noamgariani11 Add files via upload 3677a9a · 3 months ago

23 lines (13 loc) · 1.67 KB

Preview Code Blame Raw

Description

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

Solution

This Hack the Box Academy module explains the upload exploit well. It shows that by using this php script you can get a web shell.

The file upload tries to make sure that the file is a PNG by looking at the magic bytes and file extension. First, the script could be converted to Hex with CyberChef and then added the PNG Magic Bytes found here:

```
89 50 4E 47 0D 0A 1A 0A
```

By appending that to the start of the file, then converting back from hex with CyberChef and downloading the file will get the script. The name looks for png but it doesn't have to be at the end of the file name just somewhere in the file name. This allows it to be a php file named `filename.png.php` .

Once successfully uploaded to the site the file could be reached by going to the file destination within the website.

```
http://atlas.picoctf.net:60322/uploads/filename.png.php
```

This gives the shell. Commands like `ls` , `pwd` , `ls ../` , could all be ran now in this web shell. Originally it puts you in the `/var/www/html/uploads` and with `ls ../` it shows the contents of `/var/www/html/` . There is a file called `MFRDAZLDMUYDG.txt` that looks interesting and when using this command to check the file contents, `cat ../MFRDAZLDMUYDG.txt` , it gives the flag.

Flag: `picoCTF{c3rt!fi3d_Xp3rt_tr1ckst3r_ab0e...}`