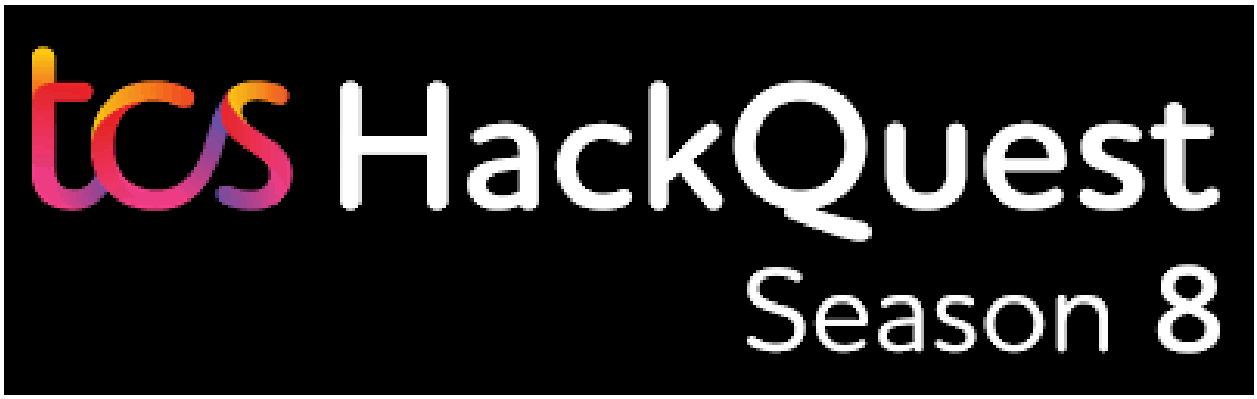
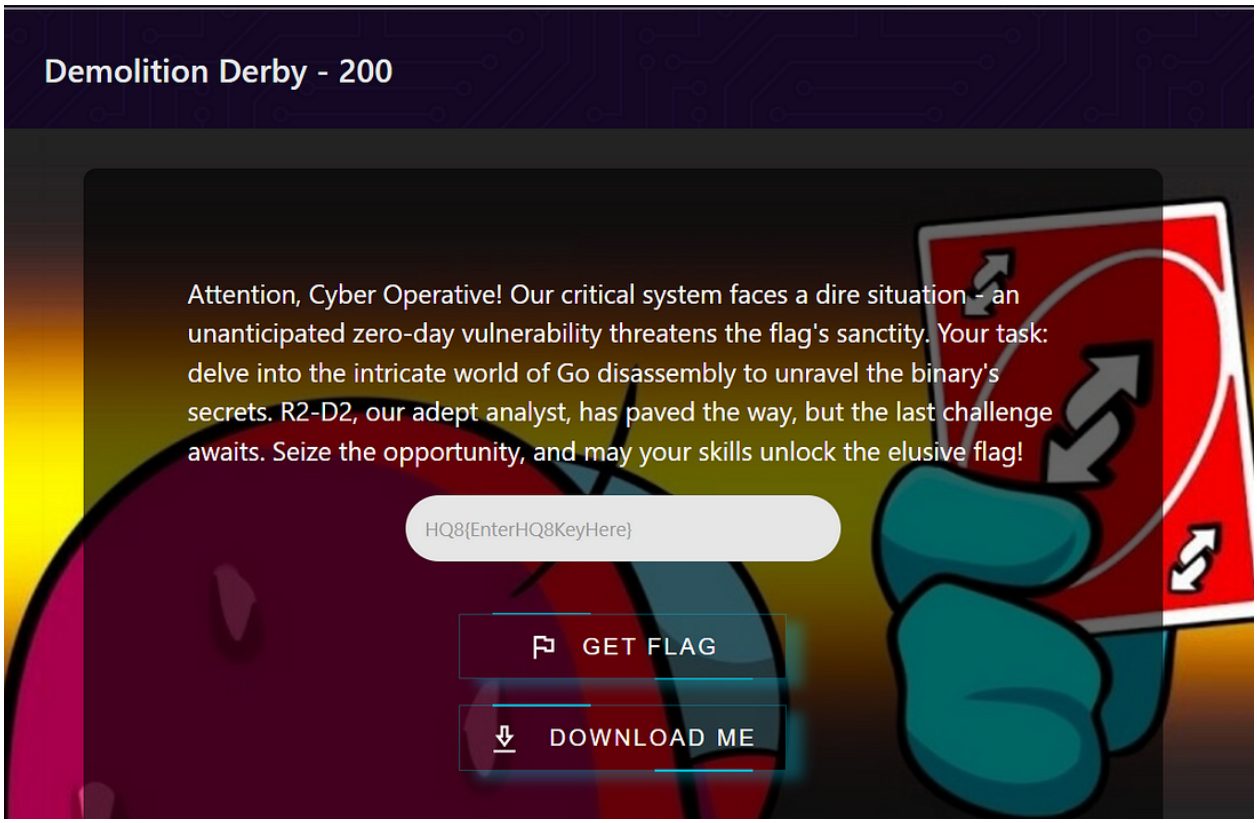
TCS HACKQUEST SEASON 8 Writeup

TCS HackQuest is an online cybersecurity competition organized by Tata Consultancy Services (TCS).In HackQuest, participants complete a series of challenges in 6 hours, presented in three categories: beginner, intermediate, and expert. The top-performing participants receive up to INR 5 lakhs in prizes, and certification of merit. Exceptional performers may also get the chance to work with the TCS Cybersecurity Centre of Excellence. First Round happened in 27 January 2024 and then second round held on February 10, 2024, from 10 AM to 12 PM.

