CTF Report

Full Name: Rachael Ayomide Fanifosi
Program: HCS - Penetration Testing 1-Month Internship
Date: 11/03/2025

Category: Web 2.0

Description: Web 2.0 transformed the internet from static websites to interactive and user- driven platforms. It enabled social media, real-time collaboration, and user-generated content on sites like Facebook, YouTube, and Wikipedia. This era emphasized participation, sharing, and dynamic web applications.

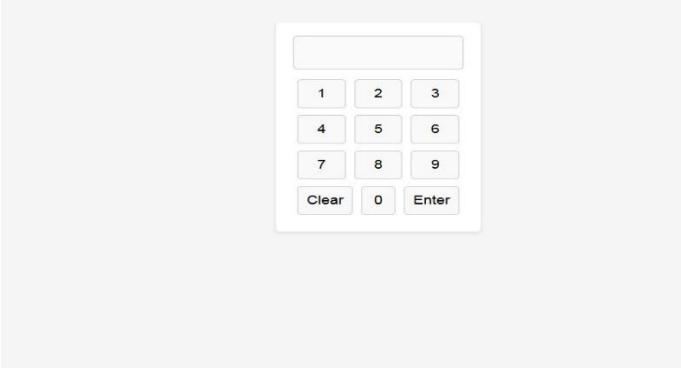
Challenge Overview:

a) **Lock web** - 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.

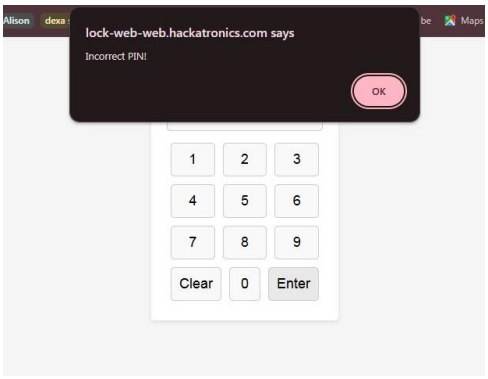
Steps for Finding the Flag:

1. Go to https://lock-web-web.hackatronics.com

2. You will see the page like pin lock interface.



3. **Observation-** I observed the URL no changes to be appeared. I try to find any clue around the pin lock interface nothing happened. Randomly enters the pin by guessing nothing happened.



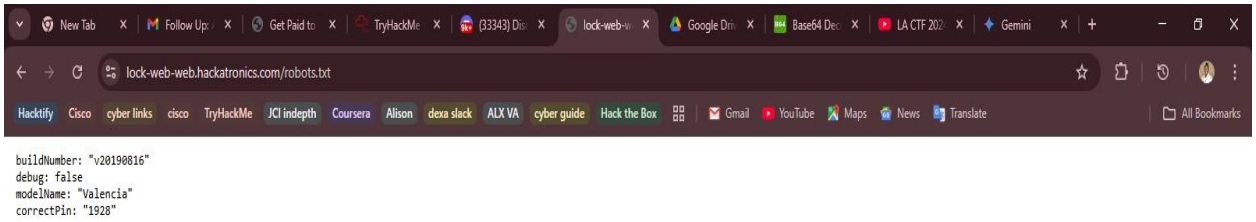
4. **Reconnaissance** like viewed page source, explored http request, hidden files, hints or comments nothing found.

Observation

- **Analyzing** the given hints details: Think like a robot beep bop.
- **Finding and searching** for the specifically word "ROBOT" and the connections between a web application and a robot beep bop.
- **Understanding** and I came to know while doing **Manual Enumeration.**

