

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.

The image shows a challenge interface. At the top, there's a button labeled "Challenge" and a badge that says "128 Solves". Below that, the challenge title is "RSA-256" and the number of solves is "839". A description follows: "Based on the military-grade encryption offered by AES-256, RSA-256 will usher in a new era of cutting-edge security... or at least, better security than RSA-128." Below the description, it says "By Jeriah (@jyu on discord)". There are two buttons at the bottom: "Flag" and "Submit". To the right of the challenge interface is a separate window titled "vals.txt" containing the following text:

```
N =  
774836924670844489658144187308662786169235178  
00664484047176015901835675610073  
e = 65537  
c =  
437112066243438070066563784709878686863659436  
34542525258065694164173101323321
```

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!

The image shows a Google search results page. The search query is "RSA-256 dcode.fr". The results page includes a navigation bar with "All", "Images", "Shopping", "Videos", "News", "More", and "Tools". It also shows the number of results: "About 311,000 results (0.23 seconds)". The first result is from "dCode" with the URL "https://www.dcode.fr/rsa-cipher". The snippet for the result is "RSA Cipher Calculator - Online Decoder, Encoder, Translator".

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!



Beginner: Anti-dcode.fr

100

I've heard that everyone just uses dcode.fr to solve all of their crypto problems. Shameful, really.

This is really just a basic Caesar cipher, with a few extra random characters on either side of the flag. Dcode can handle that, right? >:)

The '{', '}'; and '_' characters aren't part of the Caesar cipher, just a-z. As a reminder, all flags start with "utflag[".

By Khael (MalfunctionOnal on Discord).

⬇️ LooongC...

Submit

Correct

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.

Challenge 77 Solves

Contracts

943

Magical contracts are hard. Occasionally, you sign with the flag instead of your name. It happens.

By Samintell (@samintell on discord)

⬇️ document...

