Correct

UTCTF2024 WriteUp

Robin Goods

siciday
pauwow
bagx
Swaggytree
earl_camilo

March 30 - April 1, 2024

I. About the CTF

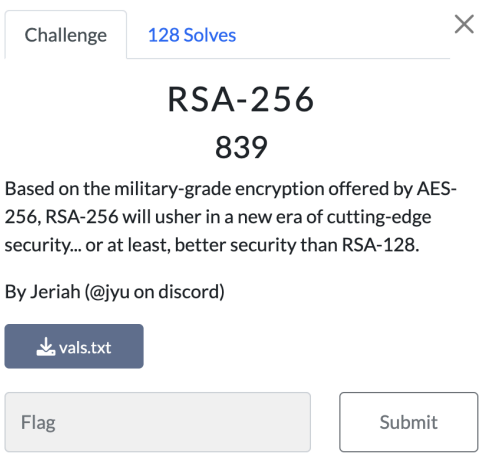
UTCTF 2024, organized by UT ISSS, is a Capture the Flag (CTF) competition happening from March 29th, 6 PM CDT, to March 31st, 6 PM CDT. Teams worldwide will immerse themselves in this cybersecurity challenge, aiming to decrypt, hack, or exploit hidden flags across various problem categories like Binary Exploitation, Networking, Reverse Engineering, Cryptography, and the Web.

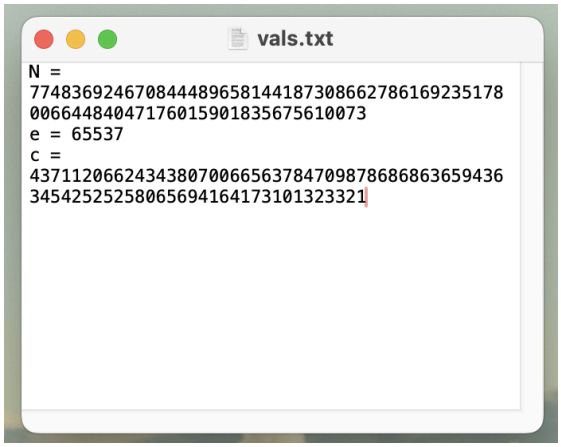
II. Flags Obtained

A. Cryptography

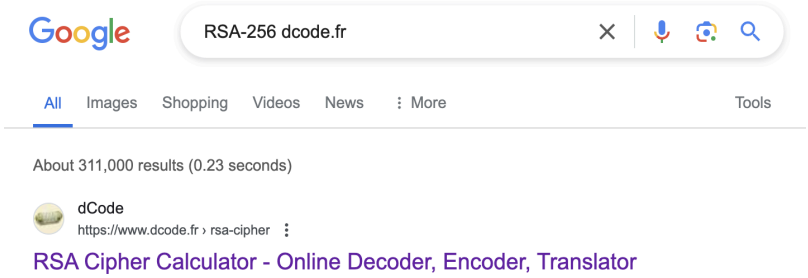
1. RSA-256

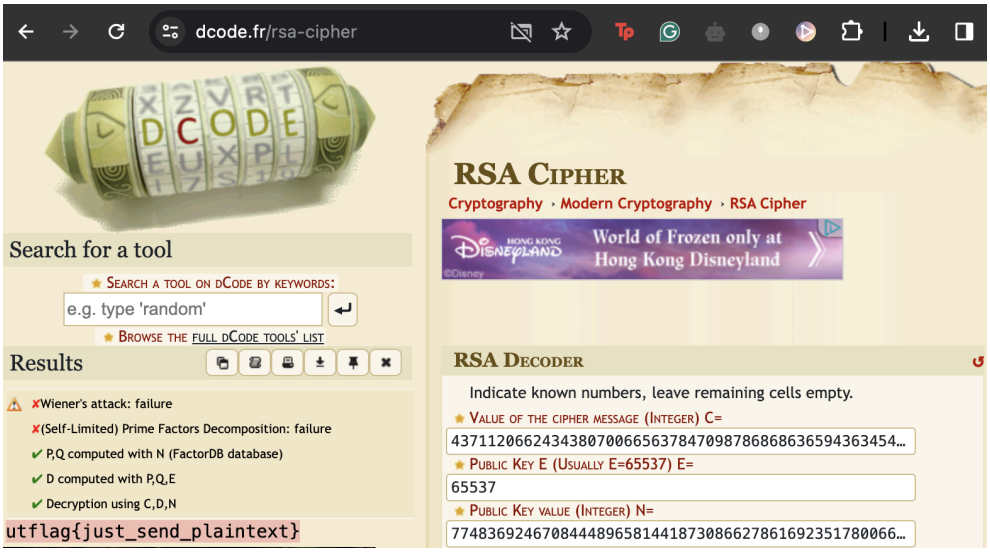
I downloaded the challenge file, which was a text file. Then, I opened it to see its contents.



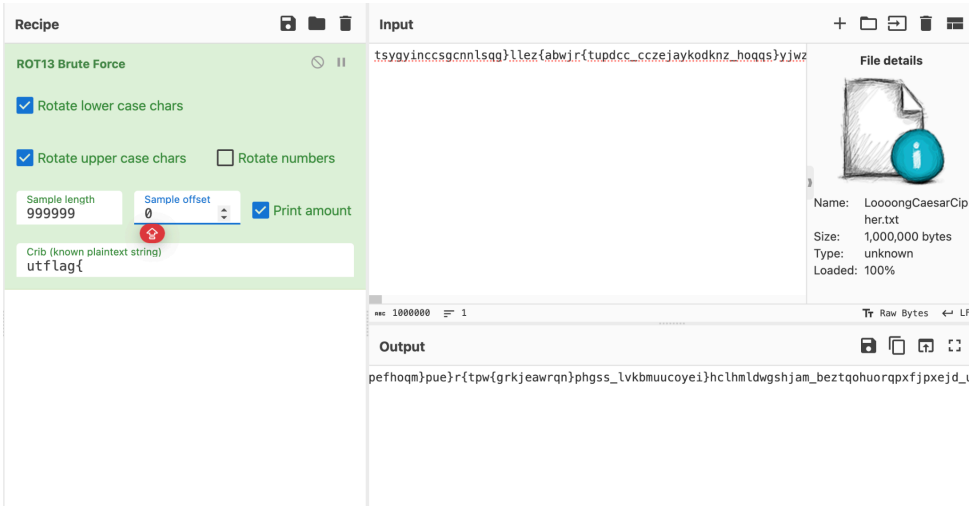


Since the challenge mentioned the RSA-256 cipher, I searched it up using the trusty dcode.fr tool. I inputted the corresponding values, and voila, the flag appeared!

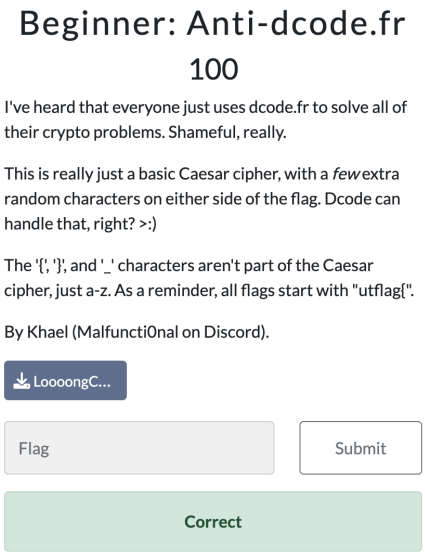




2. Anti-dcode.fr
   I downloaded the 1MB .txt file, and the ciphertext was really long. I uploaded the file onto CyberChef and since the challenge mentioned it was a Caesar Cipher, I used the ROT13 Brute Force Recipe to find the flag. According to my Google Search, ROT13 is the equivalent of the Caesar Cipher on Cyberchef.



