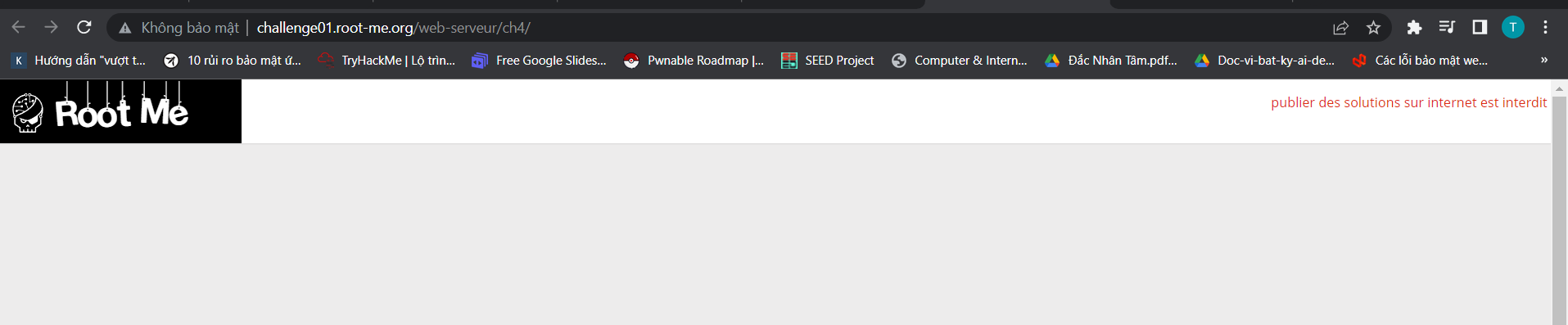
**5. HTTP - Directory indexing**



* Truy cập vào challenge ta được 1 trang web như trên không có gì cả
* Ta thử Ctrl + U xem như thế nào

Ảnh có chứa văn bản

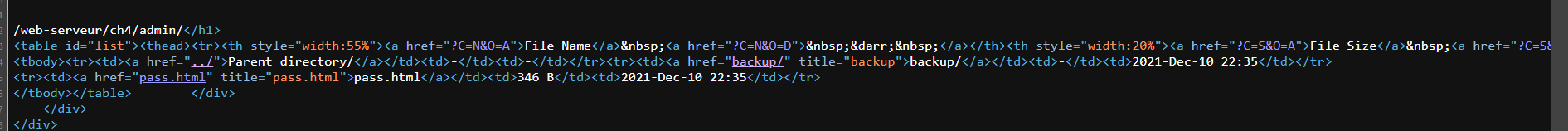
Mô tả được tạo tự động

* Ta thấy được có 1 đường dẫn “admin/pass.html” ta truy cập vào thử

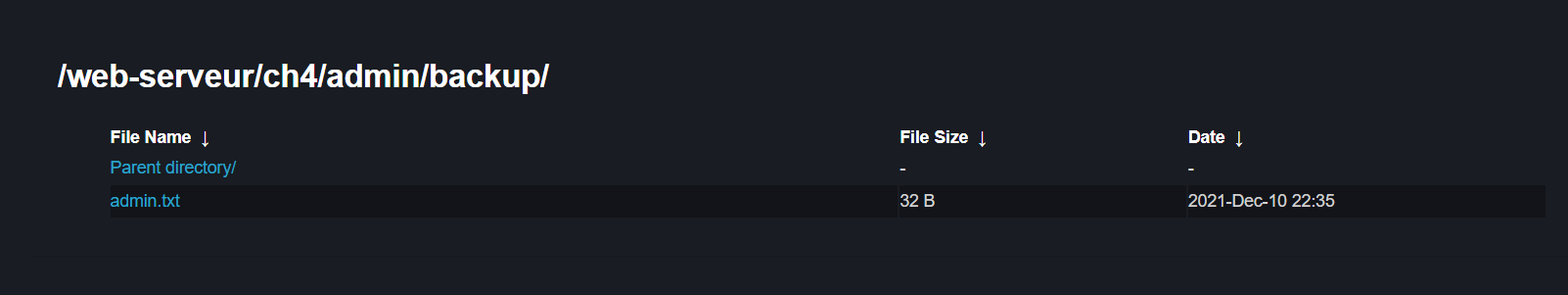
Ảnh có chứa văn bản

Mô tả được tạo tự động

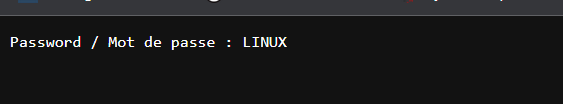
* Đại khái là ta đã bị lừa



* Ta thử lùi về admin xem có gì không
* Ta kiểm tra xem ở đây nó liệt kê ra danh sách các thư mục để ý tệp tin “backup” xem trong đó có gì

