

## Objective

Explore “Authentication Anywhere” cloud service and find your neighbor's secrets by exploiting IDOR.

---

## Steps Taken

### 1. Enumerate

- Visit the VM's web URL (e.g., `http://<IP>/`).
- A login form appears with a hint: “use guest account (Ctrl+U)”.

### 2. Source Code Review

- View page source (Ctrl+U) to reveal hardcoded credentials: `guest:guest` and a hidden note about an `admin` account.  
[reddit.com+15medium.com+15iboverflow.github.io+15ahmadnazir19470.medium.com+5medium.com+5medium.com+5reddit.comadityasrivastava.in+3medium.com+3medium.com+3iboverflow.github.io+4medium.com+4medium.com+4](https://medium.com/@15iboverflow/15ahmadnazir19470-medium-com-5medium-com-5medium-com-5reddit-comadityasrivastava-in-3medium-com-3medium-com-3iboverflow-github-io-4medium-com-4medium-com-4)

### 3. Login as Guest

- Use the credentials to access the site, landing on a URL like:  
`.../profile.php?user=guest`.

### 4. IDOR Exploit

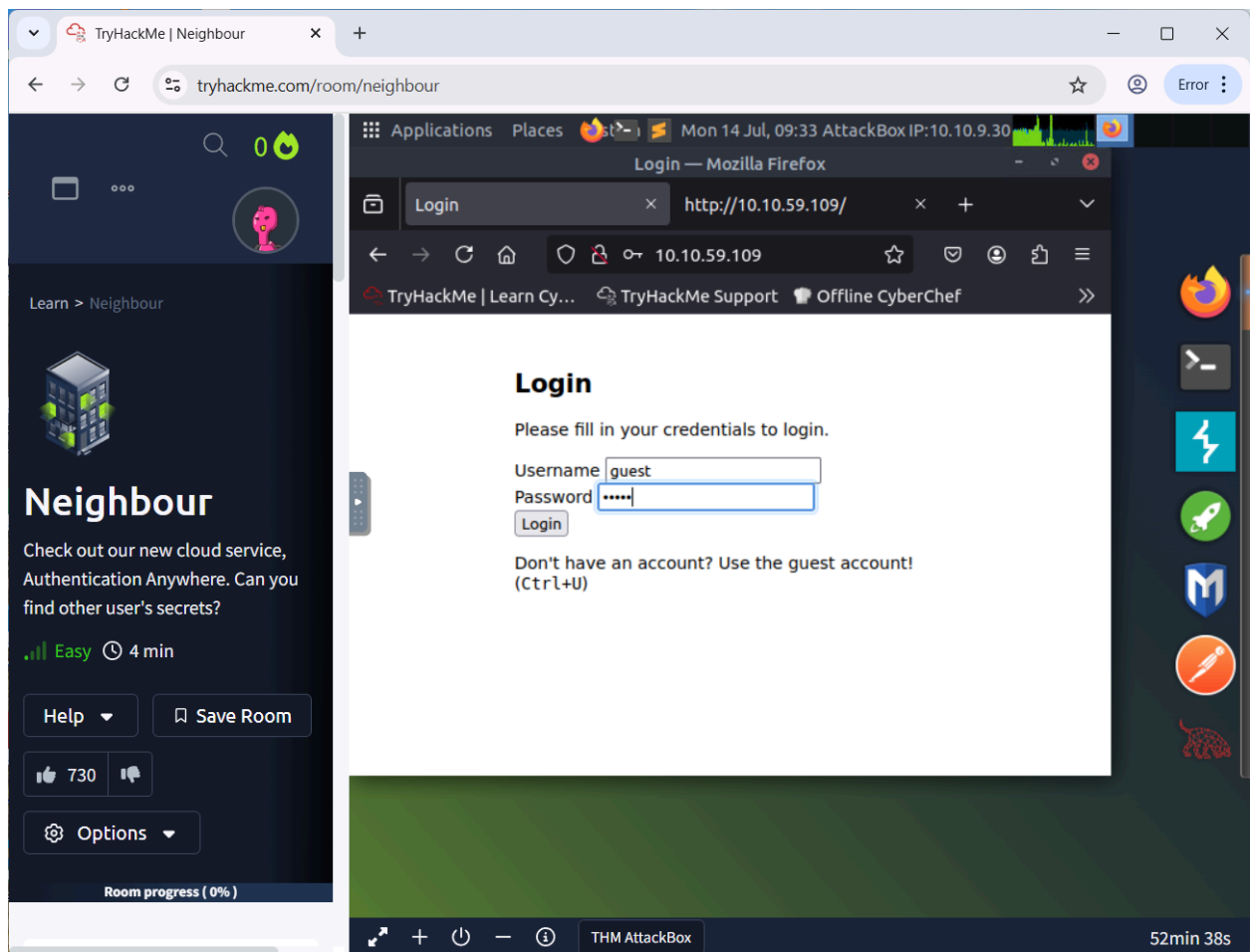
- Modify the URL parameter manually to `user=admin`.
- 

