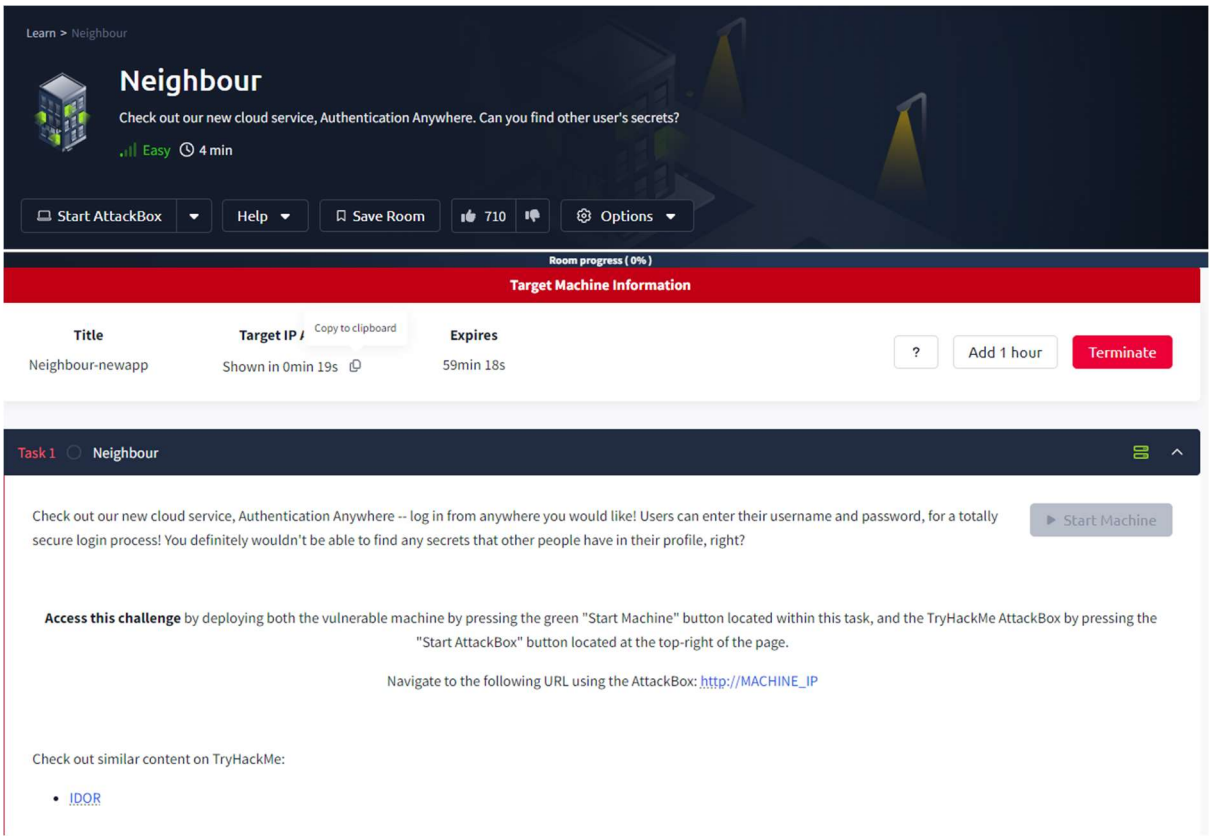
TryHackMe - Neighbour Writeup

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.

