

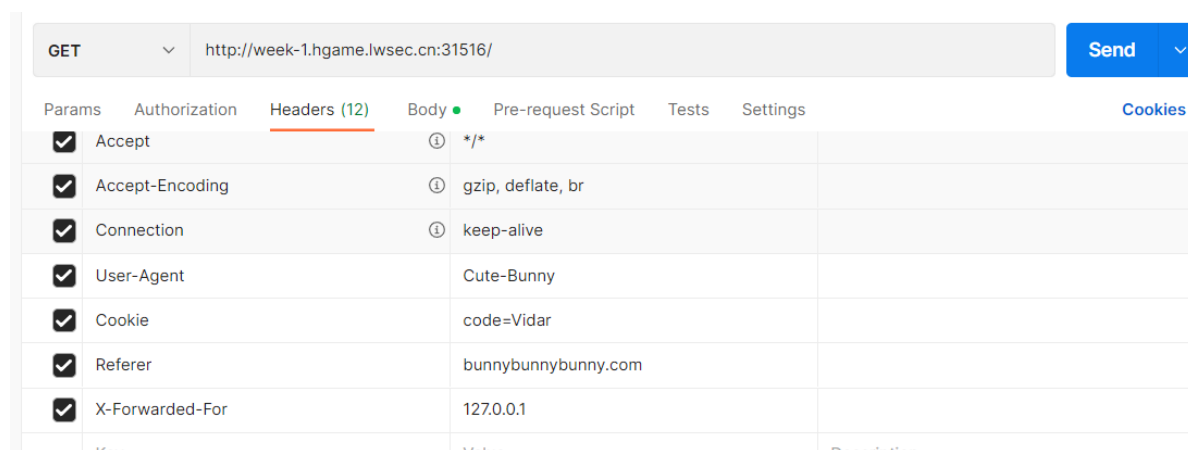
Web

Classic Childhood Game

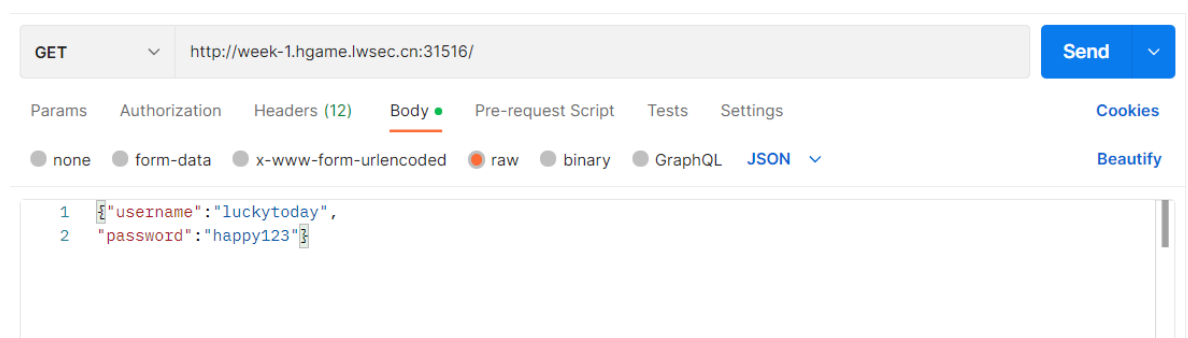
一个js小游戏,查看源码在Events.js的最后面发现一串字符串,十六进制转成明文base64两次即可得到flag