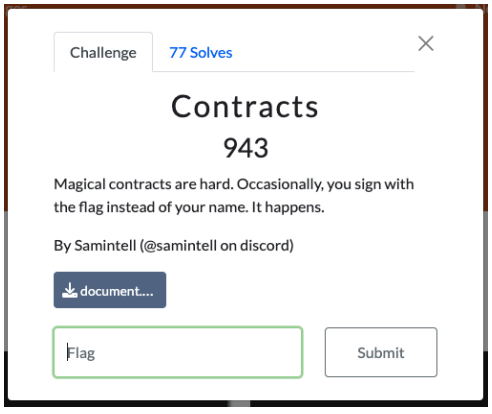
   I guessed and set the length to how much I thought the text would be. There was only one output that appeared, so I saved that instance, ctrl+f, and found the flag!

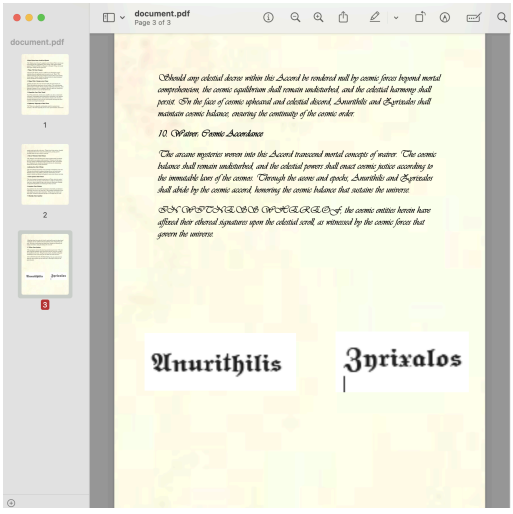


B. Forensics

1. Contracts

   I downloaded the file and found it was a PDF. Upon inspection, it appeared to be a contract with two images serving as signatures. This struck me as suspicious, so I made a mental note to extract or analyze them later.

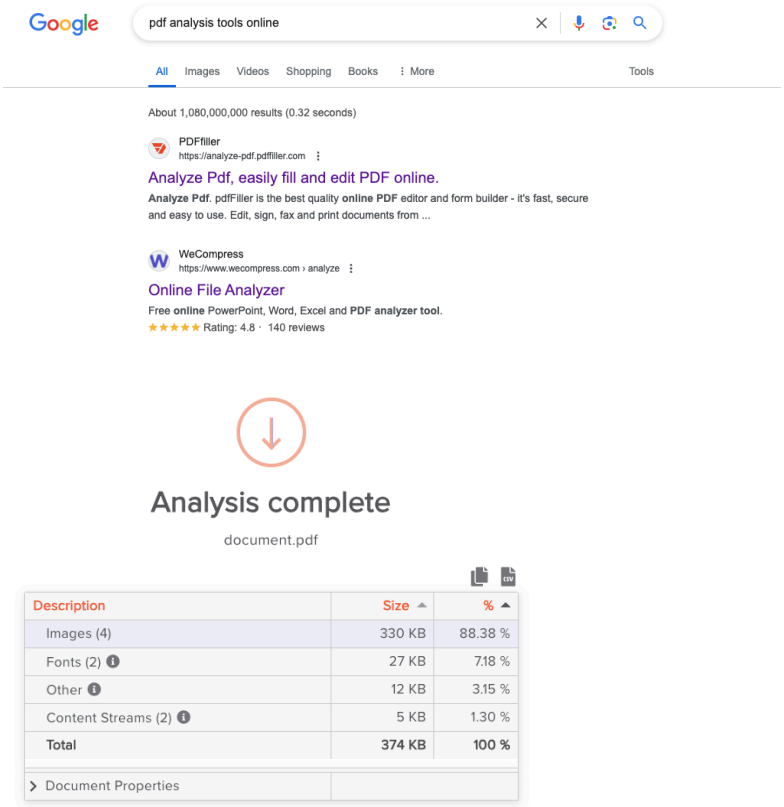




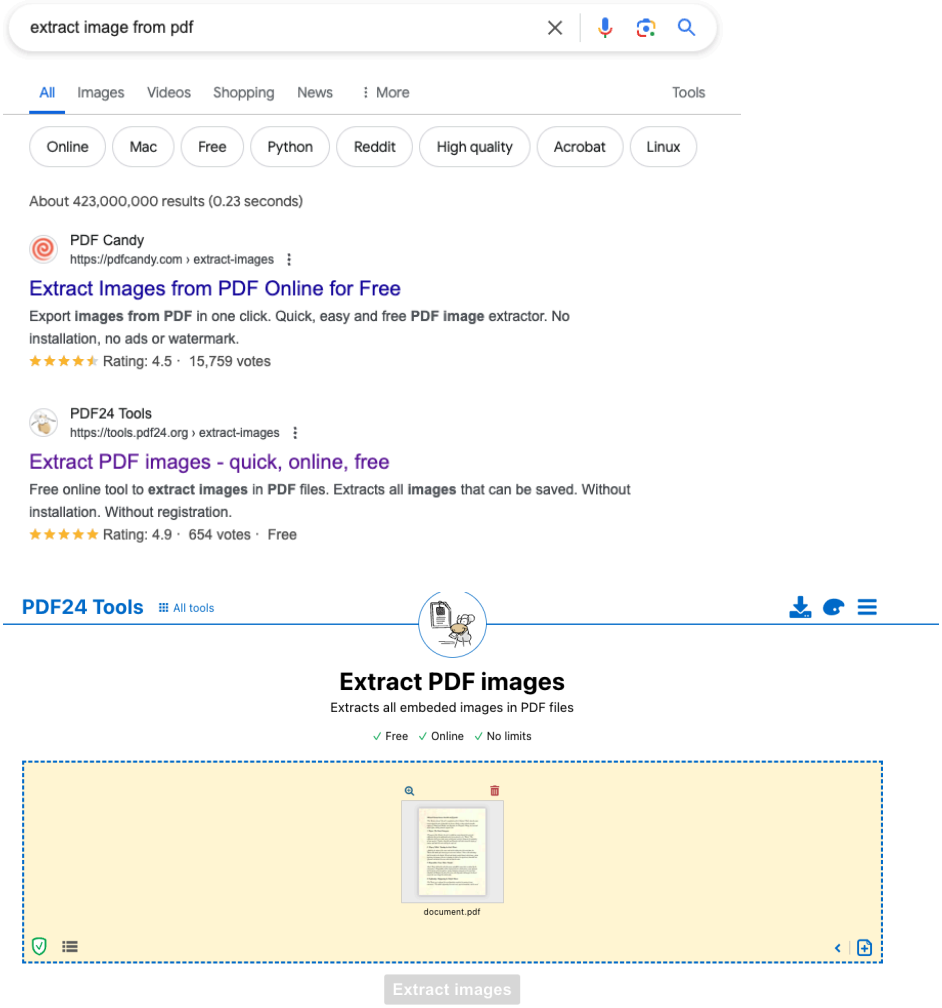
- I checked the metadata of the pdf file but found nothing unusual.

```
[sophiaelen@Sophias-MacBook-Air Downloads % exiftool document.pdf
ExifTool Version Number         : 12.76
File Name                       : document.pdf
Directory                       : .
File Size                       : 383 kB
File Modification Date/Time     : 2024:03:30 08:57:54+08:00
File Access Date/Time           : 2024:03:30 08:57:58+08:00
File Inode Change Date/Time     : 2024:03:30 08:57:56+08:00
File Permissions                : -rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.7
Linearized                      : No
Page Count                      : 3
Language                        : en
Tagged PDF                      : Yes
XMP Toolkit                     : 3.1-701
Producer                        : Microsoft® Word for Microsoft 365
Creator                         : Karim, Joshua C
Creator Tool                    : Microsoft® Word for Microsoft 365
Create Date                     : 2024:03:28 20:37:05-05:00
Modify Date                     : 2024:03:28 20:37:05-05:00
Document ID                     : uuid:5A792244-E90A-45AA-9549-930FBFA38328
Instance ID                     : uuid:5A792244-E90A-45AA-9549-930FBFA38328
Author                          : Karim, Joshua C
```

