**Flags Documentation**

**Title:** PGP Encryption  
**OS:** Linux  
**Difficulty:** Basic  
**Total Flags:** 1  
**Answers:** ZHAL2022{YzBuZ3JAdHZsQHQxb25zIQ==}  
**Steps to find flag:**

1. Download the contents on CTFd and extract the file (there should only be flag.zip visible)
2. Check the ‘show hidden files’ option, in which 2 .txt files will appear
3. Using an online PGP decrypting tool, use the private key to decrypt the PGP message in totally\_not\_here.txt
4. To find the password to decrypt the message, toggle to the hint tab to retrieve the hint on the password
5. Using the decrypted message, extract flag.zip and read flag.txt

**Title:** Rosicrucian Code  
**OS:** Linux  
**Difficulty:** Basic  
**Total Flags:** 1  
**Answers:** ZHAL2022{Y29uZ3JAdHVsQCtpb25z}  
**Steps to find flag:**

1. Download the contents on CTFd and extract the file (there should be a .png and flag.zip files)
2. Using an online tool, decrypt the Rosicrucian code to retrieve the password to flag.zip
3. With the password, extract flag.zip and read flag.txt

**Title:** ECBDIC  
**OS:** Linux  
**Difficulty:** Basic  
**Total Flags:** 1  
**Answers:** ZHAL2022{eTB1X2hAdjNfZm92bmRfbWU=}  
**Steps to find flag:**

1. Use an ECBDIC table to decrypt the long line of numbers
2. Decrypted message is the flag

**Title:** Secret Diary Entry  
**OS:** Linux  
**Difficulty:** Basic  
**Total Flags:** 2  
**Answers:** ZHAL2022{YW4wdGhlcl9mbEBn}, ZHAL2022{U09BQ0kyMDNJMTg0Tk9X}  
**Steps to find flag:**

1. Download the contents on CTFd and extract the file (there should only be 4.txt visible)
2. Check the ‘show hidden files’ option, in which a .txt and flag.zip files will appear
3. Read my\_secret\_password.txt and riddle out the password from the hints provided (beta)
4. Read user.txt to retrieve flag
5. Using an online steganography tool, decode deardiary.png to retrieve the second flag

**Title:** reMorse  
**OS:** Linux  
**Difficulty:** Basic  
**Total Flags:** 1  
**Answers:** ZHAL2022{Q29UZ3JHDHVSYXRPB25ZIQ==}  
**Steps to find flag:**

1. Use an online morse code translator to decode the code provided in CTFd
2. The decrypted message is the flag

**Title:** Vignere  
**OS:** Linux  
**Difficulty:** Basic  
**Total Flags:** 2  
**Answers:** ZHAL2022{bGtuZGd2aXJoZw==}, ZHAL2022{bjB0aDFuZ19oM3Iz}  
**Steps to find flag:**

1. Download the contents on CTFd and extract the file (there should be a flag.zip file)
2. Decode the vigenere to get the password to flag.zip (connect)
3. Read flag.txt to get the first flag before solving the riddle to retrieve the password to the second flag (piano)
4. Read flag.txt in flag2.zip to get the second flag

**Title:** Zodiac Killer  
**OS:** Linux  
**Difficulty:** Basic  
**Total Flags:** 2  
**Answers:** ZHAL2022{Ym05eWFYZHY=}, ZHAL2022{cmlvd2VvcGZucXByb24z}  
**Steps to find flag:**

1. Download the contents from CTFd and extract file (there should be 9.jpg and nine.zip)
2. Decode 9.jpg to gain the password to extract nine.zip (home/nine)
3. There should be 3 files in the extracted file (clue.txt and flag.zip)
4. Read clue.txt to retrieve the first flag and the clue to unlock the next one (nineofwands)
5. Extract flag.zip to get the second flag, using the password found through the clue

**Title:** Attacked  
**OS:** Linux  
**Difficulty:** Basic  
**Total Flags:** 2  
**Answers:** ZHAL2022{d3JpbmhvZ28}, ZHAL2022{ajBobkRlbk1Acms=}  
**Steps to find flag:**

1. Download the contents from CTFd and extract the file (there should be 10.txt and ten.png in the zipped file)
2. Use an online steganography tool to decode ten.png, where there are 2 flags present
3. Decode the second flag using an online spelling alphabet decoder