## Key Concept

- **IDOR** (Insecure Direct Object Reference):  
Occurs when the app uses client-controlled input (like `user=` in the URL) without proper access checks, enabling unauthorized access.
-

## ✓ Summary

- Found guest credentials in source.
- Logged in as guest.
- Changed `user=guest` → `user=admin` in URL.
- Gained unauthorized access to admin page and retrieved flag.



TryHackMe | Neighbour

tryhackme.com/room/neighbour

Room progress ( 0% )

- IDOR

Answer the questions below

Find the flag on your neighbor's logged in page!

Answer format: \*\*\*\*{\*\*\*\*\*}

Submit

Created by cmnatic

Room Type Users Created

Free Room.	in	975
Anyone can	Room	days
deploy	34,829	ago
virtual		
machines in		
the room		
(without		
being		
subscribed)!		

Applications Places

Mon 14 Jul, 09:37 AttackBox IP:10.10.9.30

http://10.10.59.109/profile.php?user=admin — Mozilla Firefox

• Welcome

http://10.10.59.109/profile.php

view-source:http://10.10.59.109/p

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef

```
UTF-8">
</title>
<!--
  unit could be vulnerable, need to update -->
  esheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.2/css/bootstrap.min.css">
  4px sans-serif; text-align: center; }

">Hi, <b>admin</b>. Welcome to your site. The flag is: flag{66be95c478473d91a5358f2440c7
gout.php" class="btn btn-danger ml-3">Sign Out of Your Account</a>
```

THM AttackBox

49min 16s

TryHackMe | Neighbour

tryhackme.com/room/neighbour

Room progress ( 0% )

task 1 neighbour

Check out our new cloud service, Authentication Anywhere -- log in from anywhere you would like! Users can enter their username and password, for a totally secure login process! You definitely wouldn't be able to find any secrets that other people have in their profile, right?

[Start Machine](#)

**Access this challenge** by deploying both the vulnerable machine by pressing the green "Start Machine" button located within this task, and the TryHackMe AttackBox by pressing the "Start AttackBox" button located at the top-right of the page.

Navigate to the following URL using the AttackBox: <http://10.10.59.109>

Check out similar content on TryHackMe:

- [IDOR](#)

**Answer the questions below**

Find the flag on your neighbor's logged in page!

[Submit](#)

Mon 14 Jul, 05

http://10.10.5

Welcome

TryHackMe | Learn Cy...


```
...vulnerable, need to updat
https://stackpath.bootst
...ext-align: center;
...>. Welcome to your si
class="btn btn-danger ml-3">
```

48min 45s

TryHackMe | Neighbour






tryhackme.com/room/neighbour


Error



Woop woop! Your answer is correct

### Congratulations on completing Neighbour!!! 🎉

<div>Points earned</div> <div> 30</div>	<div>Completed tasks</div> <div> 1</div>	<div>Room type</div> <div> Challenge</div>	<div>Difficulty</div> <div> Easy</div>	<div>Streak</div> <div> 1</div>
--	---	---	--	--

 This room counted toward joining the league 🎯

Leave Feedback

Continue