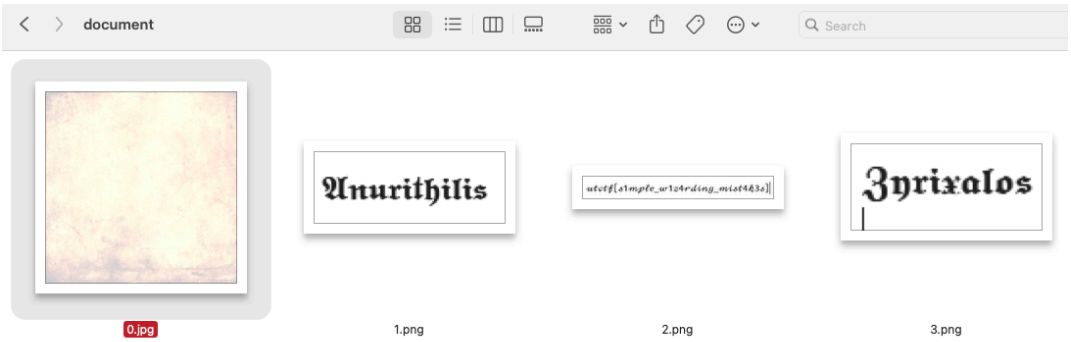
- Next, I searched for PDF analysis tools and came across https://www.wecompress.com/en/analyze. This site revealed four images, which was odd since only two were visible in the PDF.

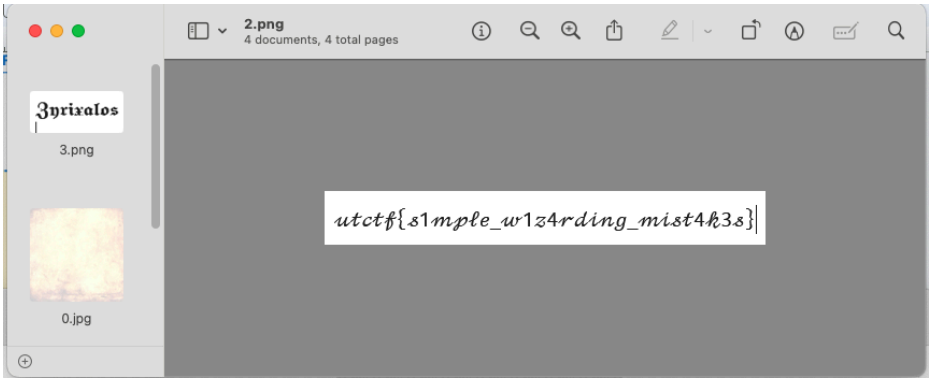


To extract the images, I searched for an image extractor from PDF and found https://tools.pdf24.org/en/extract-images. After using it, I downloaded a zip file containing the images.

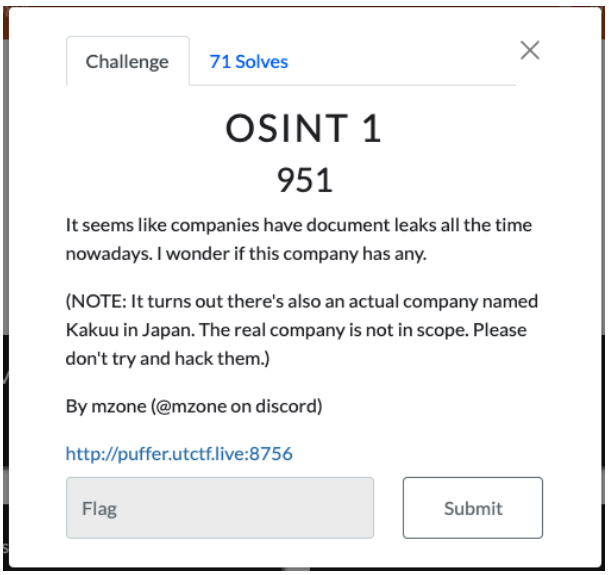


Upon extracting the zip file, I found the images, and there it was—the flag was right there in one of them.

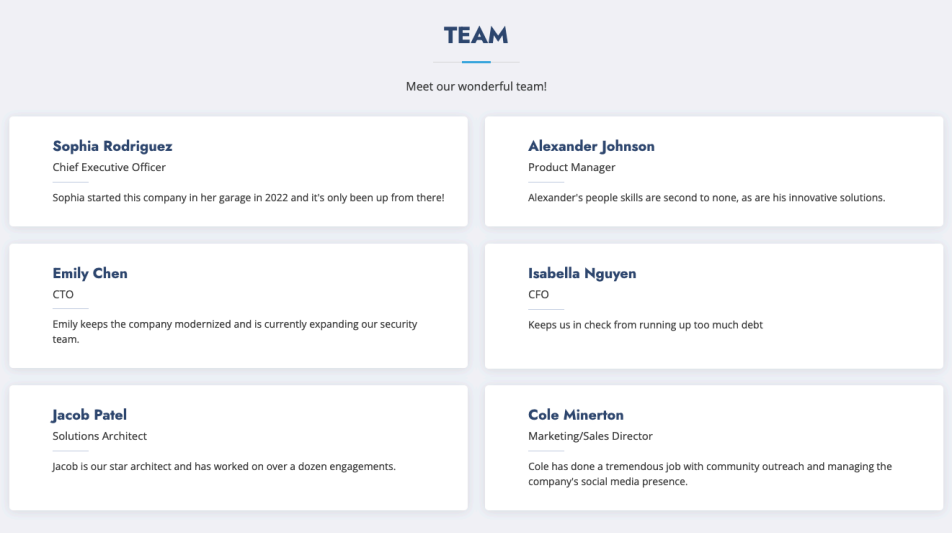




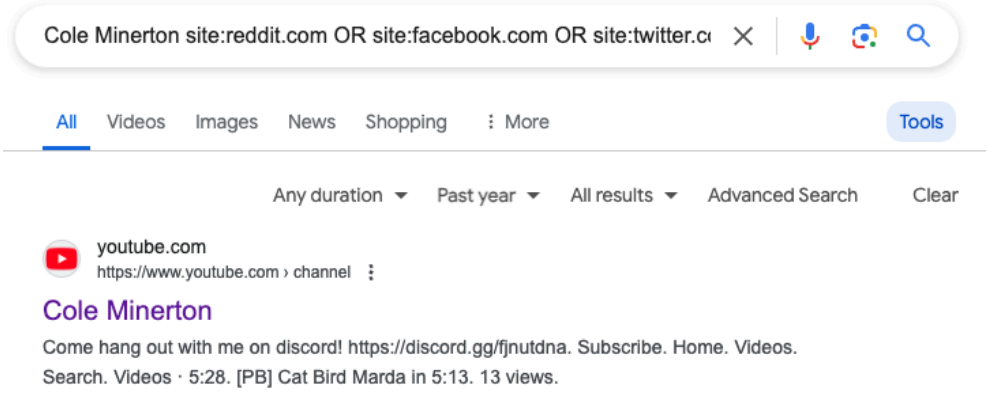
2. OSINT 1



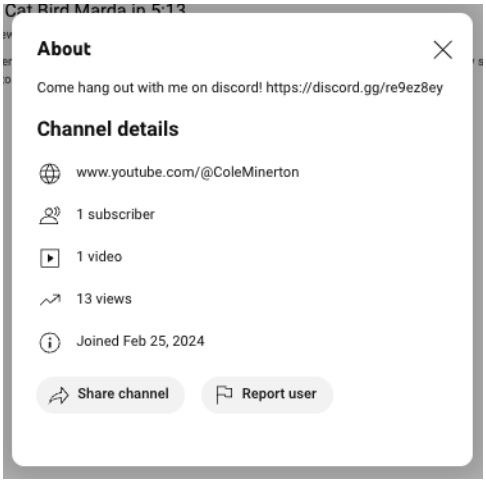
When the link was clicked, it brought us to the company webpage of Kakuu Corporation with some filler data. The only unique data were these names, and since it was an OSINT challenge, we figured we'd have to search for the leaked document.

