***CRAC CTF MSIT 2023-REPORT***

~ Prepared by – Saahieb Singh and Harman Kaur

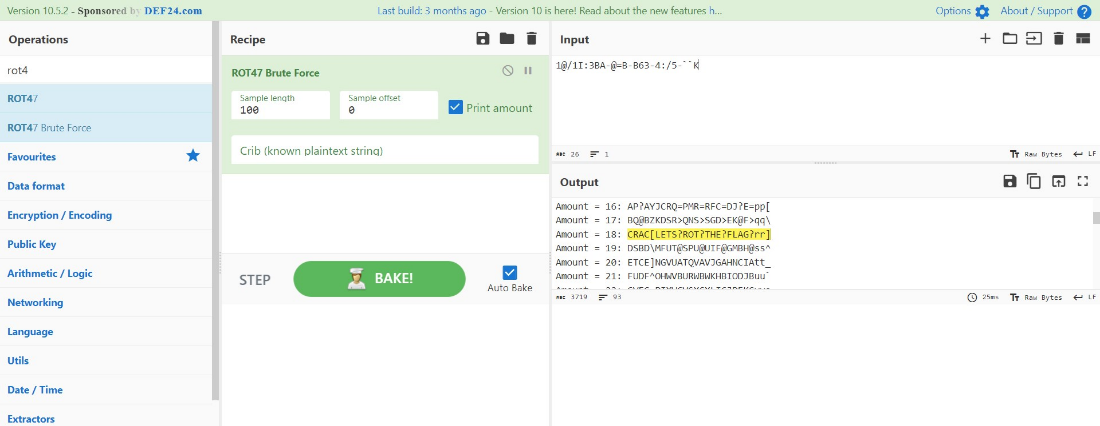
* CRYPTOGRAPHY

A screenshot of a computer

Description automatically generated

*Solution –*

1. Open <https://gchq.github.io/CyberChef/>
2. Use ROT 47 brute Force.
3. Enter the string provided.



1. As seen in the image above at amount 18 we got our flag.

**FLAG – CRAC[LETS?ROT?THE?FLAG?rr]**

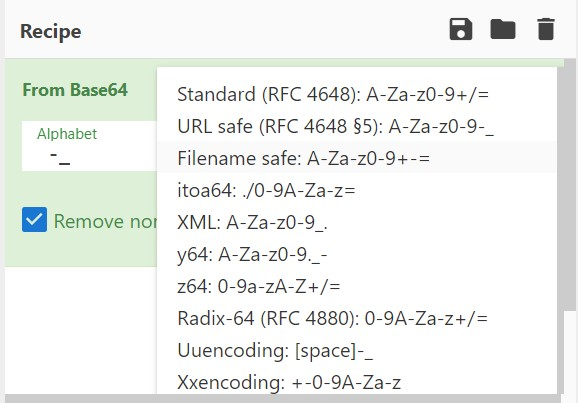
A close up of a text

Description automatically generated

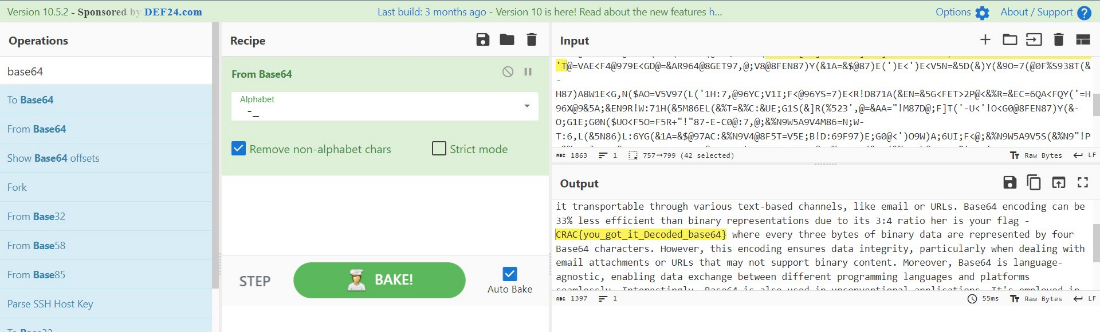
FILE – https://github.com/IMHarman/CRAC-CTF-MSIT-2023/blob/main/challenge\_text

*Solution –*

1. Open <https://gchq.github.io/CyberChef/>
2. Use base64.
3. Enter the string provided.
4. Use different variations for the solution in the text.