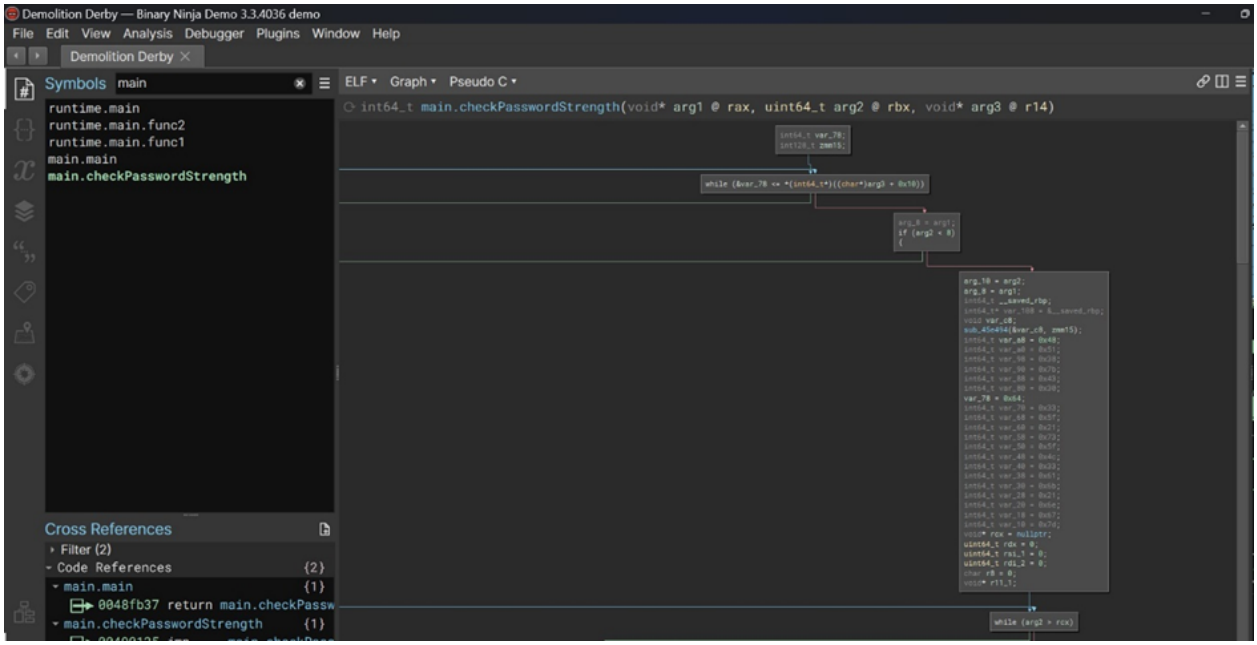


Round 1

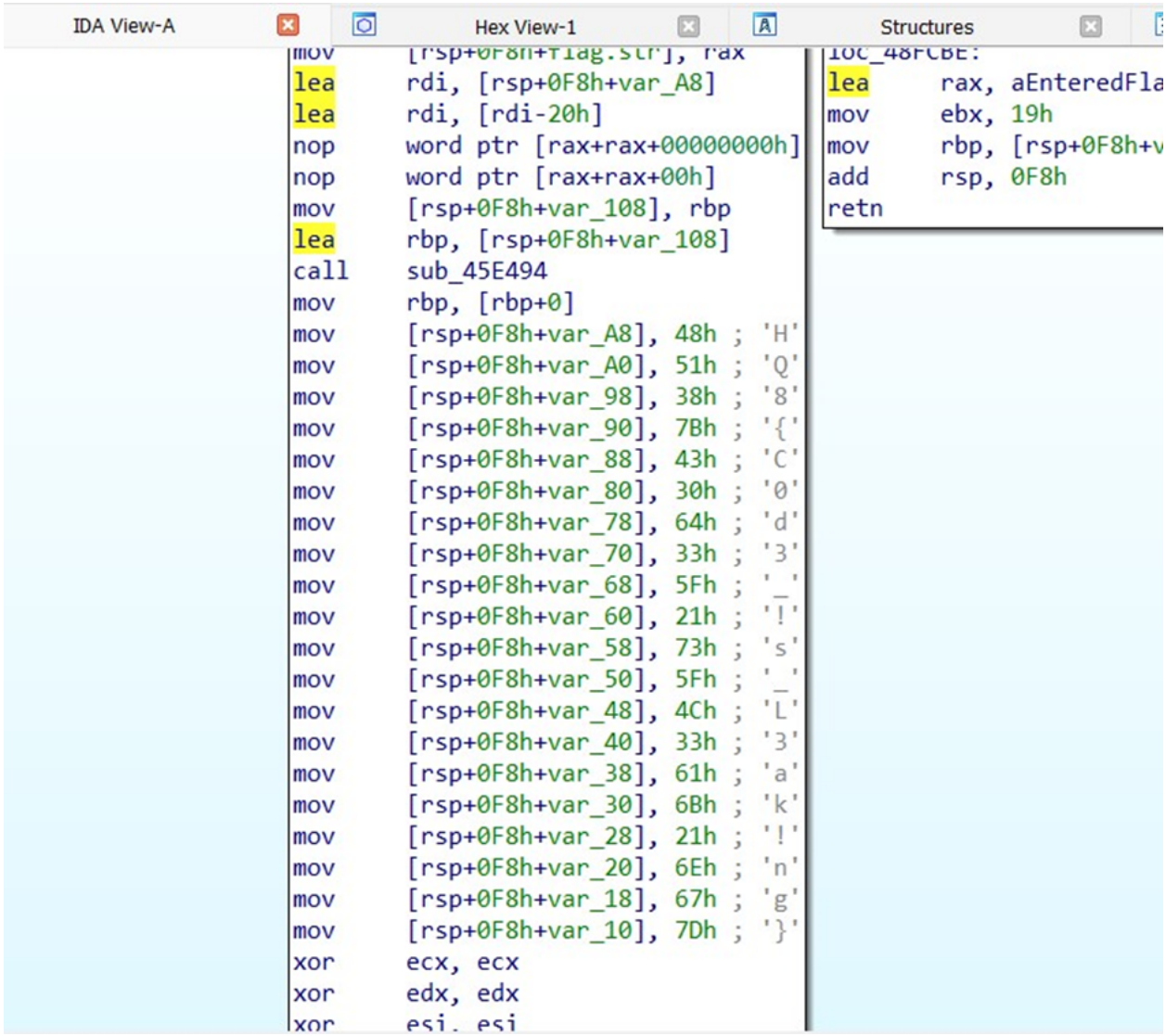
Demolition Derby — 200



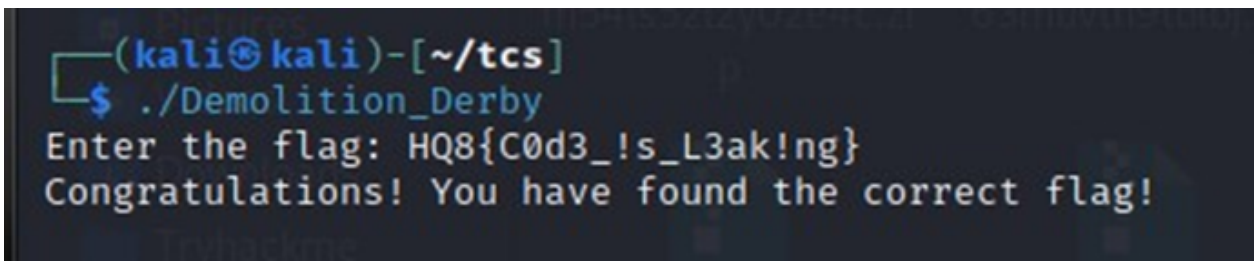
I opened the file in my kali and gave file command and it was ELF file so opened it in Binary Ninja and IDA.



I used both because It is easier to view pseudo c in binary ninja and graphical view is better in IDA.I checked the password strength function and got the flag where looking into the hex view in IDA. I checked for the flag strength and when entering the correct flag it gave you found the flag.


IDA View-A
Hex View-1
Structures
mov [rsp+0F8h+flag.str], rax
lea rdi, [rsp+0F8h+var_A8]
lea rdi, [rdi-20h]
nop word ptr [rax+rax+00000000h]
nop word ptr [rax+rax+00h]
mov [rsp+0F8h+var_108], rbp
lea rbp, [rsp+0F8h+var_108]
call sub_45E494
mov rbp, [rbp+0]
mov [rsp+0F8h+var_A8], 48h ; 'H'
mov [rsp+0F8h+var_A0], 51h ; 'Q'
mov [rsp+0F8h+var_98], 38h ; '8'
mov [rsp+0F8h+var_90], 7Bh ; '{'
mov [rsp+0F8h+var_88], 43h ; 'C'
mov [rsp+0F8h+var_80], 30h ; '0'
mov [rsp+0F8h+var_78], 64h ; 'd'
mov [rsp+0F8h+var_70], 33h ; '3'
mov [rsp+0F8h+var_68], 5Fh ; '_'
mov [rsp+0F8h+var_60], 21h ; '!'
mov [rsp+0F8h+var_58], 73h ; 's'
mov [rsp+0F8h+var_50], 5Fh ; '_'
mov [rsp+0F8h+var_48], 4Ch ; 'L'
mov [rsp+0F8h+var_40], 33h ; '3'
mov [rsp+0F8h+var_38], 61h ; 'a'
mov [rsp+0F8h+var_30], 6Bh ; 'k'
mov [rsp+0F8h+var_28], 21h ; '!'
mov [rsp+0F8h+var_20], 6Eh ; 'n'
mov [rsp+0F8h+var_18], 67h ; 'g'
mov [rsp+0F8h+var_10], 7Dh ; '}'
xor ecx, ecx
xor edx, edx
xor esi, esi
loc_48FCBE:
lea rax, aEnteredFla
mov ebx, 19h
mov rbp, [rsp+0F8h+v
add rsp, 0F8h
retn


(kali㉿kali)-[~/tcs]
$ chmod +x Demolition_Derby
(kali㉿kali)-[~/tcs]
$ ./Demolition_Derby
Enter the flag: dsjfjbjd
Flag strength: Weak
Try Again!


(kali㉿kali)-[~/tcs]
$ ./Demolition_Derby
Enter the flag: HQ8{C0d3_!s_L3ak!ng}
Congratulations! You have found the correct flag!

Code de Tour — 100

Given Description: Bienvenue to our Cyber Security CTF challenge! Preparez-vous for an exciting journey into the world of binary reversing. Explorez the intricacies of function calls as you unravel the secrets hidden within. Embracez the challenge and showcasez your skills in this thrilling adventure. Pouvez-vous déchiffrer le code and discover the flag? Bonne chance, mes amis! Let the cyber exploration begin!

