LinkedIn: Kelvin Kimotho

AUTHOR: JUNIAS BONOU

Description

I found a web app that can help process images: PNG images only!

Additional details will be available after launching your challenge instance.

This challenge laur
instance on demar
Its current status is
NOT_RUNNING

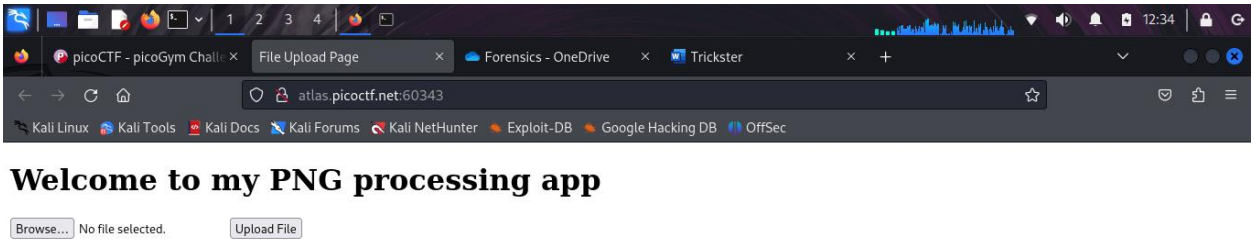
Launc
Instanc

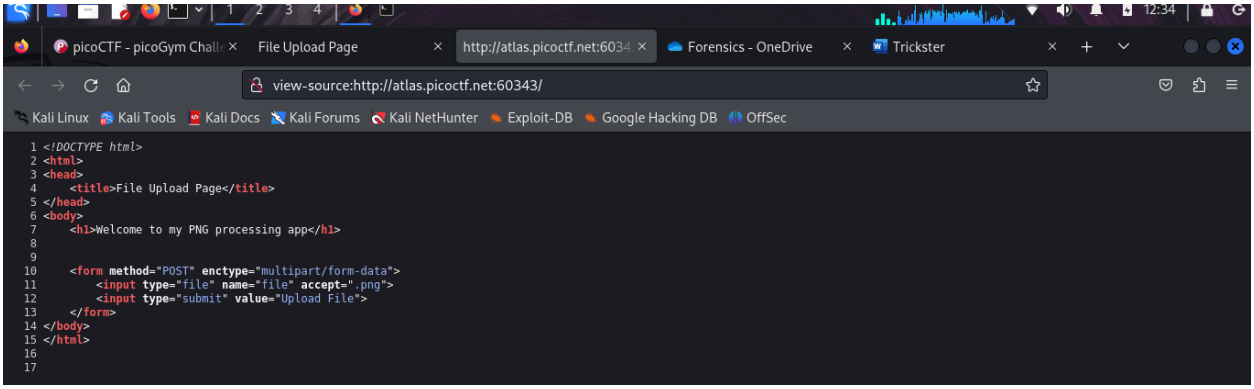
Hints

(None)

