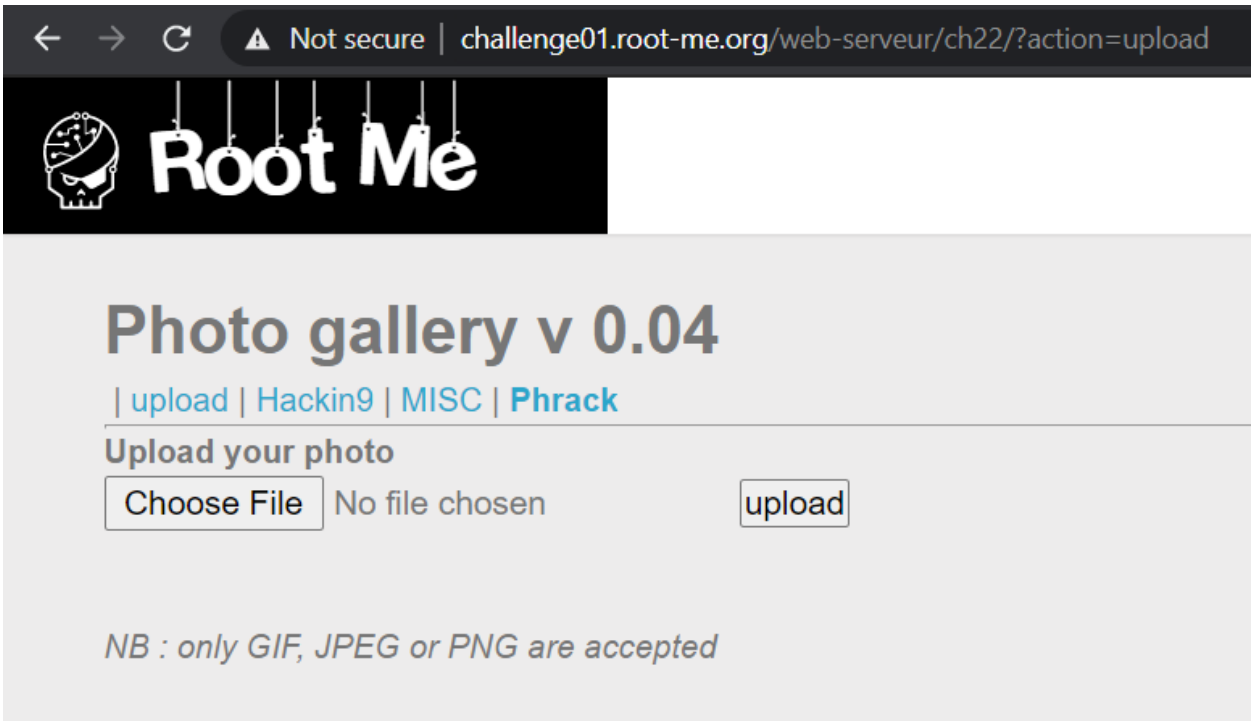
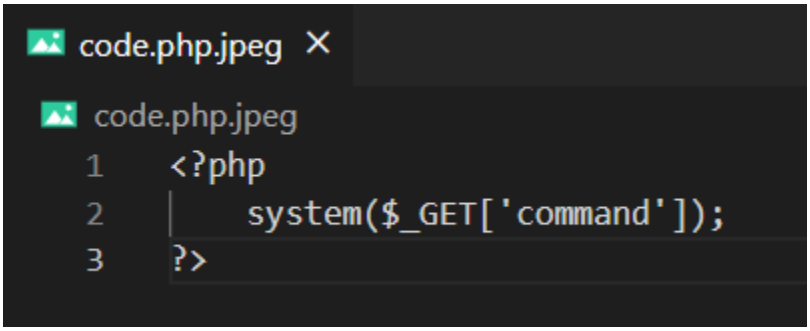
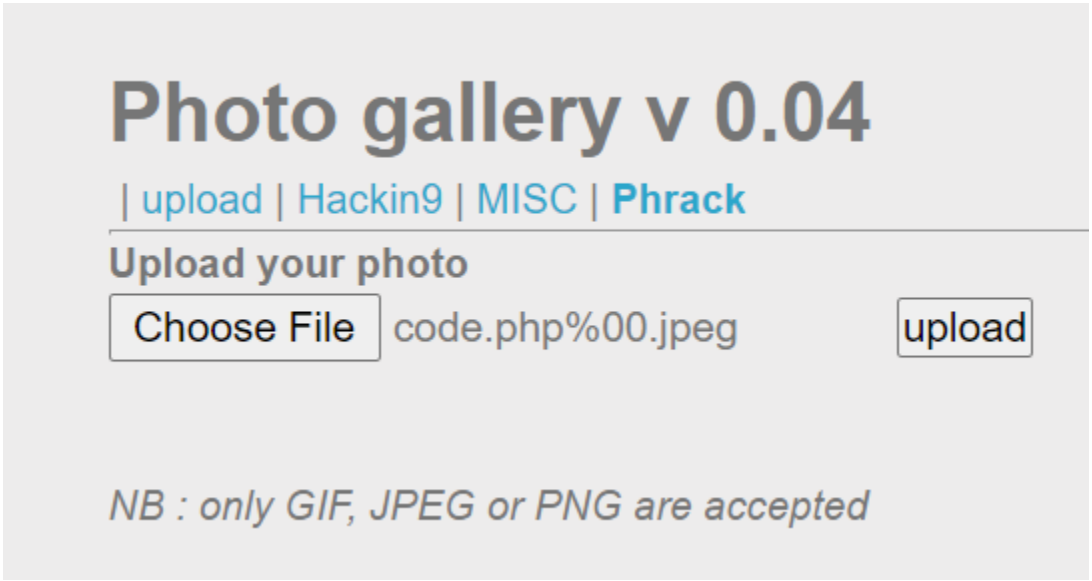


Giao diện trang web cho phép upload file kiểu ảnh như hình trên.

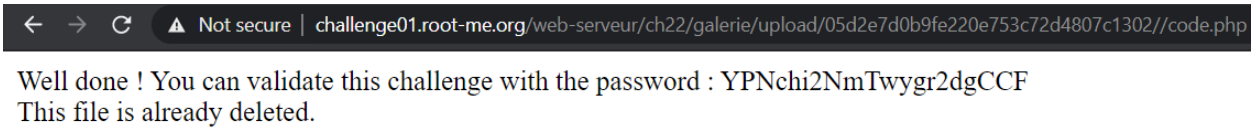


Đoạn code trên cho phép exploit trang web thông qua parameter command trong URL. Quan trọng là phải tìm cách upload được file này lên server.

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.



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



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