**Title:** Locked out of School  
**OS:** Linux  
**Difficulty:** Basic  
**Total Flags:** 3  
**Answers:** ZHAL2022{WkhBTDIwMjJ7c3Vwm3JfUEA1NXdvcmR9}, ZHAL2022{supr\_P@55word}, ZHAL2022{bHdlaXZud29pdm53}  
**Steps to find flag:**

1. Download the contents from CTFd and extract the file (there should only be 11.txt and school.zip visible)
2. Read 11.txt and decode the binary (to ebcdic so users will have to refer to ebcdic table to find the clue)
3. Ensure that show hidden files is ticked to find the hidden folder, eleven
4. Read password.txt to find the first flag
5. Decode the base64 string in between the curly brackets of the first flag to get the second flag and the password of school.zip
6. Extract school.zip with the password retrieved and read flag.txt to get the last flag

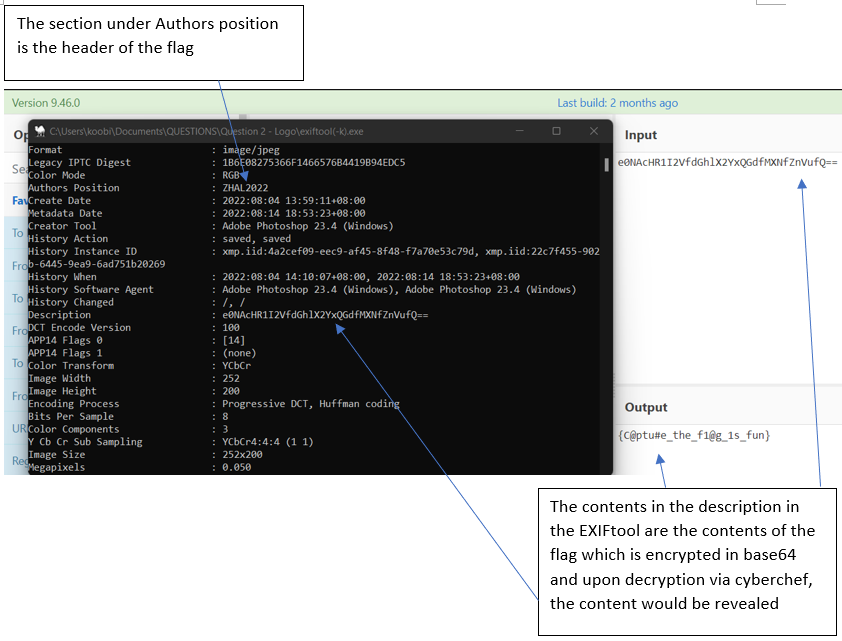
**Title:** Corrupted  
**OS:** Linux  
**Difficulty:** Basic  
**Total Flags:** 1  
**Answers:** ZHAL2022{cmlvbmJwZXBiMTIxMw==}  
**Steps to find flag:**

1. Download the corrupted jpg image from CTFd
2. Use HxD to open the corrupted image so that can see how it is corrupted (the first few signatures are not correct)
3. Replace the incorrect signature with the correct one to and save as (DO NOT SAVE)
4. The jpg should be an image of the flag for the question