Photo by FlyD on Unsplash

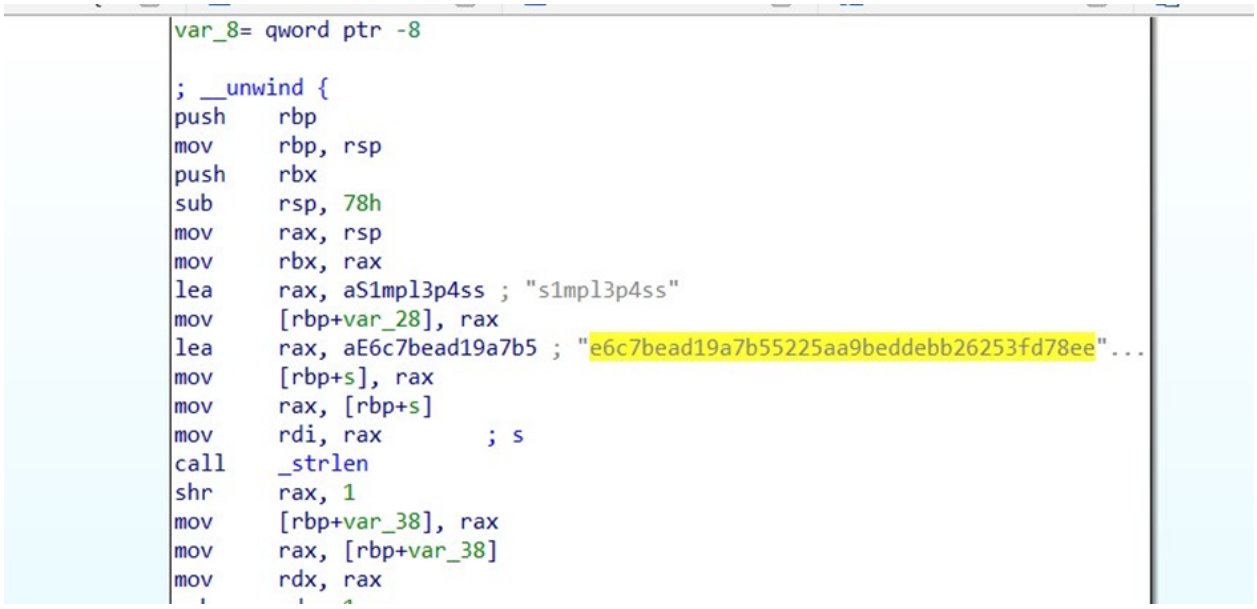
I opened the file in my kali and gave file command and it was ELF file.

```
0x3ff0 .got.plt (PROGBITS) {0x3fe8-0x4030} Writable data

00003ff0  int64_t data_3ff0 = 0x0
00003ff8  int64_t data_3ff8 = 0x0
00004000  int32_t (* const printf)(char const* format, ...) = printf
00004008  int64_t (* const RC4_set_key)() = RC4_set_key
00004010  int32_t (* const puts)(char const* str) = puts
00004018  int32_t (* const __isoc99_sscanf)(char const* s, char const* format, ...) = __isoc99_ssc
00004020  uint64_t (* const strlen)(char const*) = strlen
00004028  int64_t (* const RC4)() = RC4
.got.plt (PROGBITS) section ended  {0x3fe8-0x4030}
```

I found it was RC4 encoded and used dcode fr website to decrypt the encoded text with secret key which found while navigating through the functions.

s1mpl3p4ss -KEY e6c7bead19a7b55225aa9beddebb26253fd78eee2a4ae1d64d52a07afcc7e3c7 -MESSAGE



Optimus Prime — 100

Given Description:
Join forces with Optimus Prime in an epic cyber quest! The fate of this world hangs in the balance as he seeks to crack the enigmatic pieces that hold the key to opening a portal. Your mission, should you choose to accept it, is to assist Prime on his intergalactic journey. Unleash your inner hacker, solve the puzzle, and help Prime reach his planet. The universe awaits your cyber prowess!

Source: https://www.pikpng.com/

1. I tried the RSA algorithm since the challenge.txt file contains n,e and c.
2. I used the dcode fr to decode the RSA CIPHER.
3. Which gave me flag as HQ8{c03a8384a71a8e6c566021ed5ca7ec7b}

n =
640649591649238760648749454734070499855431199929927381192527492312531424642036475187774554751099725816847326210729988980667283034333005852915275829794302763577876340268691160953915143111111742063951958176727373208372403649446099798446019862214628453640703966657230299029326533689434526528541741970707476312421010842609122878492866446995822924731526600040353306161490164969570129488330389317119439845630357848051934749211646250684688429279053142689421537200786809373453651211294043846330191830603471297782966405009353821868678504078933879204821412164983393460811064331443524855717954057177930404412386599258571984394331
e = 65537
c =
624991281606742468651125562590679965356738988009961697620717533408631

10312202219605753552964777131581907276429364704840428034730643882542
81647530385783259491991063551475221829596568142396740158474010222153
56182943226805406357052900766998501800092513173442030724147024073540
86224185759766835382339908211222131209886450287075719367939944030523
97760907994391760980287259192429794905753019258764799624910913874265
20497656404474802368337008878109155473081465676232862339985280315648
75614456256089530316540216679491304264497133836837731620885431061291
81483213691005097307436933237315184636287532406635356649575632891248
04816

Key Generation:

- $n = p \times q$
- $\phi(n) = (p-1) \times (q-1)$
- $d \times e \equiv 1 \mod \phi(n)$

Encryption:

- $C \equiv M^e \mod n$

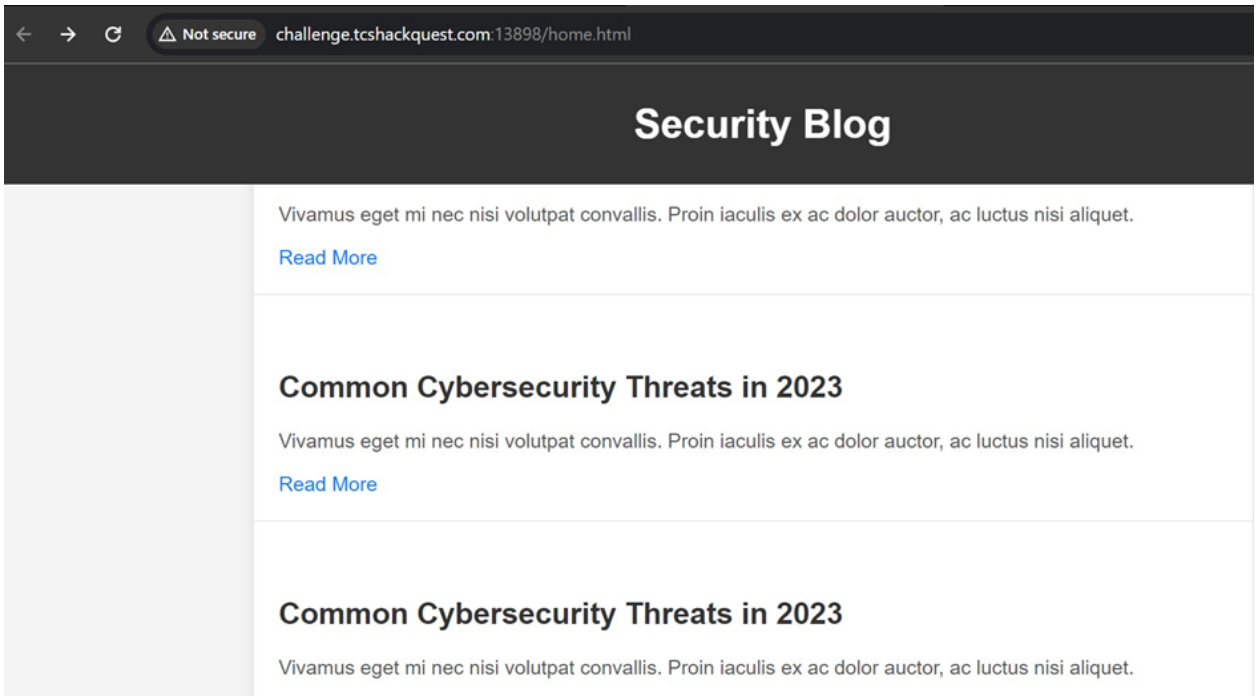
Decryption:

- $M \equiv C^d \mod n$

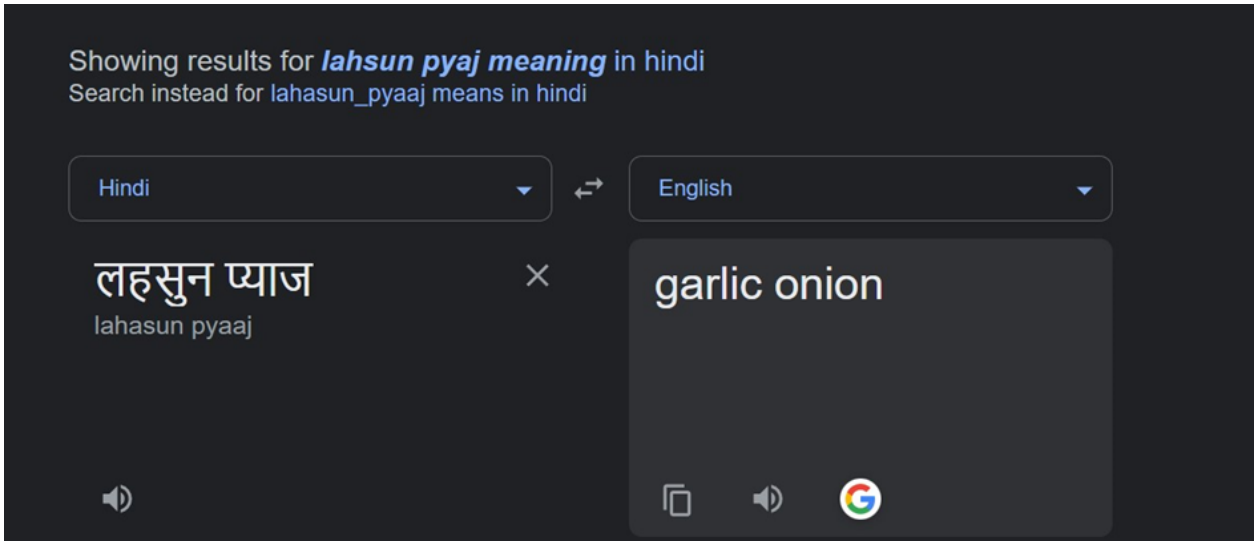
The Rivest-Shamir-Adleman (RSA) algorithm is a public-key encryption algorithm that uses asymmetric encryption to encrypt and decrypt data.

