

Forbidden Paths

Description

Can you get the flag?

Here's the [website](#).

We know that the website files live in `/usr/share/nginx/html/` and the flag is at `/flag.txt` but the website is filtering absolute file paths. Can you get past the filter to read the flag?

I open the website.



It has a simple gui where u input a filename and it cats' it.

Now I don't see any flag.txt here.

If I do enter the path of flag.txt :

Not Authorized

This led me to think that perhaps we don't have permission because we are currently in a child directory and flag.txt is in one of the higher levels.

So I put in ..

To take me a level higher in the directory, but that removes the gui, leaving you helpless.

I then tried ../flag.txt

But

File does not exist

So maybe it was even higher up.

I ended up searching how to go up multiple levels in a path

And ended up in a stack overflow exchange where I saw this :

Here is all you need to know about relative file paths:

- **Starting with** / returns to the root directory and starts there
- **Starting with** ../ moves one directory backward and starts there
- **Starting with** ../../ moves two directories backward and starts there (and so on...)
- **To move forward**, just start with the first sub directory and keep moving forward.

I kept going backwards in the hierarchy using ../flag.txt, ../../flag.txt, ../../../../flag.txt

And sure enough, on hitting ../../../../flag.txt :

picoCTF{7h3_p47h_70_5ucc355_e5fe3d4d}