Mave

一、信息收集

```
┌──(root㉿kali)-[/home/kali/Desktop/Maze]
└─# nmap --min-rate 10000 -p- 10.0.2.23
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-04 04:05 EDT
Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 92.59% done; ETC: 04:06 (0:00:04 remaining)
Nmap scan report for 10.0.2.23
Host is up (0.0017s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:E6:73:74 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 91.52 seconds

┌──(root㉿kali)-[/home/kali/Desktop/Maze]
└─#
```

22、80端口；

10.0.2.23/robots.txt

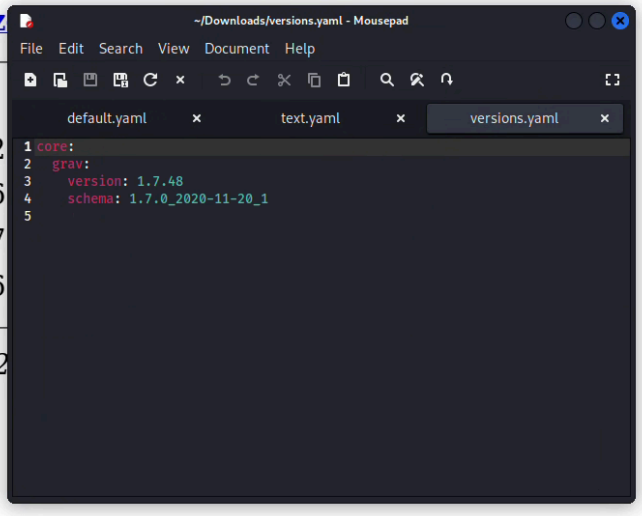
```
User-agent: *
Disallow: /.github/
Disallow: /.phan/
Disallow: /assets/
Disallow: /backup/
Disallow: /bin/
Disallow: /cache/
Disallow: /logs/
Disallow: /system/
Disallow: /tests/
Disallow: /tmp/
Disallow: /user/
Disallow: /vendor/
Disallow: /webserver-configs/
Allow: /user/pages/
Allow: /user/themes/
Allow: /user/images/
Allow: /
Allow: *.css$
Allow: *.js$
Allow: /system/*.js$
```

10.0.2.23/user/config/

Index of /user/config

Name	Last modified	Siz
Parent Directory		
security.yaml	2025-08-14 23:49	2
site.yaml	2024-10-28 07:31	16
system.yaml	2024-10-28 07:31	57
versions.yaml	2025-08-14 23:49	6

Apache/2.4.62 (Debian) Server at 10.0.2.2



grav cms 版本号为1.7.48

```
┌──(root㉿kali)-[/home/kali/Desktop/Maze]
└─# searchsploit grav
```

Exploit Title	Path
BitDefender GravityZone 5.1.5.386 - Multiple Vulnerabilities	linux/webapps/34086.txt
Cobian Backup 11 Gravity 11.2.0.582 - 'Password' Denial of Service (PoC)	windows/local/50790.py
Cobian Backup Gravity 11.2.0.582 - 'CobianBackup11' Unquoted Service Path	windows/local/50791.txt
Grav CMS 1.4.2 Admin Plugin - Cross-Site Scripting	php/webapps/42131.txt
Grav CMS 1.6.30 Admin Plugin 1.9.18 - 'Page Title' Persistent Cross-Site Scripting	php/webapps/49264.txt
Grav CMS 1.7.10 - Server-Side Template Injection (SSTI) (Authenticated)	php/webapps/49961.py
Grav CMS 1.7.48 - Remote Code Execution (RCE)	php/webapps/52402.txt
GravCMS 1.10.7 - Arbitrary YAML Write/Update (Unauthenticated) (2)	php/webapps/49973.py
GravCMS 1.10.7 - Unauthenticated Arbitrary File Write (Metasploit)	php/webapps/49788.rb
Gravity Board X 1.1 - 'csscontent' Remote Code Execution	php/webapps/1510.pl
Gravity Board X 1.1 - CSS Template Unauthorized Access	php/webapps/26111.txt
Gravity Board X 1.1 - Login SQL Injection	php/webapps/26106.txt
Gravity Board X 2.0 Beta (Public Release 3) - SQL Injection	php/webapps/11583.pl
Gravity Board X 2.0 Beta - SQL Injection / (Authenticated) Code Execution	php/webapps/8350.txt
Gravity Board X 2.0 Beta - SQL Injection / Cross-Site Scripting	php/webapps/5791.txt
Gravity GTD 0.4.5 - Local File Inclusion / Remote Code Execution	php/webapps/7344.txt
gravy media CMS 1.07 - Multiple Vulnerabilities	php/webapps/8315.txt
Gravy Media Photo Host 1.0.8 - Local File Disclosure	php/webapps/8996.txt
WordPress Plugin Aviary Image Editor Addon For Gravity Forms 3.0 Beta - Arbitrary File Uplo	php/webapps/37275.txt
WordPress Plugin Gravity Forms 1.8.19 - Arbitrary File Upload	php/webapps/39969.php