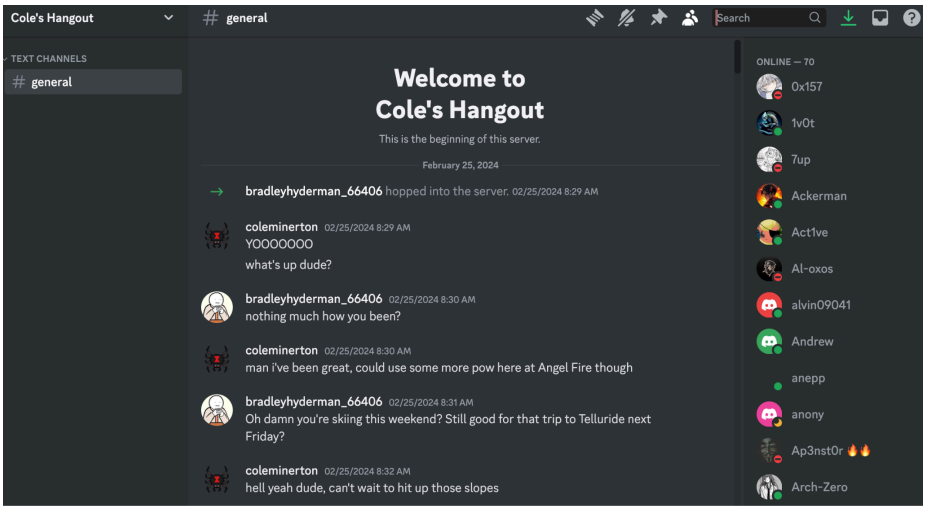


Out of all the names, this was the most interesting and made the most sense since the account was created only a month ago.

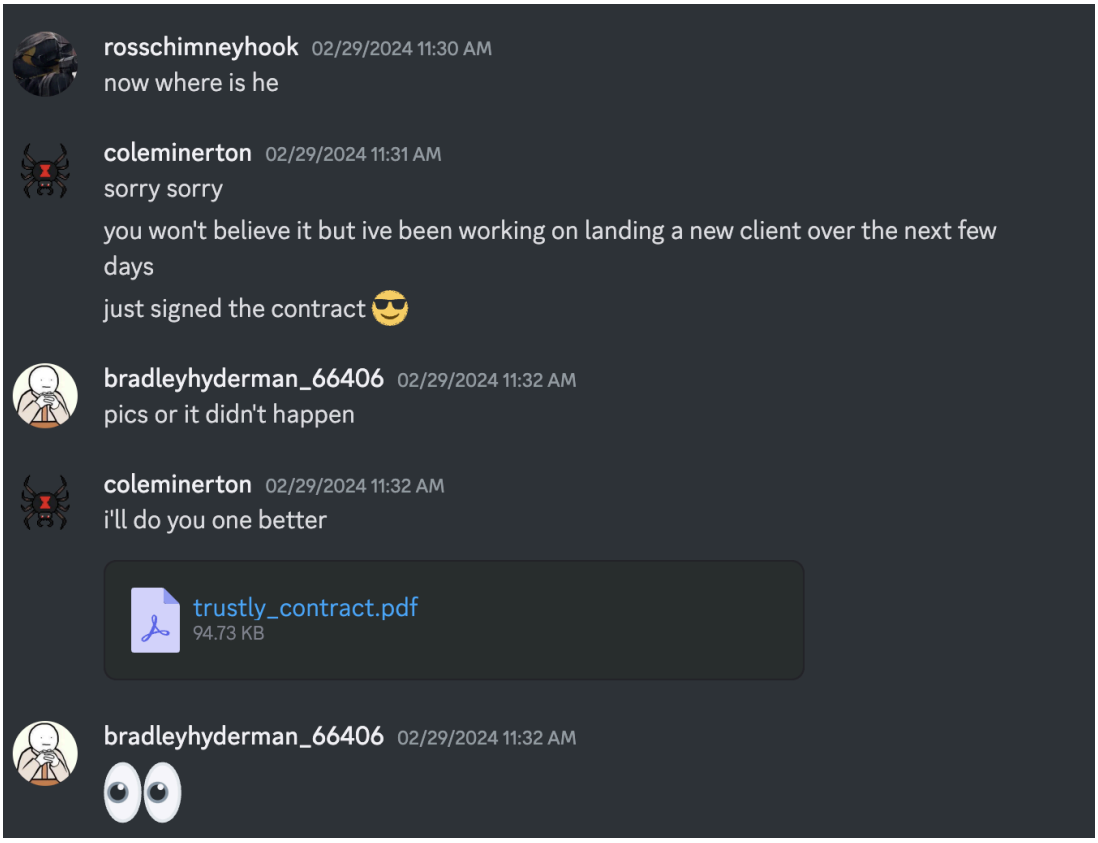


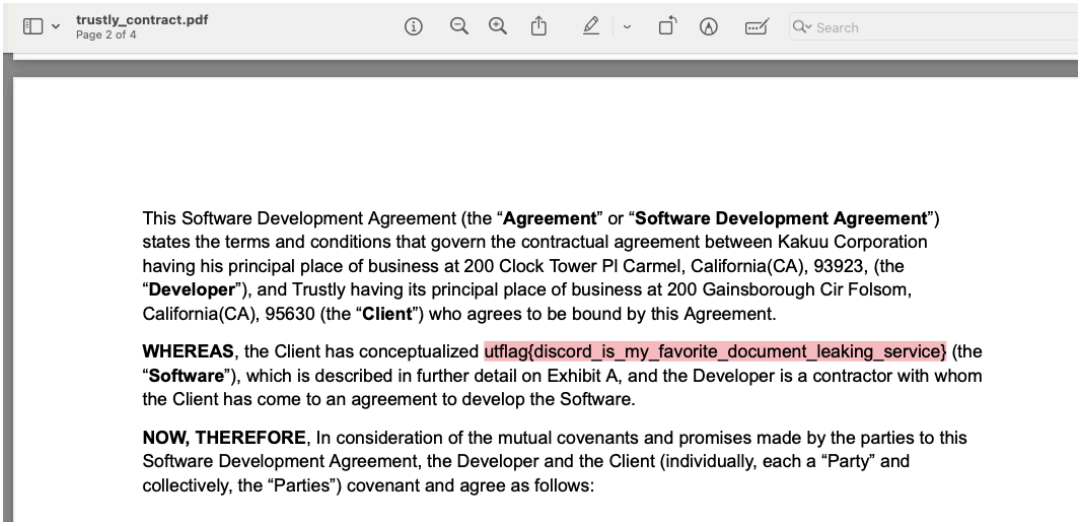
His YouTube About information contained a link to a discord channel.





