

HGAME 2023 Week1 writeup by lc622

HGAME 2023 Week1 writeup by lc622

MISC

Sign In

e99p1ant_want_girlfriend

神秘的海报

Where am I

Crypto

RSA

Pwn

test_nc

Web

Classic Childhood Game

MISC

Sign In

base64解码得到flag

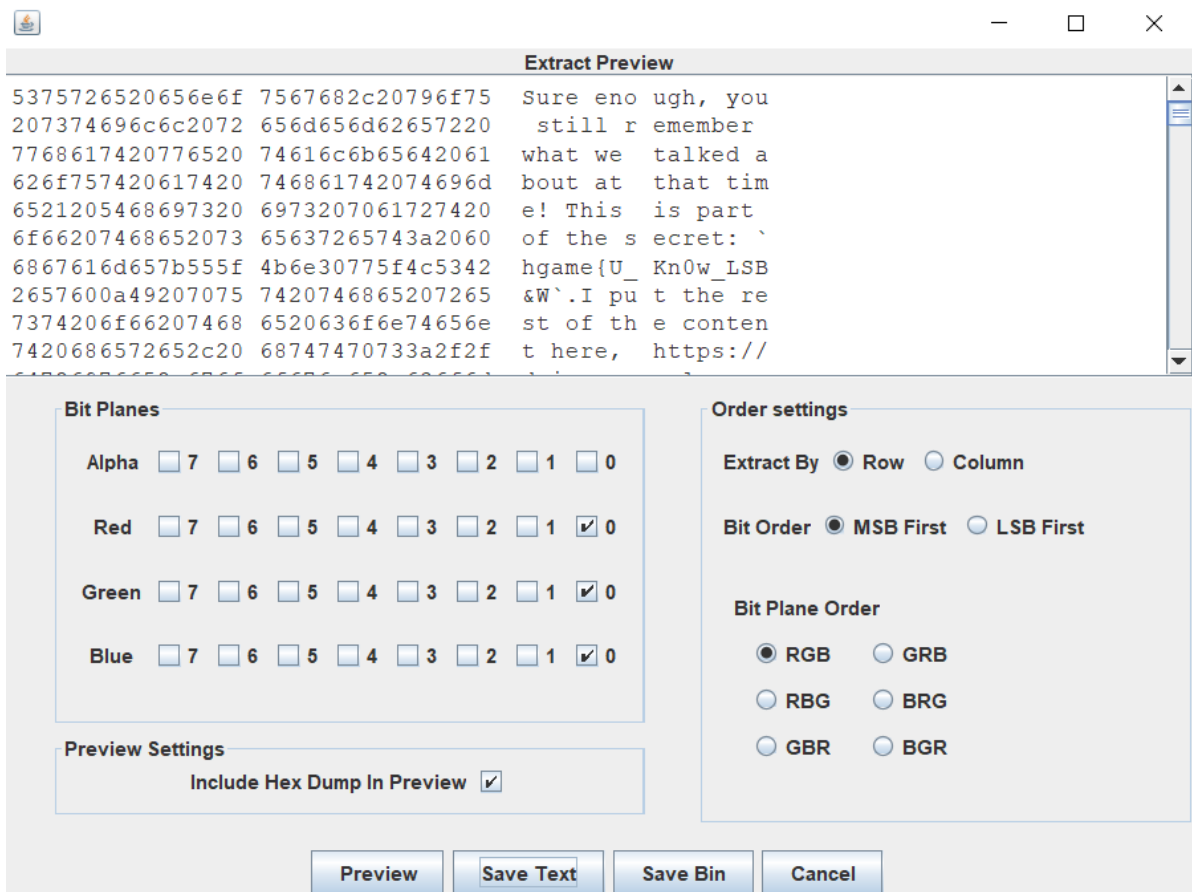
e99p1ant_want_girlfriend

题目提示CRC检验，winhex打开图片，修改图片的高度，得到flag



神秘的海报

用binwalk检查图片没有隐藏其他文件，考虑是LSB，把图片丢进stegsolve，看到一大串英文，告诉一部分flag，另外一部分在google云盘的一首歌里面，下载下来（题目提示steghide隐写）