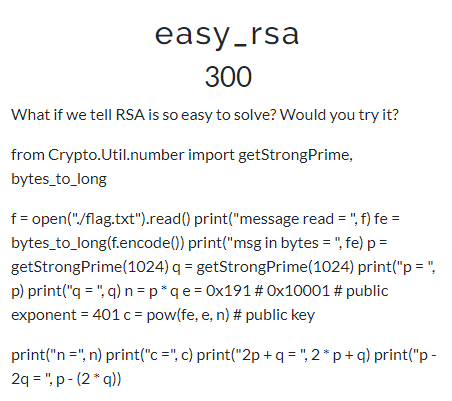


1. Use - Uuencoding: [space]-.



1. As seen in the image above we got our flag in the paragraph of the output.

**FLAG - CRAC{you\_got\_it\_Decoded\_base64}**



FILE - <https://github.com/IMHarman/CRAC-CTF-MSIT-2023/blob/main/out_crypto.txt>

*Solution –*

1. Q

**FLAG –**

* REVERSE ENGINEERING

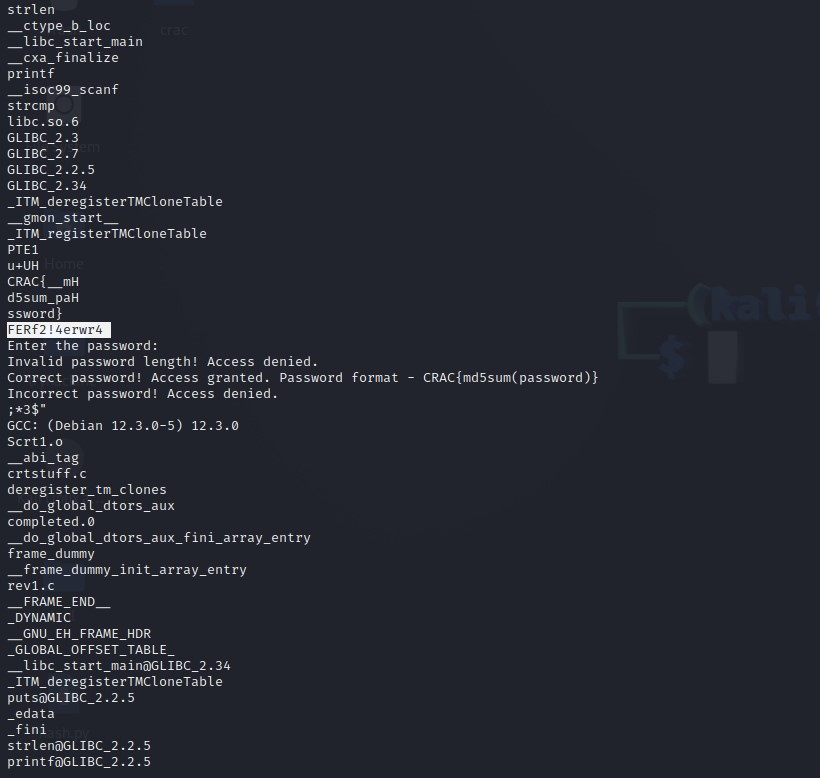
A close up of a computer code

Description automatically generated

FILE - <https://github.com/IMHarman/CRAC-CTF-MSIT-2023/blob/main/rev1>

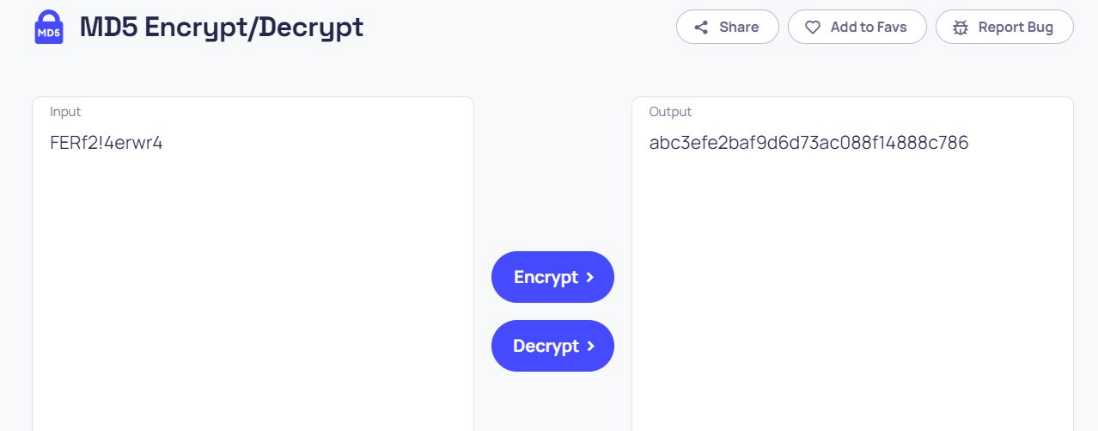
*Solution –*

1. Switch to Linux for better performance. Make this file executable by the command – *chmod u+x rev1*
