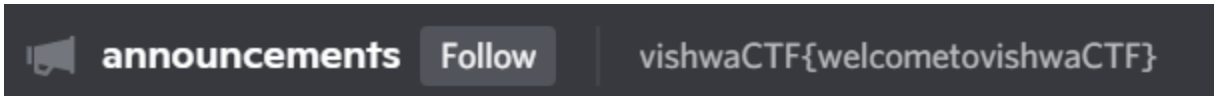
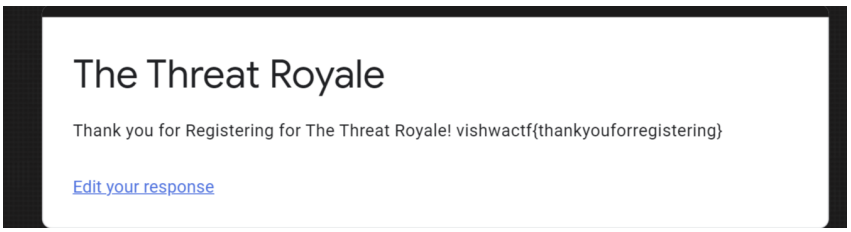
VishwaCTF Achieved Flags Write Up

---

1. **Discord- The flag for this challenge is hidden on discord in announcements channel. Find the flag.**



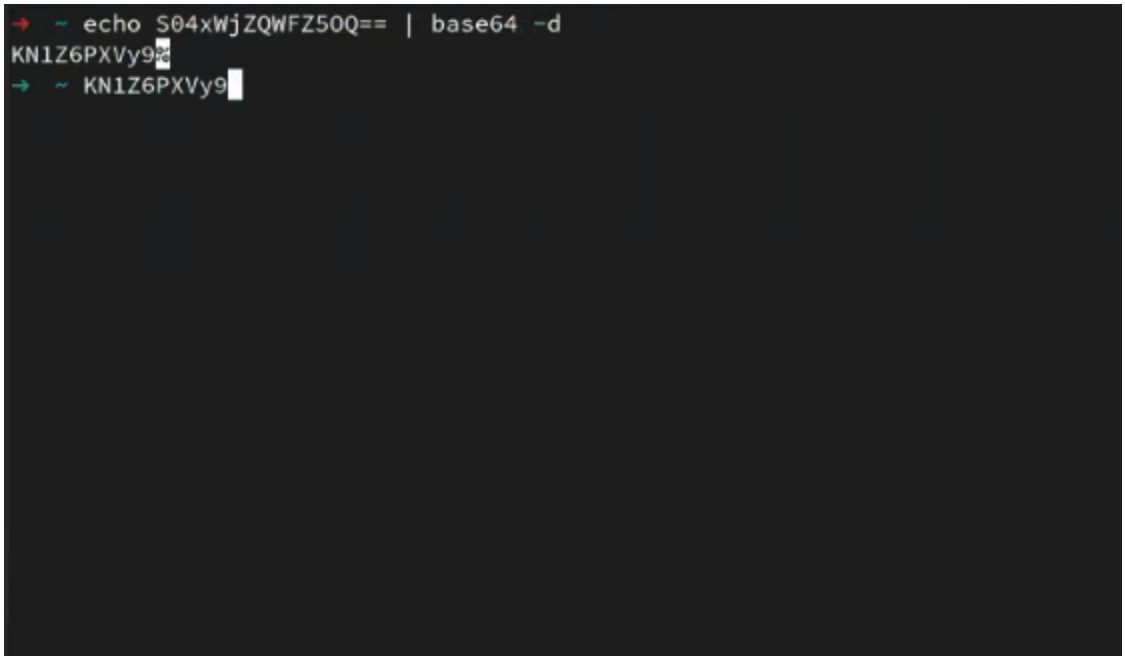
2. **Trivia 1 - This is a Debian-derived Linux distribution managed and funded by Offensive Security If there are any spaces, use an "_" instead of it.**
    a. This flag was pretty straightforward, however, they were looking for the full name, not just 'Kali' for the flag.
    b. vishwaCTF{Kali_linux}
3. **Trivia 2- Who coined the term virus in computer?Name any one. If there are any spaces, use an "_" instead of it.**
    a. Len Adleman, although he was the co-partner with Fredrick Cohen, and Cohen is mainly attributed to it, his name was not accepted as the flag. Thus I used his partner's name.
    b. vishwaCTF{Len_Adleman}
4. **Trivia 3- The first virus to infect Windows 95 files is If there are any spaces, use an "_" instead of it.**
    a. Originally I thought the answer to this question was the i love you virus that sprouted up in the early 2000s, however, there was one earlier that specifically targeted Windows 95, Boza, that I recall learning about from a Youtube video on the history of viruses.
    b. vishwaCTF{Boza}
5. **The Threat Royale- The flag is hidden in the Threat Royale google form on our website... find it there!!!**
    a. My first instinct was to dissect the code for the page. After looking at the basic HTML, I had the bright idea... What if I just fill out the form? So I did, with the letter A in every field, and once I submitted it, the flag was handed to me.