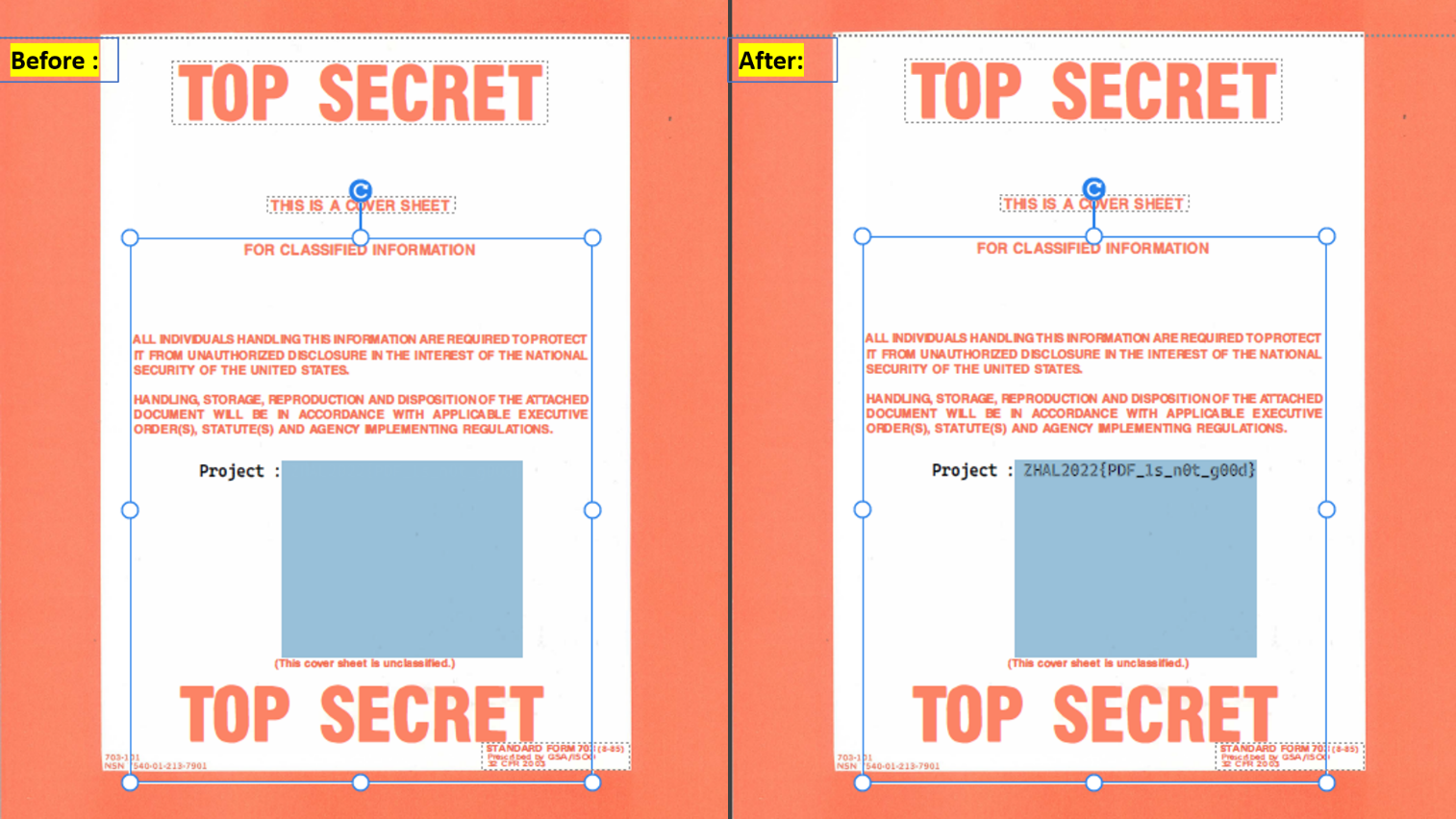
**Title:** Door  
**OS:** Linux  
**Difficulty:** Basic  
**Total Flags:** 2  
**Answers:** ZHAL2022{MHBlJl9zZXNAbWU=} , ZHAL2022{c0ngr@ts\_0n\_f1nd1ng\_the\_f1@g}  
**Steps to find flag:**

1. Download image (locked\_door.jpg) from CTFd
2. Use online tool (<https://stylesuxx.github.io/steganography/>) to decode a hidden message within the image which gives a flag
3. Continuing to part 2 of the challenge and download both items (password\_for\_zipfile.txt and another\_door.zip)
4. After solving a riddle to get the password (openme), unlock the encrypted folder (another\_door.zip)
5. Once unlocked, use jphs (provided in Documents/Tools in host machine) to uncover the hidden flag in the image (opened\_door.jpg)
6. The password used to uncover the hidden data would the decrypted contents of the previous flag (ZHAL2022{MHBlJl9zZXNAbWU=}), which is 0pe&\_ses@me
7. Save the file and open with text editor to receive the second flag

