

Тачка сплелась с таким адресом:

<http://10.80.166.170/>

К таске шла подсказка IDOR, перейдем на веб-сайт.

Нас встречает окошко авторизации со следующим содержанием:

# Login

Please fill in your credentials to login.

Username

Password

Login

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

Что ж, попробуем зайти под кредами guest guest

Видим это:



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

Sign Out of Your Account

в поисковой строке видно:

`http://10.80.166.170/profile.php?user=guest`

`user=guest`

Вспоминаем подсказку:

*IDOR (Insecure Direct Object Reference) — это уязвимость безопасности, при которой приложение позволяет пользователю получить доступ к конфиденциальным данным, просто изменив идентификатор объекта.*

Попробуем написать admin вместо guest



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

Sign Out of Your Account

Вот наш флаг)

```
# flag{66be95c478473d91a5358f2440c7af1f}
```