Submit

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

```
[sophiaelen@Sophas-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 :
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.

Google

pdf analysis tools online

All Images Videos Shopping Books More Tools

About 1,080,000,000 results (0.32 seconds)

 PDFfiller
https://analyze-pdf.pdffiller.com

Analyze Pdf, easily fill and edit PDF online.
Analyze Pdf. pdfFiller is the best quality online PDF editor and form builder - it's fast, secure and easy to use. Edit, sign, fax and print documents from ...

 WeCompress
https://www.wecompress.com/analyze

Online File Analyzer
Free online PowerPoint, Word, Excel and PDF analyzer tool.
★★★★★ Rating: 4.8 · 140 reviews

Analysis complete

document.pdf

| Description | Size | % |
|-----------------------|--------|---------|
| Images (4) | 330 KB | 88.38 % |
| Fonts (2) ⓘ | 27 KB | 7.18 % |
| Other ⓘ | 12 KB | 3.15 % |
| Content Streams (2) ⓘ | 5 KB | 1.30 % |
| Total | 374 KB | 100 % |
| > Document Properties | | |

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.

extract image from pdf

All Images Videos Shopping News More Tools

Online Mac Free Python Reddit High quality Acrobat Linux

About 423,000,000 results (0.23 seconds)

 PDF Candy <https://pdfcandy.com/extract-images>

Extract Images from PDF Online for Free
Export Images from PDF in one click. Quick, easy and free PDF image extractor. No installation, no ads or watermark.

★★★★★ Rating: 4.5 · 15,759 votes

 PDF24 Tools <https://tools.pdf24.org/extract-images>

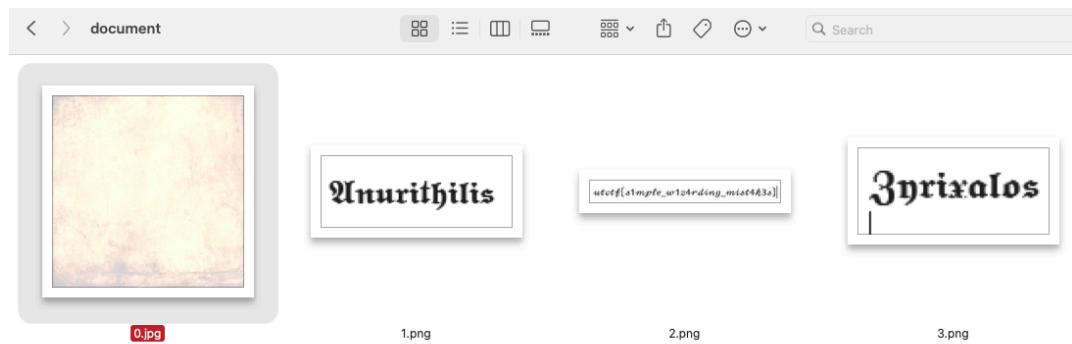
Extract PDF images - quick, online, free
Free online tool to extract images in PDF files. Extracts all images that can be saved. Without installation. Without registration.

★★★★★ Rating: 4.9 · 654 votes · Free

PDF24 Tools All tools



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

Challenge 71 Solves X

OSINT 1

951

It seems like companies have document leaks all the time nowadays. I wonder if this company has any.

(NOTE: It turns out there's also an actual company named Kakuu in Japan. The real company is not in scope. Please don't try and hack them.)