6. **So Forgetful! - Once my friend was connected to my network, he did some office work and left. Next day he called me that he forgot his password, and wanted me to rescue him <3**
    a. I took the pcap file I was given and opened it in Wireshark. I immediately started looking at the HTTP logs, knowing that they don't disguise plaintext. I found this almost immediately:

```
0000  08 00 27 3d 47 5d 08 00  27 38 2c 5c 08 00 45 00   ··'=G]·· '8,\··E·
0010  00 5d ec 95 40 00 40 06  3a 00 0a 00 00 05 0a 00   ·]··@·@· :·······
0020  00 01 e7 1b 1f 90 e9 d7  8e c2 65 ad ce d8 80 18   ········ ··e·····
0030  01 c9 d2 3f 00 00 01 01  08 0a 00 06 61 ad 00 06   ···?···· ····a···
0040  7f d8 75 73 65 72 69 64  3d 73 70 69 76 65 79 70   ··userid =spiveyp
0050  26 70 73 77 72 64 3d 53  30 34 78 57 6a 5a 51 57   &pswrd=S 04xWjZQW
0060  46 5a 35 4f 51 25 33 44  25 33 44                  FZ5OQ%3D %3D
```

    b. I tried entering this password as a flag, but it was rejected. I consulted with one of my team members, who said it looked like Base-64 encoding. He showed me how to use the terminal to get the correct password.



    c. Flag vishwaCTF{KN1Z6PXVy9}

7. **The Last Jedi- What it takes do you have?**
    a. For this one, I took the image and immediately started doing image analysis on it in Linux. I first checked to make sure it was in fact a .jpg file
        i. Command: file Y0D4.jpg
    b. The file indeed was a .jpg file, so I continued analyzing with other tools.
        i. Command: exiftool Y0D4.jpg
    c. This didn't reveal anything promising either
        i. Command: strings Y0D4.jpg
    d. This one revealed something interesting:

```
!_MACOSX/Sacred archives/Dont open
_MACOSX/Sacred archives
Sacred archives/Dont open
_MACOSX
Sacred archives
QO_:B
0_MACOSX/Sacred archives/Dont open/is_this_it.jpg
/Sacred archives/Dont open/Is_This_Really_It.jpg
narki@Narki-BLADE:~/Downloads$
```

    e. I tried using binwalk, a tool for searching a given binary image for embedded files and executable code. Binwalk created a file that had a .rar file in it. For whatever reason, it wouldn't extract properly on my Linux machine, so I switched over to my Windows machine, extracted it, and was given two new .jpg images. Sending the images back to my Linux machine, I proceeded to go through the same process I had on the original, and came across two flags in the string dumps for the images.

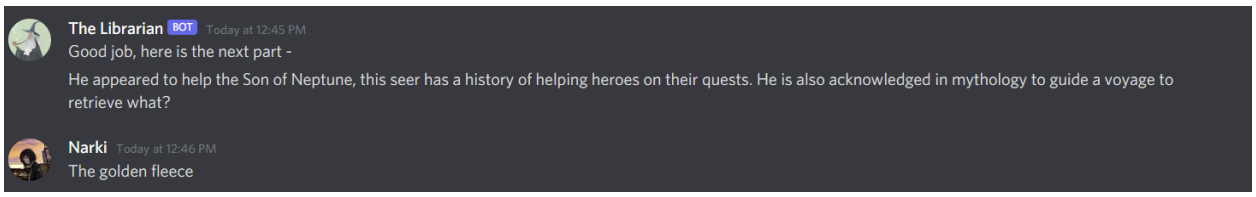
```
,lmC"lS
^^y<p
flag:{J0K3S 0N Y0U}
```

```
/c'd
flag:{H1DD3N_M34N1NG}
```