Become A Member



如图发送请求头即可,最后要发送json格式的用户名和密码



Guess Who I Am

根据/api/getQuestion和/api/Score以及/api/verifyAnswer页面

写脚本根据question找到id

```
#defalut列表是vidar成员的信息(太长就不放了,链接可下载)
#https://github.com/Potat0000/vidar-website/blob/master/src/scripts/config/member.js
```

```

url3 = 'http://week-1.hgame.lwsec.cn:32460/api/getScore'
url2 = 'http://week-1.hgame.lwsec.cn:32460/api/verifyAnswer'
url1 = 'http://week-1.hgame.lwsec.cn:32460/api/getQuestion'
cookie="session=MTY3MZA3Njk1OHxEid1CQkFFQ180SUFBukFCRUFBQU9fLUNBQU1HYzNSewFXNW5EQTBQZj0b1lxeHNAVzVvUWlVsa0EybhVhVkdQVDFQudBR2MzUn1hVzVvUREFnQUJuTnZiSFpswkFocGJuUUVBZ0FFfPjw_jL0yVzVhQ6UU5kMWAU5986JnLZt7ceOg_TM92bL"    #score=2的cookie
headers={
    "Cookie":cookie,
}

def findid(ques):    #遍历找到id
    for i in range(100):
        if(ques==default[i]['intro']):
            return default[i]['id']

while 1:
    rquestion = requests.get(url1, headers=headers)
    question = rquestion.json()['message']    #question
    print(question)
    data = {
        "id": findid(question)
    }
    answer = requests.post(url2, data=data, headers=headers)    #post id
    # print(answer.text)
    cookie = answer.headers['set-cookie']    #找到set-cookie
    # print(cookie)
    headers = {
        "Cookie": cookie,
    }
    score = requests.get(url3, headers=headers)
    print(score.text)

```

```

{"message":97}
18级 / 会一丢丢crypto / 摸鱼
{"message":98}
18级 / 莫得灵魂的开发 / 茄粉 / 作豚 / 米厨
{"message":99}
17 级 / Web
{"message":"hgame{Guess_who_i_am^Happy_Crawler}"}
20级 / web / 想学iot

```

Show Me Your Beauty

文件上传有前后端的过滤,上传jpg后抓包改为xxx.php即可

Crypto

RSA

很基础的题,套公式即可,先分解N

N分解工具

本地DB查询

factor网站查询

调用yafu.exe

终止yafu.exe

素数库去重

输入

13512713834829975737419644706264085841692035009832009999311594971905135421354559
66432167395554539461960781108347263754759817912230694513640241819528180568020895
67064926510294124594174478123216516600368334763849206942942824711531334239106807
454086389211139153023662266125937481669520771879355089997671125020789

输出

p=112391349878049935867635590281872450576525502195152017686447707338690881853207
40938450178816138394844329723311433549899499795775655921261664087997097294813
q=120229126614209415925697517318026393750884274634301622521130826196178370109130
02515450223656942836378041122163833359097910935638423464006252814266959128953

《爱我中华》+++轩禹+++CTF_RSA工具2.2 By:风二西 2022.02.12

【常 规】

【密 钥】

【模 式】

【其他攻击】

Prime(P,Q)

p=112391349878049935867635590281872450576525502195152017686447707338
69088185320740938450178816138394844329723311433549899499795775655921
261664087997097294813
q=120229126614209415925697517318026393750884274634301622521130826196
17837010913002515450223656942836378041122163833359097910935638423464
006252814266959128953

Modulus(N)

13512713834829975737419644706264085841692035009832009999311594971905
13542135455966432167395554539461960781108347263754759817912230694513
64024181952818056802089567064926510294124594174478123216516600368334
76384920694294282471153133423910680745408638921113915302366226612593
7481669520771879355089997671125020789

Public(E)

65537

Private(D)

69282117014504302108545539377738653348877086287192761340444056677290
13540875473607893814002078770007904873094997445212237270776321131123
99704069758852609042550361994960209501078277201219738409208305762310
5441255322021300555406002727516866721730033424506711203632263424560

密文(C)

11067479267401774824323235118589601966043471834200168690652778987626
49763286861341019721254939384349927870029155625004754806932973608676
81000092725583284616353543422388489208114545007138606543678040798651
83602743338328217708103415158993502429201720720905682925015221918351
8400364871109559825679273502274955582

明文(M)