Deceptive Mayhem — 200

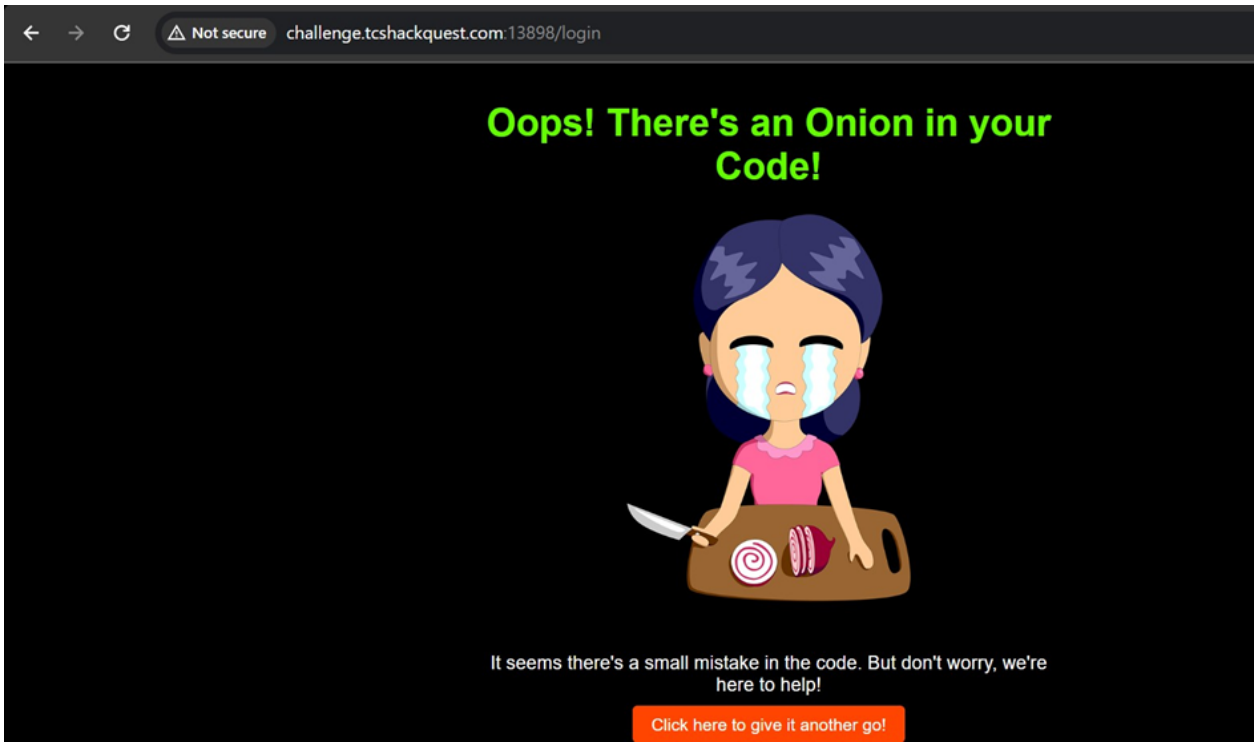
Given Description: A key piece of information that sheds light on the activities of threat group “Lahasun_Pyaaj” is concealed within a seemingly benign website. At first glance, the site reveals a clear static facade, luring unsuspecting visitors into a false sense of security. However, the true machinations of “Lahasun_Pyaaj” unfold in a hidden forum accessible only through the special powers. Your mission is to decode the dual nature of the digital labyrinth, exposing the group’s plans to hack and leak breaches. Delve into the shadows, extract critical information, and thwart their nefarious schemes before it’s too late.



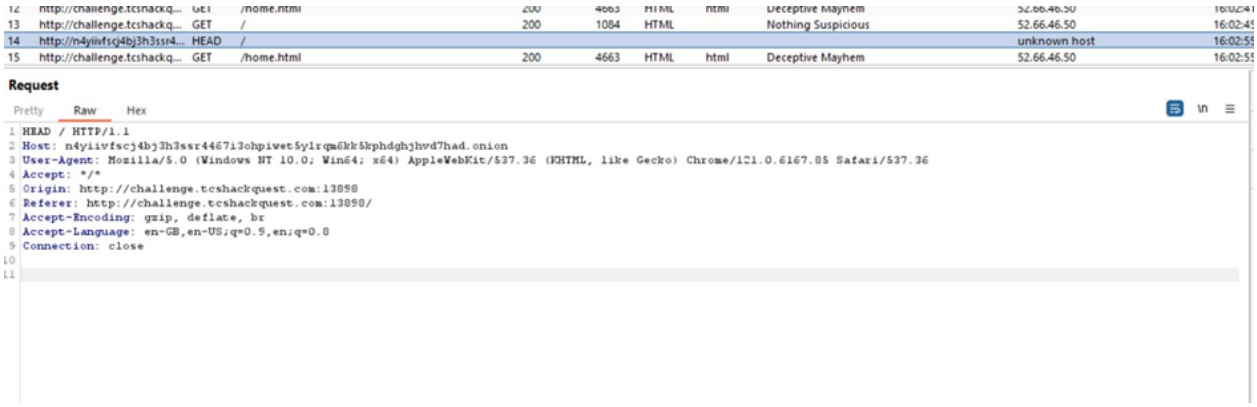
I first opened the website and it has nothing interesting and I read the description again and found the word “Lahasun_Pyaaj” I searched google what is that I found as garlic onion which refers to onion that means there is something in the onion website and also it has hint “hack and leak breaches” that means only if found onion link I can proceed further.