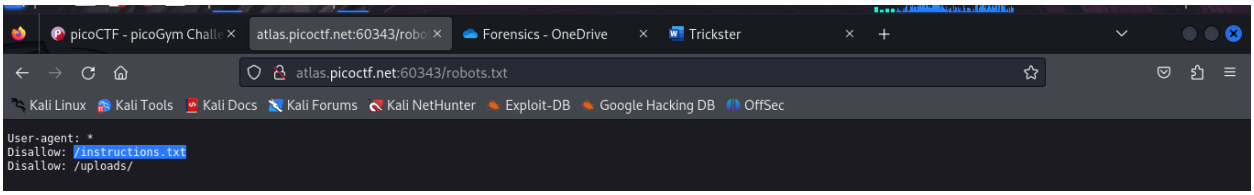
Solution

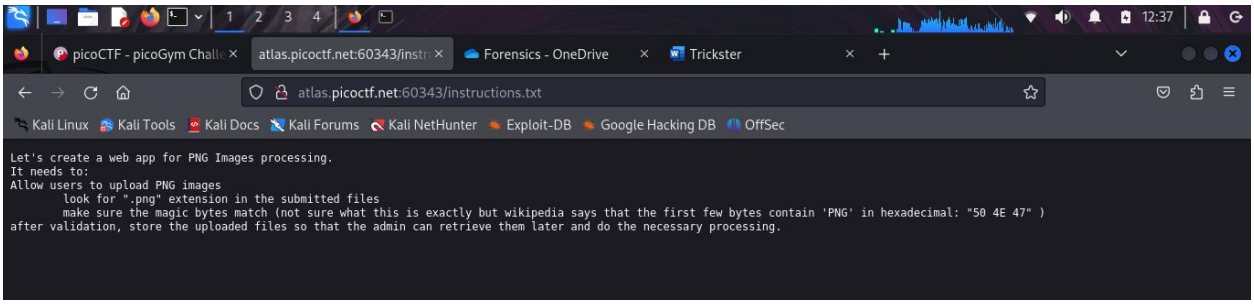
With no given hints, I started by examining the source code for the website pages but i found nothing interesting.



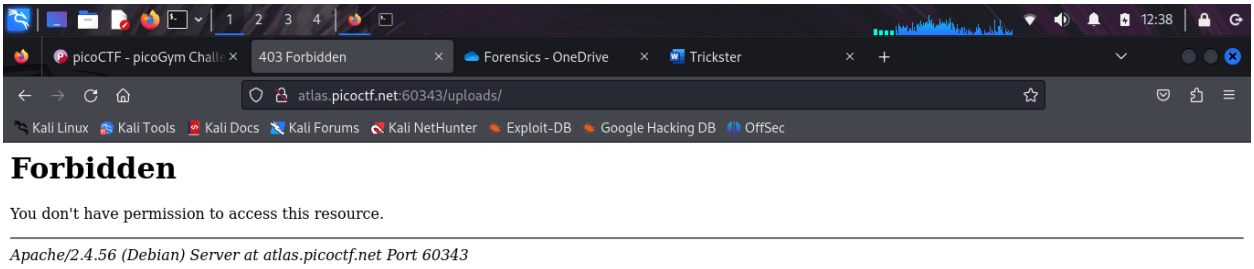


I went looking for any available information from the robots.txt file out of curiosity and I realized we had an **instructions.txt** whose contents were.

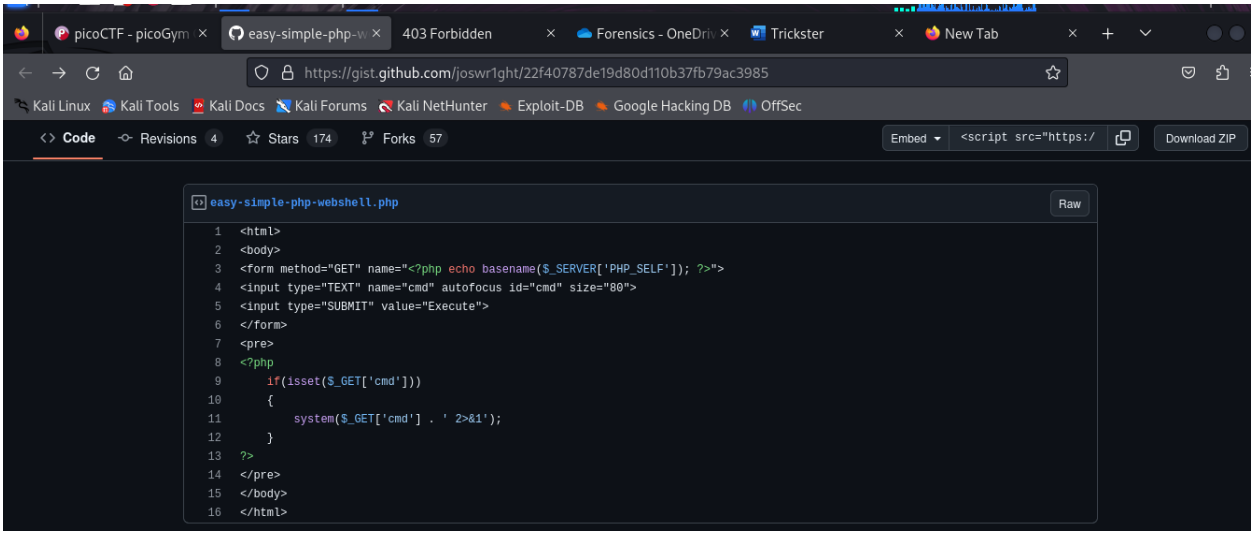




The uploads directory within the web server was not directly accessible.