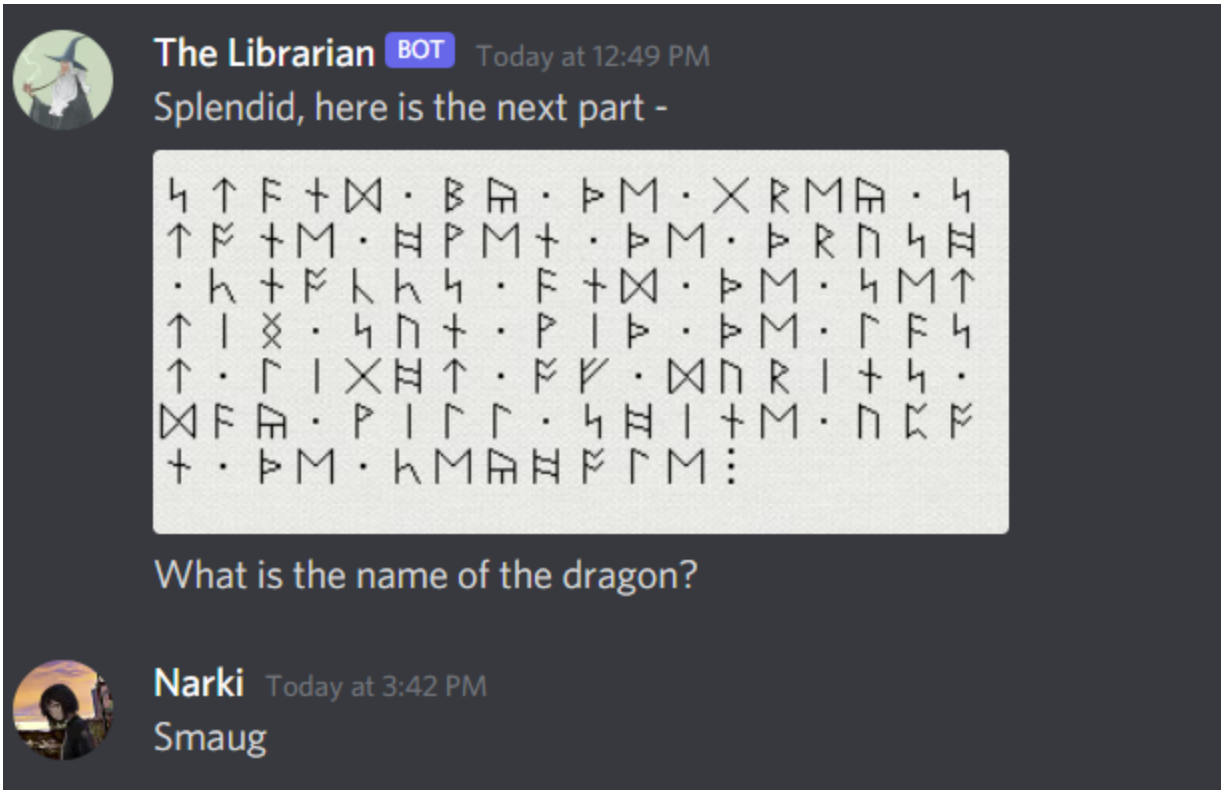
I guessed correctly: the flag for this challenge is vishwaCTF{H1DD3N_M34N1Ng}

8. **The Library- Send a 'hello' to "The Librarian" from the bot list on the Discord server, and he shall guide you further.**
    a. This was a multi-part question in which all questions had to be answered correctly to retrieve the flag. All the questions had to do with literature.

b. In this question, the Librarian was referring to the book “The Man in the Mist.” Although I had never read the book, I was familiar with the premise enough (and Agatha Christie) to get the reference. I googled the sparknotes of the book and found the specific time that was wanted in the answer. At first, I saw the (without am/pm) and was scratching my head when inputting it in military time -- It wanted normal 12 hour time, I just needed to read more closely.



