HACKTIFY cybersecurity

CTF Report

Full Name : Sachin Madhumitha Sree D
Program : HCS-Penetration Testing 1-Month Internship
Date : 09-03-2025

CHALLENGE-1

Category: Web
Description: A challenge focused on analyzing web application behavior and uncovering hidden files.

Challenge Overview:
In this challenge, you must explore the given web application and identify hidden files or directories that may contain valuable information. Pay close attention to common misconfigurations that can leak sensitive data.

Steps for Finding the Flag:

1. **Initial Reconnaissance:** Start by analyzing the website's structure and available resources. Look for common files that may provide insights.
2. **Checking robots.txt:** Access the robots.txt file by navigating to https://lock-web-web.hackatronics.com/robots.txt .This file often contains disallowed directories that might hold sensitive information.
3. **Exploring Restricted Directories:** Use the discovered paths to check for files that might expose data or hints.
4. **Flag Retrieval:** Once the flag is found, capture and document it for submission.

Flag: flag{V13w_r0b0t5.txt_c4n_b3_u53ful!!!}

CHALLENGE-2

Category: Web
Description: A challenge that requires exploring a web application, navigating through different pages, and analyzing external resources to uncover hidden information.

Challenge Overview:
In this challenge, you will need to thoroughly explore the web application and analyze various elements to find the flag. Pay close attention to scripts, external resources, and hidden files that may contain useful information.

Steps for Finding the Flag:

1. **Initial Reconnaissance:** Start by exploring https://the-world-web.hackatronics.com and navigate through its pages to understand the structure.
2. **Dashboard Exploration:** Go to https://the-world-web.hackatronics.com/dashboard.html and investigate its contents for any hints or vulnerabilities.
3. **Analyzing External Resources:** Examine external scripts like https://kit.fontawesome.com/3bb29e5d19.js to see if they leak any useful information.
4. **Finding the Flag:** Discover and access https://the-world-web.hackatronics.com/secret.txt, which contains an encoded Base64 flag.
5. **Decoding the Flag:** Convert the Base64-encoded text to reveal the final flag.

Flag: FLAG{Y0u_hav3_4xpl0reD_th3_W0rLd!}

CHALLENGE-3

Category: Network Forensics
Description: A challenge focused on file forensics and data recovery techniques.

Challenge Overview:
In this challenge, you are provided with a corrupted PNG file. Your task is to analyze and repair the file to retrieve the hidden flag. Understanding file structures and utilizing forensic tools will be key to solving this challenge.

Steps for Finding the Flag:

1. **File Analysis:** Inspect the corrupted PNG file using tools like binwalk, xxd, or file to determine the nature of the corruption.
2. **Header Examination:** Identify if the file's header is damaged or missing, as this is a common issue with corrupted PNG files.
3. **Repairing the File:** Use tools such as **EaseUS Data Recovery** or **PNG repair tools** to attempt reconstruction of the damaged file.
4. **Extracting the Flag:** Once repaired, open the file to reveal the flag embedded within.

Flag: flag{m3ss3d_h3ad3r$}

CHALLENGE-4

Category: OSINT (Open Source Intelligence)
Description: A challenge that requires using open-source investigation techniques to track down hidden information on the internet.

Challenge Overview:
In this challenge, you must uncover confidential secrets hidden by Mr. TrojanHunt. By utilizing search engines and online archives, you will piece together clues to retrieve the flag.

Steps for Finding the Flag:

1. **Google Search:** Search for "Mr. TrojanHunt" on Google and examine the search results.
2. **Finding the Right Link:** Click on the **third** link in the search results, which leads to https://archive.org/details/secret_202103.
3. **Exploring the Archive:** Navigate through the archived page and inspect the text or available files.
4. **Retrieving the Flag:** Identify the hidden text containing the flag and document it for submission.

Flag: flag{Tr0j3nHunt_t1m3_tr4v3l}

CHALLENGE-5

Category: Cryptography
Description: A challenge that involves decoding an esoteric programming language to uncover the hidden flag.

Challenge Overview:
In this challenge, you receive a recipe written in an esoteric language similar to Chef. Your task is to interpret and correct the code, run it, and extract the hidden Brainfuck code, which must then be decoded to reveal the flag.

Steps for Finding the Flag:

1. **Understanding the Recipe:** Open the provided recipe.txt file and recognize that it is written in the **Chef** esoteric programming language.
2. **Finding an Interpreter:** Search Google for "Chef esolang interpreter" and use an online tool to execute the code.

3. **Fixing Syntax Errors:** Some commands in the script contain grammatical errors (e.g., "until crack" should be "until cracked"). Fix these errors before running the script.
4. **Extracting Brainfuck Code:** When executed, the Chef script outputs a **Brainfuck** program.
5. **Decoding Brainfuck:** Run the extracted Brainfuck code (++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>>>++++++++++++++++++++++.<<++++++++++++++++++.>>----.----------.<<++++.----.-----.>>.++++++++++++++++++++.<<++++++++.>>-.++++.<<.>>----------.<<----------.) in a **Brainfuck interpreter** to retrieve the final flag.

Flag: flag{y0u_40+_s3rv3d!}