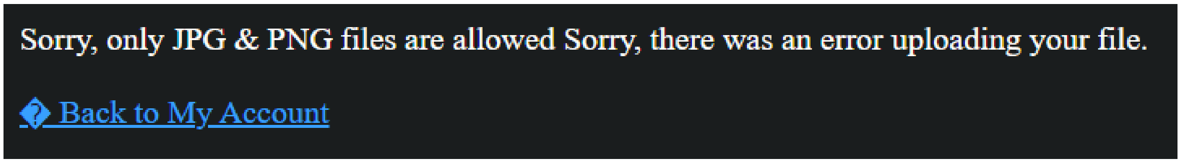
Web shell upload via obfuscated file extension

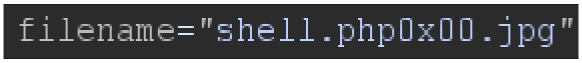
1. This lab contains a vulnerable image upload function. Certain file extensions are blacklisted, but this defense can be bypassed using a classic obfuscation technique.

2. First, I uploaded the shell file. But it didn't upload.



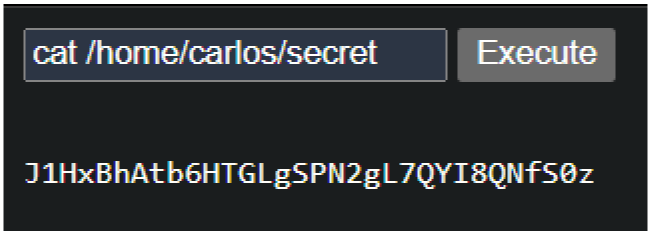
Sorry, only JPG & PNG files are allowed Sorry, there was an error uploading your file.

3. I think that the backend checks the filename extension. So, the first thing that came to mind was null byte. I modify the filename to :



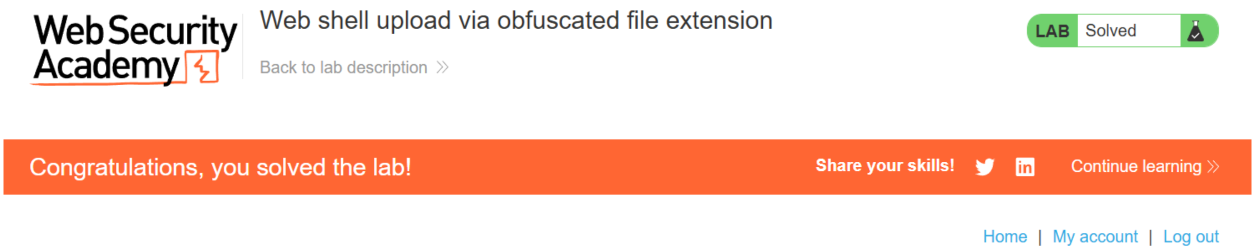
```
filename="shell.php0x00.jpg"
```

The website accept it and upload the file and I solved the lab.



```
cat /home/carlos/secret
```

```
J1HxBhAtb6HTGLgSPN2gL7QYI8QNfS0z
```



Web shell upload via obfuscated file extension

Congratulations, you solved the lab!