

TryHackMe - Neighbour Writeup

Introduction

The "Neighbour" challenge explores web vulnerabilities on a cloud-based login service, **Authentication Anywhere**. The goal is to identify insecure handling of user data that could expose sensitive information from other users' profiles. The room focuses on authentication flaws and insecure access controls.

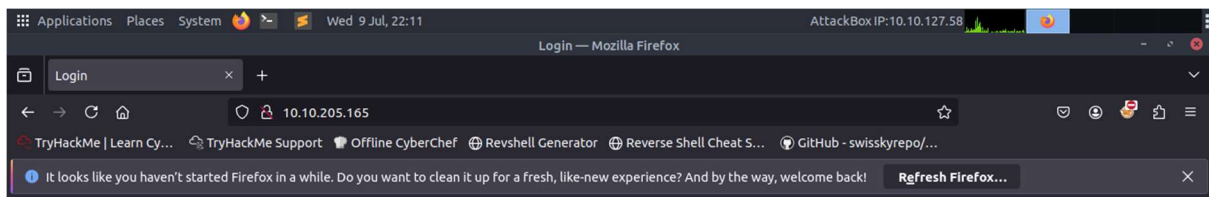
The screenshot shows the TryHackMe interface for the 'Neighbour' room. At the top, there's a header with 'Learn > Neighbour' and a small icon of a building. Below this, the room title 'Neighbour' is displayed, followed by a description: 'Check out our new cloud service, Authentication Anywhere. Can you find other user's secrets?'. The difficulty is marked as 'Easy' with a green icon and a timer of '4 min'. There are buttons for 'Start AttackBox', 'Help', 'Save Room', a thumbs up icon with '710', and an 'Options' dropdown. Below the header, a red bar indicates 'Room progress (0%)' and 'Target Machine Information'. A table lists the target machine: 'Neighbour-newapp' with a 'Target IP /' field, a 'Copy to clipboard' button, and an 'Expires' field showing '59min 18s'. There are also buttons for '?', 'Add 1 hour', and 'Terminate'. The main content area is titled 'Task 1' and 'Neighbour'. It contains a description of the challenge: '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?'. There is a 'Start Machine' button. Below this, it says '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.' It then provides a URL: 'Navigate to the following URL using the AttackBox: http://MACHINE_IP'. At the bottom, it says 'Check out similar content on TryHackMe:' and lists a link to 'IDOR'.

Tools Used

- Browser

Enumeration

The website presents a login form that accepts any **username** and **password**.



Login

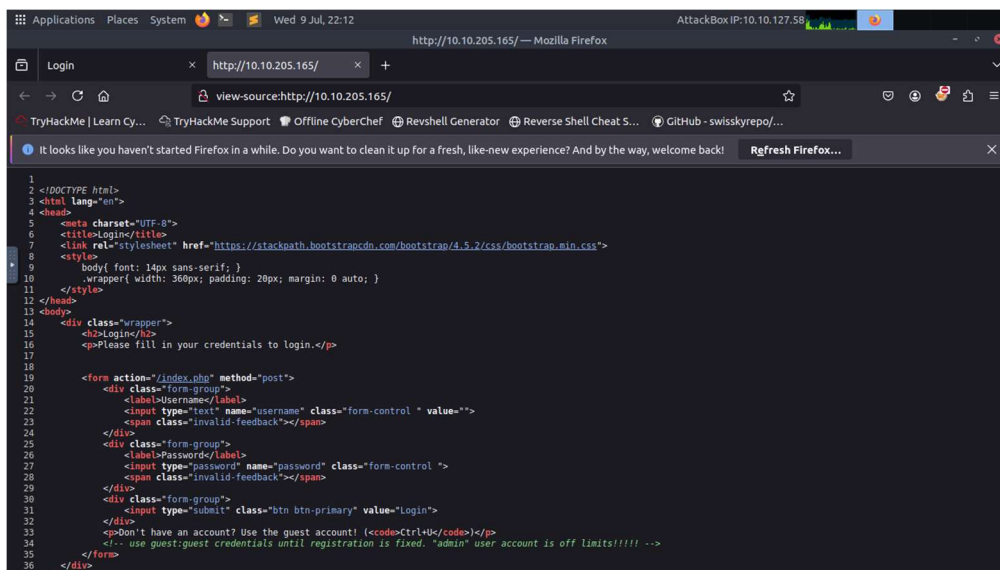
Please fill in your credentials to login.

