

week2-Nse4u Wp

week2-Nse4u Wp

web

Liki的生日礼物

misc

Telegraph: 1601 6639 3459 3134 0892

DNS

crypto

white give rsa


web


Liki的生日礼物

根据提示条件竞争，百度一下得知：服务器在处理多线程任务时，如果共用了同一个共享空间，

可能会产生条件竞争的问题。就是可能在某一线程任务对共享空间的变量还没来得及修改，另一个线程任务就引用了他，可能就会产生一些判断的漏洞

1. 点进题目，发现是个购买页面，发现花完所有钱也还差两个兑换卷
2. 根据提示条件竞争，用多线程任务，触发条件竞争漏洞
3. 于是发包，intruder

 **Request Engine**

 These settings control the engine used for making HTTP requests when performing attacks.

Number of threads:	<input type="text" value="100"/>
Number of retries on network failure:	<input type="text" value="3"/>
Pause before retry (milliseconds):	<input type="text" value="2000"/>

4.

4. Burp Suite Professional v1.7.32 - Temporary Project - licensed to surferxyz

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 2 3

Target Positions Payloads Options

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: **Sniper**

GET /API/?m=getinfo HTTP/1.1
Host: birthday.iki.link
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: */*
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
X-Requested-With: XMLHttpRequest
Connection: close
Referer: https://birthday.iki.link/shop.html
Cookie: PHPSESSID=k8e3au9t6ms0hq2s8n3dcu46n4

Start attack

Add \$
Clear \$
Auto \$
Refresh

0 matches Clear

0 payload positions Length: 419

5.

5. Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	342	
1	null	200	<input type="checkbox"/>	<input type="checkbox"/>	342	
2	null	200	<input type="checkbox"/>	<input type="checkbox"/>	342	
3	null	200	<input type="checkbox"/>	<input type="checkbox"/>	342	
4	null	200	<input type="checkbox"/>	<input type="checkbox"/>	342	
5	null	200	<input type="checkbox"/>	<input type="checkbox"/>	342	
6	null	200	<input type="checkbox"/>	<input type="checkbox"/>	342	
7	null	200	<input type="checkbox"/>	<input type="checkbox"/>	342	
8	null	200	<input type="checkbox"/>	<input type="checkbox"/>	342	
9	null	200	<input type="checkbox"/>	<input type="checkbox"/>	342	