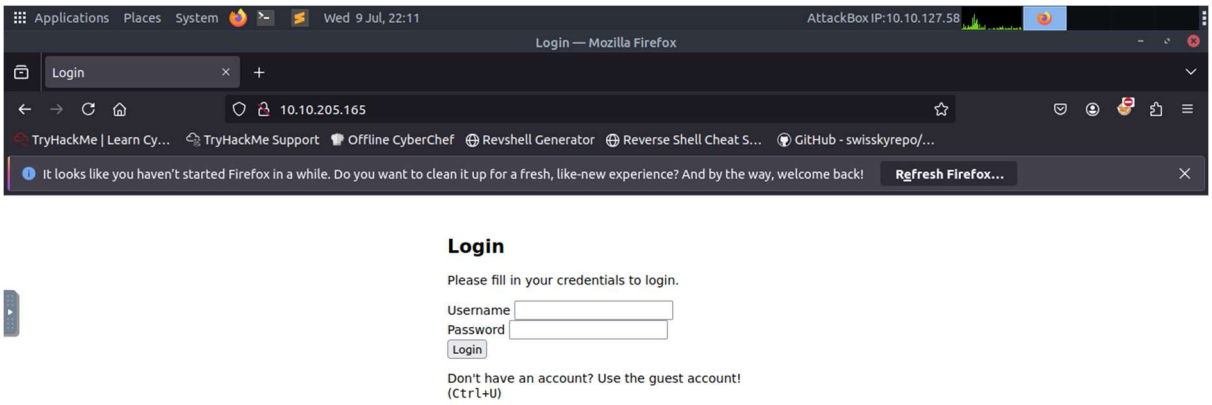


Tools Used

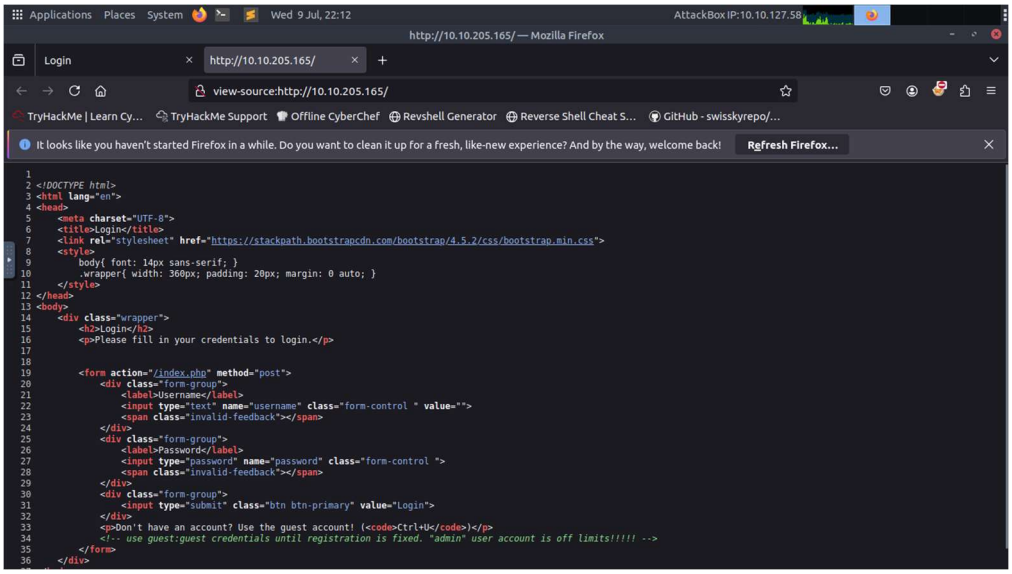
- Browser

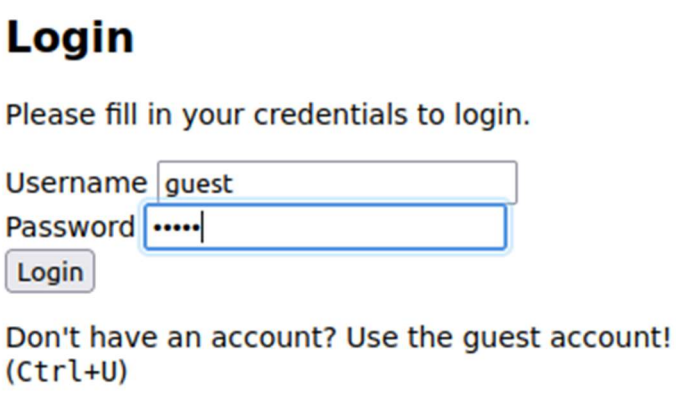
Enumeration

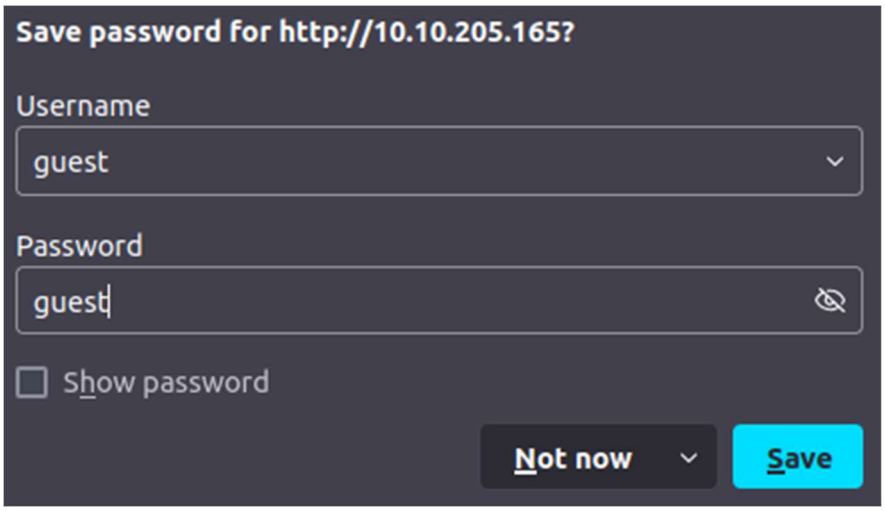