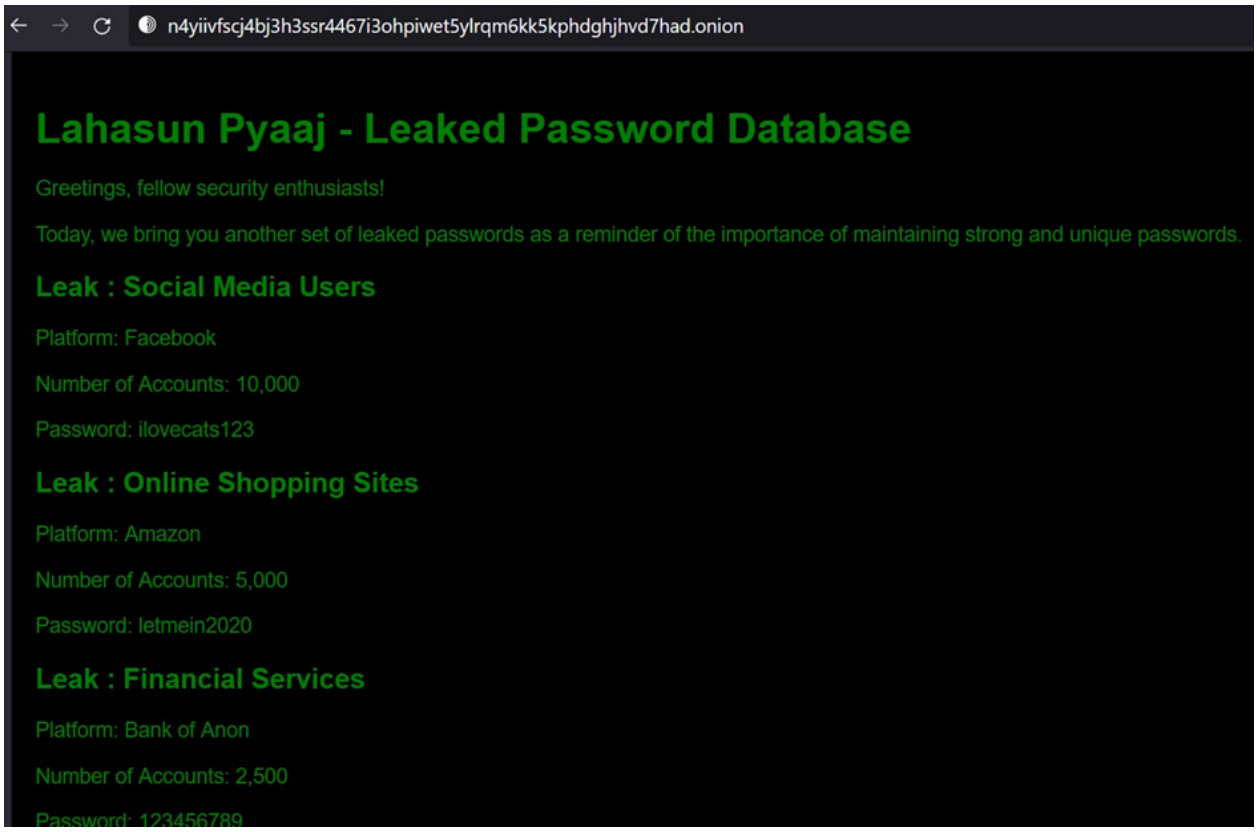


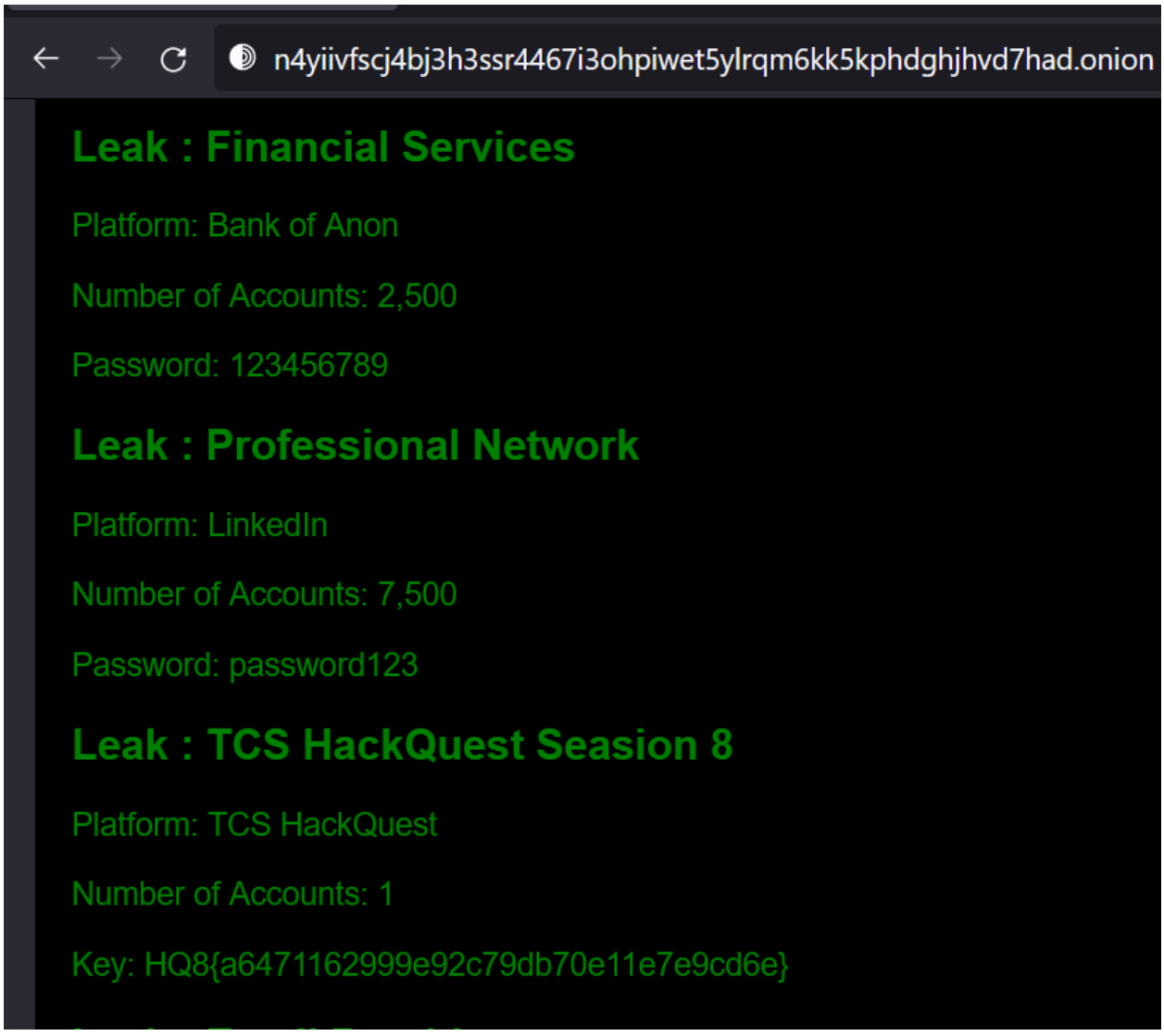
I tried to login in the website and it gave me “There is onion in your code” then only I tried visiting http history in burp suite and got the flag and submitted.

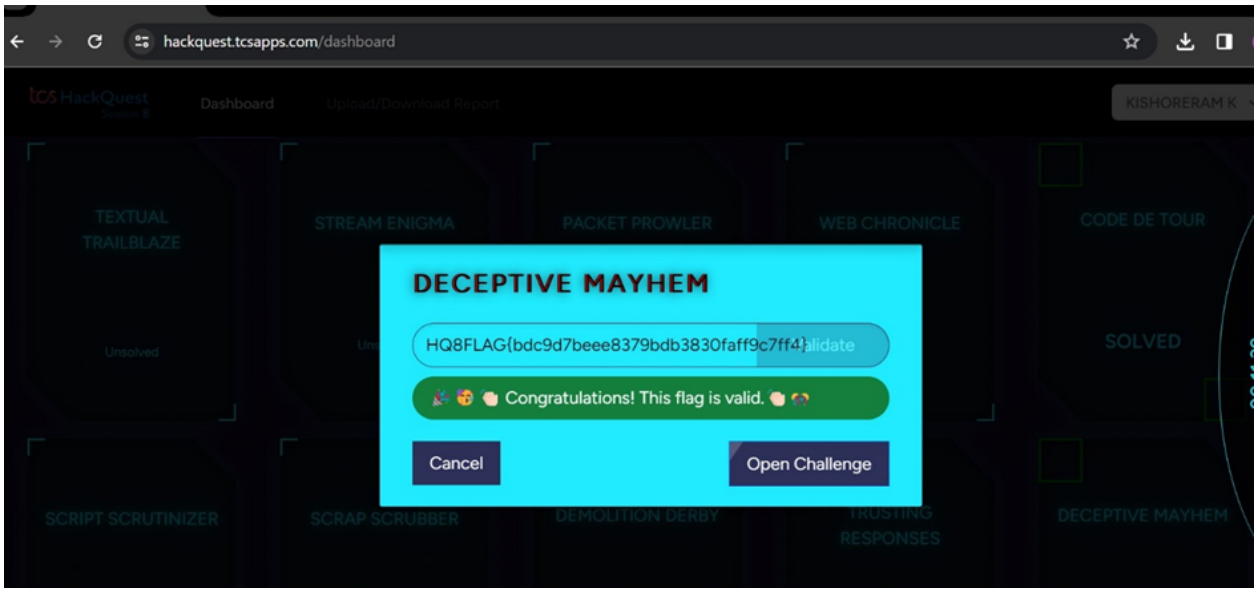


I intercepted the request with Burpsuite and viewed the HTTP History and found the onion url and I opened in TOR BROWSER and found the Leaked password database where I found the flag.




n4yiivfscj4bj3h3ssr4467i3ohpiwet5ylrqm6kk5kphdghjhvd7had.onion
Lahasun Pyaaj - Leaked Password Database
Greetings, fellow security enthusiasts!
Today, we bring you another set of leaked passwords as a reminder of the importance of maintaining strong and unique passwords.
Leak : Social Media Users
Platform: Facebook
Number of Accounts: 10,000
Password: ilovecats123
Leak : Online Shopping Sites
Platform: Amazon
Number of Accounts: 5,000
Password: letmein2020
Leak : Financial Services
Platform: Bank of Anon
Number of Accounts: 2,500
Password: 123456789


n4yiivfscj4bj3h3ssr4467i3ohpiwet5ylrqm6kk5kphdghjhvd7had.onion
Leak : Financial Services
Platform: Bank of Anon
Number of Accounts: 2,500
Password: 123456789
Leak : Professional Network
Platform: LinkedIn
Number of Accounts: 7,500
Password: password123
Leak : TCS HackQuest Seasion 8
Platform: TCS HackQuest
Number of Accounts: 1
Key: HQ8{a6471162999e92c79db70e11e7e9cd6e}