Username

Password

Don't have an account? Use the guest account!
(Ctrl+U)

On viewing the page source, we get the guest and admin credentials.



Save password for http://10.10.205.165?

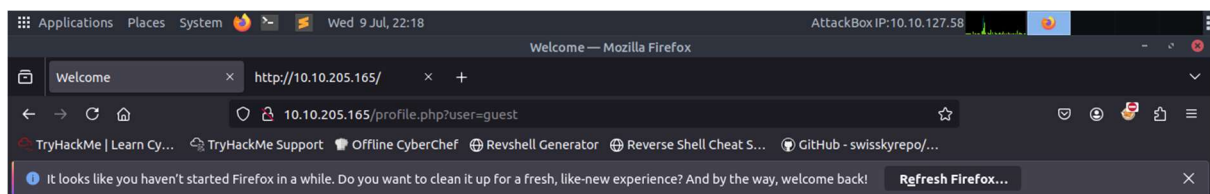
Username
guest

Password
guest

☐ Show password

Not now **Save**

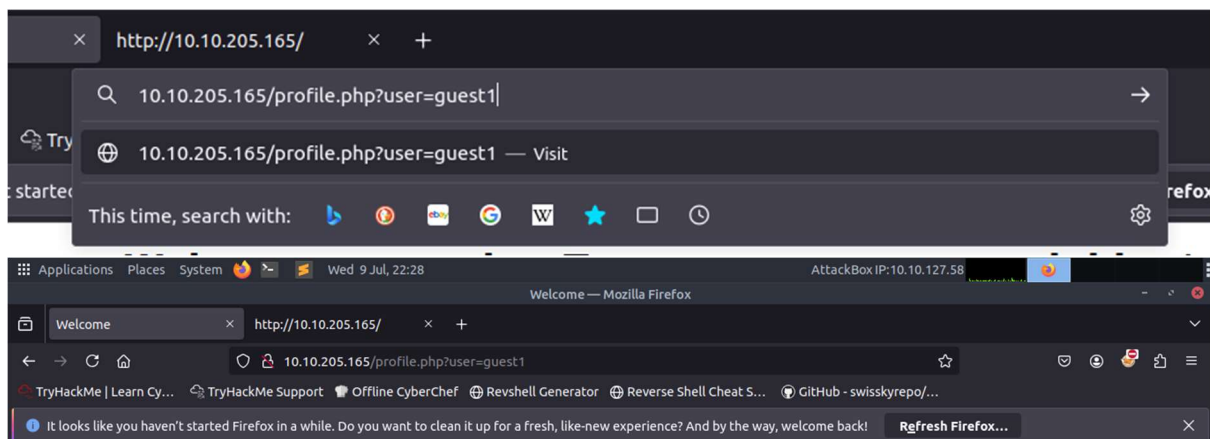
After inputting, the user & password as the guest, we get logged onto guest's account.



Hi, guest. Welcome to our site. Try not to peep your neighbor's profile.

[Sign Out of Your Account](#)

