

A blue text on a white background

Description automatically generated

## Round 1 report

# Contest Date: - 27th January 2024

|  |  |
| --- | --- |
| CT ID | DT20234931846 |
| Name | ASHUTOSH KUMAR SINGH |
| College/University | M.S. ENGINEERING COLLEGE (VTU) |
| City | BENGALURU |
| Challenges solved & the total score | 8 SOLVED |
| Anything else that you want us to know |  |

**(Copy & paste the table x times if you solved x challenges)**

|  |
| --- |
| **Challenge Title: WEB CHRONICLE** |
| **Flag: HQ8FLAG{368ef8d0ec6fd5ebb63681ef93bd881}** |
| **Approach (Step by Step):**   1. So, This Challenge was little bit tricky. First I started analysing all the files that were given to me in the web chronicle zip. There were many json files . I started going through the json source code 2. Later after analyzing the source code I gone through the bookmarks.json and found a Pastebin url   After opening the Pastebin file I was able to find the  This encrypted flag I decrypted and using cyberchef and go the correct flag. key  **Challenge Title: CODE DE TOUR**  This Challenge was one of the interesting challenge , here I was given a ELF Binary file named  Decrypt  At first in kali linux I checked which type of file it was  Here I came to know that it was an elf binary and I need to disassemble it I tried to run radare2 here but was unable to open it so it tried using online disassembler    Here in the source code I was able view the string  And the password which was using  ARC4 algorithm so , I made a python script to decrypt the string with the password    So in this way I was able to find this flag  **Challenge Title: Optimus Prime**  **Flag: HQ8FLAG{c2b8c1d94d3f3afda53c4b09a4593a3}**    I Found two approaches I solving this challenge  so this challenge was a RSA decryption so we can use two methods here as the value of n , e , c  modulus    n, the ciphertext    c, and the public exponent    e we can also use the formula *m*=*cd*mod*n*    Here I have used dCode.fr tool to decrypt the RSA cipher but instead we can also make of the tool  RsaCtf tool for decryption  **We can use by the command**  **Python3 RsaCtfTool.py -n < value of n> -e < value of e> --uncipher <cipher text>**  Using the above command we were able to decrypt the key and got the correct flag    **Challenge Title: Deception Mahem**  **Flag : HQ8FLAG{bdc9d7beee8379bdb3830faff9c7ff4}**  I tried to change the site directory nae with robots.txt     Then the response was the above image which said Oops! There’s an Onion your code . Then an idea clicked in my mind to intercept the traffic using burpsuite so i intercepted the traffic using burpsuite and crawled the web traffic source code and in the response section I found the onion link which I can only open using the tor browser  So I downloaded the tor browser       Then I opened the Url with in the tor browser and it was leading the above page with flag key  This was one of the amazing experience for as it felt adventurous for me |