The website presents a login form that accepts any **username** and **password**.



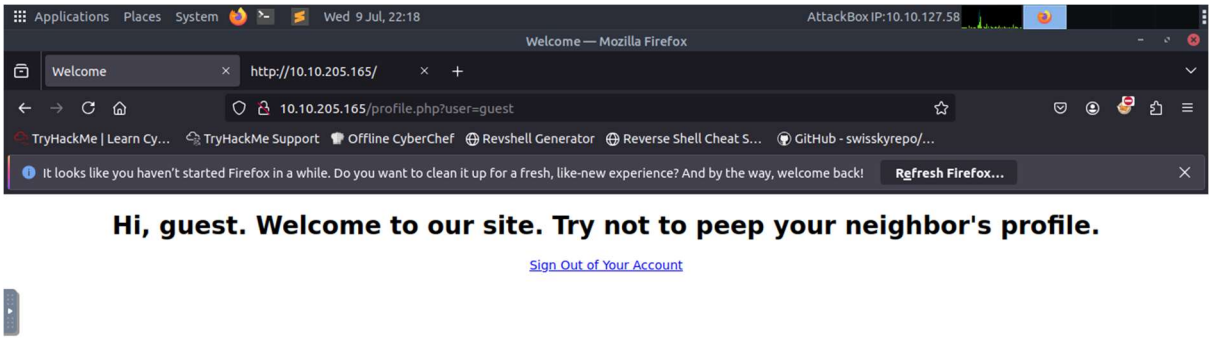
On viewing the page source, we get the guest and admin credentials.



