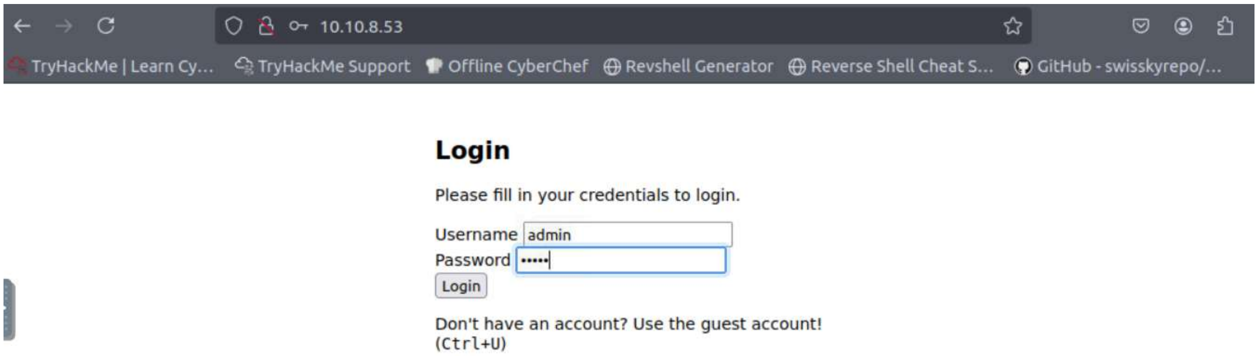
Mulearn x OWASP Kerala Cyber Security Bootcamp Task - 1

Tryhackme - Neighbour challenge

Step 1 : Navigate to web page [10.10.8.53](10.10.8.53)
Step 2 : Trying to login as admin



Login

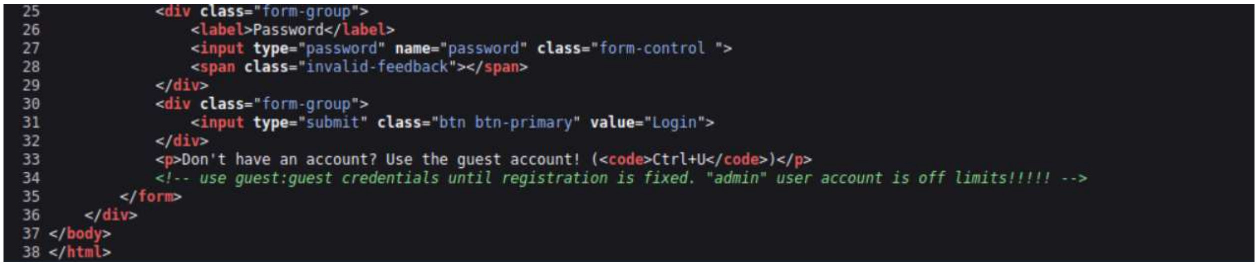
Please fill in your credentials to login.

Username admin
Password •••••
Login

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

Result : Account not found and advised to use guest account

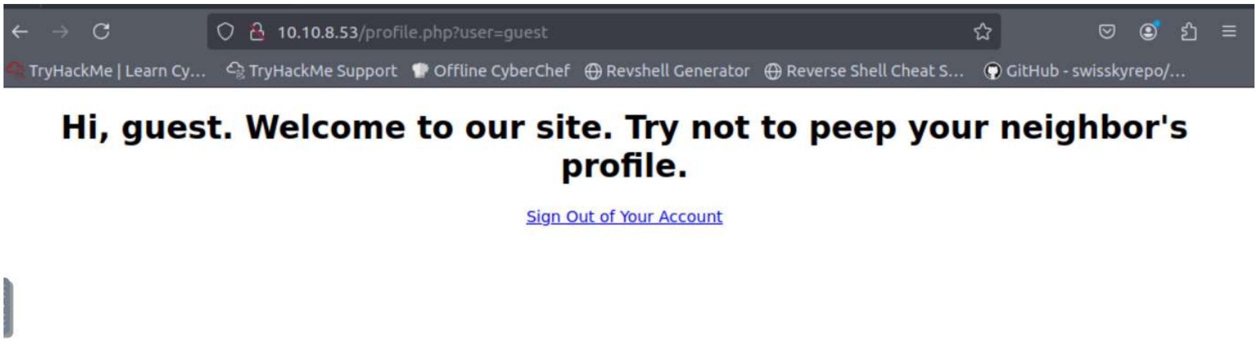
Step 3 : Checking source code of Login page



```
            <div class="form-group">
                <label>Password</label>
                <input type="password" name="password" class="form-control ">
                <span class="invalid-feedback"></span>
            </div>
            <div class="form-group">
                <input type="submit" class="btn btn-primary" value="Login">
            </div>
            <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!!!!! -->
        </form>
    </div>
</body>
</html>
```

