



Neighbor

Active Machine Information

Title	IP Address	Expires	
Neighbour-newapp	10.10.151.21	54m 30s	<div>? Add 1 hour</div> <div>Terminate</div>

100%

Task 1 Neighbour

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?

▶ Start Machine

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://10.10.151.21>

Check out similar content on TryHackMe:

- [IDOR](#)

Enumeration

```

(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn 10.10.151.21
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-22 02:37 EDT
Nmap scan report for 10.10.151.21
Host is up (0.19s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 15.78 seconds

```

```

(kali㉿kali)-[~]
└─$ sudo nmap -sV -sC -A -Pn -p 22,80 10.10.151.21
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-22 02:38 EDT
Nmap scan report for 10.10.151.21
Host is up (0.19s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 41f7ab08913b27f33938437cb3f43893 (RSA)
|   256 e126a691701f62918e172474f6d440ac (ECDSA)
|_  256 4b675bc0085a20aea34a3aea028e9145 (ED25519)
80/tcp    open  http      Apache httpd 2.4.53 ((Debian))
|_ http-server-header: Apache/2.4.53 (Debian)
|_ http-title: Login
|_ http-cookie-flags:
|   /:
|   PHPSESSID:
|_   httponly flag not set

```

Open web browser and enter the **IP ADDRESS** of the target machine → It brings us to a login page

← → ↻ 🏠 10.10.151.21/login.php ☆ 🔒 🧑🏻 🧑🏻 🧑🏻 ☰

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Login

Please fill in your credentials to login.

Username

Password

Login

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

Press `Ctrl + U` as mentioned at the end of the login form to view the `guest` 's cred

```
<p>Don't have an account? Use the guest account! (<code>Ctrl+U</code>)</p>
<!-- use guest:guest credentials until registration is fixed. "admin" user account is off
limits!!!! -->
```

Exploit (Using IDOR vulnerable)

Login with the above cred (`guest:guest`)

← → ↻ 🏠 10.10.151.21 ☆ 🛡️ 🔥 👤 ☰

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Login

Please fill in your credentials to login.

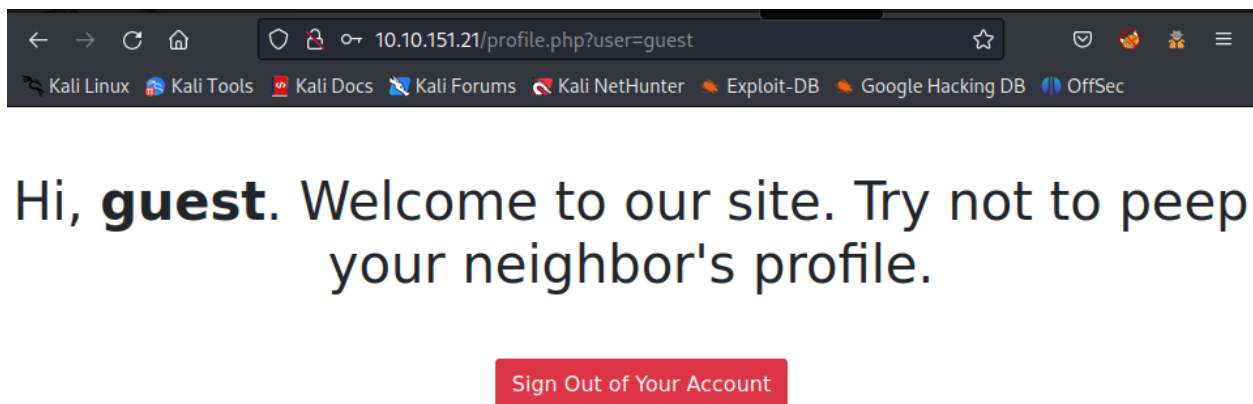
Username

Password

Login

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

The application routes us to a Welcome Page with the following URL

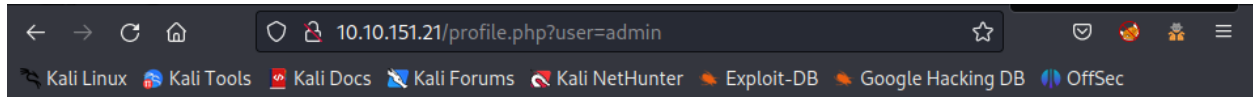


```
http://10.10.151.21/profile.php?user=guest
```

Attract on the query parameter `?user` , the `guest` param is displayed in plain text → Try to modify it to another username (`admin`)

```
http://10.10.151.21/profile.php?user=admin
```

The client return the Welcome Page for the `admin` user with the Flag



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

[Sign Out of Your Account](#)