HACKTIFY
cybersecurity

CTF Report

Full Name: Geshom Lukoshi
Program: HCS - Penetration Testing 1-Month Internship
Date: 9th March 2025

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

Steps for Finding the Flag:

1. **Reconnaissance**: I had to go through instagram, facebook profiles and google to find the specific word for Mr.TrojanHunt, nothing was found!

2. **Analyzing** the description very carefully, Mr.TrojanHunt 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 Process:**
    - Click on https://archive.org/ for extracting data.
    - **Found** these data "**secret_202103**" in archive.org/details/secret_202103

- Now click on show all files button in that page you will redirected in these https://archive.org/download/secret_202103
- There will be file name **secret.txt** will be present click on that you will get flag. □ **Direct Link** https://dn790008.ca.archive.org/0/items/secret_202103/secret.txt

Flag Retrieval: flag{Tr0j3nHunt_t1m3_tr4v3l}

Challenge Overview: □ 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. Downloading the file, found that it was an image of some kind of studio or hall (Theater).

2. **Reconnaissance and observation**:
   - I tried to extract data from the image, but nothing was found.
   - I did a google image search, many similar images appeared but to no avail as to who took the picture.

3. **Description about Image:** the image was taken inside a (theater) Sydney Opera House in New South Wales, Australia.

4. **Social media footprints:**

   - **Pinterest:** The similar image was matching on Pinterest, but it was uploaded by the user sailpawar72927.

5. I utilized many tools to match the image, but nothing was found.

6.**Analyzing**: The hints details: “review”

7. **Crawl:** through the Google maps I then searched and searched for Sydney Opera House in New South Wales Australia map link:

8. I looked through so many google reviews and checked for the photo, but to no avail. I

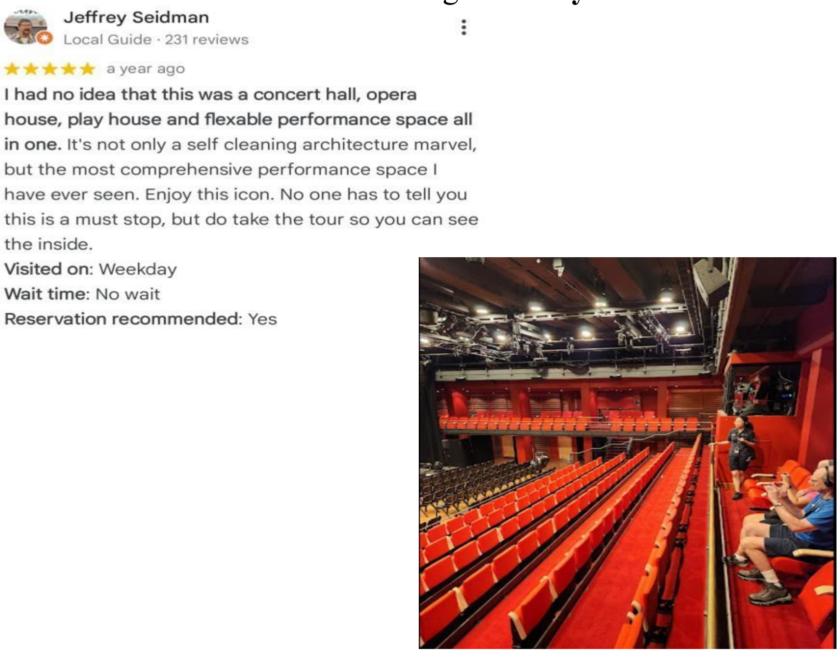
then look closely on the google map, I discovered that there are 2 different type of opera houses:

1. Sydney Opera House Concert Hall,

2. Sydney Opera House.

9. I Change my keywords for searching in google map: I searched for 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**