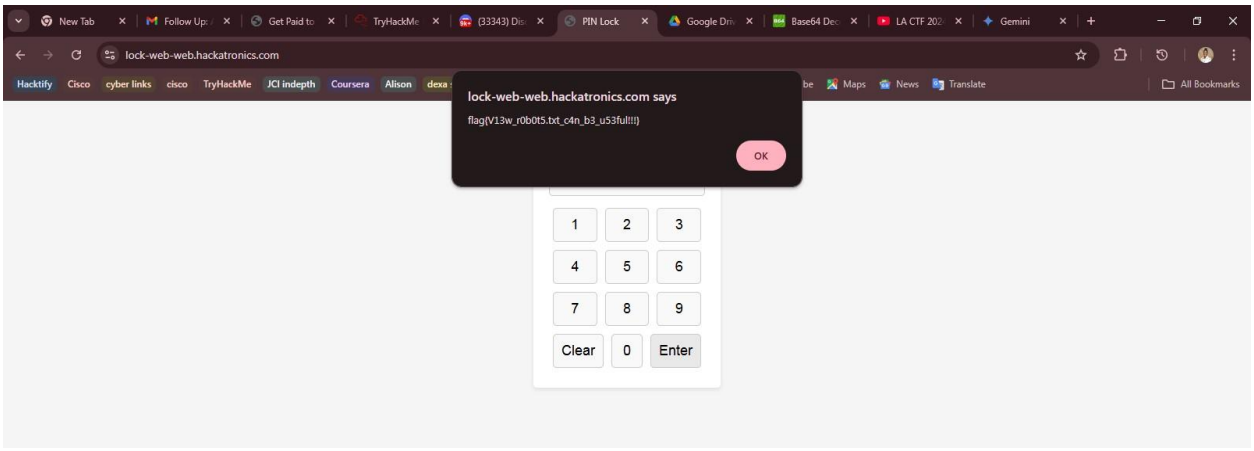
5. **Guessing common directories** like admin, uploads, config, backup. I came to know about the **robots.txt** it means website use robots.txt file to tell search engine bots which pages they can or can't access.

Site- https://lock-web-web.hackatronics.com /robots.txt



6. Found the sensitive information and correct Pin-1928, putting the pin in pin lock, and retrieving the flag.

7. Flag Retrieval



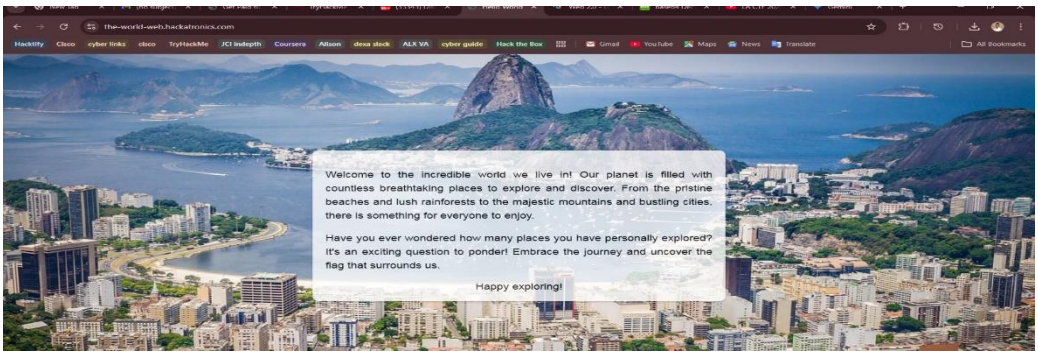
8. **Flag {V13w_r0b0t5.txt_c4n_b3_u53ful!!!}**

b) **The World** - 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. Your mission: dig deep into this website to find hidden paths and uncover the flag.

Steps for finding the flag

1. Go to https://the-world-web.hackatronics.com

2. You will see page like these, click on Happy exploring button that redirect you on another page.



3. **Reconnaissance:** Explored and gone through all the pages that this web application contains, from inspecting page it, explored http request, hidden files, hints or comments nothing found.

4. **Doing Manual Enumeration:** Guessing common directories like admin, uploads, config, backup, robots, sitemap, but to be found that secret.txt works.

Site: https://the-world-web.hackatronics.com/secret.txt

Here I got the **cipher code** also, that has to be decoded.

Decoding the code
RkxBR3tZMHVfaGF2M180eHBsMHJlRF90aDNfVzByTGQhfQ== With the help of base64 decode.
Site- https://www.base64decode.org/

After decoding the cipher, I got the flag also.

