

PICOCTF 2023

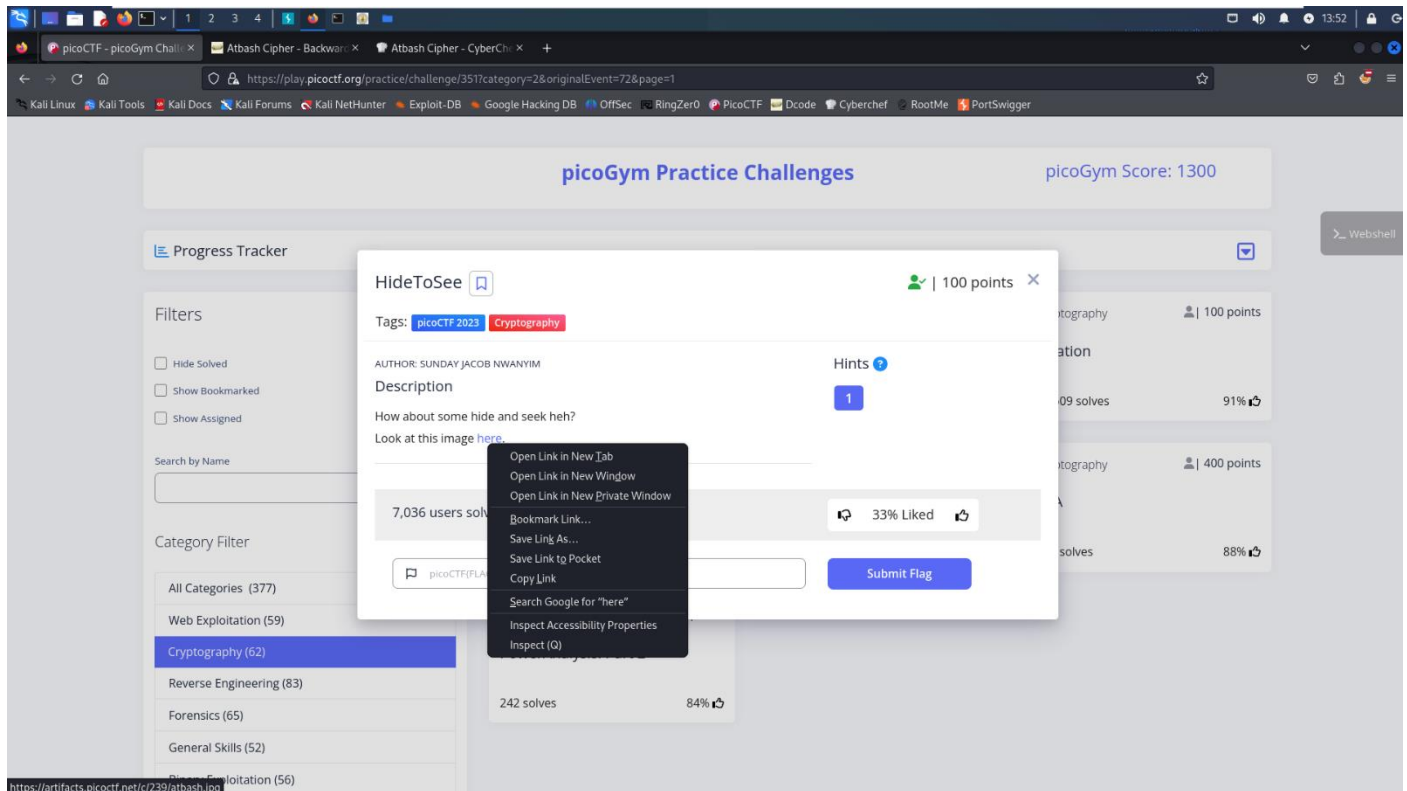
CATEGORY : Cryptography

Challenge : HideToSee

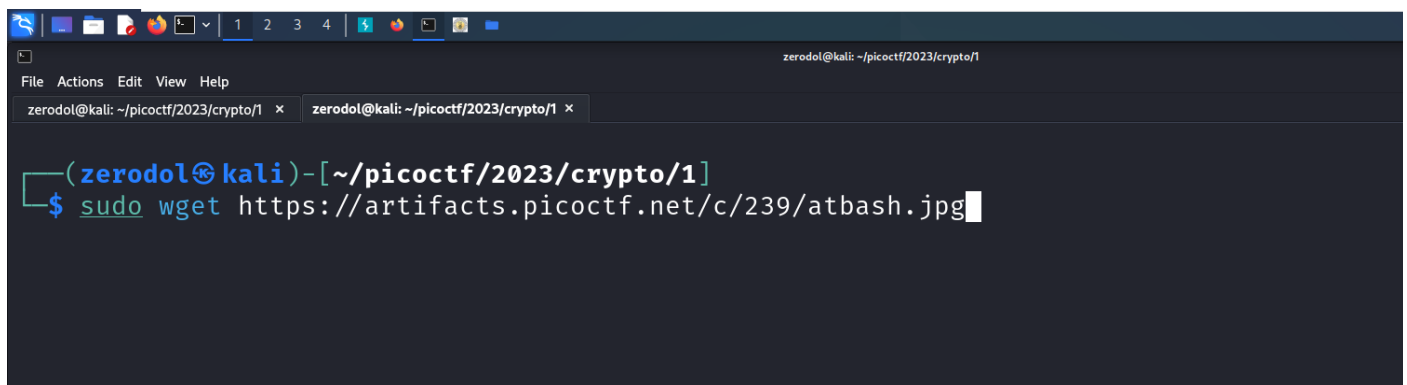
Points : 100

WRITEUP

First I copy the link of the file