2. Using *./rev1* the software asks for the password.
3. So to find it lets find for the strings present in the rev1 file. For this use the command – *strings rev1.*

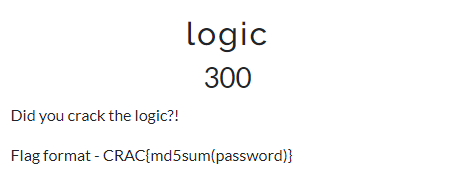


Here we found the password of the rev1 executable file.

1. Now convert the string to md5sum to get the flag for the CTF.



**FLAG - CRAC{abc3efe2baf9d6d73ac088f14888c786}**



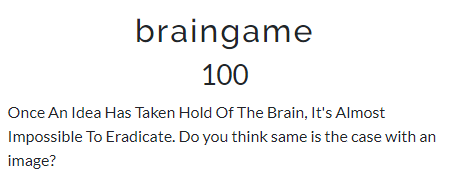
FILE - <https://github.com/IMHarman/CRAC-CTF-MSIT-2023/blob/main/rev2>

*Solution –*

1. Q

**FLAG –**

* Stegnography



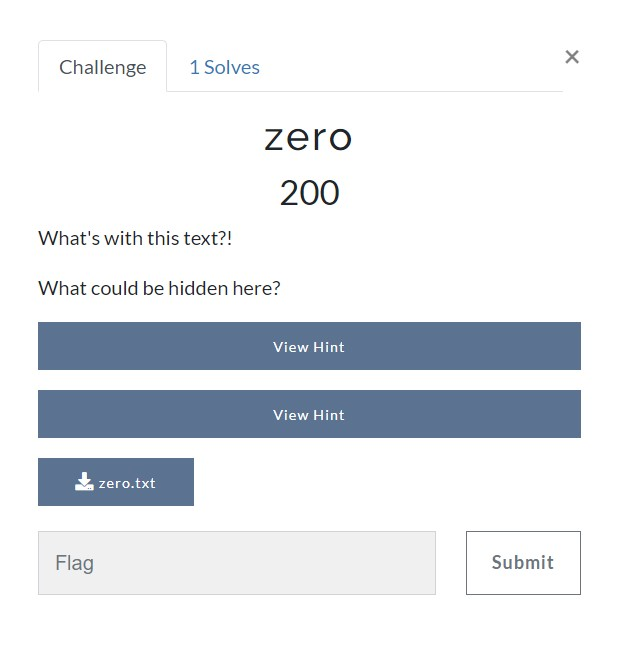
FILE - <https://github.com/IMHarman/CRAC-CTF-MSIT-2023/blob/main/inception.jpeg>