Shellcodes: No Results

尝试poc失败；

二、获取立足点

大佬提示：tftp服务；

```
┌──(root㉿kali)-[/home/kali/Desktop/Maze]
└─# nmap -sU --top-ports 20 10.0.2.23
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-04 22:21 EDT
Nmap scan report for 10.0.2.23
Host is up (0.0016s latency).

PORT      STATE         SERVICE
53/udp    closed        domain
67/udp    closed        dhcps
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
123/udp   closed        ntp
135/udp   closed        msrpc
137/udp   closed        netbios-ns
138/udp   closed        netbios-dgm
139/udp   closed        netbios-ssn
161/udp   closed        snmp
162/udp   closed        snmptrap
445/udp   closed        microsoft-ds
500/udp   closed        isakmp
514/udp   closed        syslog
520/udp   closed        route
```

猜测存在文件；获取user.txt

```
┌──(root㉿kali)-[/home/kali/Desktop/Maze]
└─# tftp 10.0.2.23
tftp> ls -liah
?Invalid command
tftp> get user.txt
tftp>

┌──(root㉿kali)-[/home/kali/Desktop/Maze]
└─# ls
49773.py    CVE-2025-50286  ferox-http_10_0_2_23-1756975217.state  result.txt
52402.txt   default.md      reports                                user.txt

┌──(root㉿kali)-[/home/kali/Desktop/Maze]
└─# cat user.txt
flag{user-4e79af9d9b43464228ae1100839a2575}
username:bamuwe
need:bruteforce
```

爆破获取身份凭据：

bamuwe : hahaha

三、提权

```
bamuwe@Maze:~$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
bamuwe@Maze:~$
```

没啥特殊的，看/home目录下用户；爆破得到以下凭据

```
lingmj      piggies
ll104567    prettywoman
ta0         packers1
todd        princess101
```

爆破完发现，首页有todd用户。。。。

切换用户，查看权限，均无法利用

查看sudo --version；尝试提权脚本失败；

根据经验，查看/opt目录；

有个脚本，扔给AI审计；

File "/opt/log_backup_service.py", line 10, in <module>...

这个问题非常典型。你看到的 `PermissionError: [Errno 13] Permission denied: '/var/log/log_backup_service.log'` 错误，表示你的脚本没有权限在 `/var/log/` 目录下创建或写入日志文件。

错误原因分析

- **权限问题：** `/var/log/` 目录通常是只有 `root` 用户才有写入权限的。
- **非 Root 用户运行：** 你的脚本很可能是以普通用户（比如 `lingmj`）的身份运行的。当脚本试图执行 `logging.basicConfig()` 来初始化日志文件时，它尝试在 `/var/log/` 目录下创建一个名为 `log_backup_service.log` 的文件。由于普通用户没有这个权限，操作系统拒绝了该操作，从而抛出 `PermissionError`。

为什么会这样?

这个问题再次印证了我们之前对脚本安全漏洞的分析。

1. **脚本的运行方式：** 尽管你之前的图片显示脚本可能以 `root` 权限运行（作为服务），但你现在手动执行 `python3 log_backup_service.py` 时，它会以你当前登录的用户身份运行，而这个用户很可能不是 `root`。
2. **不安全的硬编码路径：** `logging.basicConfig()` 中的日志文件路径 `/var/log/log_backup_service.log` 是硬编码的。这种做法假设脚本总是以拥有足够权限的用户（如 `root`）运行。但在实际环境中，这可能导致权限问题。

```
bamuwe@Maze:/home$ cd /tmp
bamuwe@Maze:/tmp$ ls
root.txt.20250904224238.bak  systemd-private-8d7e48c21b184e93aa4d90cebf46d0bd-apache2.service-fkqBci
root.txt.20250904224338.bak  systemd-private-8d7e48c21b184e93aa4d90cebf46d0bd-systemd-logind.service-E7y5Li
root.txt.20250904224438.bak  systemd-private-8d7e48c21b184e93aa4d90cebf46d0bd-systemd-timesyncd.service-P9HFsf
bamuwe@Maze:/tmp$ cat root.txt.20250904224338.bak
flag{root-6195bd8a9d755a41e493440a804f46d4}
bamuwe@Maze:/tmp$ cat /etc/log
log_backup_service/ logcheck/           login.defs          logrotate.conf      logrotate.d/
bamuwe@Maze:/tmp$ cat /etc/log_backup_service/config.json
{
  "source_log_path": "/root/root.txt",
  "backup_dest": "/tmp",
  "run_as_user": "backup_user"
}
bamuwe@Maze:/tmp$
```

找到/etc/log_backup_service/config.json 文件；拥有读写权限；
修改目录以及文件；获取到root.txt

同时也可以读取shadow文件，爆破root用户密码