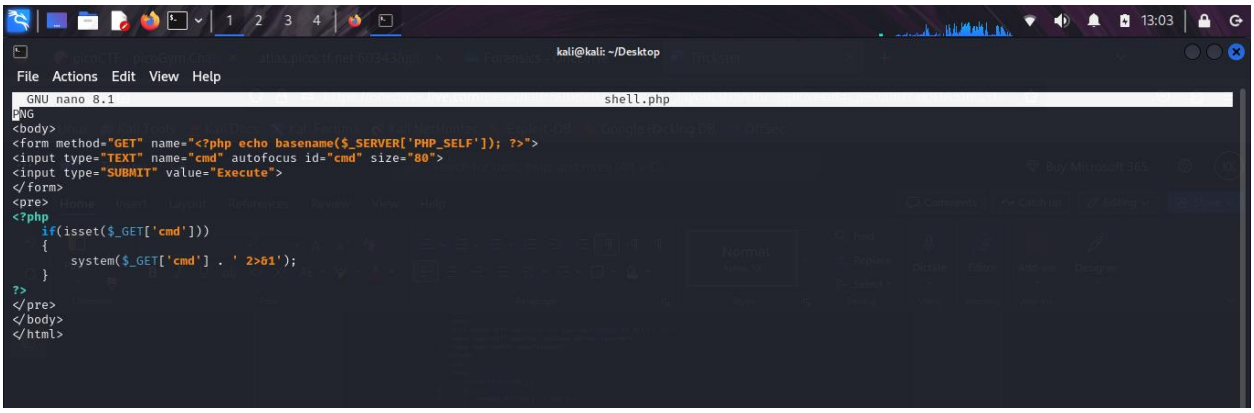


Since the application allowed uploads, I went ahead and downloaded a web shell from GitHub which I uploaded as an Image in the required Png format.

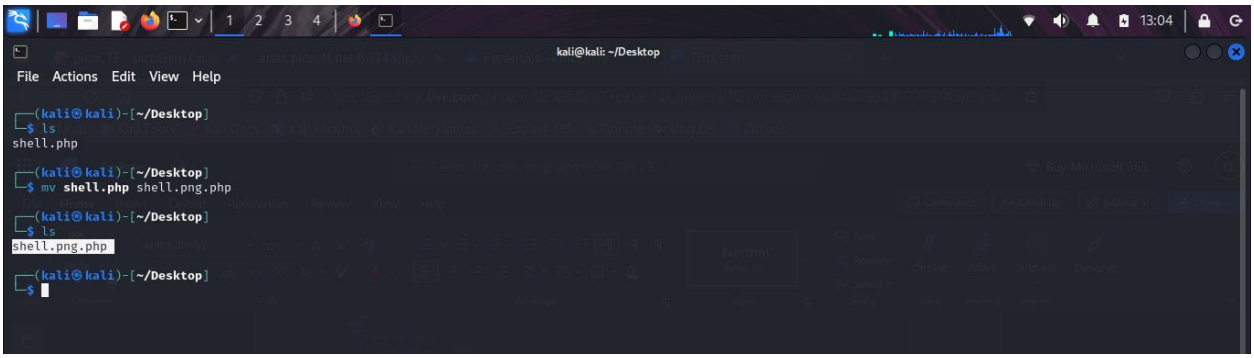


I had to append PNG at the beginning of the script to make sure the magic bytes match (not sure

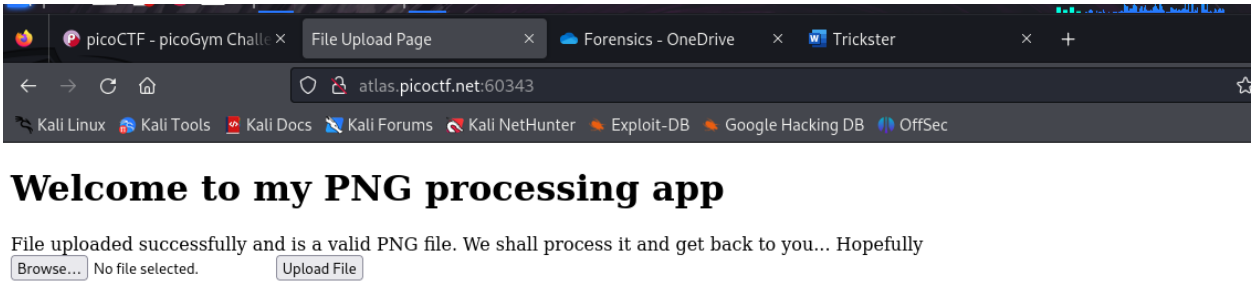
what this is exactly but wikipedia says that the first few bytes contain 'PNG' in hexadecimal: "50 4E 47")



