CTF Report

Full Name:
BELKEBIRKAOUTHAR

Program: HCS - Penetration Testing 1-Month Internship
Date: 10/03/2025.

Category: {WEB2.0}

Description: L0Ck_Webge

Overview:

It’s important to follow good content discovery methodology on sites you are testing. This is NOT always something like dirbuster or other bruteforcing approaches?

Steps for Finding the Flag:

1. **1** : **Click the provided link** to access the site requiring a PIN to unlock the content.
2. **Try to find the PIN** by manually entering several attempts.
3. **Open Burp Suite** and begin intercepting the HTTP requests sent by the site.
4. **Send the intercepted request** to Intruder in Burp Suite.
5. **Load your payload** in Intruder to perform a brute-force attack on the PIN.
6. **Launch the brute-force attack** by sending multiple attempts until you get a response with "success = true."
7. **Once the correct PIN is found**, you retrieve the flag and unlocked content.

Flag: FLAG{V13w_r0b0t5.txt_c4n_b3_u53ful!!!}

Category: {WEB2.0}

Description: the world

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

Steps for Finding the Flag:

1. **Analyze the webpage**: No visible hints were found on the page, so the next step was to perform a more detailed analysis.
2. **Perform directory fuzzing with FFUF**:Use the ffuf tool to fuzz for hidden directories and files.The initial command used was:
   ffuf -u https://the-world-web.hackatronics.com/FUZZ -w /usr/share/wordlists/dirb/common.txt This revealed some restricted files and directories like .htaccess and .htpasswd, but no direct access to the flag.
3. **Modify the approach by adding file extensions**: Include file extensions like .txt, .php, and .html to the fuzzing process.The modified command was:
   ffuf -u https://the-world-web.hackatronics.com/FUZZ -w /usr/share/wordlists/dirb/common.txt -e .txt,.php,.html This led to the discovery of the secret.txt file.
4. **Access the secret.txt file**: Open https://the-world-web.hackatronics.com/secret.txt in the browser to find the flag in plain text.
5. **Decode the flag from base64**: Copy the content of secret.txt and decode it using a base64 decoder to obtain the final flag:

Flag: FLAG{Y0u_hav3_4xpl0reD_th3_W0rLd!}

Category: {NetworkForensics}
Description: Corrupted

Challenge Overview:

This is too EasyPeasyy!

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

Steps for Finding the Flag:

Here are the steps in bullet-point format for the CTF3 challenge:

1. **Initial Analysis :**Analyze the downloaded file using the file command to determine its type:
   -file chall.png: The result indicates that the file is corrupted.Use strings to check if the file contains any readable strings:
   -strings chall.png:This command did not return any useful results.
2. **Installing Hexedit and Repairing the File**:Since the file is corrupted, open it with a hex editor to inspect and fix its header.
3. **Installing Hexedit**:If the tool is not installed, install it using:
   sudo apt update && sudo apt install hexedit -y
4. **Modifying the Header**:Open the file with hexedit:
   -hexedit chall.png :The first 8 bytes of a valid PNG file should be:
   89 50 4E 47 0D 0A 1A 0A
   If these bytes are incorrect, modify them and save the file by pressing **CTRL + X**, then **Y** to confirm.
5. **Verification and Flag Extraction**
   a. After modifying the header, try opening the image. This time, it should display correctly.
   b. The flag is visible directly in the image:flag{m3ss3d_h3ad3r$}

Flag: flag{m3ss3d_h3ad3r$}

Category: {NetworkForensics}
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:

Voici les étapes sous forme de tirets :

1. 1 Extraire les données POST avec Tshark
2. Exécute la commande suivante (en remplaçant le fichier) : tshark -r capture.pcapng-1740909704352-300806583.pcapng -T fields -e http.file_data -Y "http.request.method == POST"
3. Extraire et analyser les données :Si tu vois des données encodées en Base64, prends-en note.Sinon, utilise un script Python pour extraire les morceaux intéressants :
4. Crée un script extract_data.py et exécute-le avec python3 extract_data.py.
5. Décoder les données Base64 :Si tu vois une chaîne comme celle-ci : ZmxhZ3ttdWx0MXBsM3A0cnRzYzBuZnVzM3N9
6. Utilise la commande suivante pour la décoder : echo "ZmxhZ3ttdWx0MXBsM3A0cnRzYzBuZnVzM3N9" | base64 -d

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. **Downloading and Extracting the .aia File:**Use the following command to extract the contents of the `.aia` file: `unzip CTF.aia-1740910120281-691025702.aia -d project_aia`
2. **Exploring the File Structure :**Use the `tree` command to display the file hierarchy: `tree project_aia`
3. **Analyzing the Scrum.bky File:** Display the content of the `Scrum.bky` file: `cat project_aia/src/appinventor/ai_23saahilt/CTF/Scrum.bky`
4. **Decoding ROT47 Encoded Text :**Decode the encoded string with the following command: `echo "7=28LE__0>F490C6GbCD\`?8N" | tr '!-~' 'P-~!-O'`

Flag: flag{t00_much_rev3rs1ng}

Category: { Reverse Engineering}

Description: DecryptQuest

Challenge Overview:

One day, one of Samarth's imaginary friends, Arjun, mysteriously hands him a text file claiming it holds encrypted secret data impossible to decode! Arjun dangles a $1,000,000 reward if Samarth manages to extract the information. However, Arjun enjoys mischief and attempts to trick Samarth by flooding the file with loads of irrelevant data. Would you assist Samarth in unlocking this top-secret information? He pledges to split the reward with you if successful !!

Flag format: flag{HCS_HCS}

Steps for Finding the Flag:

1. After downloading the file, I uses cyberchef and got Java code that can make the flag.
2. In java code the were drive link so I accessed it and decrypt its content. Then I find the hint that says to use Unix Epoch Time.
3. Then I made some corrections to make the code simple.
4. I edited my code to search for 1970 value when looping and stop the running loop when it finds it.
5. After performing this I found the flag.

Flag: flag{hjwilj111970djs}