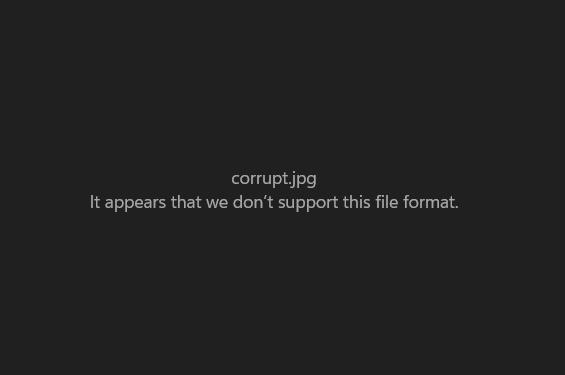
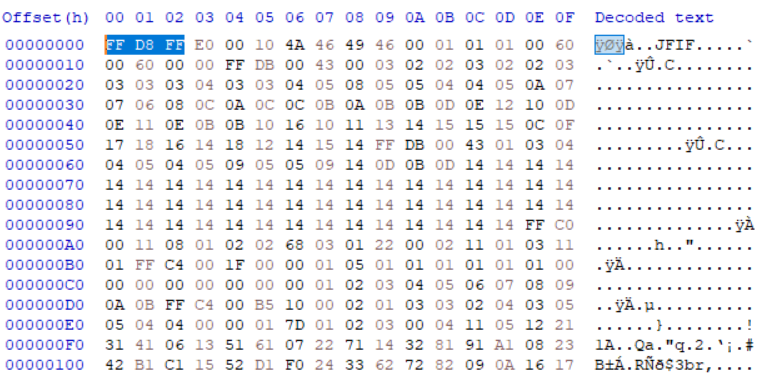
**Title:** Logo  
**OS:** Linux  
**Difficulty:** Basic  
**Total Flags:** 1  
**Answers:** ZHAL2022{C@ptu#e\_the\_f1@g\_1s\_fun}  
**Steps to find flag:**

1. Download image (CTF.jpg) from CTFd and continue on host machine
2. Using EXIFtool provided on the host machine (drag and drop image into the tool)
3. See image attached below -
4. 
5. Piecing the contents of both the authors position and description would reveal the flag

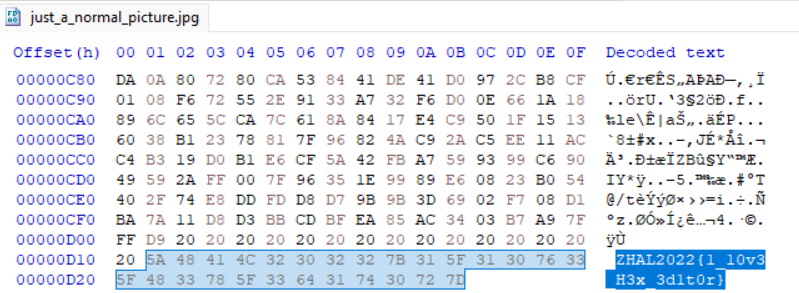
**Title:** PDF  
**OS:** Linux  
**Difficulty:** Basic  
**Total Flags:** 1  
**Answers:** ZHAL2022{PDF\_1s\_n0t\_g00d}  
**Steps to find flag:**

1. Download the artefact (secret.pdf) from CTFd
2. See image below - 
3. Upon changing the colour of the text in the PDF, the flag would be revealed.

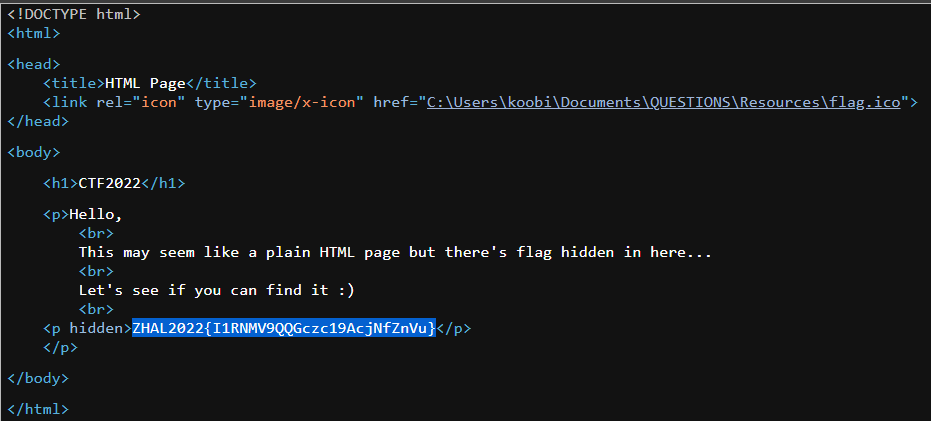
**Title:** Corrupted 2  
**OS:** Linux  
**Difficulty:** Basic  
**Total Flags:** 1  
**Answers:** ZHAL2022{h3@ders\_@r3\_h@rd}  
**Steps to find flag:**

1. Download the image (corrupt.jpg) and continue on the host machine
2. Upon the attempt to open the image, an error would show and the image would be unable to open  
   