c. In the next part, the words “voyage to retrieve” and “quests” brought me back to 7th grade when I read “The Golden Fleece and the Heroes who Lived before Achilles.” My answer was correct.



d. This next one took me a few hours to figure out. The language looked old -- perhaps it was some hieroglyphics? After google-searching the image, I found similarities to Old English, particularly the runes of the Anglo-Saxons. I knew that the clue had to do with a book, so I started searching for dragons in old mythology. With that to no avail, I began to try to translate the image with a few copies of the alphabet I found online. I ended up with the translation,

   Stand by the grey stone when the thrush knocks and the setting sun with the last light of Durins Day will shine upon the key hole.

   This was a reference from The Hobbit. The dragon took them mines from the dwarves in the Hobbit, and the whole point of the book is them journeying to the forgotten mines to reclaim the arkenstone- the token of the dwarves. The dragon's name is Smaug.

e. This was the final of the questions, the flag was in sight. I went straight to trying to determine the clues I was given. I started with reverse searching the image inside of the building -- It was the capital dome in Washington D.C. I also noticed the word “Lost” was capitalized in the clue. So I searched Lost, Washington DC, severed hand, and came up with the book The Lost Symbol. The book focuses on themes of masonry.

   I then turned to the code I was presented with and ran it in a reverse image search. I found that this was a common code called the pigpen cypher, which has a style called mason. When decoding the message, however, I was presented with gibberish.

   nisytetpristnufo

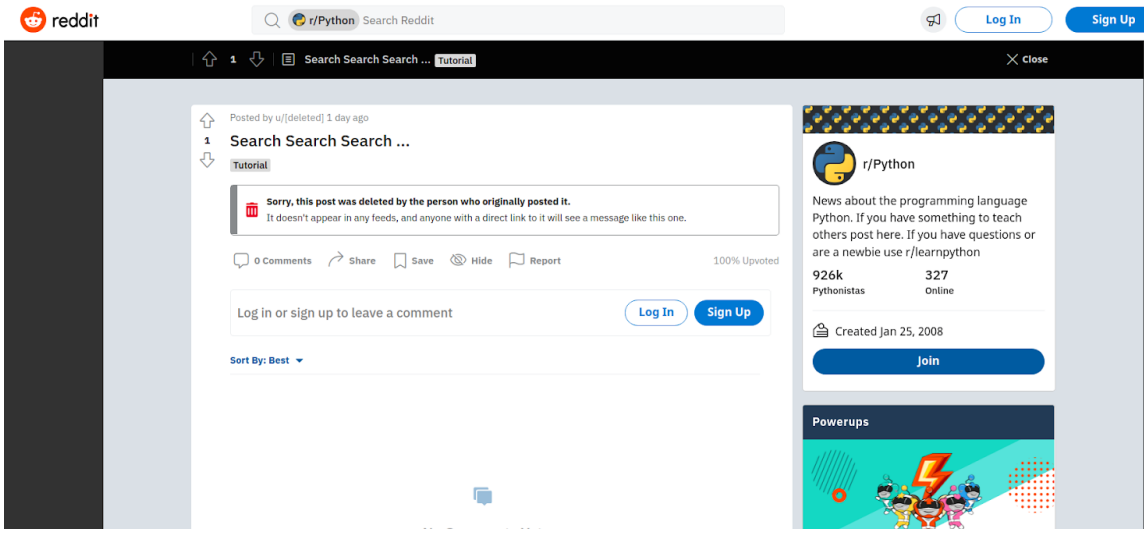
   I tried running this result through a few decoders, however, this was to no avail. It then occurred to me that the letters could just be scrambled in place. Sure enough, this was the case. Flag obtained.


osintisprettyfun
The Librarian
BOT
Today at 4:10 PM
Congratulations on getting through all the challenges, here is your flag.
vishwaCTF{b00ks_d0_b3_1nt3r3st1ng!}