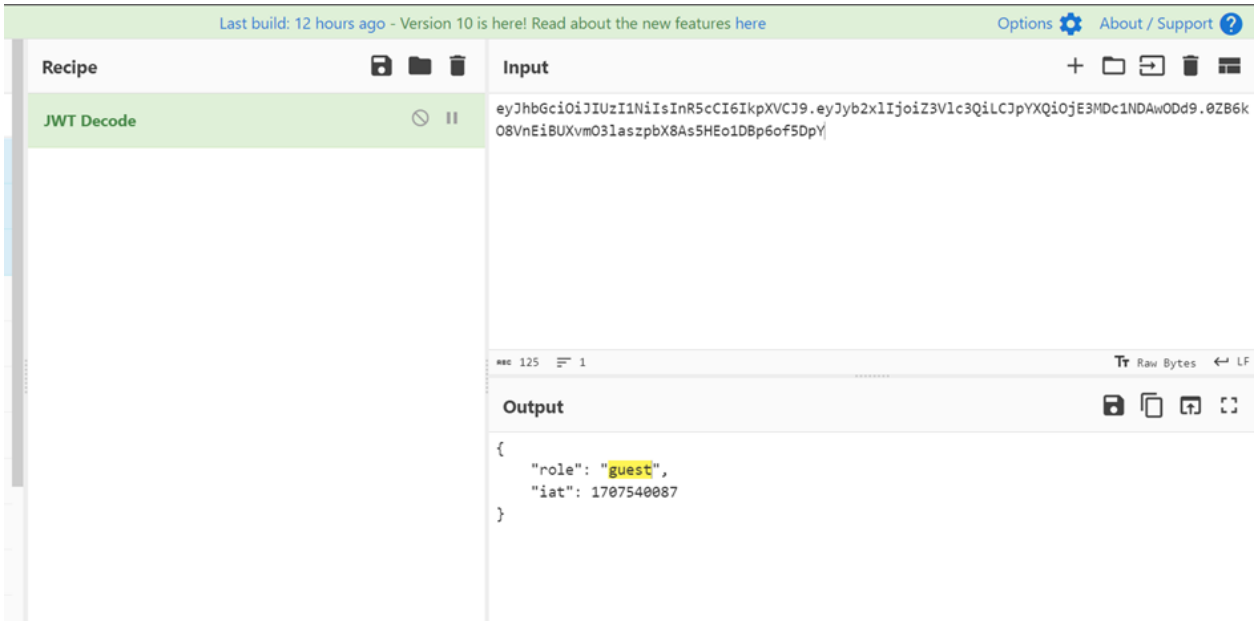

hackquest.tcsapps.com/dashboard
Dashboard
KISHORERAM K
TEXTUAL TRAILBLAZE
STREAM ENIGMA
PACKET PROWLER
WEB CHRONICLE
CODE DE TOUR
DECEPTIVE MAYHEM
HQ8FLAG{bdc9d7beee8379bdb3830faff9c7ff4}
Congratulations! This flag is valid.
Cancel
Open Challenge
SOLVED
SCRIPT SCRUTINIZER
SCRAP SCRUBBER
DEMOLITION DERBY
RESPONSES

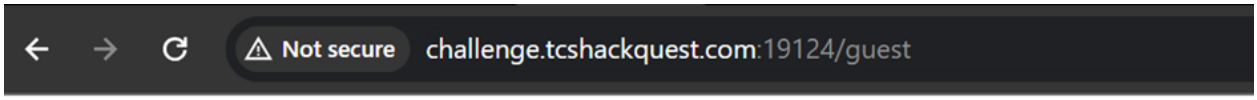
Round 2

Request tracer-100

Challenge Description:
Behind the user-friendly interface of every web application lies a complex tapestry of digital communication. This communication occurs through a series of silent requests and responses, governed by a hidden language that ensures the smooth operation of the application. Explore the intricate pathways that govern the methodical flow of information. Navigate the unseen mechanisms that shape the X-change between client and server.

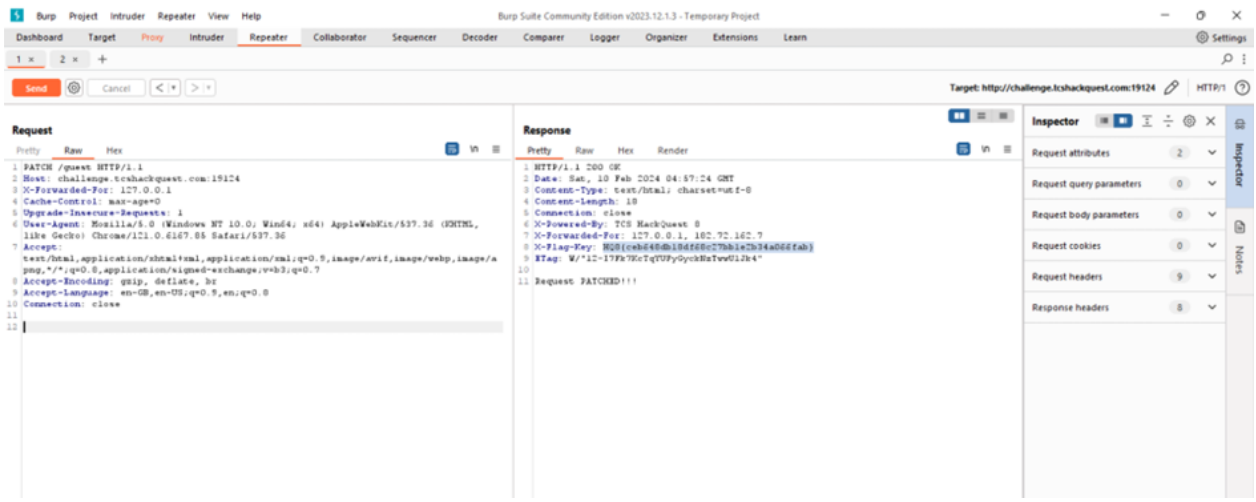
Uncover the secrets of communication protocols and the vital components that govern their behavior.





PATCH Method supported.

I website has drop-down option with traceroute button for four different sudomains for tcs website and I displayed the traceroute for the website with “*” and I could not infer anything from there then I read the source code and took the JWT Cookie and decrypted it and found the user as GUEST and requested a request in repeater in Burp-suite and I found response as PATCH Method supported and I again requested with Patch method and found the flag.



OFFICE LEAKS -200

Challenge Description:
Amidst Silicon Valley's tech frenzy, an innocent photo captured a sensitive document on a screen. Panic ensued as the photo went viral, but Arvind, a cybersecurity whiz, stepped in. Using his expertise, he tracked down the leaked document and identified the culprits. Regrettably, the leaked image continues to circulate on the internet, and we have successfully obtained a copy. Your task is to uncover the sensitive content that was inadvertently disclosed and make a report on the damage caused due to the leak.

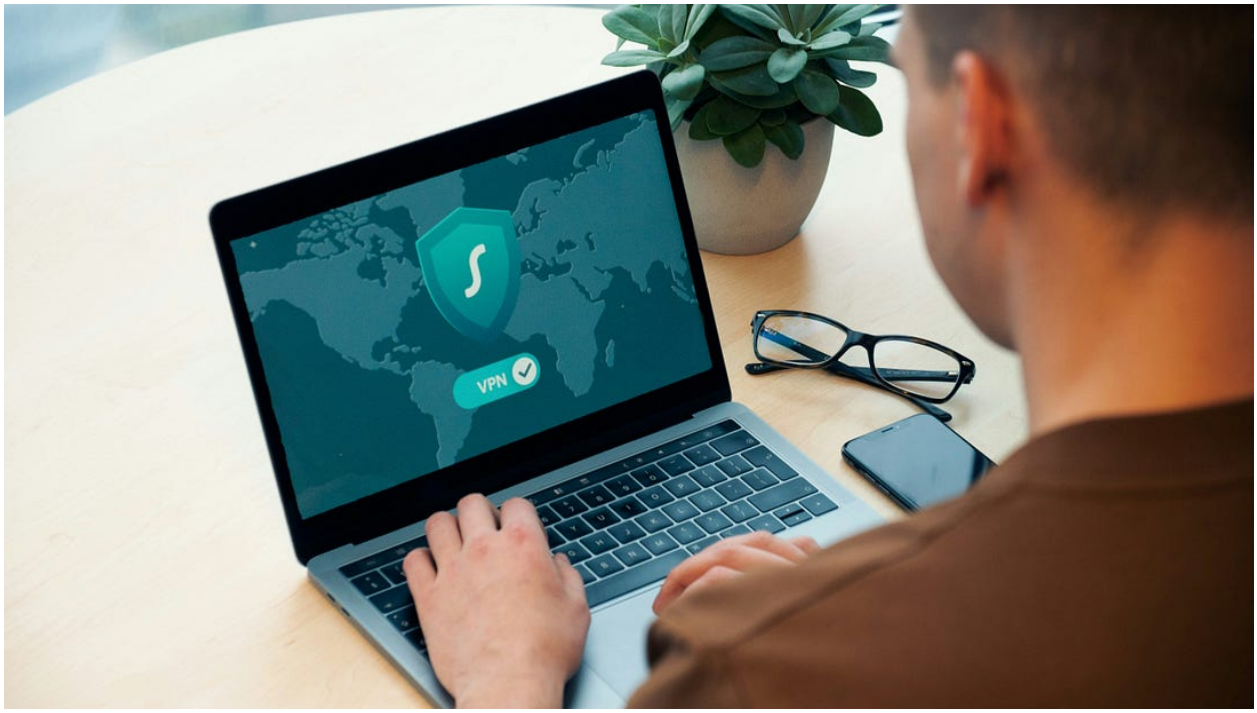


Photo by Dan Nelson on Unsplash

First I analysed the image with file command and used exiftool and started doing image forensics and also thought some file would be hidden and used steghide