141 of 500

商城

注册即送2000元，40元可换一张兑换券

52张兑换券即可兑换一台switch噢

如果你能送一台switch给liki说不定她会告诉你flag呢

用户余额	兑换券数量
0	55

兑换券

¥ 40

兑换

switch

52张兑换券

兑换

6. 然后就好了

如果你能送一台switch给liki说不定她会告诉你flag呢

用户余额	兑换券数量

Liki非常开心并把flag给了你:hgame{L0ck_1s_TH3_S0llution!!!!}

确定

兑换

switch

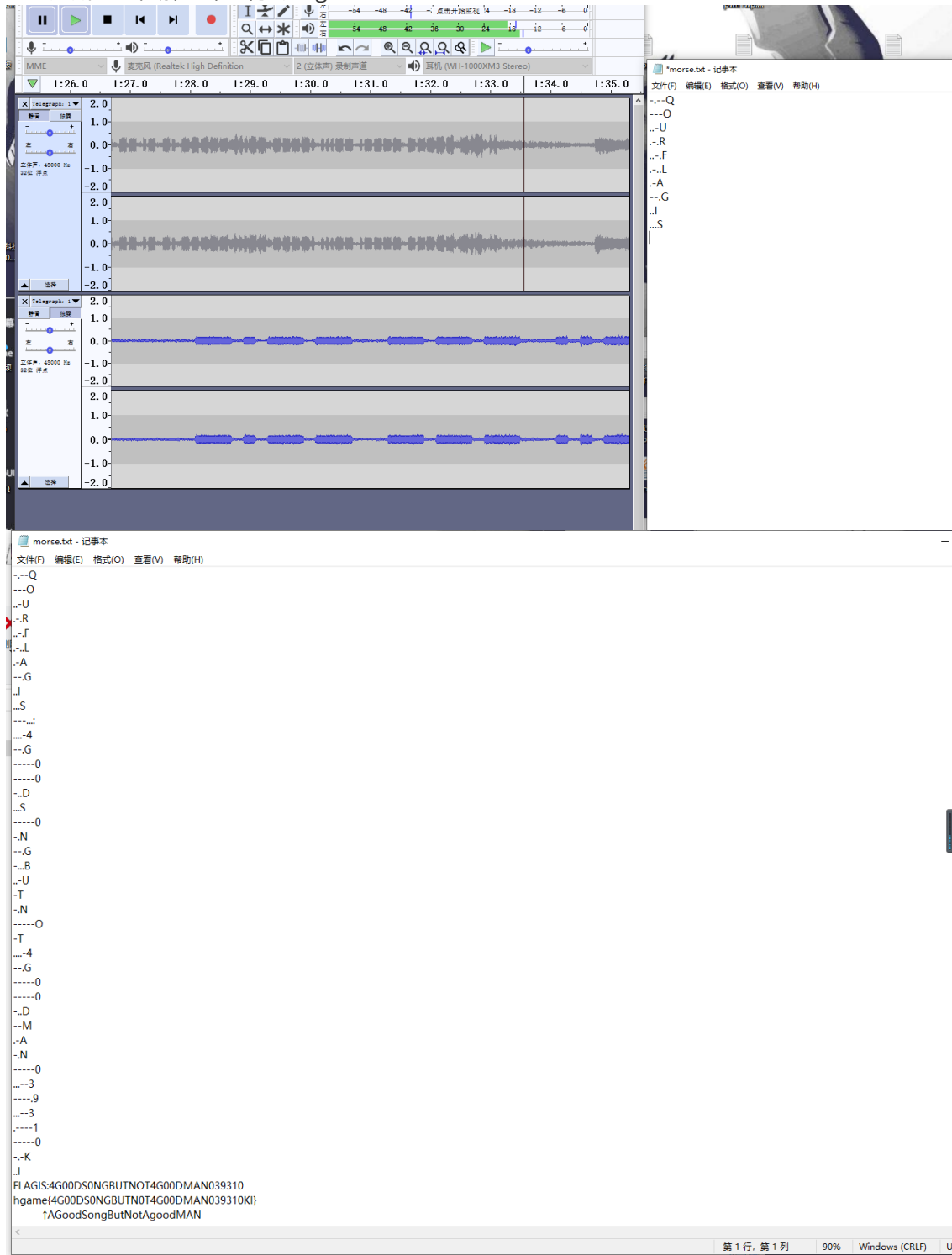
52张兑换券

7.

Telegraph: 1601 6639 3459 3134 0892

1. 打开下载的附件，发现是一个音频
2. 在1分15秒左右出现摩斯电码
3. 记录摩斯电码，解码即可得到flag

4.