2. **Archived Note - I found a note which had an Image and the following 188918664847743620481444062557186682450149766224751116402240624789234083214210205410994015621594103579536182793692141411051745422640417091358502110829921519993602452147084247481855214821169816361010316244340 0 Does it make any sense to you ?**
    a. I first scanned the QR code that I was given, and it gave me the following data:
        i. {'public': (2, 2683, 2576), 'private': 1025, 'k_value': 847}
    b. I figured there was some sort of decryption that was needing to be done, but I wanted to dig into the image and see if I could find anything. I ran the following in the terminal:
        i. strings qrcode.jpg
    c. This gave me an interesting result on the last line of the strings:

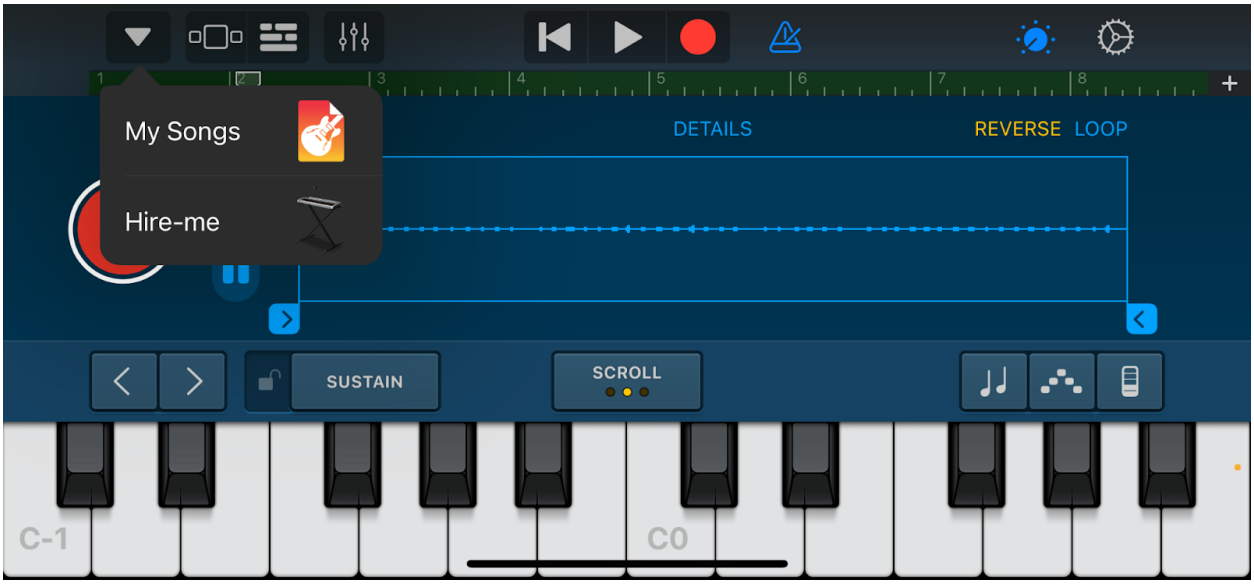
    d. I copied this, and plugged this into my goto website, dCode.fr
    e. On the webpage, I had it guess what encryption or algorithm was performed, and the top result was something called “Text Message.” I didn’t find anything of use with that one, so I went to the second best match, ASCII translation. And wouldn’t you know, there was plain as day, a link generated from the code.

f. I followed the link, and was brought here:



Without knowing the algorithm or the real purpose of this webpage, I was stumped and moved on to a different challenge.

3. **Platypus Perry- Agent John got some information that a group of people hid a bag of LSD on a dog. He needs to find the dog before it reaches the dealer.**
    a. I listened to the .mp3 that was given with this challenge, and noticed immediately that the audio sounded choppy and high pitched. I have played with enough audio samples to know it was reversed. I sent the clip to my phone, opened GarageBand (where I usually play around with audio files) and reversed the clip, playing it in a slowed playback mode.



b. When listening to the playback, these were the letters I was able to decipher. The person speaking had a slight accent and the audio wasn't purely clear, so some of the letters may have been incorrect. Either way, without distinct pauses I couldn't break up this long jumble of text to try to decode it. The flag format was supposed to be a first and last name, but who has a name longer than the english alphabet???
    i. niarbrusdiushcihwgnihdemosulleddhgimlabmobdivadyugruo