3. Use HxD provided in the host machine, repair the file header of the image (FF D8 FF) and save the image  
   
4. Upon opening, the flag would be revealed.  
   

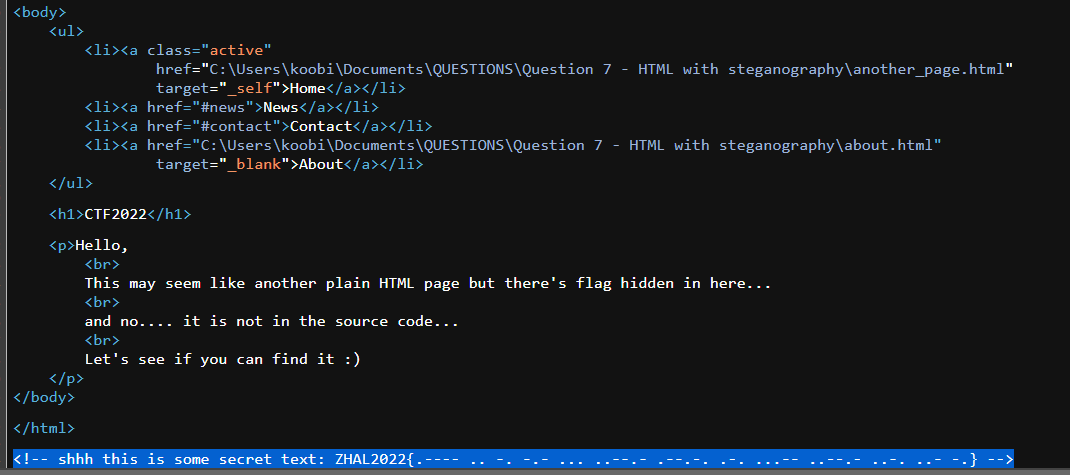
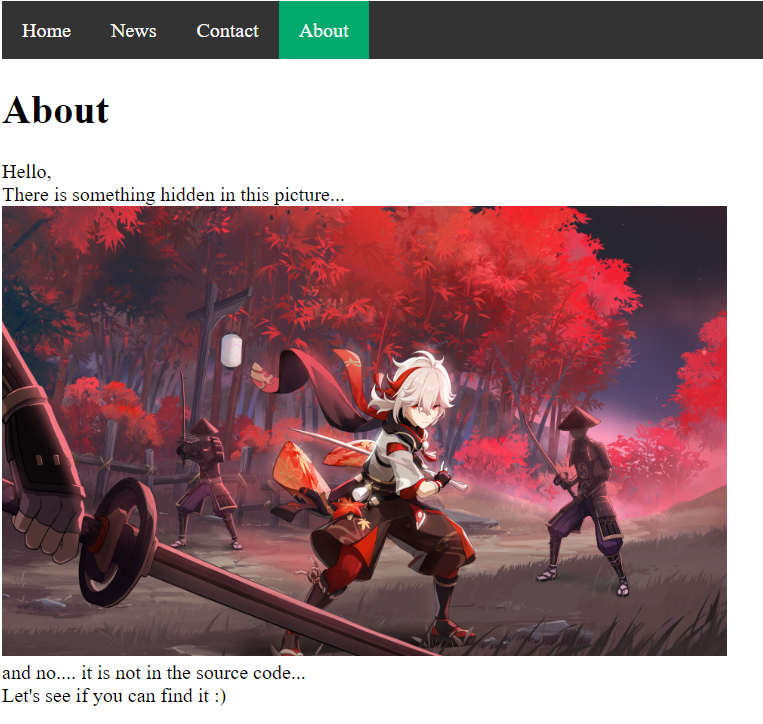
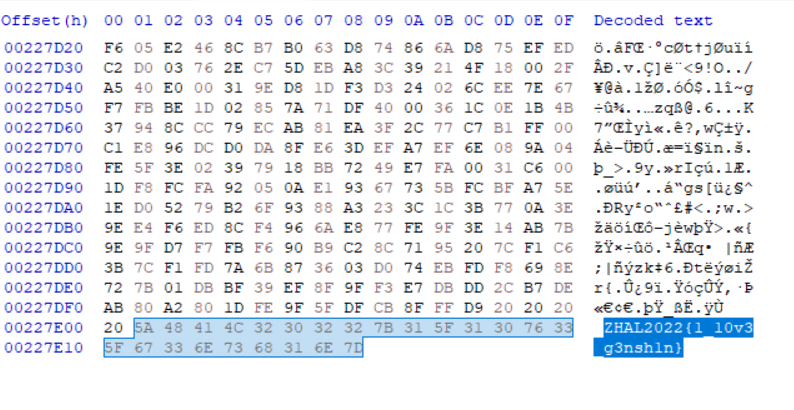
**Title:** Hidden  
**OS:** Linux  
**Difficulty:** Basic  
**Total Flags:** 1  
**Answers:** ZHAL2022{1\_10v3\_H3x\_3d1t0r}  
**Steps to find flag:**