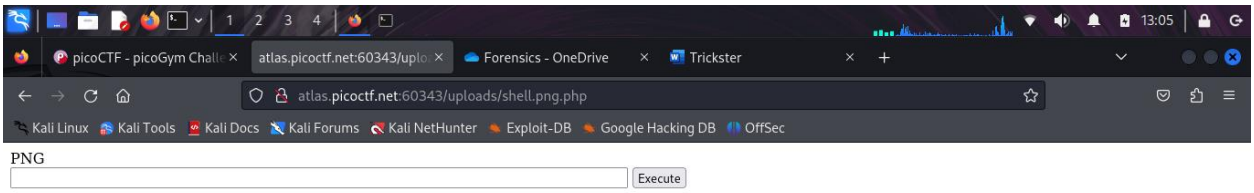
I then renamed the php shell code with a. Png extension. This shell would allow me execute commands directly to the server like I would do on terminal.



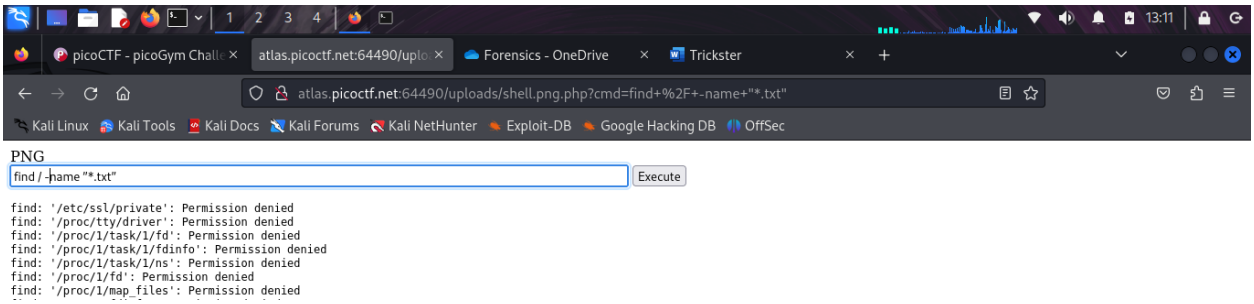
I uploaded the shell code.



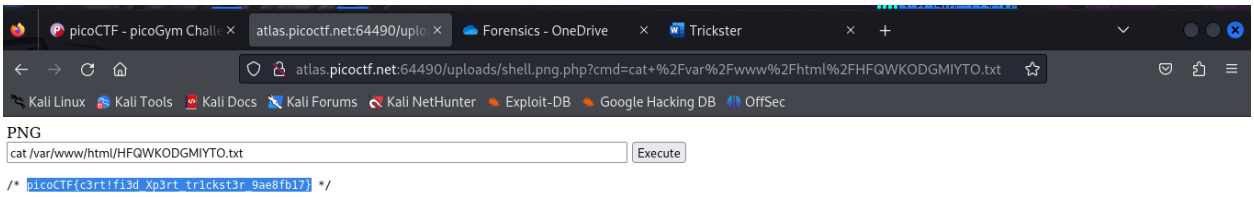
Then i tried accessing the shellcode as an image on the browser" /uploads/shell.png.php"



I then ran the following command find / -name ”*.txt” to enable me find all the text file starting from the root directory. I discovered so many files, most with access restrictions.



Among the files with no access restrictions, there was one file with a unique file name HFQWKODGMIYTO.txt. I went ahead and used the cat command to view its contents and that's how I retrieved the flag.



Flag: picoCTF{c3rt!fi3d_Xp3rt_tr1ckst3r_9ae8fb17}