by doing a right click on “here” and I click on “copy link”



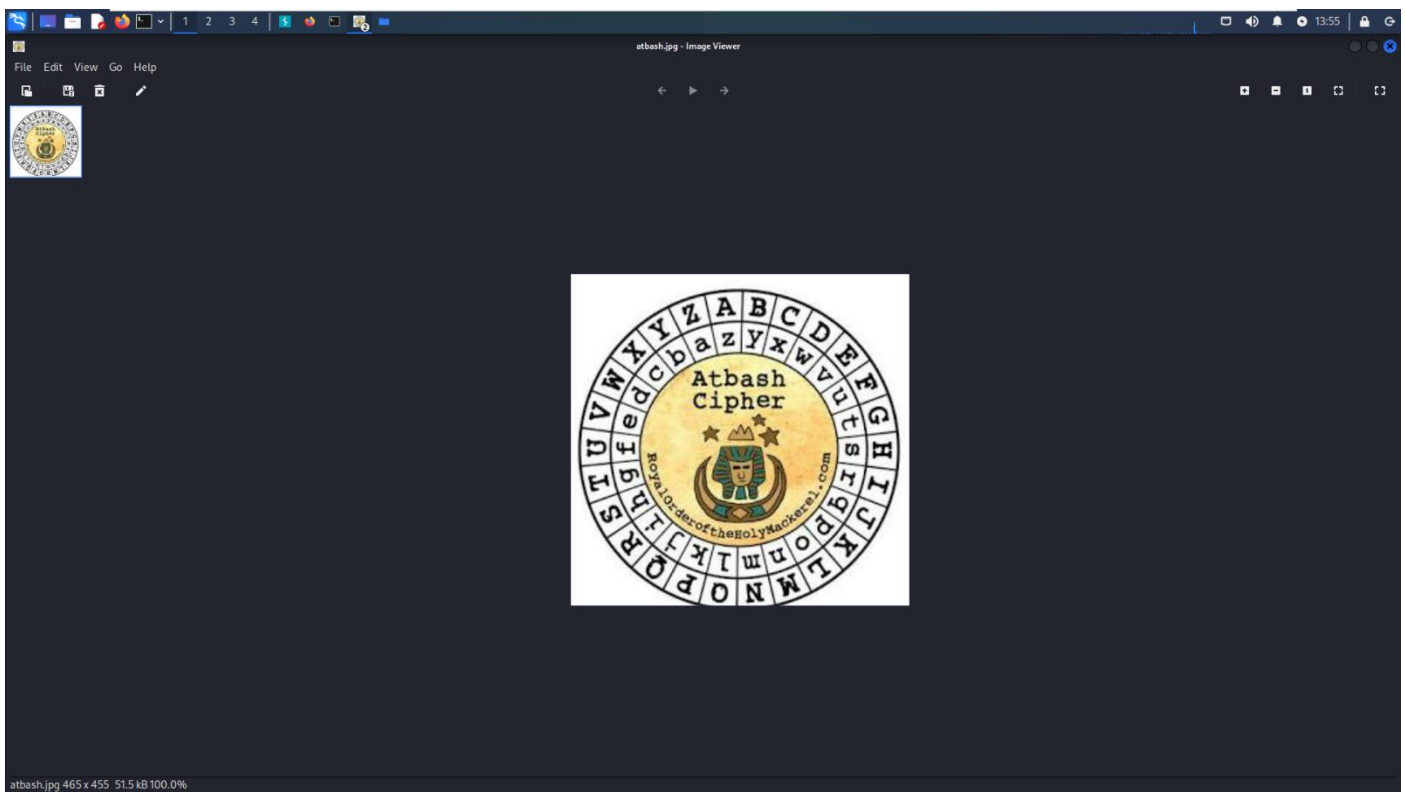
I download the file with the “**wget https://artifacts.picoctf.net/c/239/atbash.jpg**” command