1. Download the image (just\_a\_normal\_picture.jpg) from CTFd and continue on host machine
2. Open the image using HxD editor
3. The flag is appended to the very last line of the data  
   

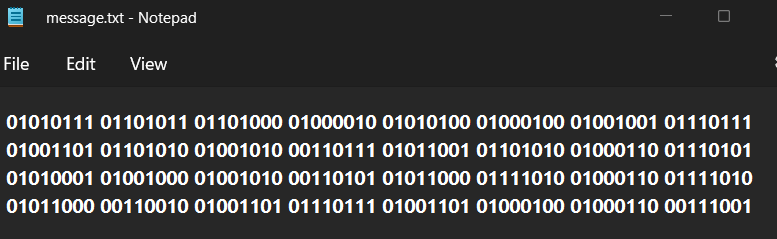
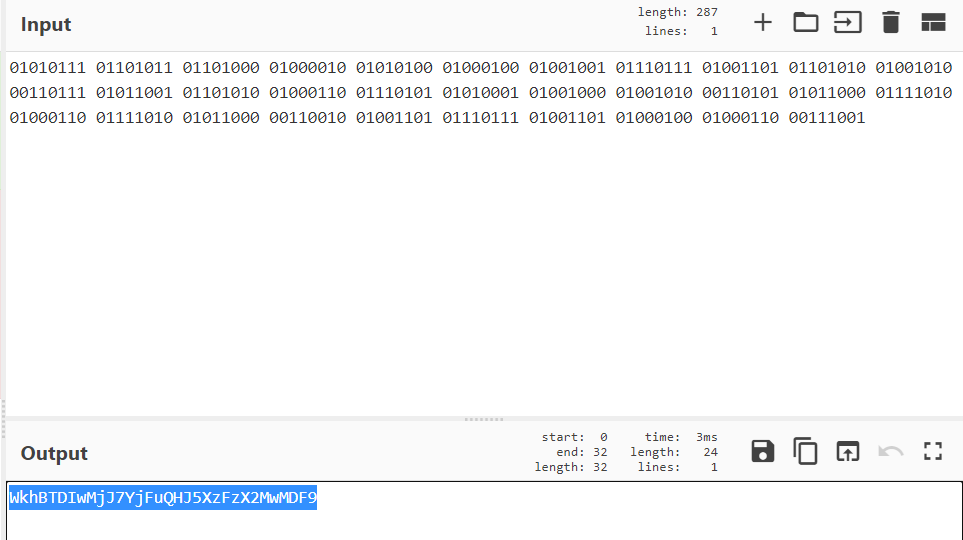
**Title:** HTML  
**OS:** Linux  
**Difficulty:** Basic  
**Total Flags:** 2  
**Answers:** ZHAL2022{I1RNMV9QQGczc19AcjNfZnVu}, ZHAL2022{W311\_d0n3\_0n\_f1nd1ng\_th3\_f1@g}  
**Steps to find flag:**

1. Download and open the HTML page from CTFd
2. Inspect the page and the first flag would be revealed  
   
3. Continuing to the second part of the challenge, download the zip file (flag.zip), participants would find that the zip file is password protected
4. As the contents of the previous flag is encrypted in base64 (ZHAL2022{I1RNMV9QQGczc19AcjNfZnVu}) , decrypting the contents of the flag would reveal the password to unlock the file (#TM1\_P@g3s\_@r3\_fun)
5. Upon opening the file, the final flag would be revealed