打开kali直接steghide，但是有6位密码，询问学长，说是弱密码，于是猜测123456，得到flag.txt文件，得到剩下一部分flag

恭喜你解到这里，剩下的Flag是 av^Mp3_Stego}，我们Week2见！

Where am I

流量包分析题，打开流量包，协议分级，可以看到大部分流量都集中在TCP和http中

▼ Frame	100.0	644	100.0	261435	139 k	0	0	0	644
▼ Ethernet	100.0	644	3.5	9270	4940	0	0	0	644
> Logical-Link Control	1.4	9	0.2	429	228	0	0	0	9
▼ Internet Protocol Version 4	98.6	635	4.9	12700	6769	0	0	0	635
> User Datagram Protocol	24.7	159	0.5	1272	677	0	0	0	159
▼ Transmission Control Protocol	72.5	467	82.5	215591	114 k	196	56851	30 k	467
Transport Layer Security	4.0	26	4.3	11138	5936	26	6504	3466	28
SSH Protocol	37.6	242	55.0	143896	76 k	242	143896	76 k	242
▼ Hypertext Transfer Protocol	0.3	2	20.6	53796	28 k	0	0	0	2
MIME Multipart Media Encapsulation	0.2	1	20.4	53462	28 k	1	53462	28 k	1
Line-based text data	0.2	1	0.0	19	10	1	19	10	1
Data	0.2	1	0.0	1	0	1	1	0	1
> Internet Control Message Protocol	1.4	9	0.7	1710	911	0	0	0	9

过滤http协议，出来一对请求包，应该是这个了，可以看到返回上传成功的字样。

No.	Time	Source	Destination	Protocol	Length	Line-based text data	SSH Protocol	Info
309	9.133359	192.168.39.128	192.168.39.39	HTTP	956			POST /upload HTTP/1.1
311	9.134187	192.168.39.39	192.168.39.128	HTTP	195	✓		HTTP/1.1 201 Created (text/plain)

0150	2d 73 74 72 65 61 6d 0d 0a 0d 0a	52 61 72 21 1a	-stream· ···Rar!·
0160	07 00 cf 90 73 00 00 0d 00 00 00 00 00 00 87		···s··· ······
0170	0f 74 24 90 35 00 bc cf 00 00 0f 7d 01 00 02 74		·t\$.5··· ···}···t
0180	88 fb 9c 38 b5 24 56 1d 33 10 00 20 00 00 00 45		···8·\$V· 3·· ···E
0190	78 63 68 61 6e 67 65 61 62 6c 65 2e 6a 70 67 00		xchangea ble.jpg·
01a0	f0 67 4e 32 18 1e 15 50 c8 8e 21 c0 12 1d f3 32		·gN2···P ··!····2
01b0	48 10 d7 00 86 8a 57 44 44 46 25 15 15 1d f2 2b		H·····WD DF%····+
01c0	2d 1d 70 18 ea ad 51 2a 88 b5 ae fa ea c0 ad 51		-·p···Q* ······Q
01d0	16 a8 8b 5a a3 a2 c4 74 82 da d1 d1 6a d5 aa c5		···Z···t ····j···
01e0	aa d6 b5 5b 16 ba eb 6a 3b c5 45 aa d7 67 bf 29		···[···j ;·E··g·)
01f0	a1 42 68 e7 3b 99 92 40 b6 fe f9 fd ef e7 c5 21		·Bh·;··@ ······!
0200	93 33 b9 dc ef 79 bf bd 3e 93 e7 f8 4f 3d 7a e7		·3···y·· >···O=z·
0210	e7 39 de 77 be 79 03 cf 24 f9 bd 3c af 4f 3e 9f		·9·w·y·· \$··<·O>·
0220	f4 2c c6 e0 23 ca 2a df 6f 2a 1b d6 c1 46 17 97		·,··#··*· o*···F··
0230	b8 74 7f 09 8c 2d c4 bc 16 1a 12 f3 7f ed ee 33		·t···-··· ······3
0240	65 a5 ad ef 24 24 2f 55 bb 76 1f ad 94 ce 41 d9		e···\$\$/U ·v····A·
0250	31 59 0b e7 62 bd 74 dc 76 6f 15 ff d7 8b 95 92		1Y··b·t· vo·····
0260	33 07 e6 de 3e 6e 1e fc f8 8f a3 65 56 fa 7e 3c		3···>n·· ···eV·~<
0270	3f 3b 2f 5b 7e fb 2f 3c 5d 5b a5 d7 8b 57 b8 fb		?;/[~·/<][···W··
0280	79 df cf 1f e2 ba e1 3b 79 6c 2f 26 bb 2b 82 b9		y·····; y1/&+··

