**CTF Report**

TryHackMe Room – Neighbor (Easy)

# 🎯 Objective

Access another user's profile and retrieve the flag by exploiting an Insecure Direct Object Reference (IDOR) vulnerability.

# ⚙️ Setup

- VPN/Platform Used: TryHackMe AttackBox (web-based Kali)

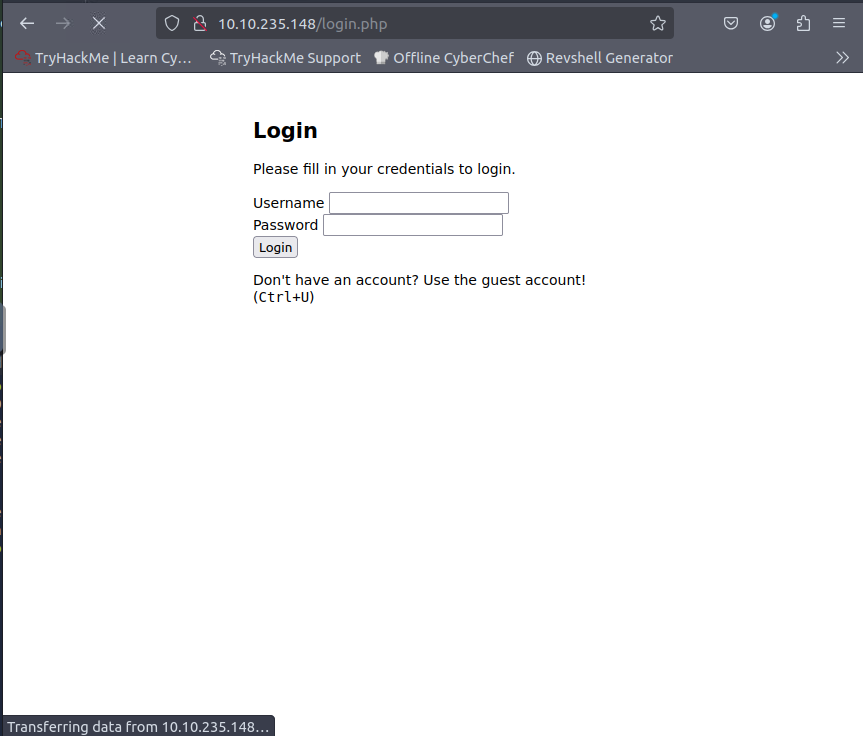
- Target Machine IP: 10.10.119.238

- VPN Status: Connected

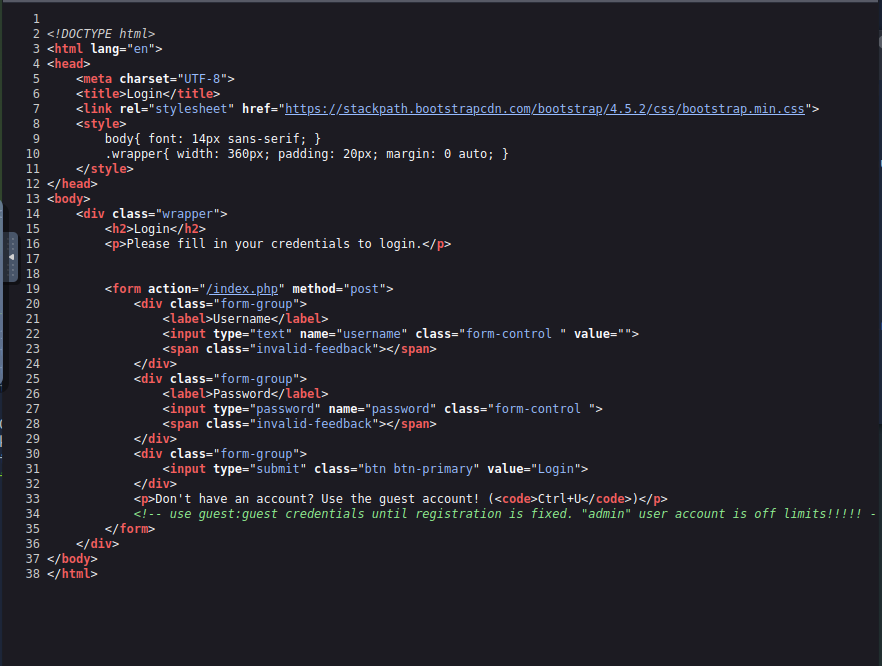
# 🛠️ Steps Taken

1. Logged into the site using credentials found in page source:

Since we cannot login, we use the guest account.



Ctrl+U -> To get the full HTML source code of the current webpage.



Here guest:guest are the credentials to the guest account.

1. Observed the URL after login: <http://10.10.119.238/profile.php?user=guest>
2. Modified the URL manually in the same tab (to preserve session): <http://10.10.119.238/profile.php?user=admin>

Since it is specifically mentioned that the admin user account is off limits.

1. Accessed the admin’s profile and found the flag: flag{example\_flag\_here}

# 🛡️ Vulnerability Type

IDOR (Insecure Direct Object Reference) – Allowed users to access other users’ data by simply modifying the URL.

# 🎓 What I Learned

• How to inspect page source for credentials

• How to manually manipulate URLs to test for IDOR

• Basic CTF process: login -> observe -> test -> flag

