BlueHens CTF 2024 Writeup

Cal Poly Security Team – Hash Slinging Hackers

21st Place / 498 International Teams

Gravity

4th Place on Team in Point Scoring

Welcome Letter

MISC – 50 points

Provided a Welcome Letter with a few notes about the CTF

An important note was some authors used udctf{} others used UDCTF{}

It's important to read all instructions because it allowed me to assist other team members in understanding what to search for in other challenges, lowercase and uppercase format.

Flag was at end of the message.

Here's your flag:
UDCTF{guessy_is_sometimes_deduction_sometimes_awful}

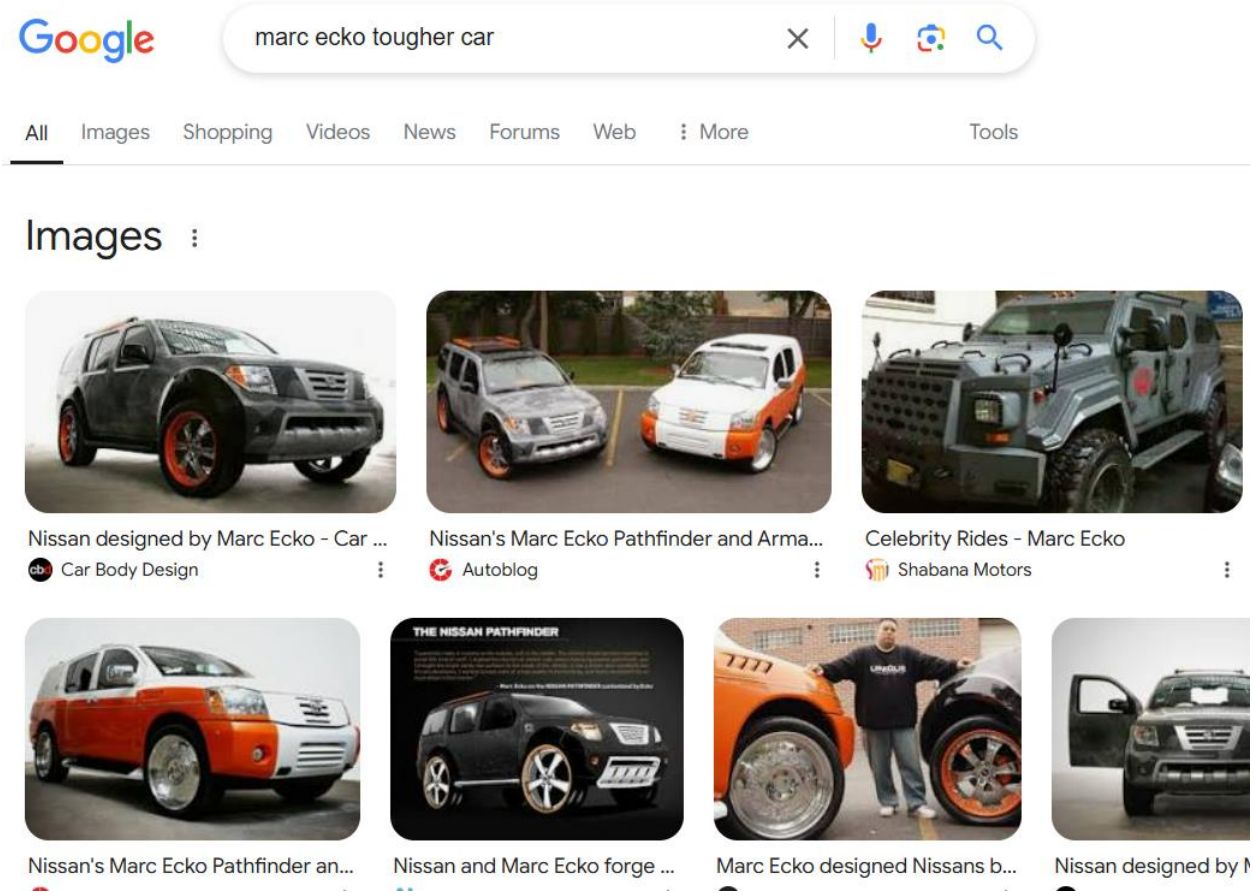
Training Problem: Intro to OSINT

OSINT – 50 points

Challenge Description: A famous person is selling their house. In this market, who wouldn't? Can you tell me who owns this house, and what the license plate of their "tough" car is? Flag format: udctf{FirstLast_licenseplate}

Provided image to download called osint1.png

First I check the info of image. Then I reverse search image using google. A name of Marc Ecko appears as home owner. I google “Marc Ecko tougher car”.



What car appears tough? The more gangster one or the SWAT looking vehicle? The swat looking vehicle. I then reverse search image that SWAT looking vehicle. I discover the name of vehicle, Gurkha. The licencse plate in all images are blurred. I then google “the gurhka marc ecko”. A youtube video appears with his license plate number.

Piecing together the flag: udctf{MarcEcko_wlj80f}

Whispers of the Feathered Messenger

FORENSICS – 100 points

Challenge: In a world where secrets flutter through the air, the bluehen carries a hidden message. A message that has been salted…. however its still a message… maybe the bluehen ignores the salt. This image holds more than meets the eye.

shasum: e717eefe9b41212b017152756b0e640f9a4f3763

bird.jpeg

Download image.

I check file info, open image in a notepad and ctrl+f keywords like udctf, maybe flag is in notes. Then follow the steganography steps from https://georgeom.net/StegOnline/checklist

1. Just to be sure what file you are facing with, check its type with `file filename`.
2. View all strings in the file with `strings -n 7 -t x filename.png`. We use `-n 7` for strings of length 7+, and `-t x` to view- their position in the file.
3. Exiftool to check all metadata
4. Binwalk to check image for hidden embedded files. My preferred syntax is `binwalk -Me filename.png`. -Me is used to recursively extract any files.
5. Java -jar stegsolve.jar used to explore colour & bit planes (Full Red, Inverse, LSB etc). Im looking static at the top of any planes. This tool also allows checking of RBGA values

I'm Hungry

OSINT – 480 points