这里可以看到是rar的压缩包，直接点开这个数据，查看分组字节流，并保存下来，改成rar文件，但是打不开报错了，这里考虑到是rar的伪加密导致报错，rar用winhex打开，修改第24个字节的第二位数字，把4改成0，保存。与此同时可以看到，里面包含一个jpg文件。用binwalk分解解压文件，得到一张黑色的图片，查看详细信息，得到经纬度位置信息，拿到flag。

GPS

纬度 39; 54; 54.17999999999931
 经度 116; 24; 14.88000000000047561
 高度 0

39; 54; 54.18
 116; 24; 14.88
 0
 hgame{116_24_1488_E_39_54_5418_N}

Crypto

RSA

一道很简单的RSA，给出c,n，求m。

先利用[factordb](#)在线分解n，得到p，q。

1351271383482997573741964470626408584169203500983200999931159497190513542135455966432167395554 Factorizel

Result:		
status (2)	digits	number
FF	309 (show)	1351271383...89 <309> = 1123913498...13 <155> · 1202291266...53 <155>

More information ↗

ECM ↗

再编写py脚本，求解

```
# SUPERL LIUCHAO
# 識貳
# 开发时间: 2023/1/6 15:59
import gmpy2
import binascii

e = 65537
n = 1351271383482997573741964470626408584169203500983200999931159497190513542135455966432167395554539461960781108347263
c = 1106747926740177482432323511858960196604347183420016869065277898762649763286861341019721254939384349927870029155625
q = 1123913498780499358676355902818724505765255021951520176864477073386908818532074093845017881613839484432972331143354
p = 1202291266142094159256975173180263937508842746343016225211308261961783701091300251545022365694283637804112216383335

L = (p-1)*(q-1)
d = gmpy2.invert(e,L) # 求逆元
m = gmpy2.powmod(c,d,n) # 幂取模, 结果是 m = (c^d) mod n

print(binascii.unhexlify(hex(m)[2:]))
```

得到flag

```
L:\python\crypto\Scripts\python.exe
b'hgame{factordb.com_is_strong!}'

进程已结束, 退出代码为 0
```