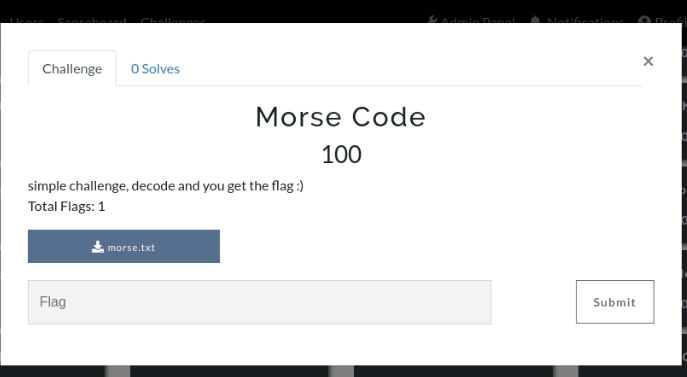
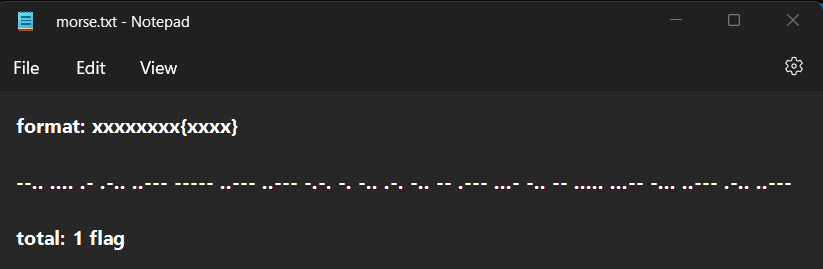
**Title:** HTML with steganography  
**OS:** here  
**Difficulty:** Ba https://outlook.office365.com/mail/inbox/id/AAQkADZmZjYwMTM0LWVkYTAtNGY2OC1hMWE2LTJhZDg5YjE1MGVkNAAQAK%2Fu6BNcBUPpkT38D1TUiqc%3D sic  
**Total Flags:** 2  
**Answers:** ZHAL2022{1INKS\_@R3\_FUN} , ZHAL2022{1\_10v3\_g3nsh1n}  
**Steps to find flag:**

1. Download the html page and open on host machine
2. Upon inspecting the page, it would be seen that that is an encrypted flag at the bottom of the code  
   
3. Decrypting the content of the flag would give the first flag
4. Moving to part 2 of the challenge, download the html page and open  
   
5. Save the image in the html page and use HxD on host machine
6. The flag would be appended at the last line of the data  
   

