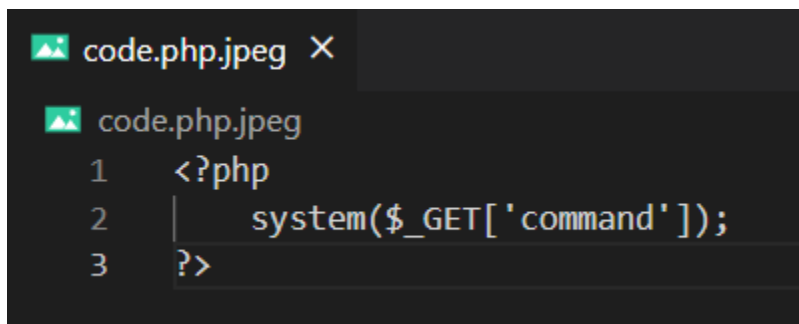



Giao diện trang web cho phép upload file kiểu ảnh như hình trên.



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.

← → ↻ ⚠ 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 hiểu 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](#)

---

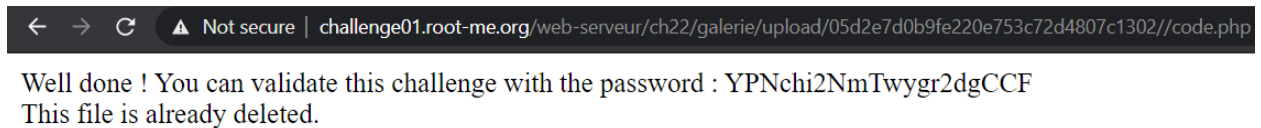
### Upload your photo

code.php%00.jpeg

*NB : only GIF, JPEG or PNG are accepted*



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



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