5. **Flag:** flag{Y0u_hav3_4xpl0reD_th3_W0rLd!}

CATEGORY: Reverse Engineering

Description: Reverse engineering is the process of analyzing a system, software, or hardware without access to its source code or design documents. It involves deconstructing compiled programs, dissecting binary files, and reconstructing the application's logic. This helps identify vulnerabilities, modify functionality, or gain deeper insights into its operations.

Challenge Overview:

a) **Decrypt Quest**: 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!!

Steps for finding the flag

1. **Download the** Answer.txt file

2. After downloading the zip file, extract it or directly open it, there is file name **Answer.txt**

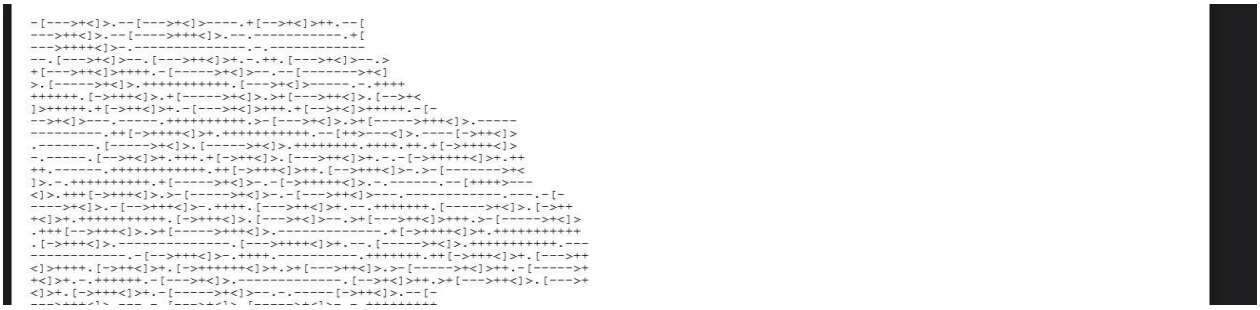
3. Open that file (Answer.txt), there will be huge scrambled code is present in that file.

4. Copy that code for **decoding** process on site: https://www.base64decode.org/

5. After decoding, copy that decoded code and paste in html pad and observed it some **java code** is present under that we will get a **drive link: https://drive.google.com/file/d/1A6Eh_oCtEniOYq8bxwrujRuyT1SU_Q-b/view?usp=sharing**

6. Browse and open that link, you will find another file name- **key.txt**

7. You will see in that file symbols like these shown in picture.



After **analyzing** it these code symbols is called Brainfuck.
{It is a minimalist esoteric programming language. It operates on a simple memory tape with an array of cells, and it uses only eight commands (+, -, >, <, [,], . and ,).}
For these to decode use on this site: https://sange.fi/esoteric/brainfuck/impl/interp/i.html

8. After decoding it, the code looks like this:
Um9zZXMgYXJlIHJlZCwKVmlvbGV0cyBhcmUgYmx1ZSwKSWYgb25lIHdhbnRzIHRvIHBpY2sgdGhlIGNvcnJlY3QgZmxhZywKVGhlbiB0aGV5IHNob3VsZCBzZWVrIHRoZSBVbml4IEVwb2NoIGFzIGEgY2x1ZQ==

This code also has to be decoded on site: https://www.base64decode.org/

9. After decoding it, result is like this:
Roses are red,
Violet are blue,
If one wants to pick the correct flag,
Then they should seek the Unix Epoch as a clue

10. **Observation**:
   a. This decoding result was the as the hint we have given.
   b. Once again trying to go through with all the coding section.

11. **Analyzing-** After properly analyzing the java code, I only took the coding part that should be run or executed, I clear out the remaining part of it.

12. **Coding and executing** the java code, finally I got the programming that was running and executing also, I got the flag that was accepted.

Welcome to the LMD machine 3000!
Please enter an integer:
571

13. **Flag Retrieval**: flag{hjwilj111970djs}

b) **Lost in the Past**- I enjoyed making small projects when I was at a young age! 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. Download the file, after that I **analyze** the file and extension the file (.aia).

