March 2025

Category: OSINT

Description: This challenge required uncovering historical data and hidden files through open-source intelligence techniques.

Challenge Overview: The "Time Machine" lab was based on discovering confidential information hidden from the government. Using domain investigation and historical data analysis, the goal was to retrieve the flag.

Steps for Finding the Flag:

1. Initial Reconnaissance:
    - Used the whois command to gather domain information for trojanhunt.com.
    - Retrieved broad details like domain creation date, update date, and name servers, but no useful information related to the flag was found.
2. Exploring Historical Data:
    - Accessed the Wayback Machine at https://archive.org/web/.
    - Searched for historical snapshots of trojanhunt.com.
    - Discovered old data and hidden files within archived versions of the site.
3. Discovery of secret.txt:
    - Within the archived data, found a hidden file named secret.txt.
    - Accessed the contents of secret.txt and retrieved the final flag.
4. Flag Retrieval: (points-100)
    - The flag was successfully extracted from the secret.txt file.

Flag: flag{Tr0j3nHunt_t1m3_tr4v3l}

Network Forensics CTF Report: Corrupted

CTF Topic: Network Forensics
CTF Name: Corrupted

Objective

The goal of this CTF was to recover a hidden flag from a corrupted PNG file provided as part of the challenge.

Steps Taken

1 File Identification and Initial Analysis

- **Command:** file chall.png-1740909420074-618633075.png
- **Output:** Data file (indicated possible corruption)

2 Header Analysis and Hex Inspection

- **Tool:** hexedit output.txt
- **Observation:** Confirmed the presence of a PNG magic header:
- 89 50 4E 47 0D 0A 1A 0A

3 Fixing the PNG Header

- **Command:**
- printf '\x89\x50\x4E\x47\x0D\x0A\x1A\x0A' | dd of=output.txt bs=1 seek=0 conv=notrunc
- **Purpose:** Correcting the PNG file header to make the file readable

4 Extraction Attempts

- **Binwalk:**
- binwalk -eMe output.txt --run-as=root

  Result: No useful files were extracted
- **Foremost:**
- foremost output.txt
    - **Result:** Audit file generated, but no files were recovered

5 Entropy Analysis

- **Command:** binwalk --entropy output.txt
- **Observation:** High entropy indicated potential compression or encryption

6 Final Analysis and Flag Discovery(points-100)

- **Tool:** hexedit
- **Discovery:** After fixing the header and inspecting the hex data, the flag was found:

flag{m3ss3d_h3ad3r$}