We figured we were on the right track because the chat was recent, and it seemed suspicious. We looked through the chat and saw this file. Upon viewing the file, we saw the flag.



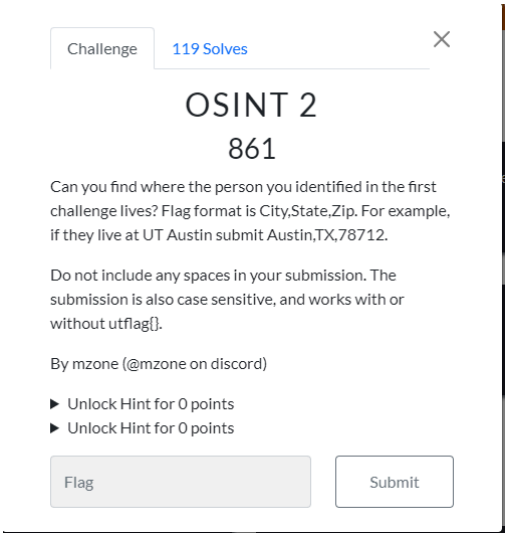


This Software Development Agreement (the "**Agreement**" or "**Software Development Agreement**") states the terms and conditions that govern the contractual agreement between Kakuu Corporation having his principal place of business at 200 Clock Tower Pl Carmel, California(CA), 93923, (the "**Developer**"), and Trustly having its principal place of business at 200 Gainsborough Cir Folsom, California(CA), 95630 (the "**Client**") who agrees to be bound by this Agreement.

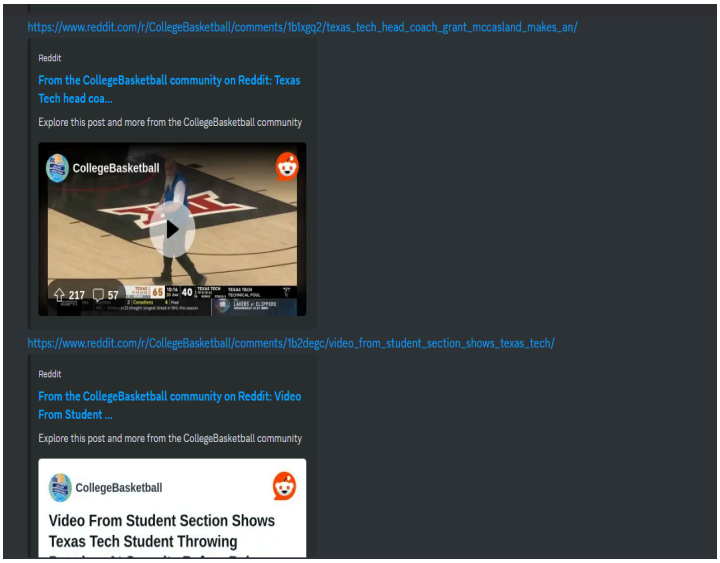
WHEREAS, the Client has conceptualized utflag{discord_is_my_favorite_document_leaking_service} (the "**Software**"), which is described in further detail on Exhibit A, and the Developer is a contractor with whom the Client has come to an agreement to develop the Software.

NOW, THEREFORE, In consideration of the mutual covenants and promises made by the parties to this Software Development Agreement, the Developer and the Client (individually, each a "Party" and collectively, the "Parties") covenant and agree as follows:

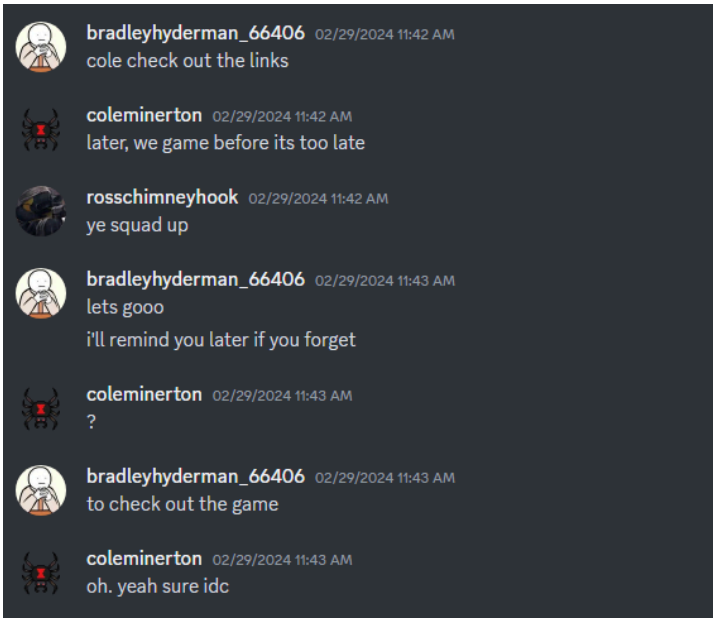
3. OSINT 2



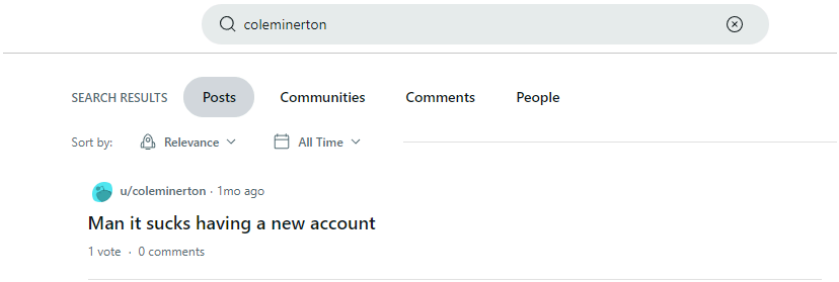
OSINT 2's challenge was to look for his location.



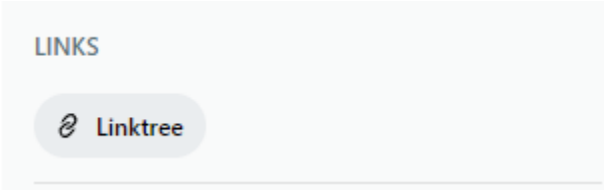
So we checked out the discord chats and found links to a basketball game that was sent to him



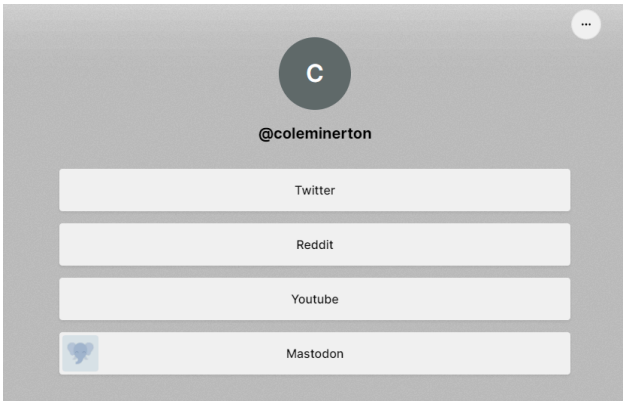
And we were hoping that he had a reddit account since they were talking about reddit posts



So I went over to reddit and searched his account and voila here he was.



He had a link tree on his accounts.



So i checked each link one by one.

We found this photo in Mastodon and remembered that he was going on a roadtrip with his buddies on this day.

At this point we just looked for Cimarron avenue that was near 2nd street and we could pinpoint exactly where he was!

