

TryHackMe Room Write-up

Title: Neighbour

Description: Check out our new cloud service, Authentication Anywhere. Can you find other user's secrets?

Author: Igor Buszta

Neighbour

Description: 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?

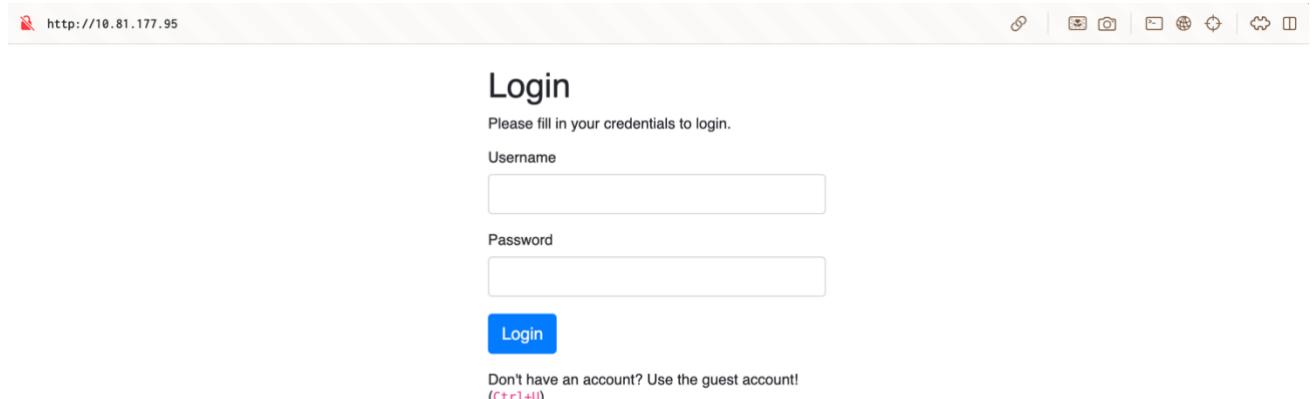
Access this challenge by deploying both the vulnerable machine by pressing the green "Start Machine" button located within this task, and the TryHackMe AttackBox by pressing the "Start AttackBox" button located at the top-right of the page.

Navigate to the following URL using the AttackBox: <http://10.81.177.95>

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

Tools: macOS, web search engine.

Room instructs us to go to the website. Let's see what's in there.



Picture 1: Webpage under the target IP.

Okay, we see a login page, but we have no credentials and bruteforcing doesn't seem like the first, obvious answer here.

At the bottom of the page, there's info that we can use guest account.

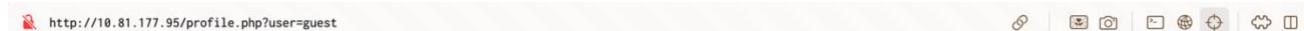
Uh-oh. The Ctrl+U doesn't seem to work. Let's inspect those elements, maybe there's something helpful there.



```
<!DOCTYPE html>
<html lang="en">
  > <head> ...
  > </head>
  > <body>
    > <div class="wrapper">
      > <h2>Login</h2>
      > <p>Please fill in your credentials to login.</p>
...   > <form action="/login.php" method="post"> == $0
    > <div class="form-group"> ...
    > <div class="form-group"> ...
    > <div class="form-group"> ...
    > <p> ...
    > <!-- use guest:guest credentials until registration is fixed -->
    > </form>
  > </div>
```

Picture 2: Inspecting the log in forms.

Nice! We've found the credentials to log in as a guest. Let's log in.



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

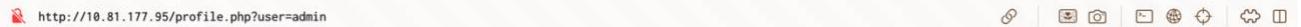
Sign Out of Your Account

Picture 3: Guest's page.

http://10.81.177.95/profile.php?user=guest

Picture 4: Guest's page URL.

The page clearly indicates manipulating the URL into tricking into thinking we're different user. What if we change the `user=guest`, which we used to log in as guest, to `user=admin`?

 http://10.81.177.95/profile.php?user=admin

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

[Sign Out of Your Account](#)

Picture 5: Admin's web page.

Here we go!