Trickster

Problem:

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

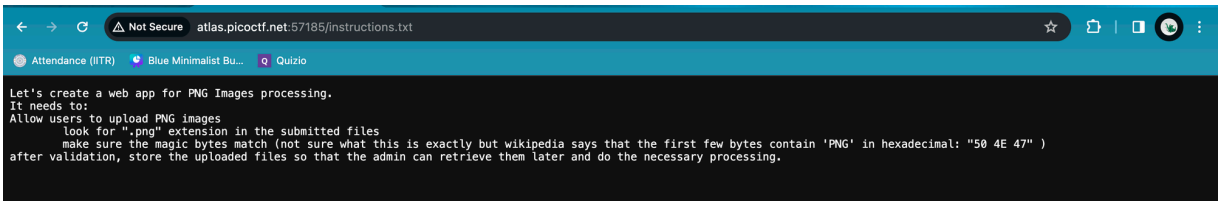
Basic Idea of the Problem:

So, a very interesting but kind of obvious problem. You got a website where you are asked to upload png files. It doesn't accept any but the PNG files. And after it uploads the png. It does nothing. Well basically, it was pretty obvious that it was a file upload vulnerability challenge.

Solution:

So, first thing first, we needed to know what kind of check were done on the file we upload, so that it believes that well its a PNG file. So I did what every desperate Web Exploit challenge solver do, and hoped there was a robots.txt, and i was lucky because there was.

so i tried to see the instructions.txt



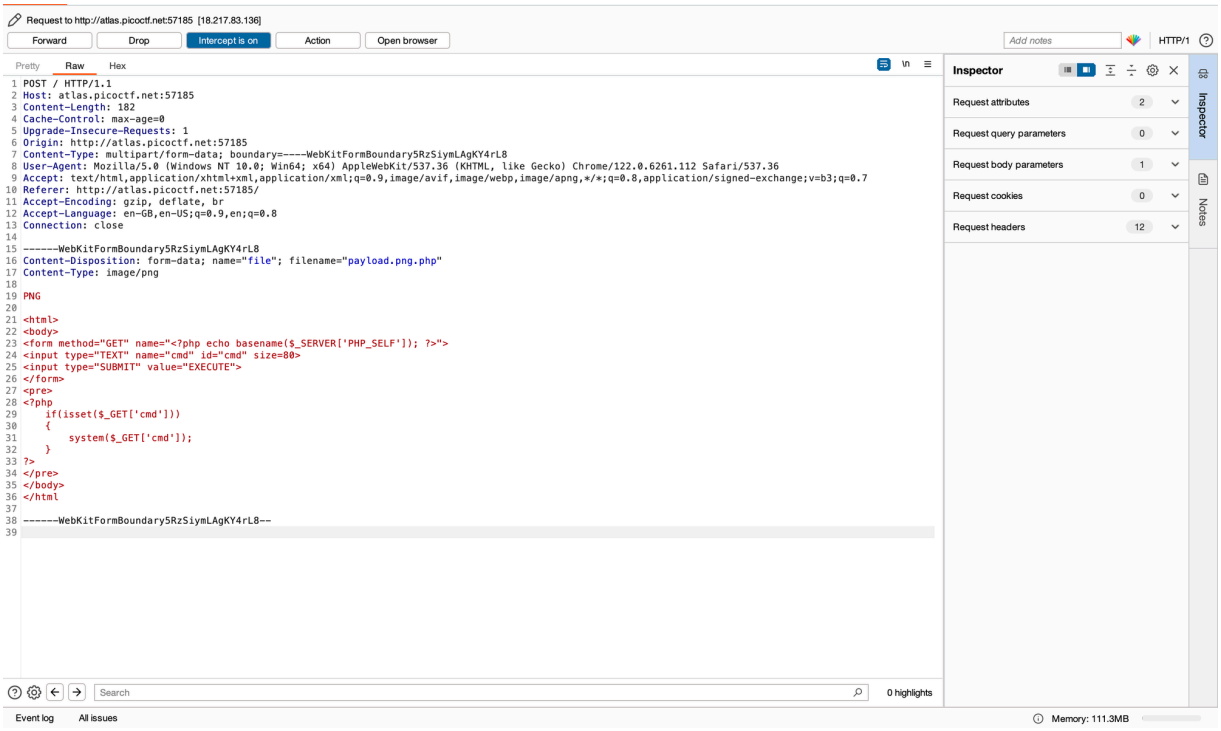
Okay so we got the conditions we were looking for:

1. Our file should have the extension .png
2. It should have PNG file's magic bytes.

Also when i tried to access the uploads folder, we didn't have the permission. Fishhyy....maybe we need to access that.

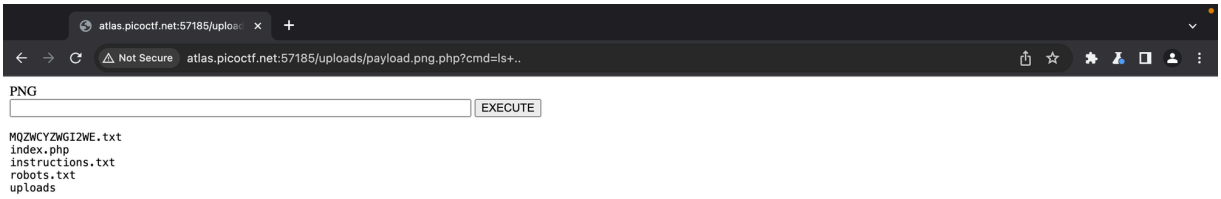
Okay so now i first created an empty file called empty.png and then opened the proxy with Burp Suite and intercepted the request of uploading my empty.png on it.

In the request, i updated the name of the file to 'payload.png.php' and then wrote some HTML and PHP in it.

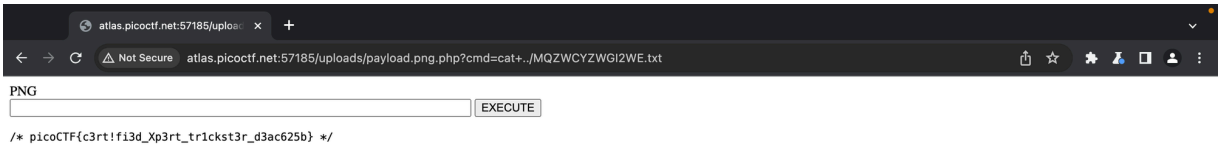


Something like this. Basically what this will do will create a form for me, and will execute shell commands on the server.

Now lets access our payload by typing it in the URL and lets add some command in the URL as well for it to execute.



And lessgooo, we can see the files. Lets read the weird named txt. file.



BINGOOO!!!! I guess we found the flag.

Flag:

```
picoCTF{c3rt!fi3d_Xp3rt_tr1ckst3r_d3ac625b}
```