By mzone (@mzone on discord)

<http://puffer.utctf.live:8756>

Flag Submit

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.

TEAM

Meet our wonderful team!

| | |
|---|--|
| Sophia Rodriguez Chief Executive Officer Sophia started this company in her garage in 2022 and it's only been up from there! | Alexander Johnson Product Manager Alexander's people skills are second to none, as are his innovative solutions. |
| Emily Chen CTO Emily keeps the company modernized and is currently expanding our security team. | Isabella Nguyen CFO Keeps us in check from running up too much debt |
| Jacob Patel Solutions Architect Jacob is our star architect and has worked on over a dozen engagements. | Cole Minerton Marketing/Sales Director Cole has done a tremendous job with community outreach and managing the company's social media presence. |

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

Cole Minerton site:reddit.com OR site:facebook.com OR site:twitter.co X | Microphone icon Image icon Search icon

All Videos Images News Shopping ⋮ More Tools

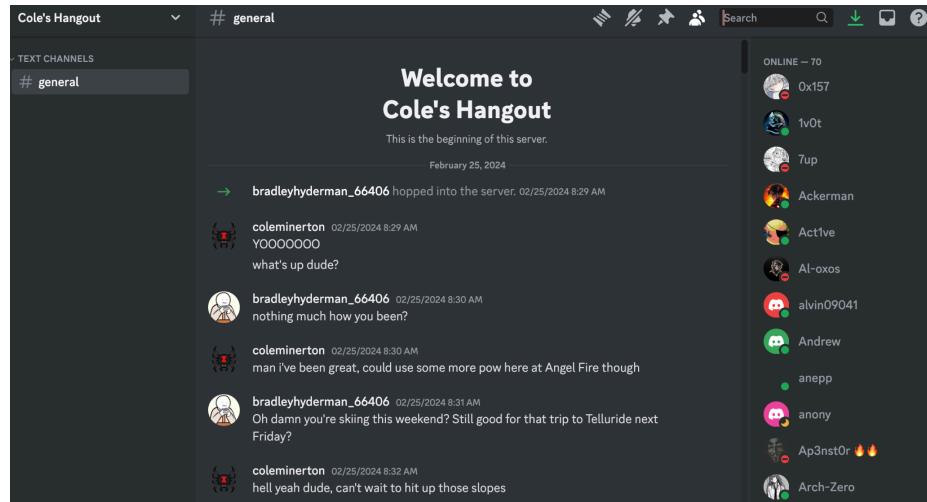
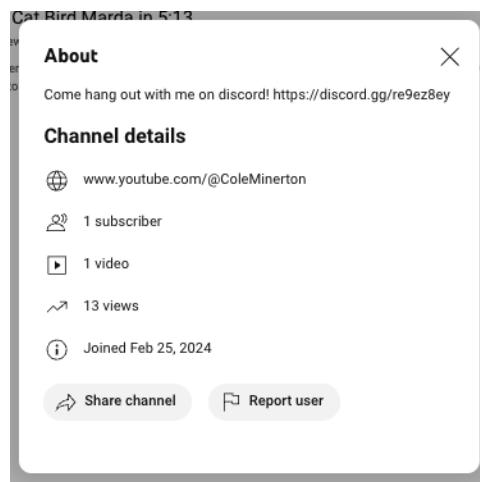
Any duration ▾ Past year ▾ All results ▾ Advanced Search Clear

 youtube.com
<https://www.youtube.com> › channel ⋮

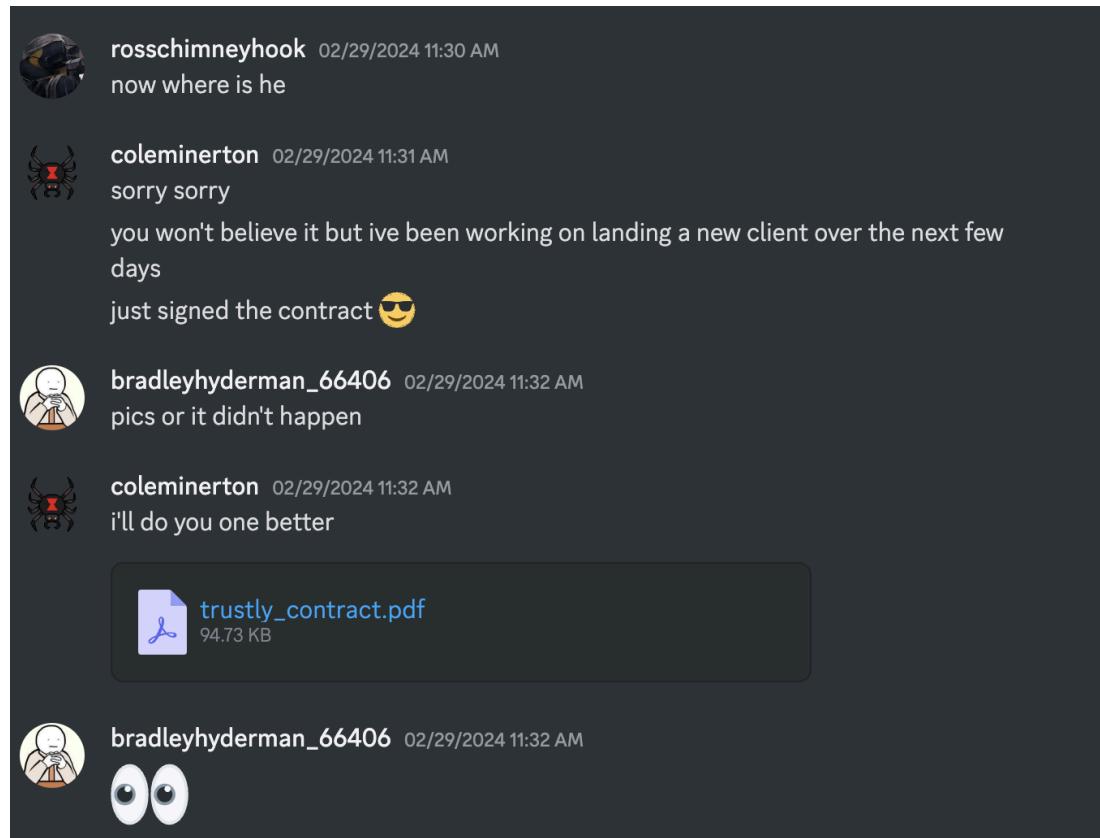
Cole Minerton

Come hang out with me on discord! <https://discord.gg/fjnudna>. Subscribe. Home. Videos.
Search. Videos · 5:28. [PB] Cat Bird Marda in 5:13. 13 views.

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.



The PDF viewer shows the following content on page 2 of 4:

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

Challenge 119 Solves X

OSINT 2

861

Can you find where the person you identified in the first challenge lives? Flag format is City.State.Zip. For example, if they live at UT Austin submit Austin,TX,78712.

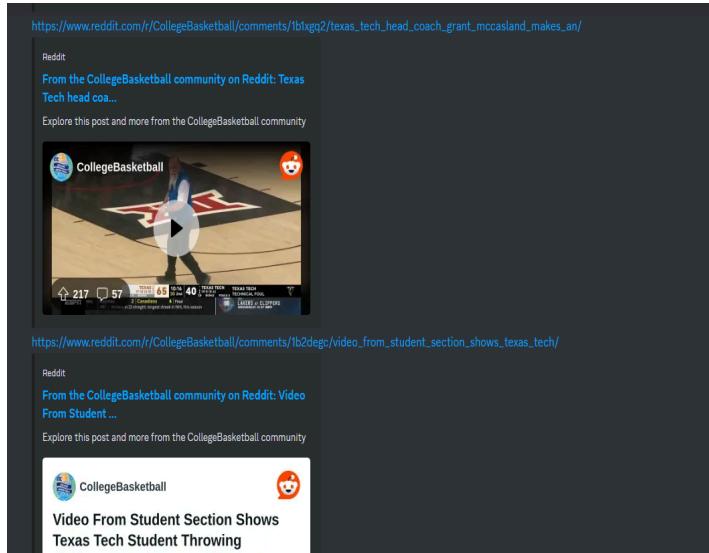
Do not include any spaces in your submission. The submission is also case sensitive, and works with or without utf8flag[].

By mzone (@mzone on discord)

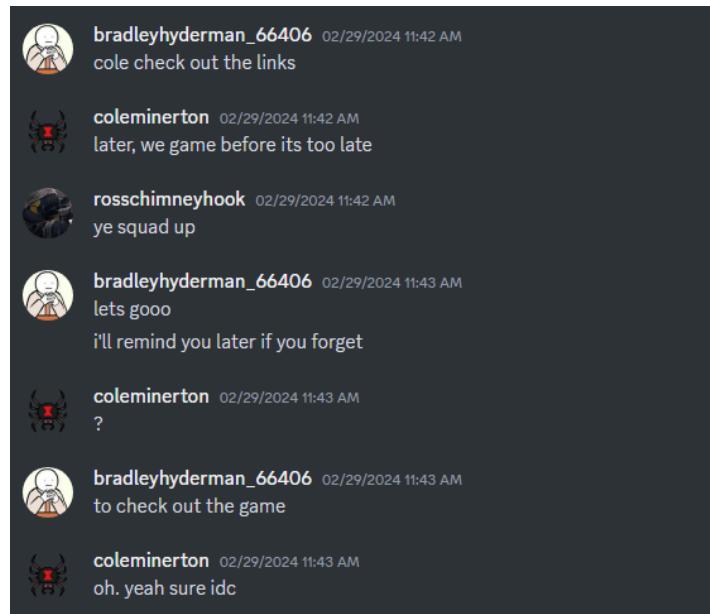
- ▶ Unlock Hint for 0 points