Result : Mentioned to use guest login

Step 4 : Logging in as guest

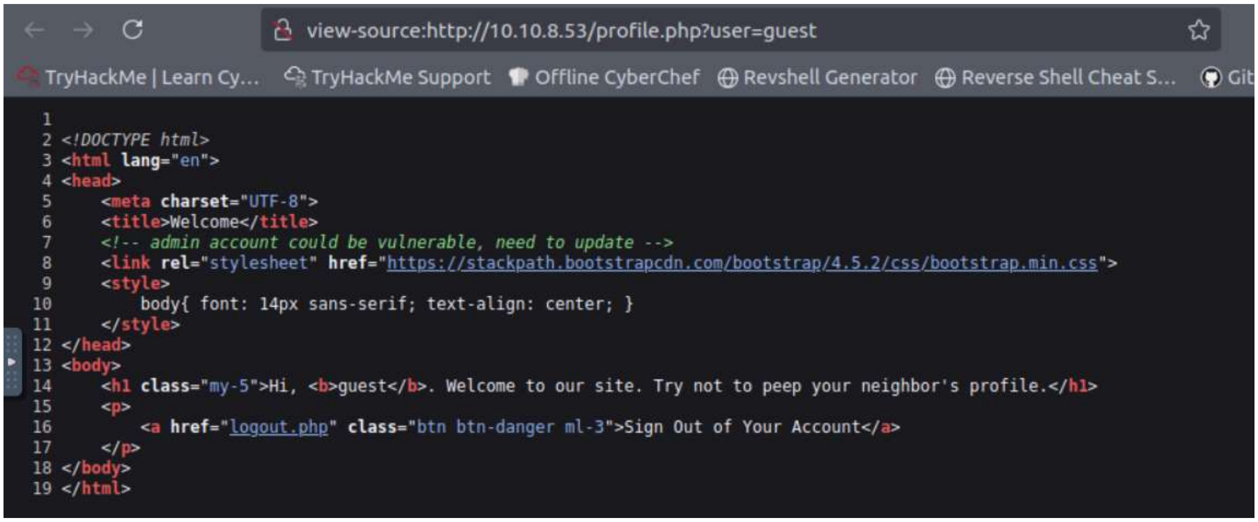


Hi, guest. Welcome to our site. Try not to peep your neighbor's profile.

Sign Out of Your Account

Logged in successfully as guest

Step 5 : Checking source code of profile page



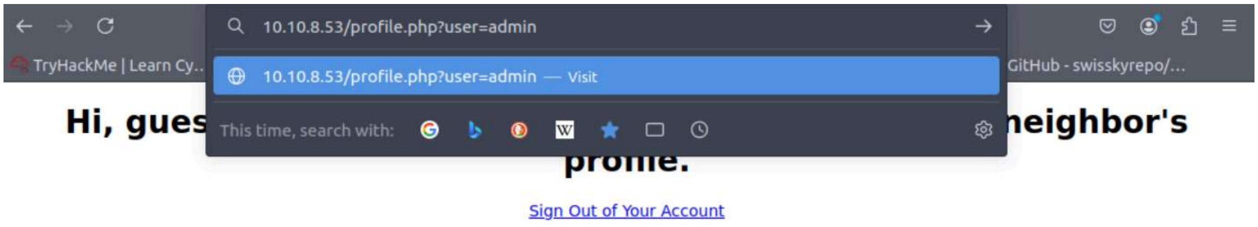
view-source:http://10.10.8.53/profile.php?user=guest

```

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Welcome</title>
    <!-- admin account could be vulnerable, need to update -->
    <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.2/css/bootstrap.min.css">
    <style>
        body{ font: 14px sans-serif; text-align: center; }
    </style>
</head>
<body>
    <h1 class="my-5">Hi, <b>guest</b>. Welcome to our site. Try not to peep your neighbor's profile.</h1>
    <p>
        <a href="logout.php" class="btn btn-danger ml-3">Sign Out of Your Account</a>
    </p>
</body>
</html>
```

Information noted : admin page is vulnerable.

Step 6 : Checking url : 10.10.8.53/profile.php?user=guest. Changing it to 10.10.8.53/profile.php?user=admin

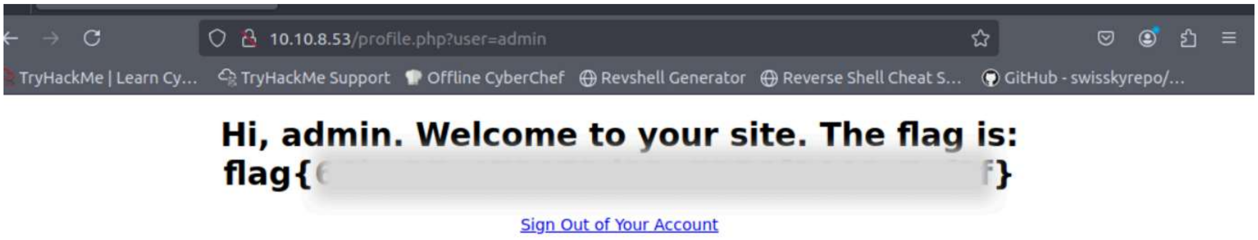


10.10.8.53/profile.php?user=admin

10.10.8.53/profile.php?user=admin — Visit

Hi, gues **neighbor's profile.**

Sign Out of Your Account



10.10.8.53/profile.php?user=admin

Hi, admin. Welcome to your site. The flag is: flag{[redacted]}

Sign Out of Your Account

Logged in as admin and flagged is captured.