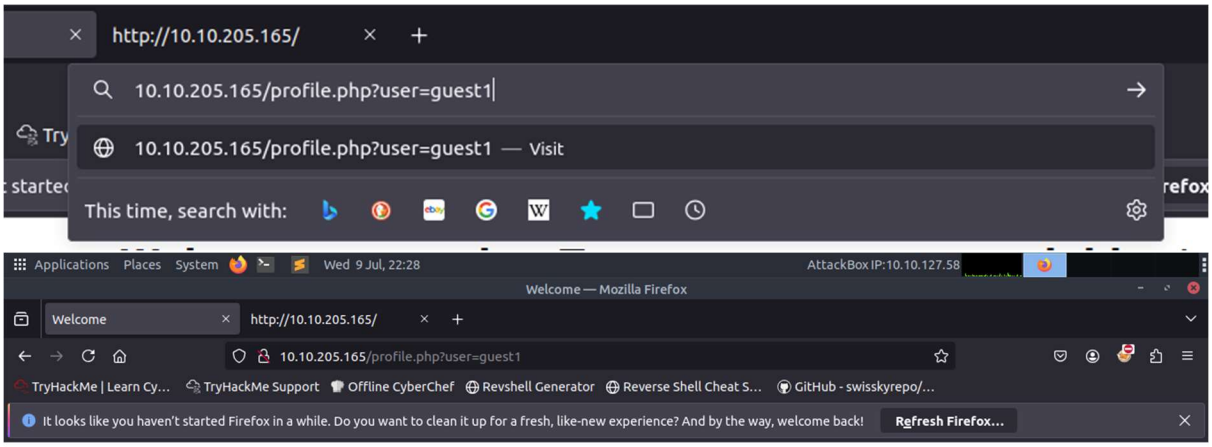




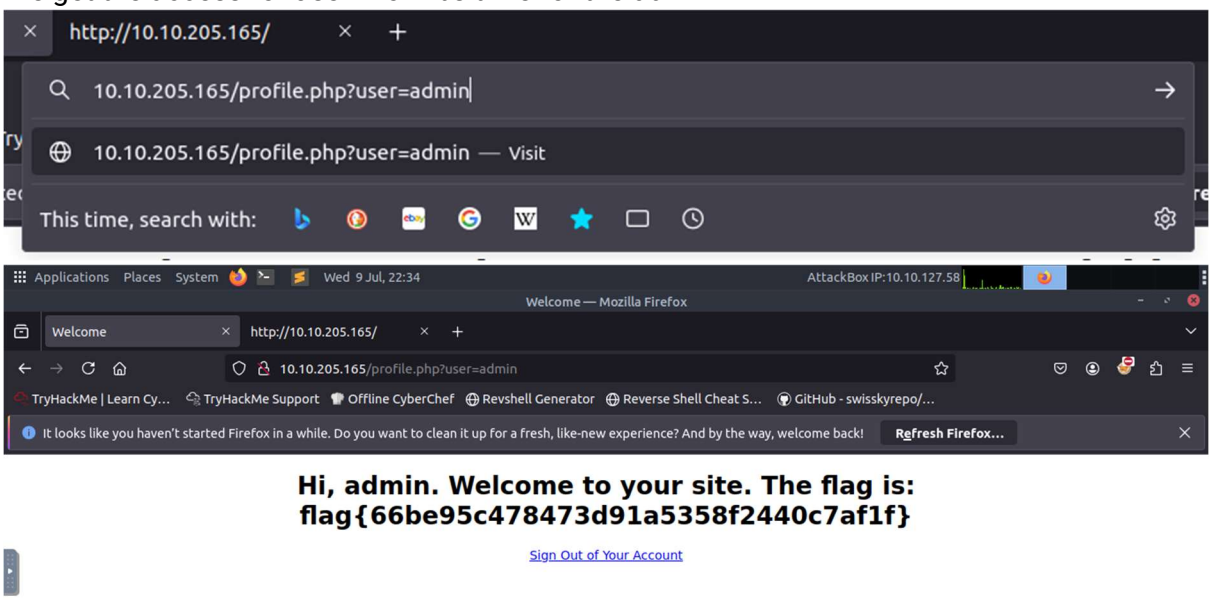
After inputting, the user & password as the guest, we get logged onto guest's account.