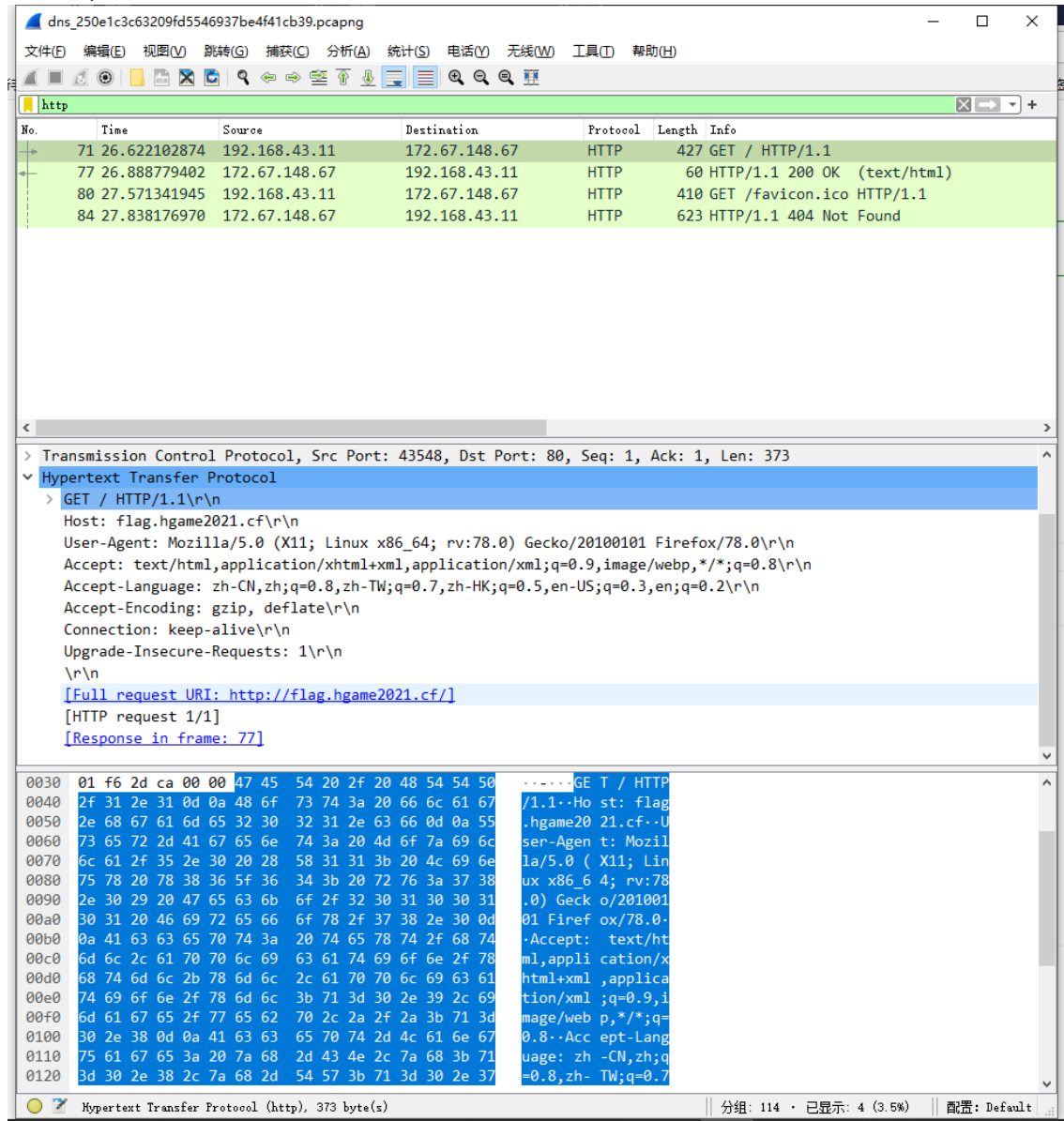


5.

DNS

1. 打开下载的附件，发现是一个流量包

2. 筛选http, 发现在某个包里有一个链接



dns_250e1c3c63209fd5546937be4f41cb39.pcapng

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

http

No.	Time	Source	Destination	Protocol	Length	Info
71	26.622102874	192.168.43.11	172.67.148.67	HTTP	427	GET / HTTP/1.1
77	26.888779402	172.67.148.67	192.168.43.11	HTTP	60	HTTP/1.1 200 OK (text/html)
80	27.571341945	192.168.43.11	172.67.148.67	HTTP	410	GET /favicon.ico HTTP/1.1
84	27.838176970	172.67.148.67	192.168.43.11	HTTP	623	HTTP/1.1 404 Not Found

> Transmission Control Protocol, Src Port: 43548, Dst Port: 80, Seq: 1, Ack: 1, Len: 373

> Hypertext Transfer Protocol

> GET / HTTP/1.1\r\n

Host: flag.hgame2021.cf\r\n

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n

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\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

\r\n

[Full request URI: <http://flag.hgame2021.cf/>]

[HTTP request 1/1]

[Response in frame: 77]

0030 01 f6 2d ca 00 00 47 45 54 20 2f 20 48 54 54 50GE T / HTTP

0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 66 6c 61 67 /1.1..Ho st: flag

0050 2e 68 67 61 6d 65 32 30 32 31 2e 63 66 0d 0a 55 .hgame20 21.cf..U

0060 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c ser-Agen t: Mozil

0070 6c 61 2f 35 2e 30 20 28 58 31 31 3b 20 4c 69 6e la/5.0 (X11; Lin

0080 75 78 20 78 38 36 5f 36 34 3b 20 72 76 3a 37 38 ux x86_6 4; rv:78

0090 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 .0) Geck o/201001

00a0 30 31 20 46 69 72 65 66 6f 78 2f 37 38 2e 30 0d 01 Firef ox/78.0-

00b0 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 -Accept: text/ht

00c0 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 ml,appli cation/x

00d0 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 html+xml ,applica

00e0 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 tion/xml ;q=0.9,i

00f0 6d 61 67 65 2f 77 65 62 70 2c 2a 2f 2a 3b 71 3d mage/web p,*/*;q=

0100 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 0.8..Acc ept-Lang

0110 75 61 67 65 3a 20 7a 68 2d 43 4e 2c 7a 68 3b 71 uage: zh -CN,zh;q

0120 3d 30 2e 38 2c 7a 68 2d 54 57 3b 71 3d 30 2e 37 =0.8,zh- TW;q=0.7

Hypertext Transfer Protocol (http), 373 byte(s) 分组: 114 · 已显示: 4 (3.5%) 配置: Default