It's an (App Inventor Archive) file extension is used by MIT App Inventor, a visual programming environment for building Android applications.

2. I **change** the file extension to (.zip) file and extracted the file.

3. Observation:
   - Folder contain the files of resource and project.
   - Going through all the files and content inside.
   - I taught of making an app after that in it some kind of flag will appear in it.
   - I follow all the procedure and steps on that website to make app, but given files contain some sort of error and I'm not able to catch it.
   - The other files like (**.scm**) (**.bky**) I opened in notepad, so that I can easily read the code.
   - I once again gone through the files and catch the word (present in the file name **Scrum.bky)**

     Cipher <field name="Cipher">7=28LE__0>F490C6GbCD`?8N</field>

4. Analyzing the cipher text type**:** 7=28LE__0>F490C6GbCD`?8N
   On site: https://www.dcode.fr/cipher-identifier

It was Rot47 cipher text.

5. **Decoding** the cipher text on site: https://www.dcode.fr/rot-47-cipher

Got the flag successfully.

6. Flag: flag{t00_much_rev3rs1ng}

Category: OSINT

Description: OSINT (Open-Source Intelligence) refers to the process of collecting, analyzing, and using publicly available information from various sources to gain insights. It is widely used in cyber security, investigations, competitive intelligence, and ethical hacking.

Challenge Overview:

a) **Time Machine:** Mr. TrojanHunt has power to travel time. He is hiding some extremely confidential file from the government. Can you help NIA to get secrets of TrojanHunt?

Steps for finding the flag:

1. **Reconnaissance**: Going through the Instagram, Facebook, google to find the specific word for Mr.TrojanHunt, nothing found!
2. **Analyzing** the description very carefully, Mr. Trojan Hunt has power to time travel.
3. **Searching** the relationship between both, found that I have to google dork, but nothing found.
4. **Gathering** more information regarding and found to be in Wayback Machine. (Wayback Machine is a digital archive of the internet maintained by the Internet Archive. It allows users to view past versions of websites by capturing snapshots over time.)

Site: https://web.archive.org/

5. Digging Processs:
    a. Click on https://archive.org/ for extracting data.
    b. **Found** these data "**secret_202103**" in archive.org/details/secret_202103
    c. Now click on show all files button in that page you will redirected in these https://archive.org/download/secret_202103
    d. There will be file name **secret.txt** will be present click on that you will get flag.
    e. **Direct Link** https://dn790008.ca.archive.org/0/items/secret_202103/secret.txt
6. Flag Retrieval: flag{Tr0j3nHunt_t1m3_tr4v3l}

b) **Snapshot Whispers-** Skeptical about my friend's recent travel claims, I requested a photo, and to my surprise, they sent me an image that seemed more like a generic internet find than a personal capture. Help me find out the name of the

photographer who clicked the photo.

Steps for finding the flag

1. Download the file, founded that it was image some kind of studio or hall

2. Reconnaissance and Observation:

   - Trying to extract data from image, but nothing found.
   - Going through google image search, many similar images appeared, nothing came in handy.

3. **Image Description:** It was Sydney Opera House in New South Wales, Australia.

4. **Social media footprints:**

   - **Pinterest:** Some similar kind of photo is been matched on Pinterest found on and checked that was uploaded on Pinterest by person name: sailpawar72927.
   - Gone though from **Instagram** of him nothing to found.

5. So many tools been used to match the image, but nothing to be found.

6. **Analyzing**: The hints details:"review"

7. **Crawl** through the Google maps and search for Sydney Opera House in New South Wales, Australia, map link: https://maps.app.goo.gl/MofvD9XnqM1Kq9gE6?g_st=ac

8.Gone through so many google reviews and check the photo, but null:

Then I look closely in google map.
It was the 2 different type of opera house:

i. Sydney Opera House Concert Hall

ii. Sydney Opera House

9. I Change my keywords for searching in google map: Sydney Opera House Concert Hall, map link: https://maps.app.goo.gl/ny4m8L2rSpp643C1A?g_st=ac

10. In that I filtered it by word "Concert hall" for fast result.

Here is the name of owner of image- **Jeffery Seidman**

11. Link of image google map that is founded
https://maps.app.goo.gl/phfVomwdNZ7gtmos7?g_st=ac

12. Got the name of owner of image as flag.
Flag Retreival: flag{Jeffrey Seidman}

Category: Crypto

Description: Cryptography is the science of using mathematics and computers to create and secure messages. It's used to protect information so that only the intended recipient can read it.