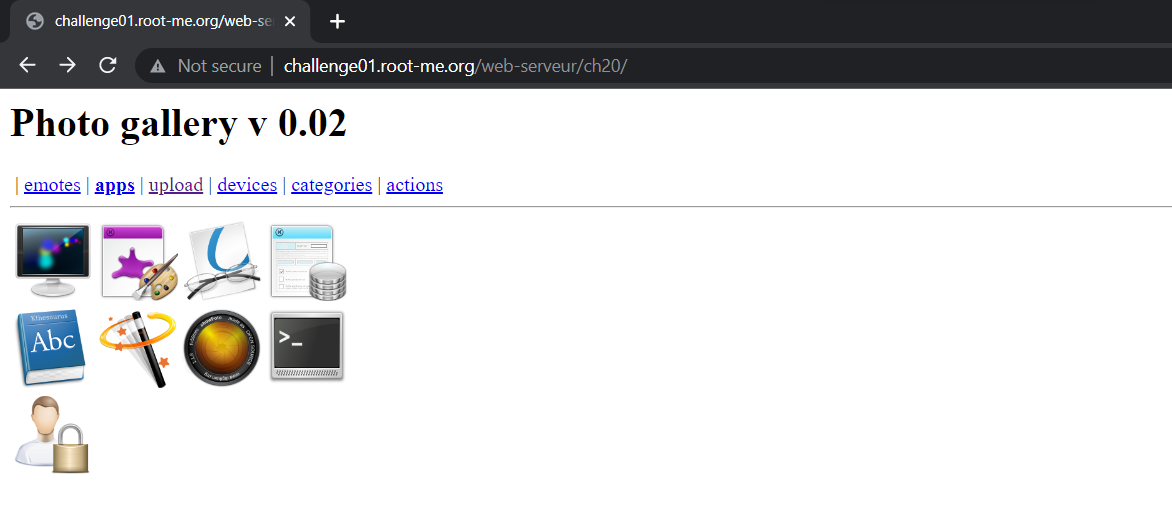


* Trong thư mục “backup” có 1 file tên là “admin.txt” và ta đọc thử xem trong đó có gì



* Đây là pass của ta
* Pass: LINUX

**6. File upload - Double extensions**



* Truy cập vào challenge ta được 1 trang web như trên
* Đại khái khi ta ấn vào 1 hình thì nó sẽ dẫn ta tới hình đó
* Ta quan tâm vào phần upload vì tên challenge cũng nói

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ở đây trang web cho ta upload 1 file ảnh có định dạng là .gif, .jpeg, .png
* Mục đích ở đây là ta sẽ viết 1 đoạn code bằng php để lấy được shell code

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Khi ta thử upload 1 file hình ảnh lên và bắt bằng burpsuite thì ở đây ta để ý phần filename sẽ là tên file của ta
* Ở dưới sẽ là những gì có trong file của ta
* Giờ ta có thể viết 1 đoạn code php để có thể lấy shellcode trực tiếp từ web sau đó bypass định dạng bằng cách đặt tên là .php.png chẳng hạn

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Sử dụng dụng lệnh exec để thực thi lệnh “cat ../../../.passwd” là để đi đến thư mục gốc của hệ thống xong sau đó ta dùng lệnh cat để đọc được
* Sau đó lưu lại dưới tên là code3.php.png
* Sau đó upload lên