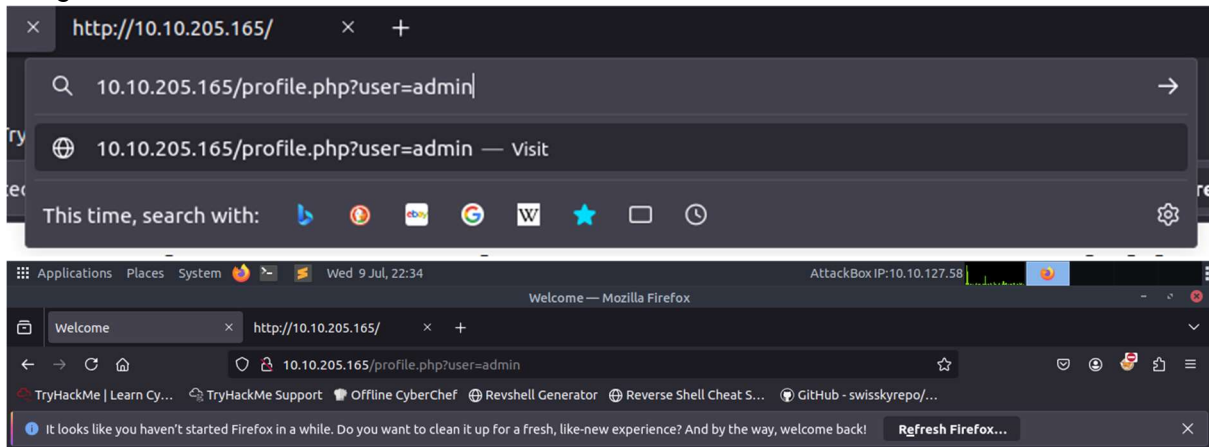
Next, we will try to access guest1's account by editing the URL.



Hi, guest1. Welcome to our site. Try not to peep your neighbor's profile.

[Sign Out of Your Account](#)

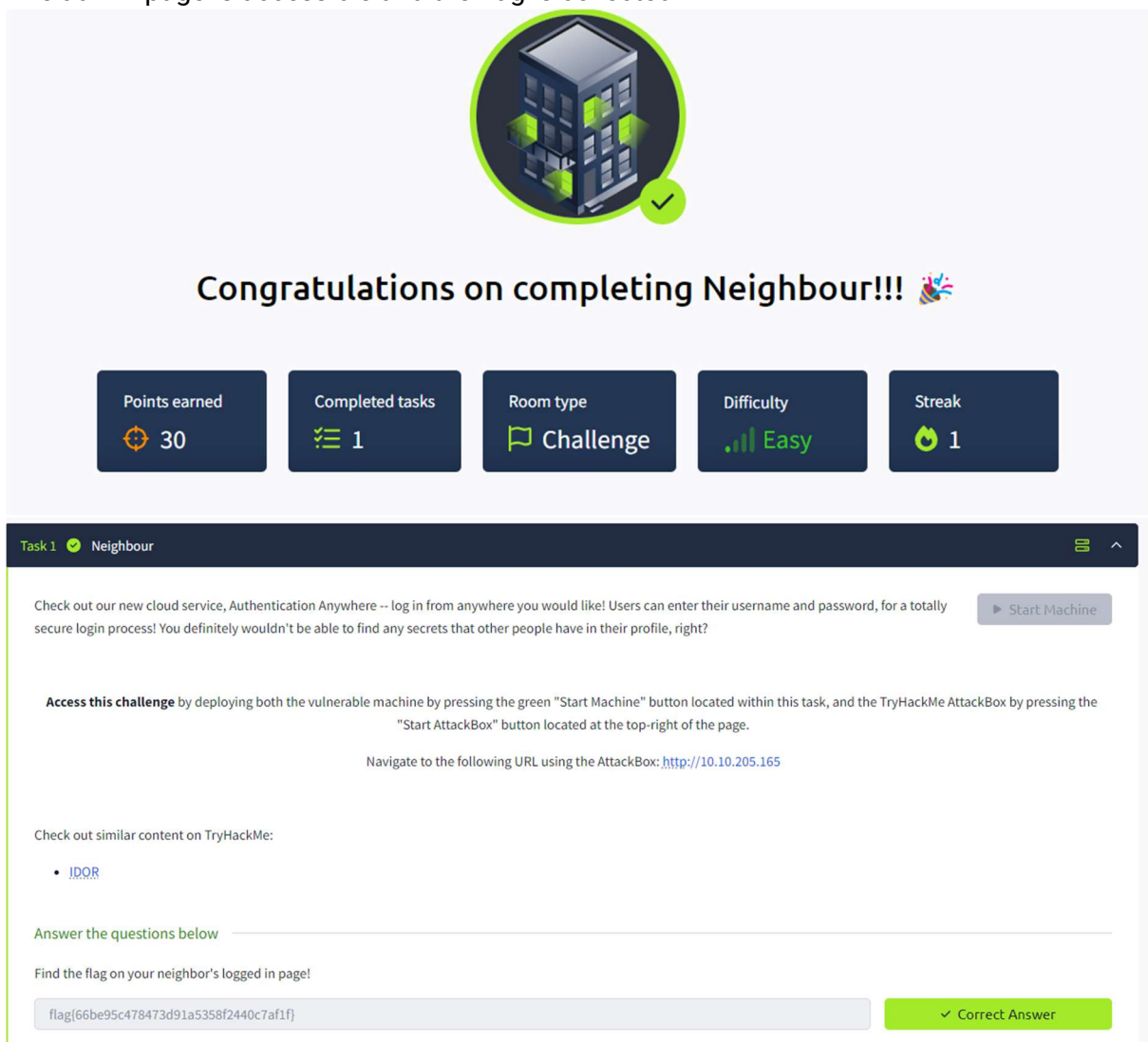
We get the access for user. Now it's time for the admin