4. OSINT 3

OSINT 3

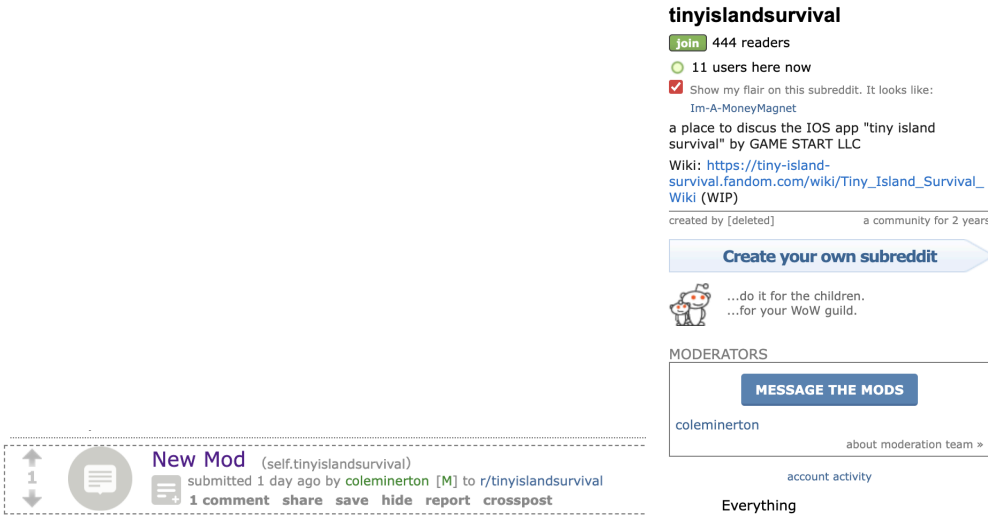
947

Can you find the person's IP address? Flag format is XXX.XXX.XXX.XXX

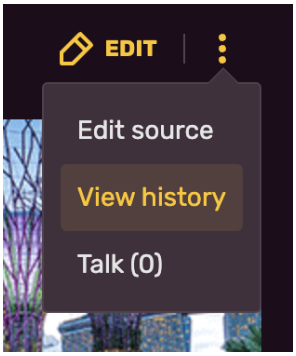
By mzone (@mzone on discord)

▼ Unlock Hint for 0 points
If you wound up on another (unrelated) discord server, then one of the sites you visited is too new.

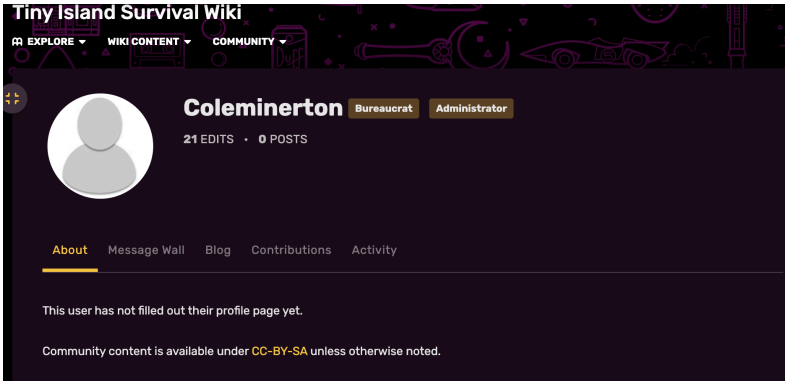
Now, we had to find Cole Minerton's IP address. So we looked through the other links in his linktree to see what else we could gather.

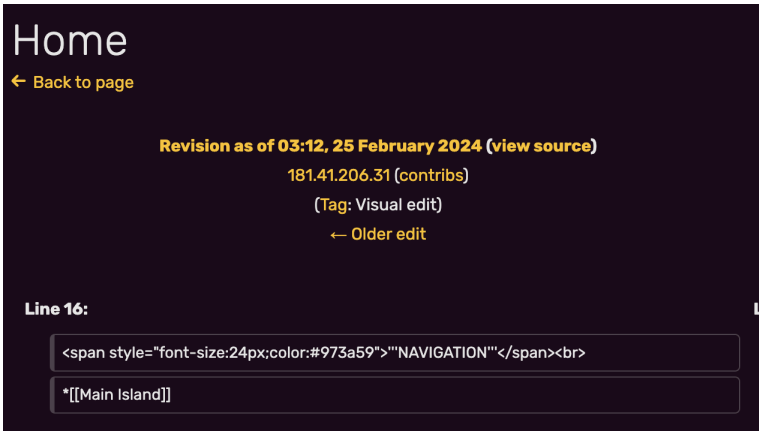


His Reddit page stood out the most because he was a mod in this game "Tiny Island Survival." The hint also mentioned landing on an unrelated discord channel which I know to be for that game as well since I wound up there too. It mentioned being "too new" so maybe we have to look for another link related to that. Using oldreddit, and clicking around, I saw the wiki page for the game.



Viewing the edit history of the wiki page allowed me to see Cole's name again and his contributions on the page. Some IP addresses were logged along with it. I entered one of it and it worked!