hgame{factordb.com_is_strong!}

这是合数或1

+++欢迎关注bilibili:风二西+++

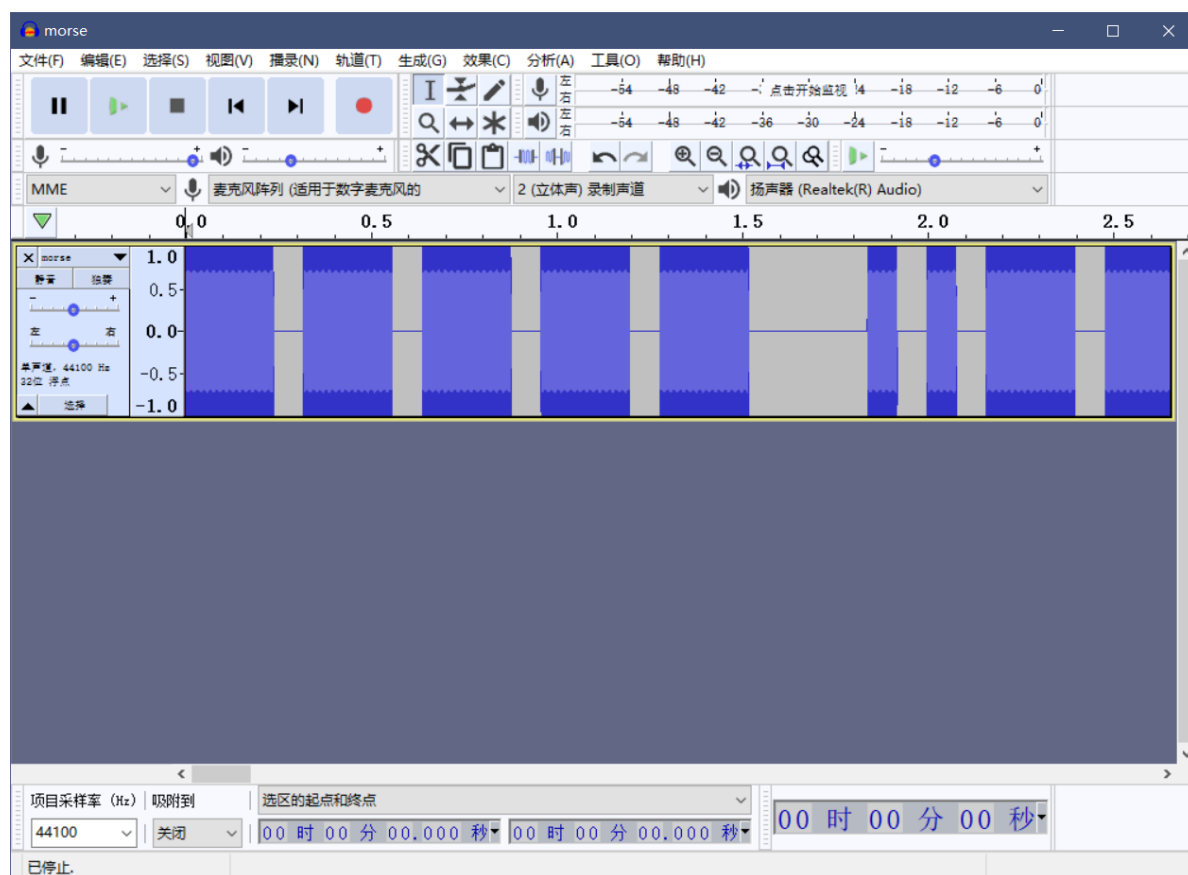
神秘的电话

附件下载后有一个base64文本,解码后是一些提示

Output time: 0ms
length: 85
lines: 1

几个星期前，我们收到一个神秘的消息。但是这个消息被重重加密，我们不知道它的真正含义是什么。唯一知道的信息是关于密钥的：“只有倒着翻过十八层的篱笆才能抵达北欧神话的终点”。

猜测是要逆向再18栏的栅栏解密



还有个音频附件,应该是摩斯密码

后来卡在北欧神话这个hint上,经出题人提示后发现是密钥vidar

From Morse Code

Letter delimiter
Space

Word delimiter
Line feed

Reverse

By
Character

Rail Fence Cipher Decode

Key
18

Offset
0

Vigenère Decode

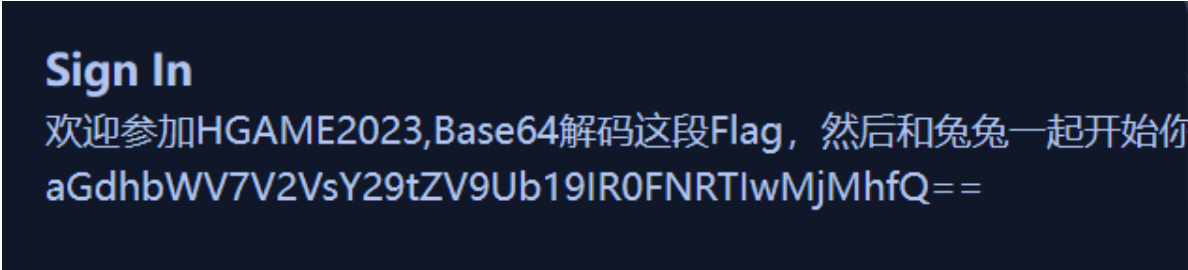
Key
vidar

Output

WELCOME_TO_HGAME2023_AND_ENJOY_HACKING

Misc

Sign In



签到,base64

Where am I

过滤http发现两个包

No.	Time	Source	Destination	Protocol	Length	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)

这里发现了rar文件的十六进制码,提取出来

▼ Data (53260 bytes)

Data: 526172211a0700cf907300000d00000000000000870f7424903500bccf00000f7d010002...

