CTF Report

Full Name: Aashutosh Thakur
Program: HCS - Penetration Testing 1-Month Internship
Date: 07/03/2025

Got Total Point:- 450

Category: OSINT(100 points)

Description: This challenge involves analyzing an encrypted file and decoding it using the ROT47 cipher to retrieve a hidden flag.

Challenge Overview: Mr. TrojanHunt has the ability to travel through time and is hiding highly confidential files from the government. The National Investigation Agency (NIA) seeks help in retrieving these secrets. The challenge requires reverse engineering an encrypted file to extract the hidden flag.

Steps for Finding the Flag:

1. **Initial Reconnaissance:** The challenge provides a downloadable file. After extracting the zip file, we navigate to the SRC folder. Continue exploring subfolders until we locate a file named scrum.bky.
2. **Input Validation Testing:** Open scrum.bky using a text editor. Copy the content of the file, which appears to be encoded.
3. **Directory Enumeration:** The content inside scrum.bky is encrypted with the ROT47 cipher.
4. **Exploitation:** Once vulnerabilities are identified, exploit them to gain unauthorized access or manipulate the application's behavior to reveal the flag. Use an online ROT47 decoder or write a script to decode it.

5. **Flag Retrieval:** After decoding, the flag is found at the bottom of the output. The flag follows the format: flag{!@#$%^&*()_+}.

6. **Flag:** flag{Tr0j3nHunt_t1m3_tr4v3l}

Category: Web(2.0)(100 points)

Description: This challenge focused on content discovery within a web application, emphasizing methodologies beyond brute force approaches like dirbuster.

Challenge Overview: The goal was to locate hidden files or directories on the given website (https://lock-web-web.hackatronics.com) to retrieve the flag. The challenge required reconnaissance techniques beyond simple brute-force enumeration.

Steps for Finding the Flag:

1. **Initial Reconnaissance:** Inspected the website manually and analyzed its structure. Used browser developer tools (Inspect Element, Console, Network tab) to look for hidden resources.
2. **Input Validation Testing:** Checked robots.txt, which often contains restricted directories. Found a reference leading to a hidden file.
3. **Directory Enumeration:**
4. **Exploitation:** Accessed the hidden file and extracted relevant information.
5. **Flag Retrieval:** the flag is found at the above of the output. The flag follows the format: flag{!@#$%^&*()_+}.
6. **Flag:** flag{V13w_r0b0t5.txt_c4n_b3_u53ful!!!}

Category: Cryptography(100 points)

Description: This challenge involves decoding an encoded message that has been encrypted using an esoteric programming language known as ReverseFuck. The objective is to extract the flag from the given file.

Challenge Overview: The challenge provides an unknown encoded file, requiring us to reverse-engineer the encoding method. By analyzing the content, we can determine that the encoding scheme belongs to ReverseFuck. Using an online decoder, we can retrieve the hidden flag.

Steps for Finding the Flag:

1. **Initial Reconnaissance:** The challenge provides a .file that contains the encoded text.

2. **Input Validation Testing:** Open the file using a text editor to view its contents in vs code. Copy the encoded string from the file.
3. **Directory Enumeration:** Navigate to https://www.dcode.fr/reversefuck-language. Paste the copied code into the decoder.

4. **Exploitation:** Loaded the file into Ghidra for function tracing. Identified an obfuscated string in memory referencing a hidden text. Click on "Decrypt" to obtain the flag.

5. **Flag Retrieval:** The decoded message reveals the flag in the format: flag{...}. Copy and document the flag for submission.

6. **Flag:** flag{R3vers3ddd_70_g3t_m3}

Category: Reverse Engineering(150 points)

Description: This challenge involves analyzing an old project file to uncover hidden text that was embedded in it years ago. The goal is to reverse engineer the project and retrieve the secret message.

Challenge Overview: A project file from my childhood was found, but the hidden text inside it is no longer visible. Using various reverse engineering techniques, I need to locate and extract the text from the project file.

Steps for Finding the Flag:

1. **Initial Reconnaissance:** Downloaded the file, then checked the file type and format.
2. **Input Validation Testing:** Used strings, binwalk, and exiftool to extract readable text. Checked for any embedded messages in the metadata.
3. **Directory Enumeration:** Open the file in a hex editor (HxD, Ghidra, or IDA Pro).
4. **Exploitation:** Loaded the file into Ghidra for function tracing. Identified an obfuscated string in memory referencing a hidden text.
5. **Flag Retrieval:** After decoding, the flag was found at the bottom of the output.
6. **Flag:** flag{t00_much_rev3rs1ng}