**Hi, admin. Welcome to your site. The flag is:
flag{66be95c478473d91a5358f2440c7af1f}**

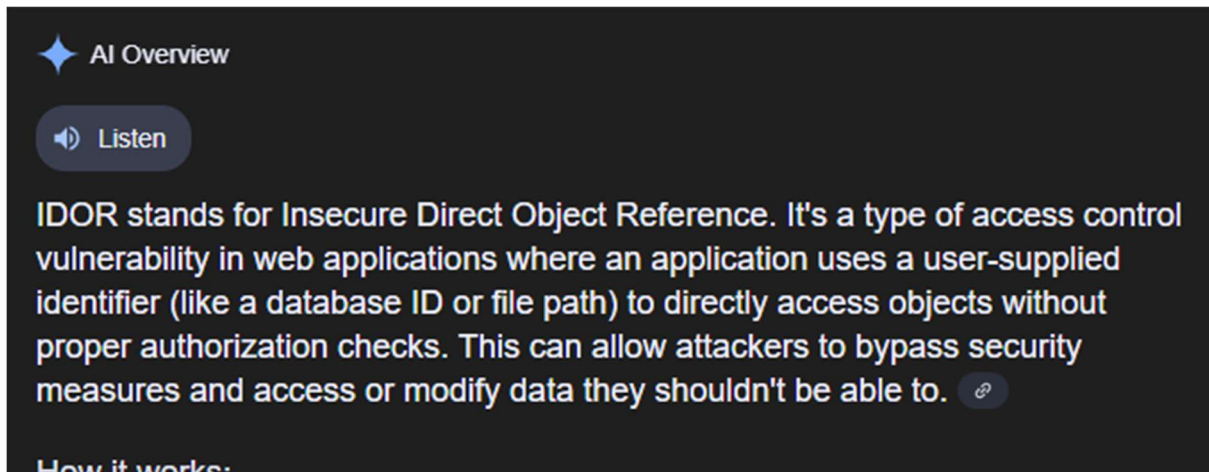
[Sign Out of Your Account](#)

The admin page is accessible and the flag is collected



Exploitation

The site does not verify whether the logged-in user is authorized to view the requested profile. This is a classic **IDOR (Insecure Direct Object Reference)** vulnerability.



Flags

flag{66be95c478473d91a5358f2440c7af1f}

Lessons Learned

- **Authentication! = Authorization:** Just because you're logged in doesn't mean you should access everything.
- IDOR is a common and dangerous flaw that occurs when user input (like a username or ID) is trusted without proper access control.
- Always verify permissions on sensitive actions and resources.

Conclusion

The Neighbour challenge was a quick and insightful dive into access control issues in web apps. It demonstrates how skipping proper checks can lead to data leaks and broken access controls. The fix? Never trust user-controlled input for sensitive resource access without validating ownership or permissions.