*Solution –*

1. Open <https://exif.tools/>
2. Upload the image and analyse the metadata of the image.
3. You’ll find the flag in it.



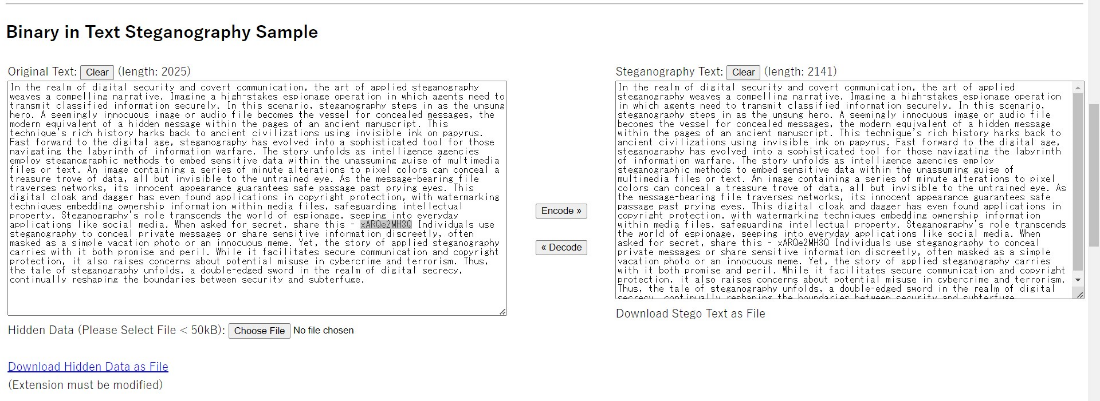
**FLAG – CRAC{Downward\_Is\_The\_Only\_Way\_Forward}**



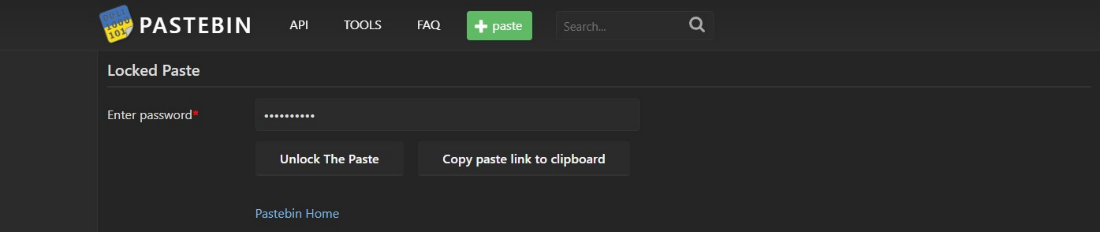
FILE – <https://github.com/IMHarman/CRAC-CTF-MSIT-2023/blob/main/zero.txt>

*Solution –*

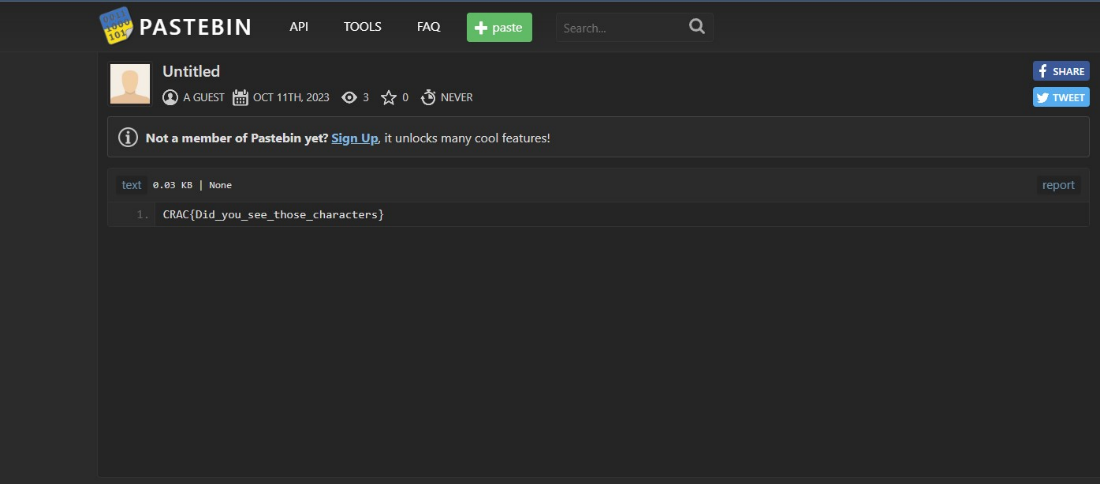
1. Open <https://330k.github.io/misc_tools/unicode_steganography.html>
2. Now paste the content from the zero.txt file in Binary in Text Steganography Sample.



1. Click on the Download hidden Data as file link and download the file
2. Open this downloaded file and here you get the pastebin website link
3. Visit the website and it will ask for the password.



1. For the password come back to the text file and find the secret code from it. Use the same code to unlock the site. And finally, you got the flag.