- ▶ Unlock Hint for 0 points

[Flag](#) [Submit](#)

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

SEARCH RESULTS Posts Communities Comments People

Sort by: Relevance All Time

u/coleminerton · 1mo ago

Man it sucks having a new account

1 vote · 0 comments

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.



Cole Minerton
@coleminerton

Mar 2

Filling up the tank before I hit the road 🚨

...

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

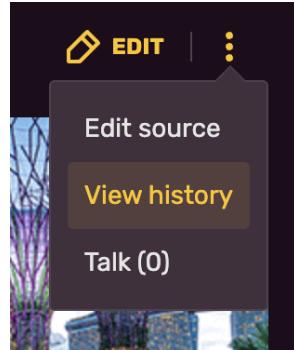
If you wound up on another (unrelated) discord server,
then one of the sites you visited is too new.

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.

The screenshot shows the subreddit page for 'tinyislandsurvival'. At the top, it says 'tinyislandsurvival' with a 'join' button (444 readers) and a '11 users here now' indicator. Below that is a checkmark next to 'Show my flair on this subreddit. It looks like: Im-A-MoneyMagnet'. A description follows: 'a place to discuss the IOS app "tiny island survival" by GAME START LLC'. It includes a 'Wiki' link (https://tiny-island-survival.fandom.com/wiki/Tiny_Island_Survival_Wiki (WIP)) and information about its creation (created by [deleted] 2 years ago). A 'Create your own subreddit' button is visible. Below this, there's a post from 'New Mod' (coleminerton) titled '(self.tinyislandsurvival)' submitted 1 day ago. The post has 1 comment, can be shared, saved, hidden, or crossposted. To the right, there's a 'MODERATORS' section with 'coleminerton' and a 'MESSAGE THE MODS' button. Below that is a 'about moderation team >' link and 'account activity'. At the bottom, there's a 'Everything' link.

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.

The screenshot shows the 'TINY ISLAND SURVIVAL WIKI' page. At the top, it says 'Welcome to the...' and 'TINY ISLAND SURVIVAL WIKI' with '3 articles · 4 files · 169 edits'. Below that is a 'ABOUT THE GAME' section, which describes the game as a mobile game played within a single screen made by Game Start LLC. It explores the island, advances deeper into the forest, and unravels the island's mystery. On the