[Length: 53260]

Last boundary: \r\n-----3fe14fb0cb2bd5a4--\r\n

2d 73 74 72 65 61 6d 0d 0a 0d 0a 52 61 72 21 1a	-stream· ··Rar!·
07 00 cf 90 73 00 00 0d 00 00 00 00 00 00 87	···s··· ······
0f 74 24 90 35 00 bc cf 00 00 0f 7d 01 00 02 74	·t\$.5··· ···}··t
88 fb 9c 38 b5 24 56 1d 33 10 00 20 00 00 00 45	···8·\$V· 3·· ···E
78 63 68 61 6e 67 65 61 62 6c 65 2e 6a 70 67 00	xchangea ble.jpg·
f0 67 4e 32 18 1e 15 50 c8 8e 21 c0 12 1d f3 32	·gN2···P ··!····2
48 10 d7 00 86 8a 57 44 44 46 25 15 15 1d f2 2b	H·····WD DF%····+

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00h:	52	61	72	21	1A	07	00	CF	90	73	00	00	0D	00	00	00	Rar!...İ.s.....
10h:	00	00	00	00	87	0F	74	24	90	35	00	BC	CF	00	00	0Fİ.t\$.5.¼İ...
20h:	7D	01	00	02	74	88	FB	9C	38	B5	24	56	1D	33	10	00	}...t^ûø8μ\$V.3..
30h:	20	00	00	00	45	78	63	68	61	6E	67	65	61	62	6C	65	...Exchangeable
40h:	2E	6A	70	67	00	F0	67	4E	32	18	1E	15	50	C8	8E	21	.jpg.ðgN2...PÈŽ!
50h:	C0	12	1D	F3	32	48	10	D7	00	86	8A	57	44	44	46	25	À..ó2H.×.†ŠWDDF%
60h:	15	15	1D	F2	2B	2D	1D	70	18	EA	AD	51	2A	88	B5	AE	...ò+-..p.ê-Q*^μ@
70h:	FA	EA	C0	AD	51	16	A8	8B	5A	A3	A2	C4	74	82	DA	D1	úêÀ-Q."<ZfçÄt,ÚŇ
80h:	D1	6A	D5	AA	C5	AA	D6	B5	5B	16	BA	EB	6A	3B	C5	45	ŇjÕªÄªÖμ[.ªej;ÄE
90h:	AA	D7	67	BF	29	A1	42	68	E7	3B	99	92	40	B6	FE	F9	ª×g¿);Bhç;™'@¶pù
A0h:	FD	EF	E7	C5	21	93	33	B9	DC	EF	79	BF	BD	3E	93	E7	ýiçÄ!"3'Üiy¿½>"ç
B0h:	F8	4F	3D	7A	E7	E7	39	DE	77	BE	79	03	CF	24	F9	BD	ø0=zçç9Pw¾y.İ\$ù½
C0h:	3C	AF	4F	3E	9F	F4	2C	C6	E0	23	CA	2A	DF	6F	2A	1B	<O>Ÿô,Æà#È*Bo*.

发现打不开提示文件头损坏,结合压缩包名字fake.rar,想到伪加密

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
h:	52	61	72	21	1A	07	00	CF	90	73	00	00	0D	00	00	00	Rar!...İ.s.....
h:	00	00	00	00	87	0F	74	20	90	35	00	BC	CF	00	00	0Fİ.t\$.5.¼İ...
h:	7D	01	00	02	74	88	FB	9C	38	B5	24	56	1D	33	10	00	}...t^ûø8μ\$V.3..
h:	20	00	00	00	45	78	63	68	61	6E	67	65	61	62	6C	65	...Exchangeable

将第24字节改成0即可打开



里面是一张图片,有经纬度信息

神秘的海报

stegsolve查看图片发现有LSB隐写有一半flag,且给出了一个下载音乐附件的网站,提示是steghide隐写,stegseek一把梭爆出密码是123456,两个flag合起来即可

e99p1ant_want_girlfriend

修改图片宽高即可,一把梭