Ảnh có chứa văn bản

Mô tả được tạo tự động

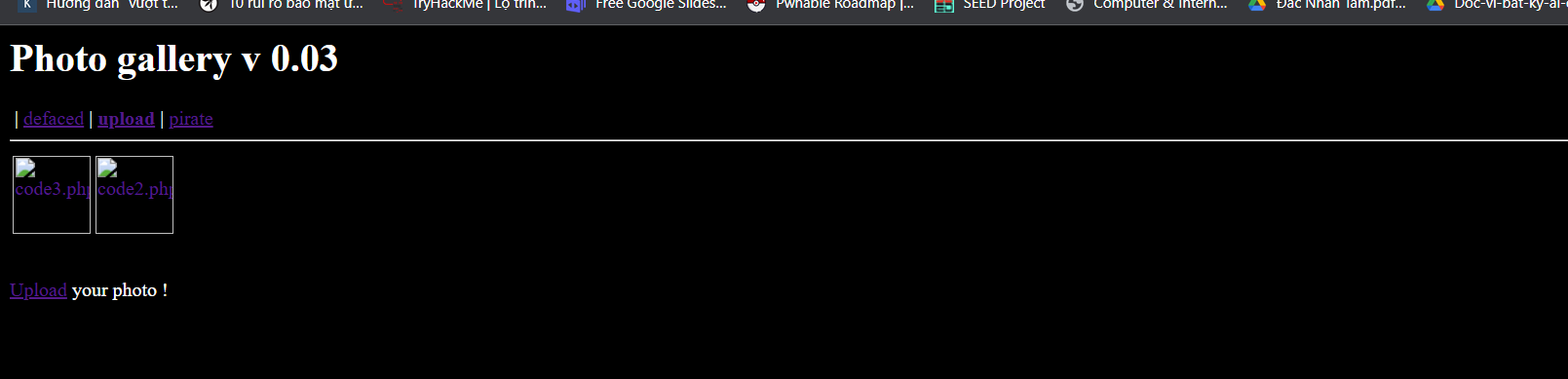
* Ta upload được thành công
* Trong đây trang web sẽ đọc nội dung trong file php và nó vẫn tưởng là file png đó và trả về cho ta kết quả lệnh ở trên

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta chỉ cần truy cập vào file là có được flag
* Flag: Gg9LRz-hWSxqqUKd77-\_q-6G8

**7. File upload - MIME type**



* Ta được cho 1 trang web challenge tương tự như ở bài trước
* Và nó cũng chỉ chọn các tệp tin GIF, JPEG, PNG

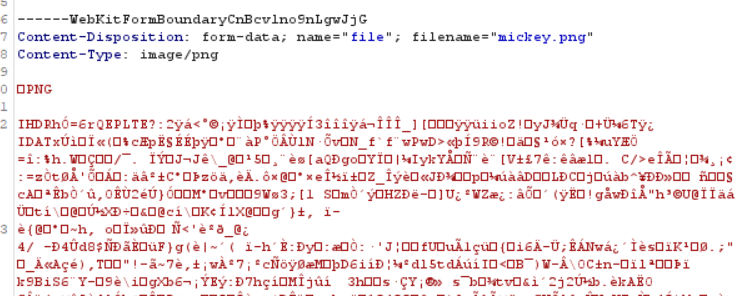
Ảnh có chứa văn bản

Mô tả được tạo tự động

* Và khi ta upload lại những file ở challenge trước thì khi mở lên nó không hiện gì cả



* Ta dùng burpsite bắt quá trình nó upload sau đó thay đổi



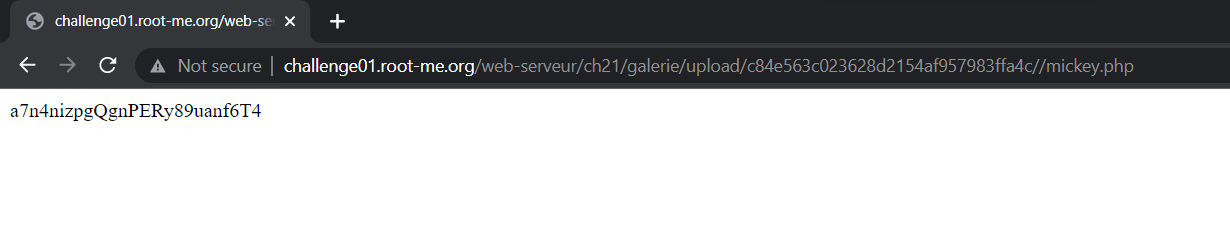
* Ở trường file name khi ta sử dụng là .php.png thì có thể upload được nhưng khi đọc thì nó không đọc được gì
* Nhưng ở challenge này ta lại có thể sửa thành .php và upload bình thường dù ở ở bước upload thủ công thì lại bị chặn

Ảnh có chứa văn bản

Mô tả được tạo tự động

Ảnh có chứa văn bản

Mô tả được tạo tự động



* Flag: a7n4nizpgQgnPERy89uanf6T4