right, there's a 'HELPFUL LINKS' sidebar with links to 'Rules of this wiki', 'Getting Started', 'How to Contribute', 'Managing your new community', 'Guides', and 'All Help articles'. At the bottom left, there's a 'NAVIGATION' sidebar with links to 'Main Island', 'Ramshackle Cottage', 'Cellar', 'Labo', and 'Underground'.



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!

Coleminerton (Message Wall | contribs) · (1,722 bytes) [−45] · (undo) [Tag: Visual edit]

22:48, 30 March 2024 202.163.68.158 (contribs) .. (1,767 bytes) [−11] · (undo) [Tag: Visual edit]

18:29, 30 March 2024 104.28.217.53 (contribs) .. (1,748 bytes) [+10] .. (Undo revision 167 by 104.28.217.53 (talk)) [undo] [Tag: Undo]

18:29, 30 March 2024 104.28.217.53 (contribs) .. (1,738 bytes) [−10] .. (undo) [Tags: Reverted, Source edit]

08:30, 25 February 2024 Coleminerton (Message Wall | contribs) .. (1,748 bytes) [−216] .. (undo) [Tag: Manual revert, Source edit]

08:28, 25 February 2024 Coleminerton (Message Wall | contribs) .. (1,964 bytes) [+216] .. (undo) [Tag: Reverted, Source edit]

03:28, 25 February 2024 Coleminerton (Message Wall | contribs) .. (1,748 bytes) [+16] .. (undo) [Tag: Visual edit]

03:14, 25 February 2024 Coleminerton (Message Wall | contribs) .. (1,732 bytes) [+47] .. (oops somehow wasn't logged in for my last edit?) [undo] [Tag: Visual edit]

03:12, 25 February 2024 181.41.206.31 (contribs) .. (1,685 bytes) [+4] .. (undo) [Tag: Visual edit]

03:07, 25 February 2024 Coleminerton (Message Wall | contribs) .. (1,681 bytes) [−35] .. (undo) [Tag: Visual edit]

03:05, 25 February 2024 Coleminerton (Message Wall | contribs) .. (1,714 bytes) [−1,479] .. (undo) [Tag: Source edit]

Tiny Island Survival Wiki

Coleminerton Bureaucrat Administrator

21 EDITS • 0 POSTS

About Message Wall Blog Contributions Activity

This user has not filled out their profile page yet.

Community content is available under CC-BY-SA unless otherwise noted.

Home

← Back to page

Revision as of 03:12, 25 February 2024 (view source)

181.41.206.31 (contribs)
(Tag: Visual edit)

← Older edit

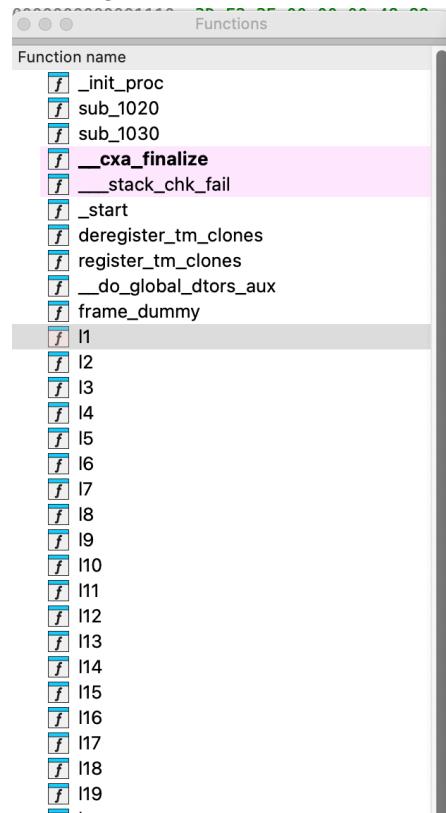
Line 16:

```
<span style="font-size:24px;color:#973a59">"NAVIGATION"</span><br>
*[[Main Island]]
```

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!

```
mov    rax, [rsp+var_0]
mov    byte ptr [rax], 66h ; 'f'
mov    byte ptr [rsp+var_0]
mov    byte ptr [rax], 6Ch ; 'l'
mov    byte ptr [rsp+var_0]
mov    byte ptr [rax], 61h ; 'a'
mov    byte ptr [rsp+var_0]
mov    byte ptr [rax], 67h ; 'g'
```

Challenge 244 Solves X

Beginner: Basic Reversing Problem

100

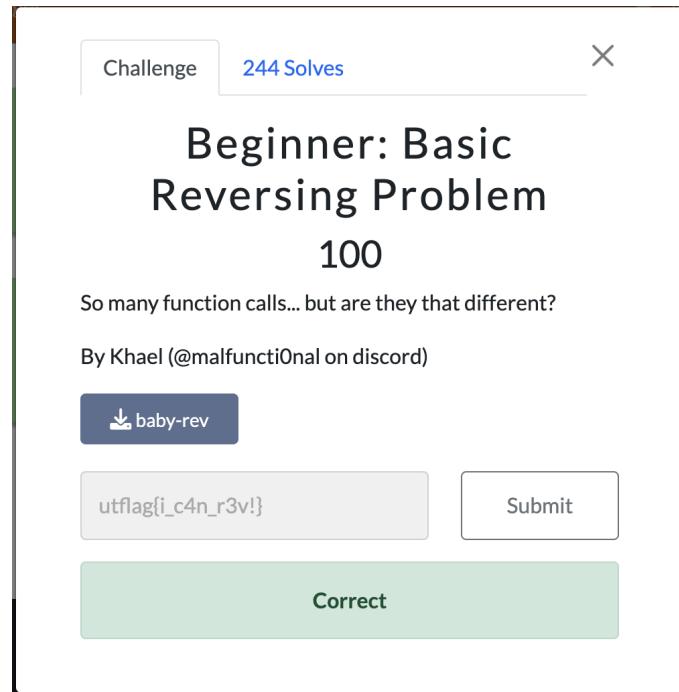
So many function calls... but are they that different?

By Khael (@malfuncti0nal on discord)

 baby-rev

utflag{i_c4n_r3v!} Submit

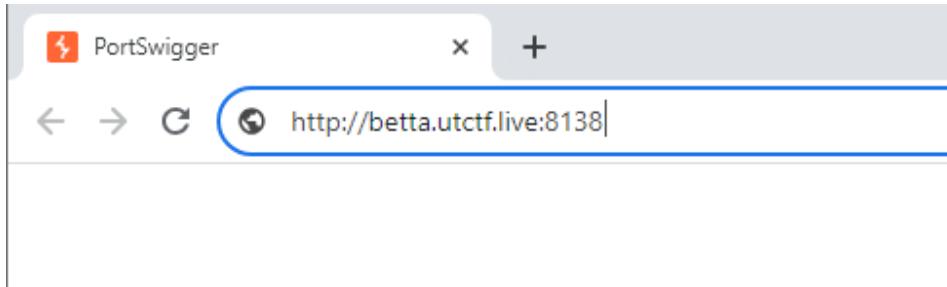
Correct

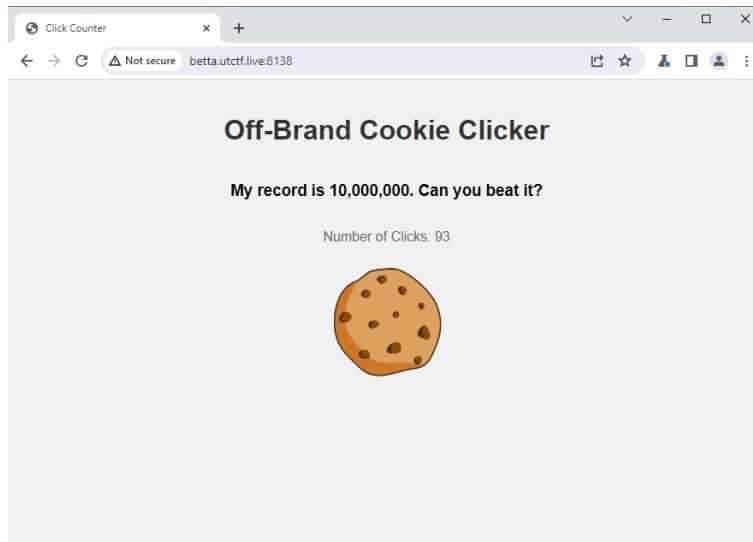


D. Web

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.





Burp Suite interface showing the Proxy tab. A context menu is open over a selected request to "http://betta.utctf.live:8138 [3.89.251.123]". The menu path "Do intercept > Response to this request" is highlighted.

- 1
- 2
- 3
- 4 Send to Intruder
- 5 Send to Repeater
- 6 Send to Sequencer
- 7 Send to Comparer
- 8 Send to Decoder
- 9 Send to Organizer
- 10 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
- Convert selection
- URL-encode as you type
- Cut
- Copy
- Paste
- Message editor documentation
- Proxy interception documentation

Pretty Raw Hex