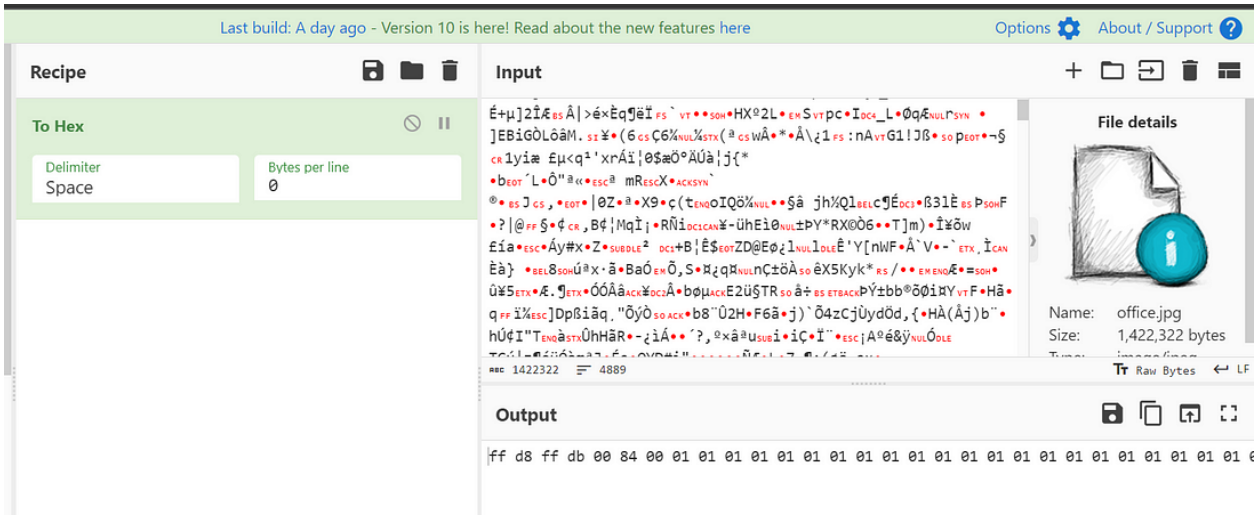
and binwalk to extract the hidden content and nothing found.

After that I used hxd editor and tried to refer magic bytes and also searched for similar challenges.

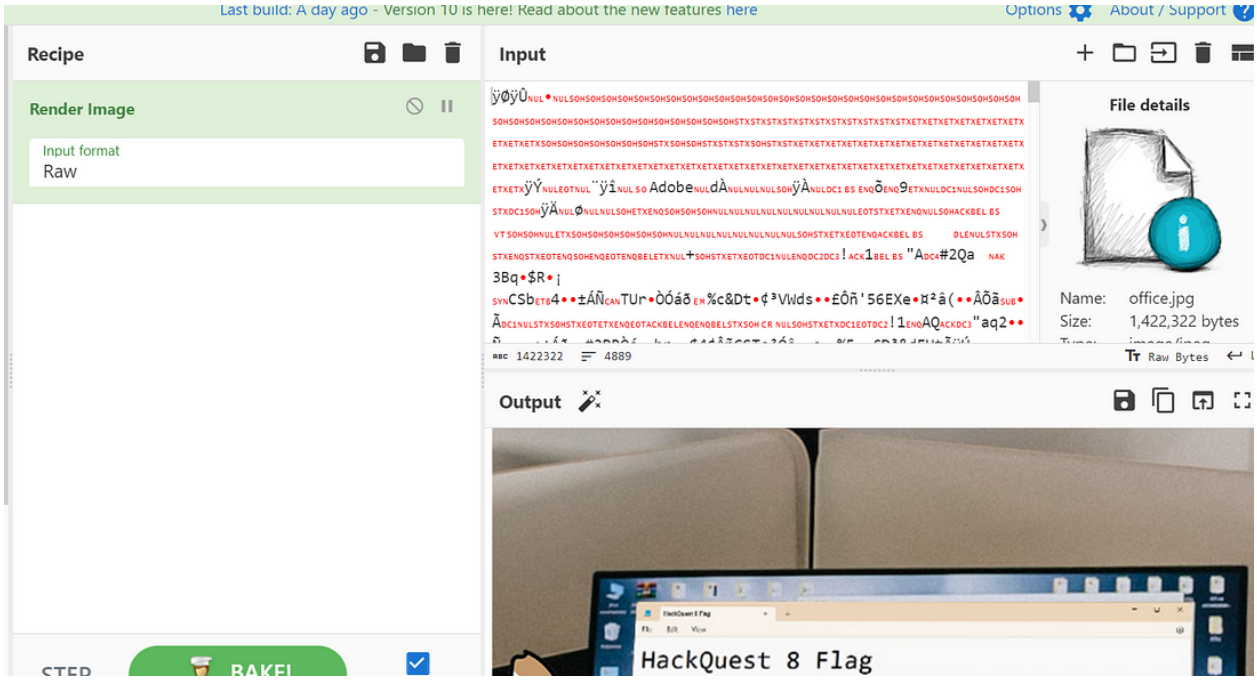
office.jpg

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	FF	D8	FF	DB	00	84	00	01	01	01	01	01	01	01	01	01	ÿØÿÛ.„.....
00000010	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	.....
00000020	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	.....
00000030	01	01	02	02	02	02	02	02	02	02	02	02	02	03	03	03	.....
00000040	03	03	03	03	03	03	03	01	01	01	01	01	01	01	02	01	.....
00000050	01	02	02	02	01	02	02	03	03	03	03	03	03	03	03	03	.....
00000060	03	03	03	03	03	03	03	03	03	03	03	03	03	03	03	03	.....
00000070	03	03	03	03	03	03	03	03	03	03	03	03	03	03	03	03	.....
00000080	03	03	03	03	03	03	03	03	FF	DD	00	04	00	A8	FF	EE	.....ÿÝ...¨ÿî
00000090	00	0E	41	64	6F	62	65	00	64	C0	00	00	00	01	FF	C0	..Adobe.dÀ....ÿÀ
000000A0	00	11	08	05	F5	05	39	03	00	11	00	01	11	01	02	11	....õ.9.....
000000B0	01	FF	C4	00	F8	00	00	01	03	05	01	01	01	00	00	00	.ÿÄ.ø.....
000000C0	00	00	00	00	00	00	04	02	03	05	00	01	06	07	08	09	.....
000000D0	0A	0B	01	01	00	03	01	01	01	01	01	01	00	00	00	00	.....
000000E0	00	00	00	00	01	02	03	04	05	06	07	08	09	10	00	02	.....
000000F0	01	02	05	02	04	05	01	05	04	05	07	03	00	2B	01	02	.....+..
00000100	03	04	11	00	05	12	13	21	06	31	07	08	22	41	14	23	.....!.1.."A.#
00000110	32	51	61	09	15	33	42	71	81	24	52	91	A1	0A	16	43	2Qa..3Bq.$R'¡..C
00000120	53	62	17	34	92	93	B1	C1	D1	18	54	55	72	94	D2	D3	Sb.4'"±ÁÑ.TUr"ÒÓ
00000130	E1	F0	19	25	63	26	44	74	82	A2	B3	56	57	64	73	95	áð.%c&Dt,¢³VWds•
00000140	96	A3	D4	F1	27	35	36	45	58	65	97	A4	B2	E2	28	83	–£Ôñ'56EXe—¤²â(ƒ
00000150	84	C2	D5	E3	1A	85	C3	11	00	02	01	02	04	03	05	04	„ÂÕã.…Ã.....
00000160	06	07	05	05	07	02	01	0D	00	01	02	03	11	04	12	21	.....!
00000170	31	05	41	51	06	13	22	61	71	32	81	91	D1	07	14	A1	1.AQ.."aq2.'Ñ..¡
00000180	B1	C1	F0	15	23	33	42	52	D2	E1	16	62	72	82	92	24	±Áð.#3BRÒá.br,'$
00000190	34	A2	C2	F1	43	53	54	73	B2	D3	E2	17	63	08	25	35	4¢ÂñCSTs²Óâ.c.%5
000001A0	83	93	A3	44	B3	26	64	45	55	74	C3	FF	DA	00	0C	03	ƒ"£D³&dEUtÃÿÚ...
000001B0	00	00	01	11	02	11	00	3F	00	3E	37	06	4C	C1	98	C1	.....?.>7.LÁ˜Á
000001C0	2D	4B	B4	B1	03	F0	CE	BF	0D	1B	CA	DA	6C	15	80	63	-K´±.ðÎ¿..ÊÚl.€c