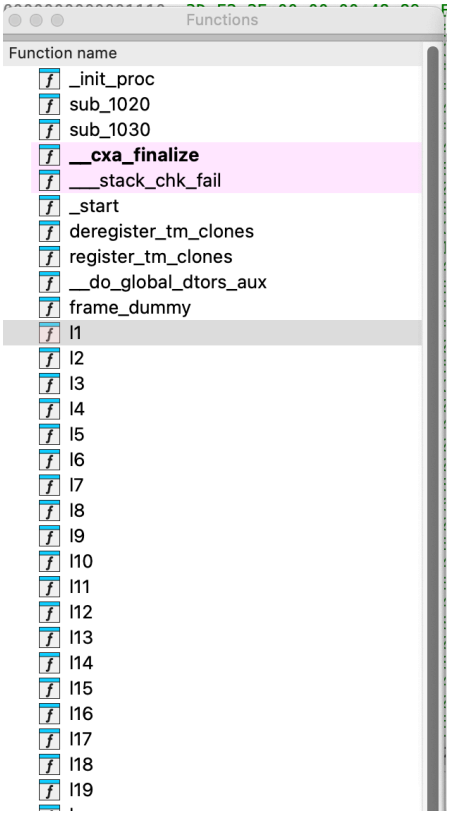




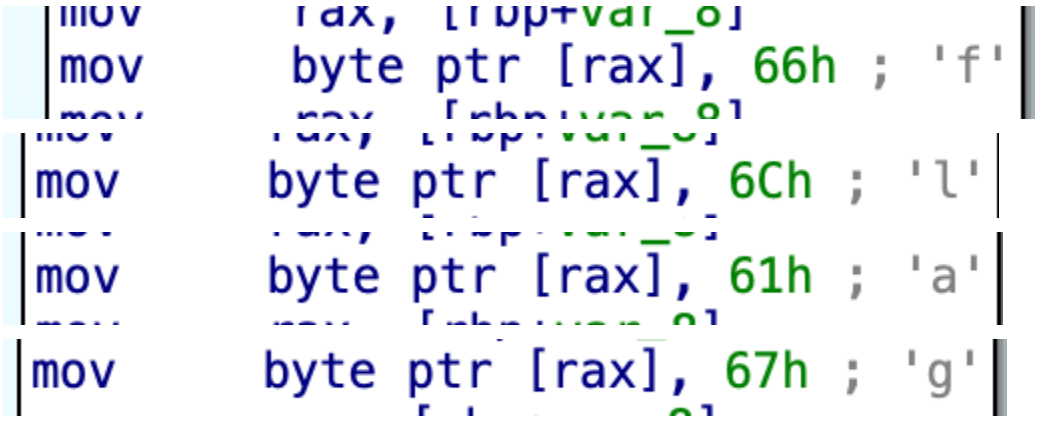
C. Reverse Engineering

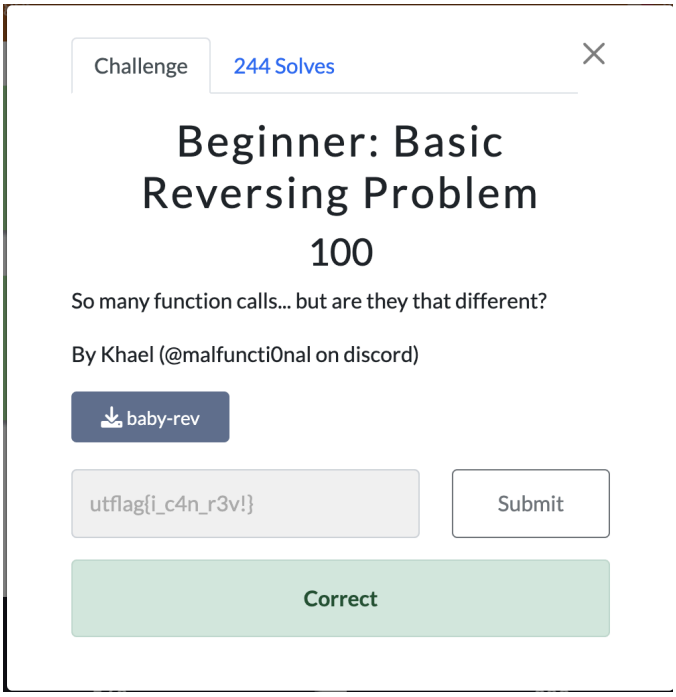
1. Basic Reversing Problem

Using ida64, I opened the ELF file and looked through the functions since the challenge mentioned it.



Looking through the functions one by one gave a line of code, which had some characters commented out and looked like the flag. I entered it, and it was the flag!

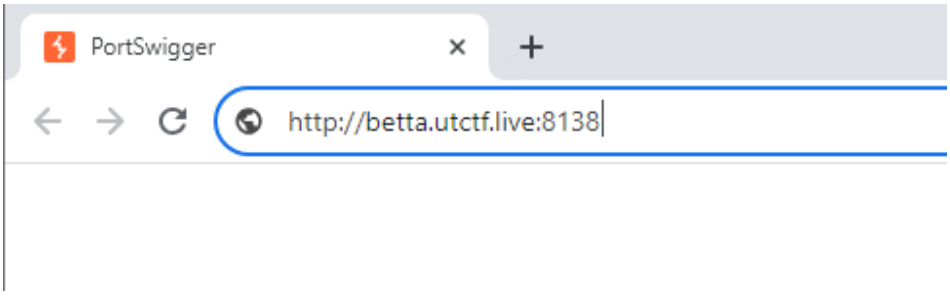


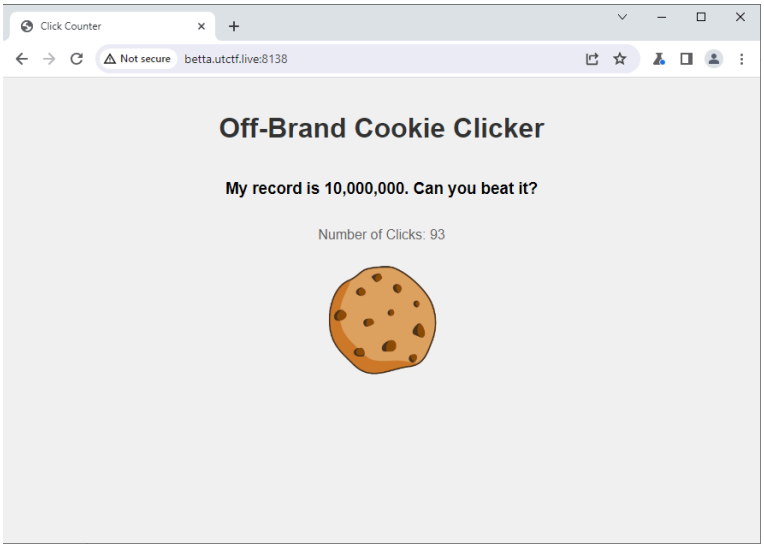


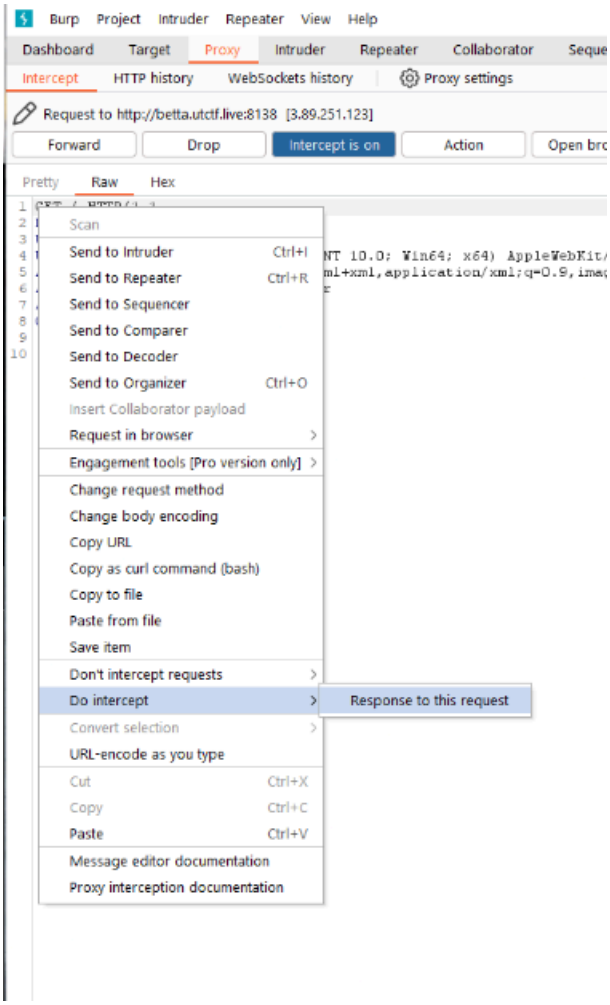
D. Web

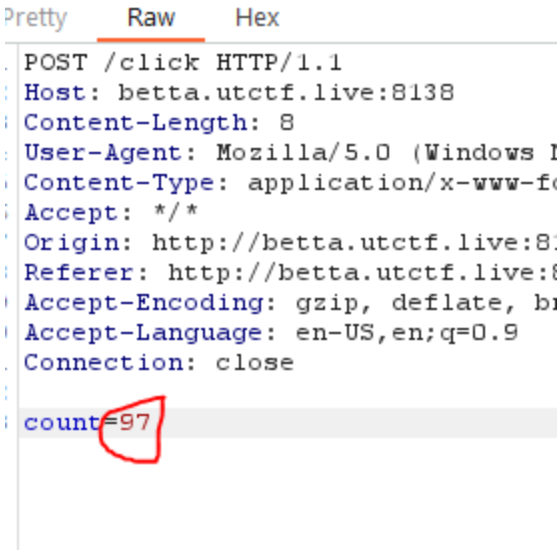
1. Beginner: Off-Brand Cookie Clicker

First I opened the website and realized that I needed to somehow modify the count of my clicks to finish the game. So I opened and set up BurpSuite.