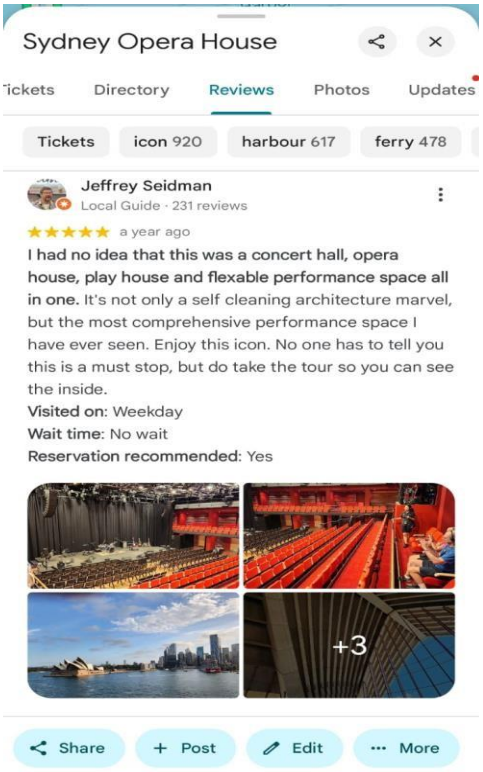


Jeffrey Seidman
Local Guide · 231 reviews

★★★★★ a year ago

I had no idea that this was a concert hall, opera house, play house and flexable performance space all in one. It's not only a self cleaning architecture marvel, but the most comprehensive performance space I have ever seen. Enjoy this icon. No one has to tell you this is a must stop, but do take the tour so you can see the inside.

Visited on: Weekday
Wait time: No wait
Reservation recommended: Yes



Sydney Opera House

Jeffrey Seidman
Local Guide · 231 reviews

★★★★★ a year ago

I had no idea that this was a concert hall, opera house, play house and flexable performance space all in one. It's not only a self cleaning architecture marvel, but the most comprehensive performance space I have ever seen. Enjoy this icon. No one has to tell you this is a must stop, but do take the tour so you can see the inside.

Visited on: Weekday
Wait time: No wait
Reservation recommended: Yes

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

12. Got the name of owner of image as flag.

Flag Retrieval: 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: Wh@t7he####- Change my mind!

Steps for Finding the Flag:

1. Download the file.

2. When I opened the file, it was gibberish, it was a "**Brainfuck programming language**".

This is a minimalist esoteric programming language. Which operates on a simple memory tape with an array of cells, and it uses only eight commands (+, -, >, <, [,], . and ,).}

3. I decoded the language on https://www.dcode.fr/reversefuck-language site.

4. After decoding the code, I then got the flag.

5. **Flag Retrieval**: **flag{R3vers3ddd_70_g3t_m3}**

Challenge Overview: Decrypt Quest!

Steps for Finding the Flag:

1. Download the Answer.zip-1740910433987-931520235 zip file.

2. Extract and open the answer.txt, I then converted the code found in the answer.txt into base64 from https://www.decode.fr/base-64-encoding.

3. After decoding, I found a java code with a drive link (which was an important discovery) the link was within code, it was commented out, the link was (https://drive.googlr.com/file/d/1A6Eh_oCtEni0Yq8bweujRuT2SU_Q-b/view?usp=

4. I opened the drive link and got the content in Brainfuck format.

5. I then went to https://www.decode.fr/brainfuck-language and decoded the brainfuck format code of the drive.

6. I got the base64 code, using the base64 converter I converted the code using the https://www.dcode.fr/base-64-encoding and got the following content:

   -Roses are red,

   -Violets are blue,

   -If one wants to pick the correct flag, then they should seek the Unix Epoch as Clue.

7. Knowing Unix Epoch as the important term, I then searched the strings “Unix Epoch introduced in” on google. And I got 1970 as the answer.

8. After analyzing the java code and compiling it, I discovered that the code was accepting numbers from 1-1106, after executing I got 1106 flags. As Unix Epoch was introduced in the year 1970, I choose the flag of that year and got the flag.

   Flag Retrieval: **flag{hlwilj111970djs}**