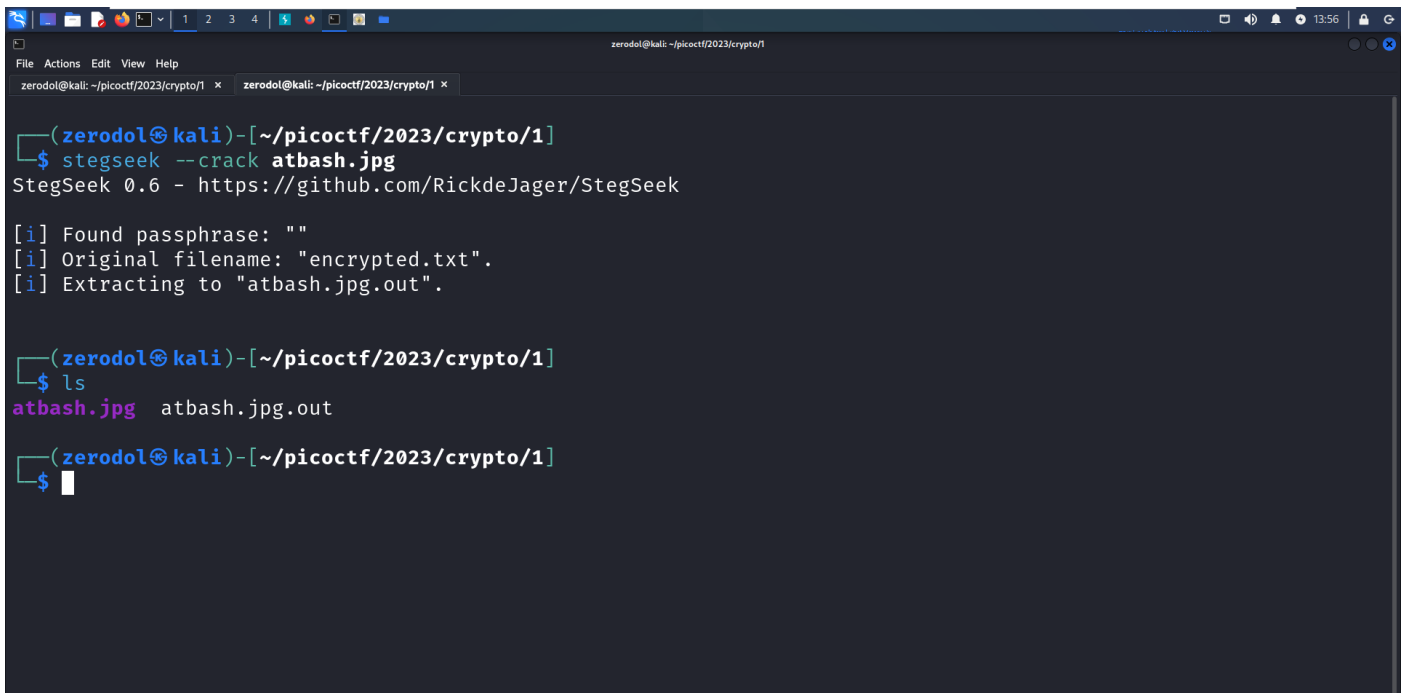
A file name « [atbash.jpg](#) » is downloaded with suggested that the file is a jpg image

```
zerodol@kali: ~/picocft/2023/crypto/1
File Actions Edit View Help
zerodol@kali: ~/picocft/2023/crypto/1 x zerodol@kali: ~/picocft/2023/crypto/1 x
(zerodol@kali)-[~/picocft/2023/crypto/1]
$ ls
atbash.jpg
```

We open it and we see that it's an image representing the “[Atbash Cipher](#)”. Keep that in mind fore now, it can be pretty useful



We can try to extract something from this image with the “**stegseek --crack atbash.jpg**” command. And we see that something has been extracted and put in “**atbash.jpg.out**”



```
(zerodol@kali)-[~/picoctf/2023/crypto/1]
$ stegseek --crack atbash.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: ""
[i] Original filename: "encrypted.txt".
[i] Extracting to "atbash.jpg.out".

(zerodol@kali)-[~/picoctf/2023/crypto/1]
$ ls
atbash.jpg  atbash.jpg.out

(zerodol@kali)-[~/picoctf/2023/crypto/1]
$
```

We can see what's inside that file with “cat atbash.jpg.out”. We have something that seems encrypted. Now if you remember the Atbash Cipher you can see where this takes us

```
zerodol@kali: ~/picocf/2023/crypto/1
$ cat atbash.jpg.out
krlXGU{zgyzhs_xizxp_1u84w779}

zerodol@kali: ~/picocf/2023/crypto/1
$
```

We can go to “cyberchef” and choose the atbash cipher and paste our encrypted sentence and Whaou, we have our flag : picoCTF{atbash_crack_1f84d779}