Challenge Overview:

a) **Success Recipe**: My friend who is a Chef sent me this recipe but i can't understand it He likes to write in weird languages Can you help me?

Step the finding the page

1. Download the file receipe.txt and open it.

2. Observation:
- I wasted so much of time just for understanding the file and the content written in it.
- Then by taking the help of ChatGPT, I just pasted the file content inside ChatGPT.
- By these I understand that it is some kind of **esolang code** most likely a **recipe-based esoteric language like Chef** or something similar.

3. After **identifying** the code language, let's decode these file with help of interpreter Site: https://esolangpark.vercel.app/ide/chef

4. Copying the content from file and pasting into code Editor tab and running it. Got the **error**.
By **observing** in execution output tab:
Loop verb mismatch:
expected 'drinked', found 'drink'
expected 'spreaded' found 'spread' etc

Because, the code in which the file contained in it was present already like that, there was so much error present in it one after another.

After solving that error, I got another code called **Brainfuck**.
(It is a minimalist esoteric programming language. It operates on a simple memory

tape with an array of cells, and it uses only eight commands [+, -, >, <, [,], . and ,]).

5. **Decoding** these symbol code on site: https://sange.fi/esoteric/brainfuck/impl/interp/i.html Got the result flag as:y0u_40+_s3rv3d!

6. **Flag Retrieval:**flag{y0u_40+_s3rv3d!}

b) **Wh@t7he####-** Change my mind!

Steps for finding the flag:

1. Download the file.

2. When I opened the file, it was **Brainfuck programming language**.
{It is a minimalist esoteric programming language. It operates on a simple memory tape with an array of cells, and it uses only eight commands (+, -, >, <, [,], . and ,).}

3. Decoding this language on site: https://www.dcode.fr/reversefuck-language

4. By decoding the code, I got the flag.

5. Flag Retrieval:flag{R3vers3ddd_70_g3t_m3

Category: Network Forensics

Description: Network Forensics is a branch of digital forensics that focuses on monitoring, capturing, analyzing, and investigating network traffic to detect cyber threats, security breaches, and malicious activities. It helps in identifying intrusions, tracking attackers, and gathering evidence for legal proceedings.

Challenge Overview:

a) **Corrupted -** This is too Easy Peasyy!

Steps for finding the file

1. Download the image file, I opened it but found to be broken .png file.

2. Applying different **basic troubleshooting** such as:

   a. Re-download the Image.

b. Try Opening with Another Program.
c. Convert or Rename the Image.

3. Then I used the tool site: https://hexed.it/

4. Here I found out that image header hex, I changed the starting header with **89 50 4E 47 0D 0A 1A 0A**

5. After changing the header of image, saving and downloading it from that site.

6. I opened that image; I found the flag picture in it.

7. Flag Retrieval:flag{m3ss3d_h3ad3r$}

b) **Shadow web-** 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

1. Download the file.

2. Open the file in wire shark tool.

3. Follow the HTTP request protocol.

4. Filtering the traffic by putting filter http.request.method=="POST" in filter display.

5. **Analyzing:** Now follow the HTTP requests stream.

6. As we are changing the HTTP request one by one.

7. In the Data Bytes section, by observing bytes are changing constantly. Taking the notes of every single characters from every request.

8. We will get the code one by one as we follow up the HTTP Request. As ZmxhZ3ttdWx0MXBsM3A0cnRzYzBuZnVzM3N9!()*

9. **Decoding** the code ZmxhZ3ttdWx0MXBsM3A0cnRzYzBuZnVzM3N9!()*
On site: https://www.base64decode.org/

10. Flag Retrieval:flag{mult1pl3p4rtsc0nfus3s}