**FLAG – CRAC{Did\_you\_see\_those\_characters}**

* Cloud Security



*Solution –*

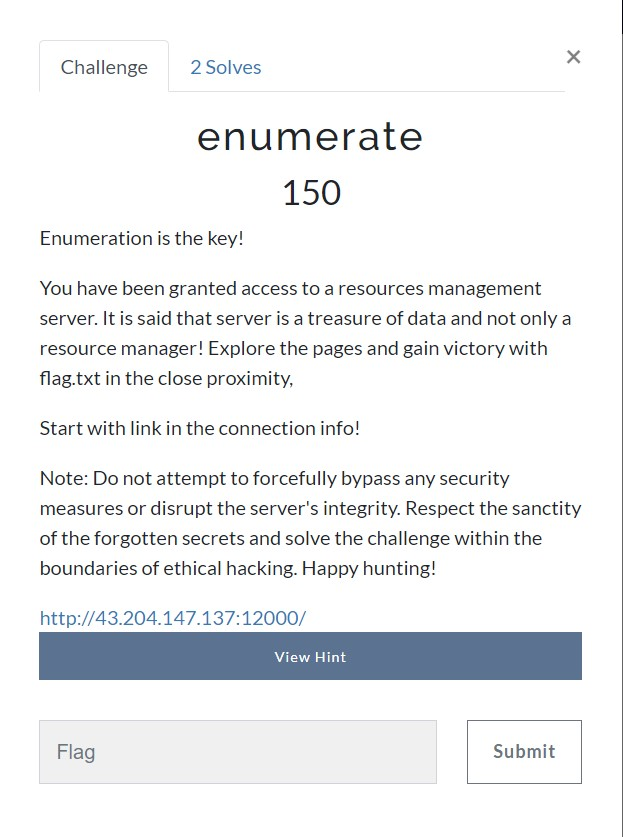
1. On web surfing and using keywords, try to gather the information that how the S3 bucket links are.
2. Analysing and creating CTF link comes to be –

<http://myfirst-webpage.s3-website.ap-south-1.amazonaws.com/>



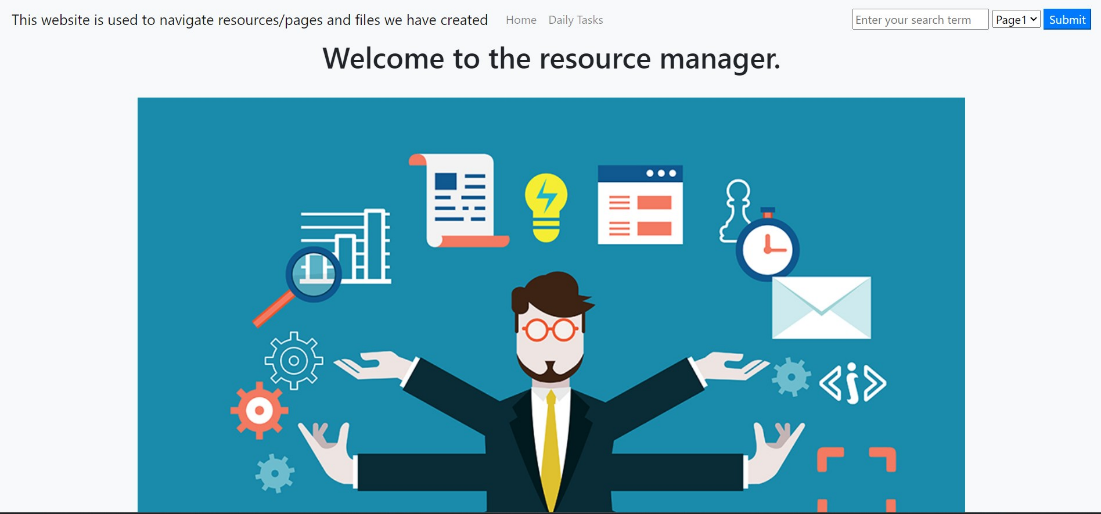
**FLAG – CRAC{You\_rock\_in\_cloud!}**

* Web application Security



*Solution –*

1. Visit the website – <http://43.204.147.137:12000/>



1. Find the vulnerable parameter, here it is “task”.
2. Click on “Daily Task” tab. And on the top right input box write the payload mentioned below: “*../flag.txt”*
3. In the page end you will find the CTF Flag.



**FLAG – CRAC{So\_Y0u\_List3d\_Th3\_Secret!}**