I referred this article from internet https://cyberhacktics.com/hiding-information-by-changing-an-images-height/

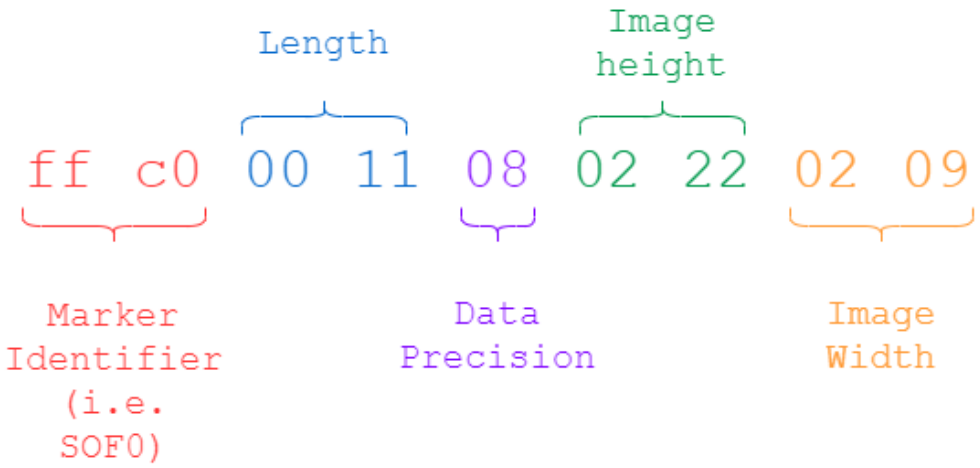


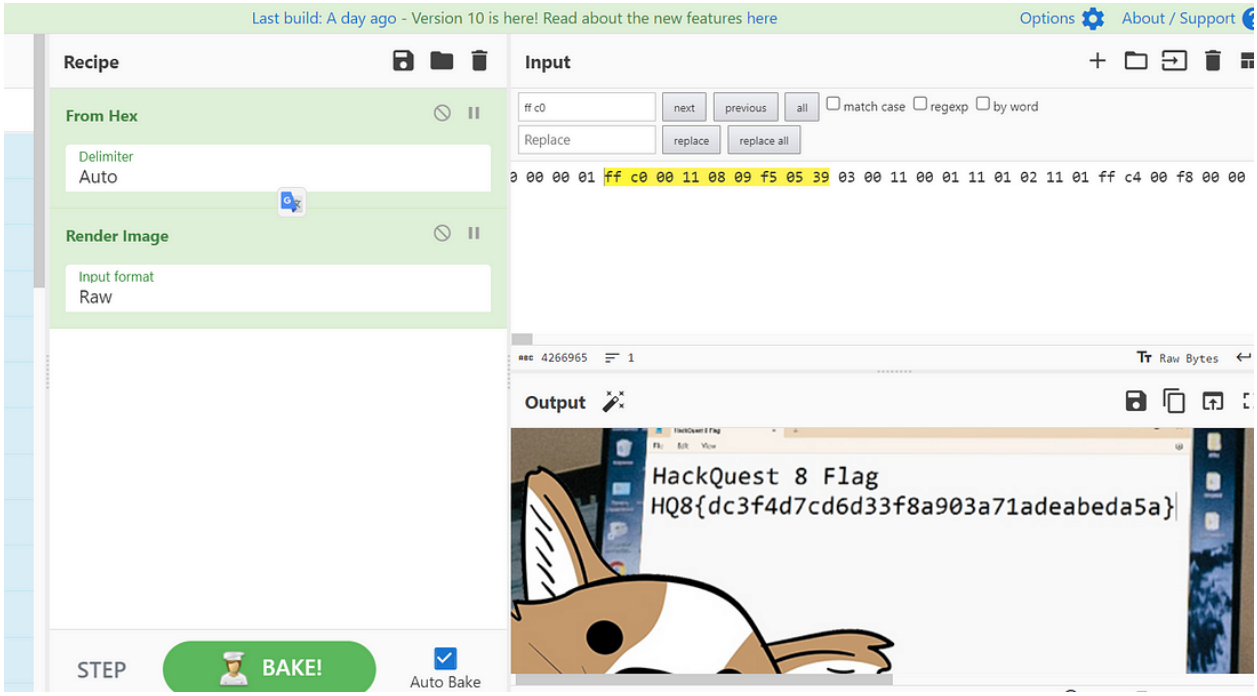
I thought the image is not in its complete portion after reading the article and rendered the image



I uploaded the image in cyberchef and imported To hex and copied the hex values. After that I inputed that Hex values and modified the values from `ff c0 00 11 08 05 f5 05 39` to `ff c0 00 11 08 09 f5 05 39`

05->09 in the 6th position of this.





After completing the CTF. I solved another challenge and I solved the QR Code challenge.

KOHRAA -100

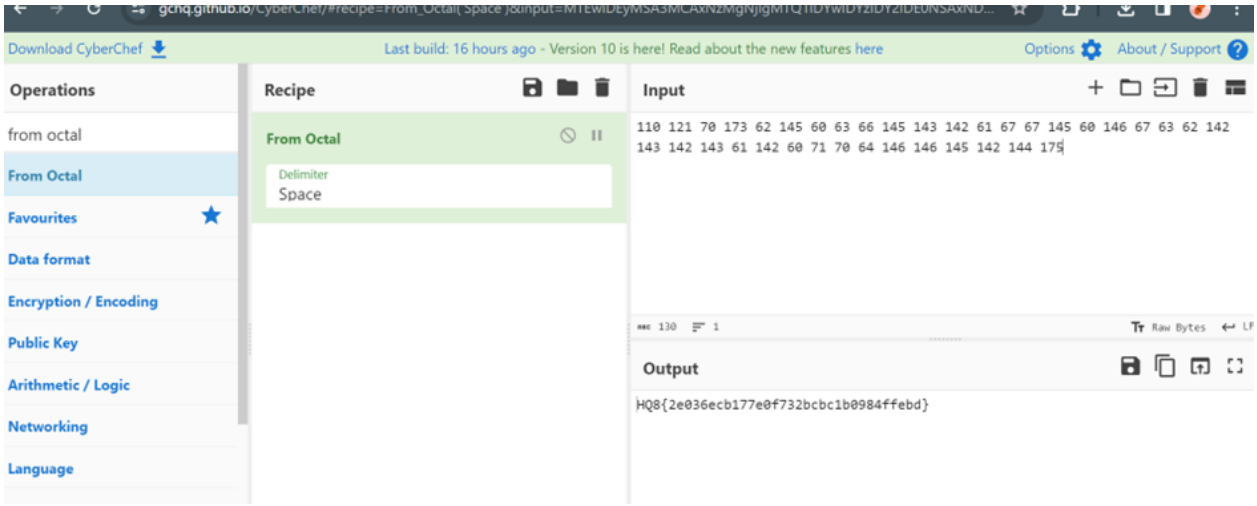
Challenge Description:
Embark on a digital journey through the haze of our Blurry Enigma Hunt! Someone intentionally blurred this image, challenging you to sharpen your skill and uncover the hidden treasure. The missing piece holds the key, and once you have pieced it together you need to uncover the message within the blurry landscape.

There was a broken QR-Code we need to fix it to get the flag and after analysing the qr code I found the left Box was missing and cropped the box using online phone editor https://www.iloveimg.com/photo-editor
and and attached there

After scanning I got the message.

BEGIN:VCARD
VERSION:3.0
N:Kohraa;
TEL:110 121 70 173 62 145 60 63 66 145 143 142 61 67 67 145 60 146 67 63 62 142 143 142 143 61 142 60 71 70 64 146 146 145 142 144 175
END:VCARD

I used Cyberchef and From Octal and got the flag


Download CyberChef
Last build: 16 hours ago - Version 10 is here! Read about the new features here
Options
About / Support
Operations
from octal
From Octal
Favourites
Data format
Encryption / Encoding
Public Key
Arithmetic / Logic
Networking
Language
Recipe
From Octal
Delimiter
Space
Input
110 121 70 173 62 145 60 63 66 145 143 142 61 67 67 145 60 146 67 63 62 142
143 142 143 61 142 60 71 70 64 146 146 145 142 144 175
Raw Bytes
Output
HQ8{2e036ecb177e0f732bcbc1b0984ffebd}


MISSION
COMPLETE
quickmeme.com