Pwn

test_nc

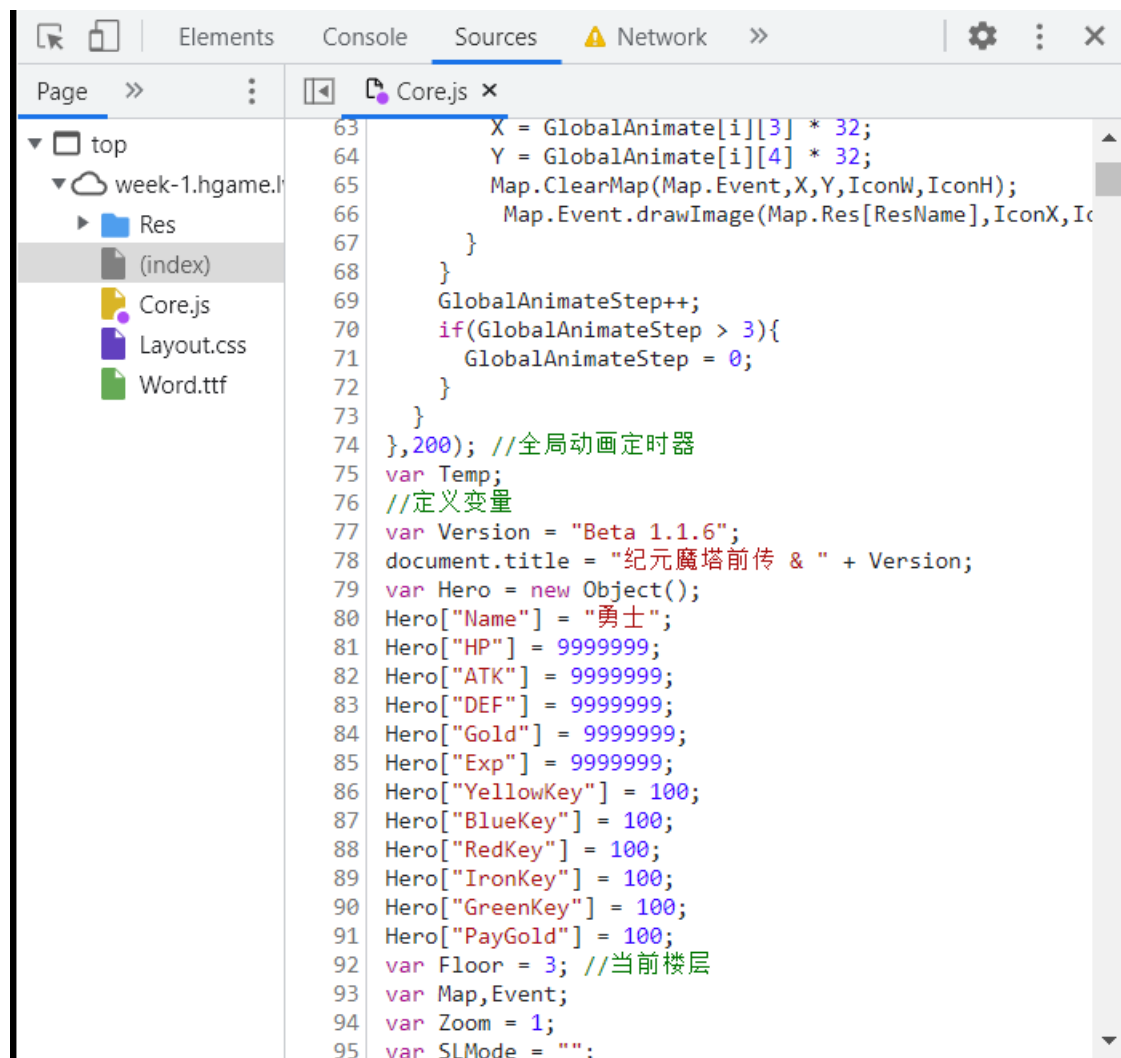
nc连接主机，ls列出看到flag文件，cat查看，得到flag。

Web

Classic Childhood Game

这一题我的思路就是，去修改js代码，因为这个游戏真的有亿点点难。

用Google浏览器打开网址，检查源代码，在sources里面，直接就看到了源码，简单判断Core.js就是整个游戏最主要最重要的代码。



```
63     X = GlobalAnimate[i][3] * 32;
64     Y = GlobalAnimate[i][4] * 32;
65     Map.ClearMap(Map.Event,X,Y,IconW,IconH);
66     Map.Event.drawImage(Map.Res[ResName],IconX,IconY);
67 }
68 }
69 GlobalAnimateStep++;
70 if(GlobalAnimateStep > 3){
71     GlobalAnimateStep = 0;
72 }
73 }
74 },200); //全局动画定时器
75 var Temp;
76 //定义变量
77 var Version = "Beta 1.1.6";
78 document.title = "纪元魔塔前传 & " + Version;
79 var Hero = new Object();
80 Hero["Name"] = "勇士";
81 Hero["HP"] = 9999999;
82 Hero["ATK"] = 9999999;
83 Hero["DEF"] = 9999999;
84 Hero["Gold"] = 9999999;
85 Hero["Exp"] = 9999999;
86 Hero["YellowKey"] = 100;
87 Hero["BlueKey"] = 100;
88 Hero["RedKey"] = 100;
89 Hero["IronKey"] = 100;
90 Hero["GreenKey"] = 100;
91 Hero["PayGold"] = 100;
92 var Floor = 3; //当前楼层
93 var Map,Event;
94 var Zoom = 1;
95 var SLMODE = "";
```

然后就是直接把里面初始的血量、攻击、经验、金币还有各种钥匙的值，直接改成9999999，然后保存，刷新网页。直接无脑通关。