```
POST /click HTTP/1.1
Host: betta.utctf.live:8138
Content-Length: 8
User-Agent: Mozilla/5.0 (Windows I
Content-Type: application/x-www-f
Accept: /*
Origin: http://betta.utctf.live:8138
Referer: http://betta.utctf.live:8138
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
count=97
```

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

```
count=100000000
```

Then the flag appeared on the browser

betta.utctf.live:8138 says

Wow, you beat me. Congrats! utflag{y0u_c1ck_pr3tty_f4st}

OK

Challenge

422 Solves

X

Beginner: Off-Brand Cookie Clicker

100

I tried to make my own version of cookie clicker, without all of the extra fluff. Can you beat my highscore?

By Khael (@malfunction10nal on discord)

<http://betta.utctf.live:8138>

Flag

Submit

You already solved this

E. Misc

1. Survey

This is what appeared after answering the google forms

UTCTF 2024 Feedback Form

thank yoU for filling ouT our Feedback form! pLeAse rate the ctf on ctftime when you Get a chance. rememBer that we will accept Your writEups for forTy-eigHt hours After the competitioN for writeup prizes. hooK em hornS!

Ginawa ang form na ito sa UTmail. I-ulat ang [Pag-abuso](#)

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}

Challenge

68 Solves



Survey

100

<https://forms.gle/VaB186QBnViSNdCt8>

By Jeriah (@jyu on discord) (blame him for the answer choices)

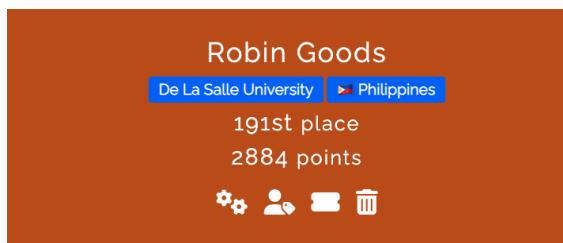
Flag

Submit

Correct

III. Results and Statistics

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



Challenges

Cryptography

| | | | |
|-------------------|--------------------------------|-------------------------|------------------------|
| RSA-256 100 | Beginner: Anti-dcode.fr 100 | numbers go brrr 481 | bits and pieces 516 |
| Cryptordle 772 | numbers go brrr 2 837 | simple signature 908 | Forgery 1000 |

Forensics

| | | | |
|--------------------|----------------|------------------|------------------------------------|
| Contracts 100 | OSINT 1 592 | OSINT 2 796 | A Very Professional Website 802 |
| Study Music 844 | OSINT 3 896 | Gibberish 990 | Insanity Check: Reimagined 994 |

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 |