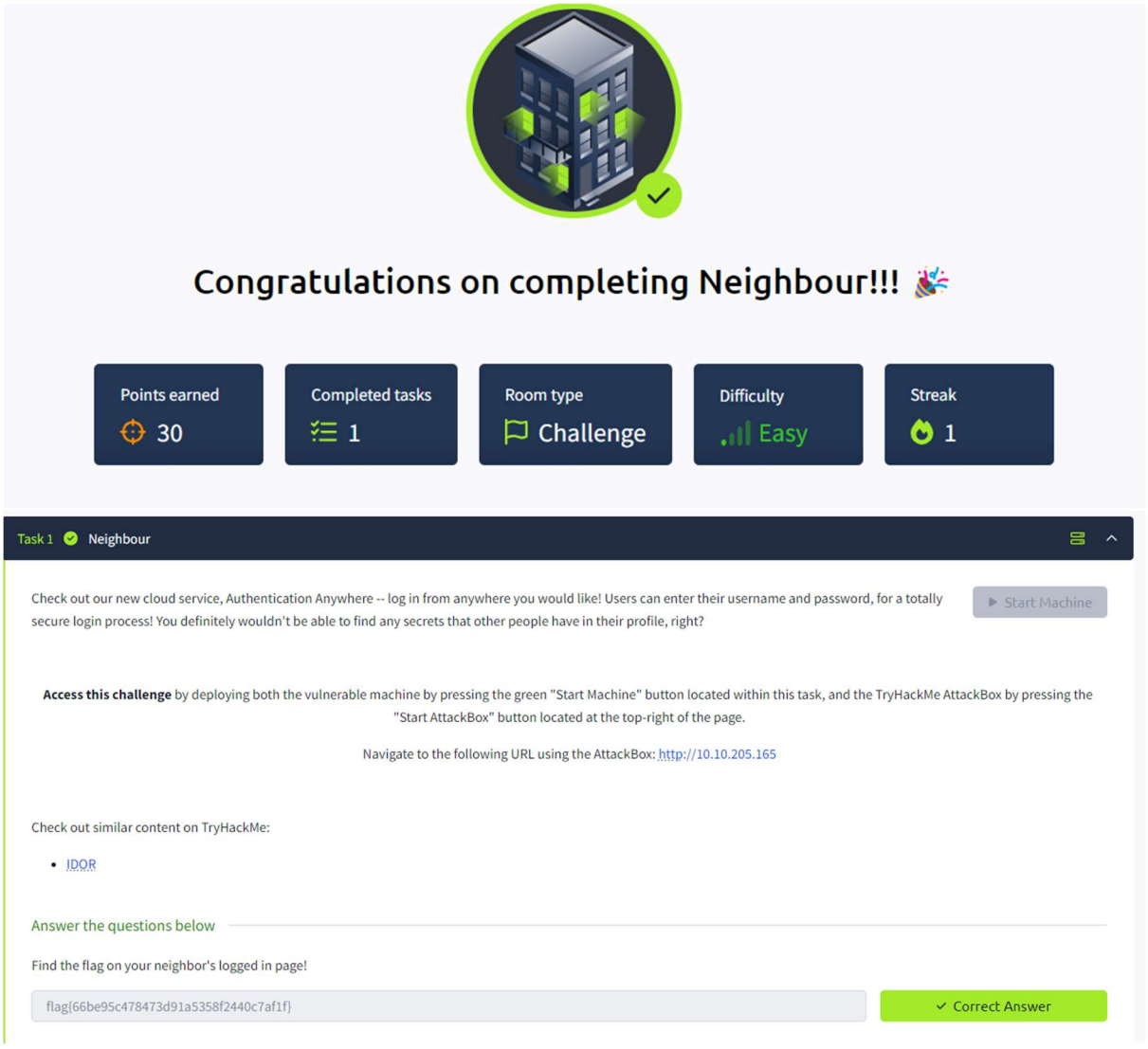
Next, we will try to access guest1's account by editing the URL.



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

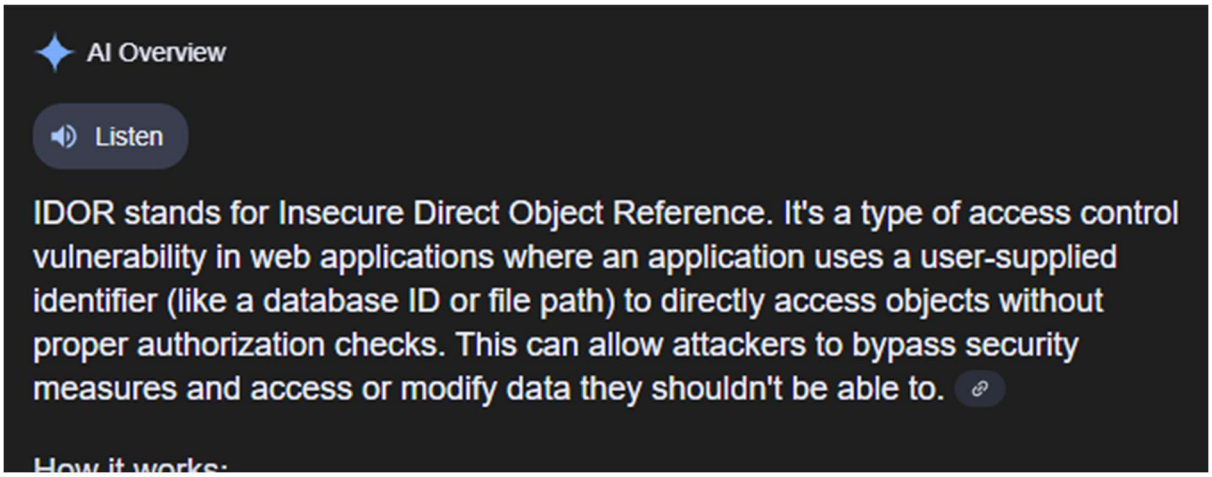


The admin page is accessible and the flag is collected



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.