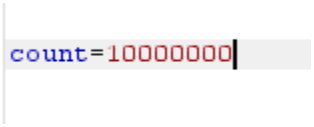



Click Counter
Not secure
betta.utctf.live:8138
Off-Brand Cookie Clicker
My record is 10,000,000. Can you beat it?
Number of Clicks: 93

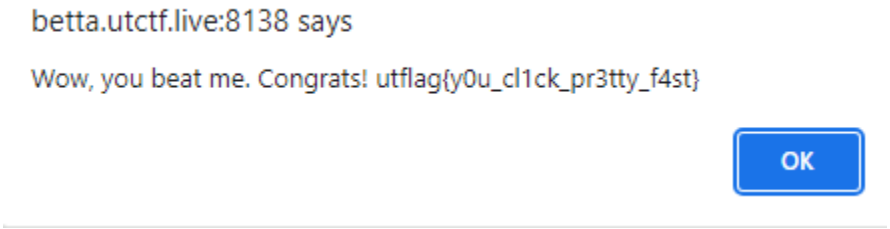

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator
Intercept HTTP history WebSockets history Proxy settings
Request to http://betta.utctf.live:8138 [3.89.251.123]
Forward Drop Intercept is on Action
Pretty Raw Hex
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
Insert Collaborator payload
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy URL
Copy as curl command (bash)
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Response to this request
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Proxy interception documentation

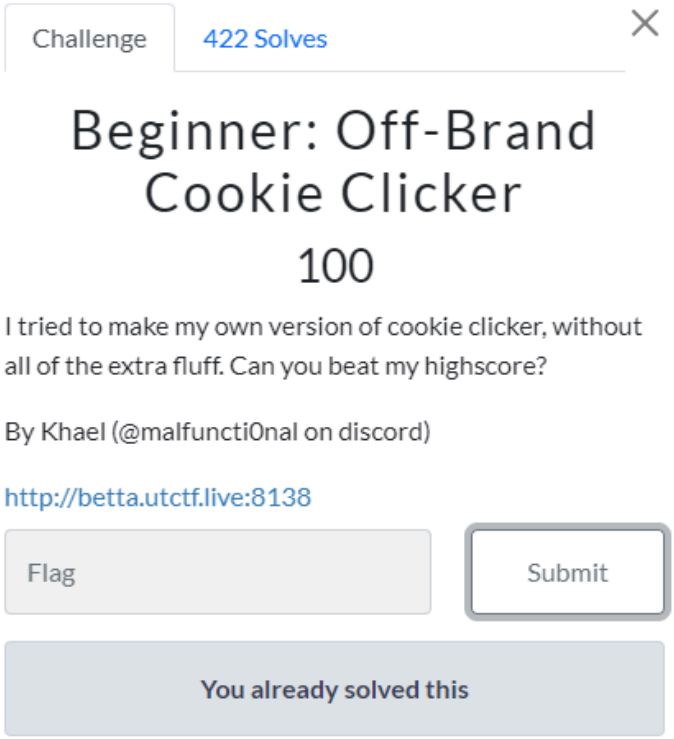


When I saw the count value, I changed the value to 10,000,000



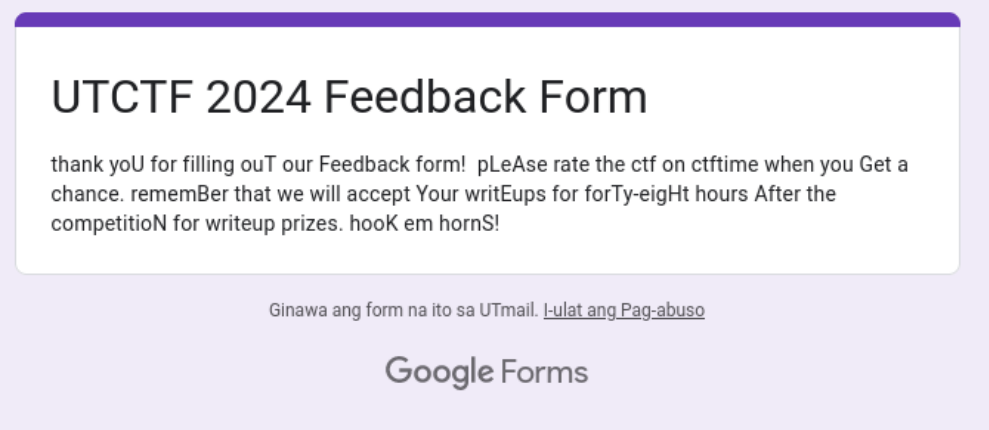
Then the flag appeared on the browser





E. Misc

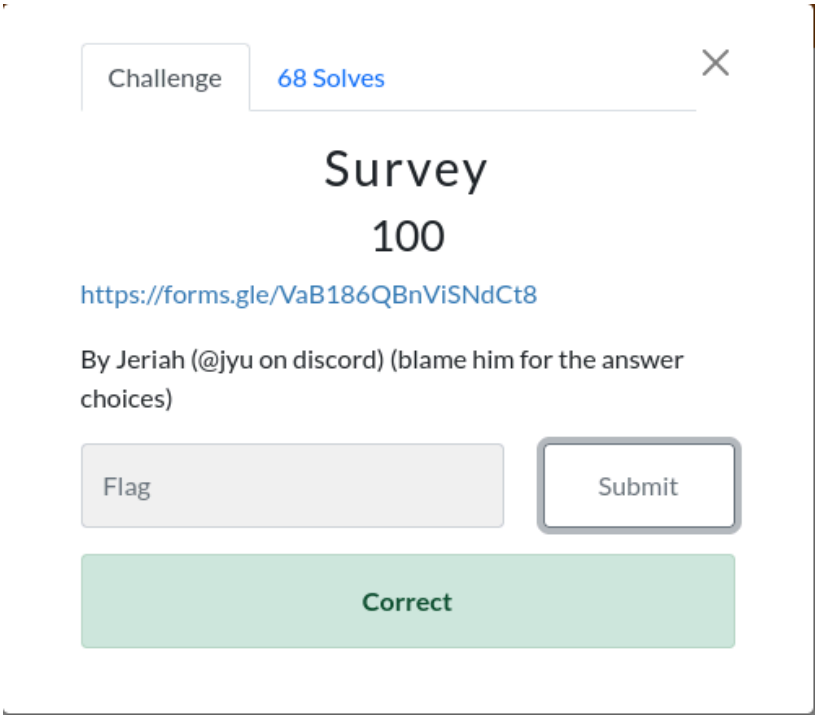
1. Survey
   This is what appeared after answering the google forms



I just looked at the capital letters and got:

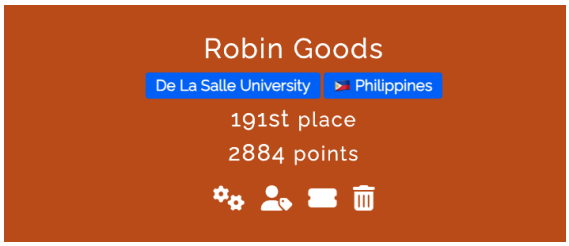
U T F L A G B Y E T H A N K S
Which I then put as the flag format:

utflag{byethanks}



III. Results and Statistics

Robin Goods managed to rank 191/854. Ranked Top 23% of teams participated in this CTF.



Cryptography

Forensics

Solves

Challenge	Category	Value	Time
Beginner: Off-Brand Cookie Clicker	Web	100	March 31st, 11:56:23 PM
Beginner: Basic Reversing Problem	Reverse Engineering	100	March 31st, 10:08:42 PM
Beginner: Anti-dcode.fr	Cryptography	100	March 31st, 9:35:41 PM
OSINT 3	Forensics	896	March 31st, 8:35:57 PM
Survey	Misc	100	March 31st, 5:29:02 PM
OSINT 2	Forensics	796	March 31st, 1:02:16 AM
OSINT 1	Forensics	592	March 30th, 11:54:38 PM
RSA-256	Cryptography	100	March 30th, 10:02:01 AM
Contracts	Forensics	100	March 30th, 9:23:19 AM