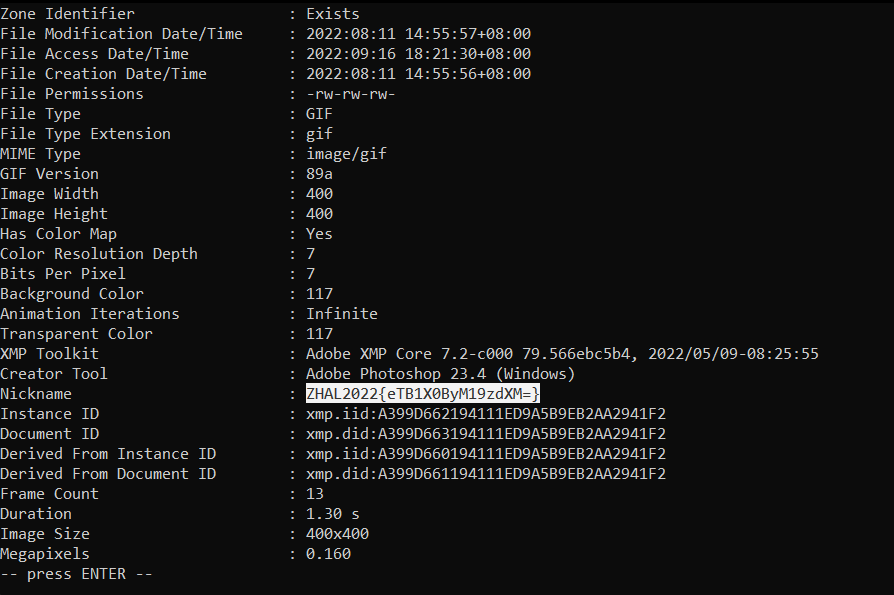
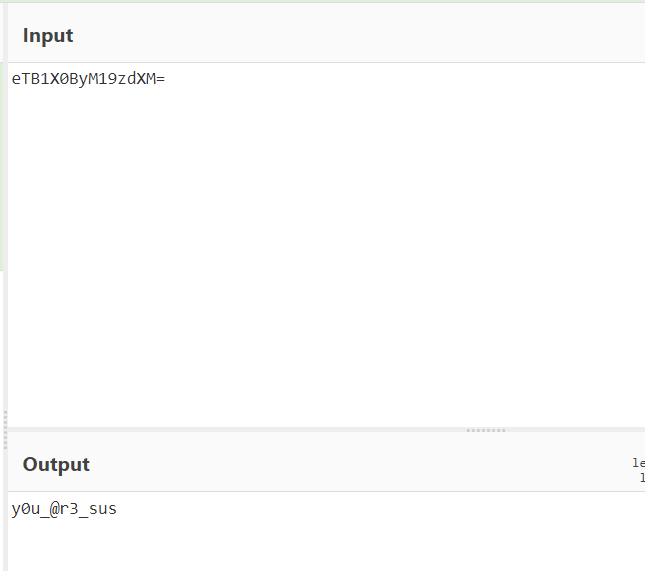
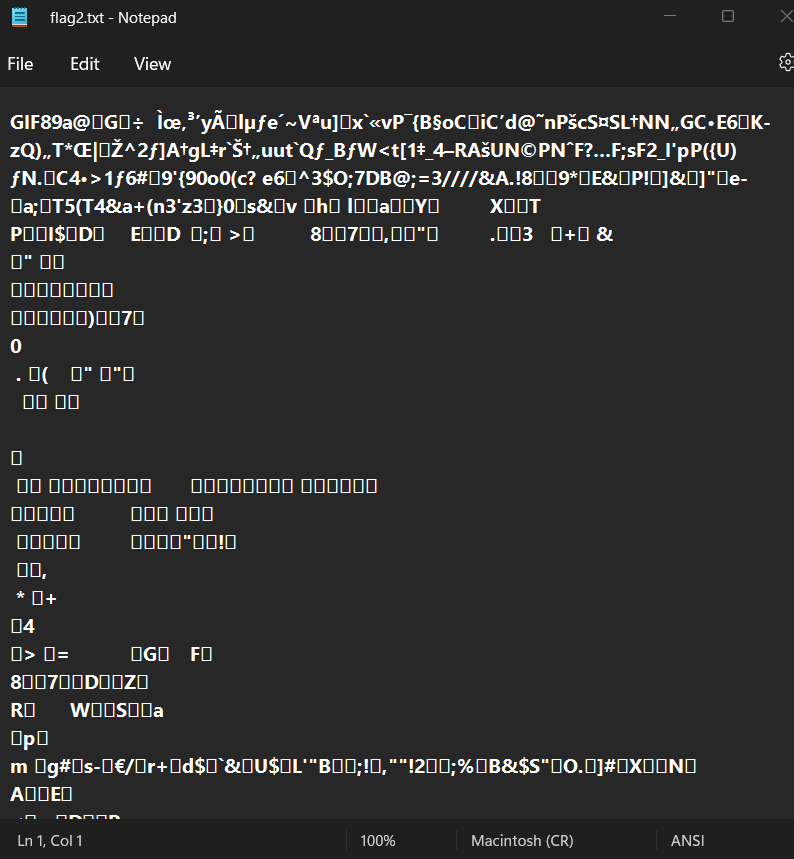
**Title:** Double Trouble  
**OS:** Linux  
**Difficulty:** Basic  
**Total Flags:** 1  
**Answers:** ZHAL2022{b1n@ry\_1s\_c001}  
**Steps to find flag:**

1. Download the .txt file and continue on host machine
2. Upon opening, the contents are in binary form and would require decryption via cyberchef  
     
   However, upon decryption, it would be seen that the contents are still encrypted and would require further decryption (base64)  
   
3. When successfully decrypted, the flag would be revealed  
   

**Title:** Morse Code  
**OS:** Linux  
**Difficulty:** Basic  
**Total Flags:** 1  
**Answers:** ZHAL2022{CNDRDMJVDM53B2L2}  
**Steps to find flag:**

1. Download and work on the file on host machine  
   
2. Once open, participants would see the following content  
   
3. To solve the challenge, simply decode the morse code message and the flag would be revealed.  
   

**Title:** Rock  
**OS:** Linux  
**Difficulty:** Basic  
**Total Flags:** 2  
**Answers:** ZHAL2022{y0u\_@r3\_sus} , ZHAL2022{d0\_y0u\_sm311\_w#@t\_th3\_r0ck\_1s\_c00king}  
**Steps to find flag:**

1. Download the .gif file and continue on the host machine
2. When opening the .gif file, participants might think that there is no flag in the file  
   
3. However, using the EXIFtool provided (drag and drop into the application), the flag can be seen under the nickname section,  
     
   However, that is not the correct flag as the contents of the flag requires decrypting to obtain the correct flag.  
   
4. Moving to the second part, download the .txt file and continue on to the host machine
5. Participants would find that the contents of the.txt file is unreadable  
   
6. To obtain the flag, participants simply need to change the extension of the file to **.gif**  
   and the flag will be revealed.  
   