
Web shell upload via extension blacklist bypass

1. This lab contains a vulnerable image upload function. Certain file extensions are blacklisted, but this defense can be bypassed due to a fundamental flaw in the configuration of this blacklist.
2. I tried to upload basic PHP shell via upload avatar, but the uploading failed.

Sorry, php files are not allowed Sorry, there was an error uploading your file.

[!\[\]\(666e09182d4cd268646ea700ea60dcdf_img.jpg\) Back to My Account](#)

3. I know that there are many alternatives to **.php** extension to bypass the extension restrictions. I search on [PayloadAllTheThings](#) and I got some alternatives. A lot of them success in bypassing the restriction on the extension while uploading and the shell file uploaded successfully but there is another problem. When I access the shell file, the content of the file displayed as plain text. I tried to chain it with path traversal vulnerability, but it was useless.
4. I think to brute force all extensions that I get from github. And it was useful. This extension “**.phar**” make the shell file uploaded and run successfully and I got **RCE** on the website.

cqYzBaCDWwXbYwxD69JYkS17qNECSNk



Web shell upload via extension blacklist bypass

[Back to lab description >>](#)

LAB Solved 

Congratulations, you solved the lab!

Share your skills!   Continue learning >>

[Home](#) | [My account](#) | [Log out](#)