3. 打开链接, 发现flag is here but not here

```
1 <html>
2 <head>
3 </head>
4 <body>
5 <script>
6     while(true){
7         alert("Flag is here but not here")
8     }
9 </script>
10 <b>Do you know SPF?</b>
11 </body>
12 </html>
13
```

5. 查看源码发现spf

6. 百度得到查看网页spf的方法

7.

```
PowerShell - Polars3He1
163.com nameserver = ns2.166.com
163.com nameserver = ns6.nease.net
163.com nameserver = ns5.nease.net
163.com nameserver = ns3.nease.net
163.com nameserver = ns4.nease.net
163.com nameserver = ns1.nease.net
163.com nameserver = ns8.166.com
> qq.com
服务器: 192.168.1.1
Address: 192.168.1.1
非权威应答:
qq.com text =
"v=spf1 include:spf.mail.qq.com ~all"
qq.com nameserver = ns4.qq.com
qq.com nameserver = ns1.qq.com
qq.com nameserver = ns2.qq.com
qq.com nameserver = ns3.qq.com
> flag.hgame2021.cf
服务器: 192.168.1.1
Address: 192.168.1.1
非权威应答:
flag.hgame2021.cf text =
"hgame{Domain_Name_System}"
>
```

crypto

white give rsa

1. 如题，就是白给的RSA，先算一下得到p和q的值

```
PowerShell - Polars3He1
+ CategoryInfo          : (ObjectNotFound: (yafu-x64.exe:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\MECHREVO> yafu-x64.exe
factor(882564595536224140639625987659416029426239230804614613279163)

fac: factoring 882564595536224140639625987659416029426239230804614613279163
fac: using pretesting plan: normal
fac: no tune info: using qs/gnfs crossover of 95 digits
starting SIQS on c60: 882564595536224140639625987659416029426239230804614613279163

==== sieving in progress (1 thread):   3888 relations needed ====
==== Press ctrl-c to abort and save state   ====

SIQS elapsed time = 0.0933 seconds.
Total factoring time = 0.1043 seconds

***factors found***
P30 = 857504083339712752489993810777
P31 = 1029224947942998075080348647219
ans = 1
PS C:\Users\MECHREVO>
```

2. 然后写个脚本就完事

```
1 from Crypto.Util.number import
  long_to_bytes, bytes_to_long, getPrime, isPrime
2 import primefac
3 def modinv(a,n):
4     return primefac.modinv(a,n)% n
5 #from question
6 n = 882564595536224140639625987659416029426239230804614613279163
7 e = 65537
8 c = 747831491353896780365654517748216624798517769637260742155527
9 #from yafu
10 p = 857504083339712752489993810777
11 q = 1029224947942998075080348647219
12 #calc
```

```
13 d = modinv(e, (p-1)*(q-1))
14 m = pow(c, d, n)
15 print(long_to_bytes(m))
16
17
```

```
gfp2.py  final.py  gmpy.py  jisuan1.py  jisuan2.py x  week2_cry
jisuan2.py > ...
1  from Crypto.Util.number import long_to_bytes, bytes_to_long, getPrime, isPrime
2  import primefac
3  def modinv(a, n):
4      return primefac.modinv(a, n) % n
5  #from question
6  n = 882564595536224140639625987659416029426239230804614613279163
7  e = 65537
8  c = 747831491353896780365654517748216624798517769637260742155527
9  #from yafu
10 p = 857504083339712752489993810777
11 q = 1029224947942998075080348647219
12 #calc
13 d = modinv(e, (p-1)*(q-1))
14 m = pow(c, d, n)
15 print(long_to_bytes(m))
16
17
```

问题 99 输出 调试控制台 终端

Windows PowerShell
版权所有 (C) Microsoft Corporation。保留所有权利。
尝试新的跨平台 PowerShell <https://aka.ms/pscore6>

PS C:\Code\python> & C:/Python27/python.exe c:/Code/python/jisuan2.py
ngame{w0w~yOU_kNoW+R5@!}
PS C:\Code\python>

in Tests