

Hgame2023 week1 wp

WEB

题目：Select Courses

做题人：R4inb0w

解题步骤：

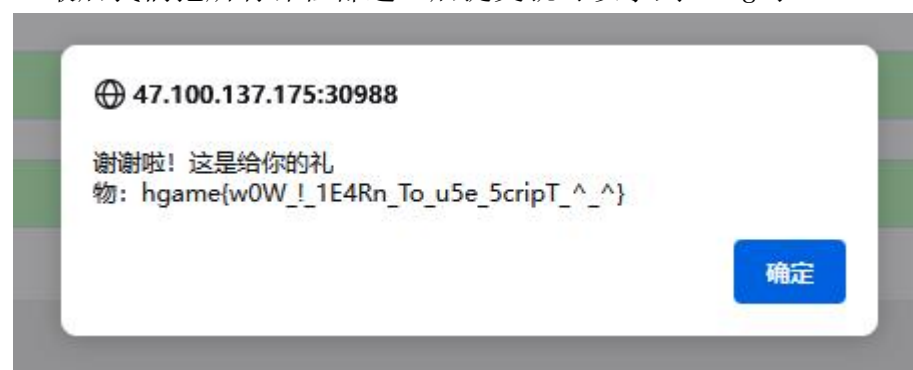
1. 一开始漫无目的的尝试没有找到有什么切入点，然后疯狂点击选课没想到成功了。然后猜想这题其实就是提交足够次数的选课就能成功的
2. 编写一个脚本用于重复提交选课信息（水平有限所以设置了点击一下提交2000次并且每次需要更改课程id号）

```
import requests
url = 'http://47.100.137.175:30988/api/courses'
data={
    "id":5
}
i=1

while i<2000:
    res = requests.post(url=url,
                        json=data)
    i+=1

print(res.text)
```

3. 最后我们把所有课程都选上后提交就可以拿到 flag 了

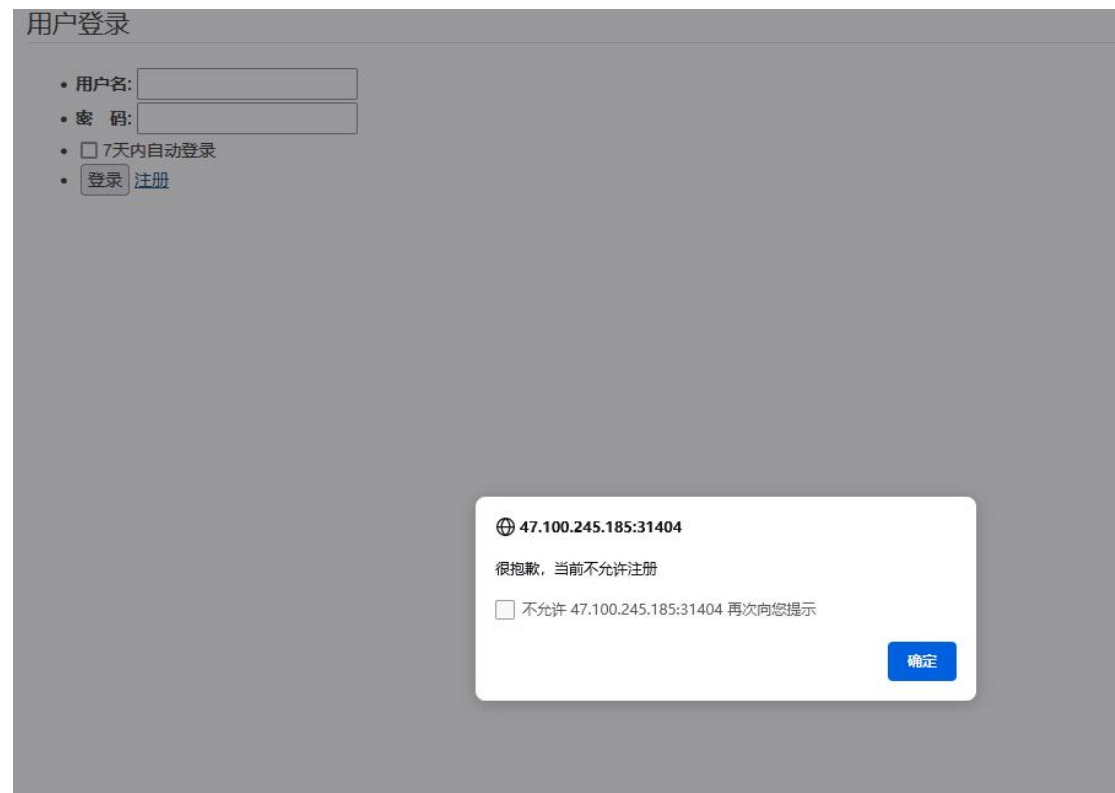


题目: Bypass it

做题人: R4inb0w

解题步骤:

1. 一开始在题目页面就提示我们这个网页需要 js 才能正常运行。



2. 在我们没有拦截 js 之前我们是进不去注册页面的。

3. 使用 web 开发者工具的拦截 js 功能后我们就可以正常的注册登录然后就拿到 flag 了

用户注册

• 用户名:

• 密码:

•

hgame{da2d367fc3377d2a7d752e93792d3d07e7f4bdf5}

题目：ezHTTP

做题人：R4inb0w

解题步骤：

1. 根据它网页给出的提示设置 http 请求头相应的信息

H	X-Real-IP: 127.0.0.1
H	Upgrade-Insecure-Requests: 1
H	Connection: keep-alive
H	Accept-Encoding: gzip, deflate
H	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
H	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
H	Host: 47.100.137.175:31116

2. 全部按照提示做完后会提示你已经给出 flag 了，经过一番搜寻后发现 flag 被藏在了 Authorization 头中用 base64 加密了，解密一下就拿到了 flag。

▼ 响应头 (326 字节) 原始

Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJGMTRnIjoiaGdhbWV7SF

RUUUF8hc18xbVAwclQ0bnR9In0.VKMdRQllG61JTReFhmbcfldq7MvJDncYpjaT7ztEDc

编码器解码器

Base64 Base32 Base58 URL HTML

{"F14g":"hgame{HTTP_!s_1mP0rT4nt}"}

MISC

题目：SignIn

做题人：R4inb0w

解题步骤：

1. 把图片丢到 word 里面拉伸一下就好了



题目: simple_attack

做题人: R4inb0w

解题步骤:

1. 解压压缩包我们可以获得一个压缩包里面的明文和一个加密的压缩包
2. 将泄露的明文用 bandzip (winrar 会有问题) 压缩成 zip 格式后丢 ARCHPR 里面跑一下就出来了
3. 然后我们得到了一段 base64 加密过后的图片源码



```
data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAB/4AAAEhCAYAAAB2sgicAAAAAXNSR0IA
AAkGAK/gEAAAAAAAAAAAAASDAS/wAAAAAAAAAAAAAAAAAJBiJfAAAAAAAAAAAAAAAAEozEPwAAAA
AAAAAAAAAACUbiHwAAAAAAAAAAAAACABCPxDwAAAAAAAAAAAAABAgpH4BwAAAAAAAAAAAAAA
nVq5c9YhtAvJD4BwAAKHJffvmlDSJxrigAAAAAXleS/rfeequ57bbb3CsAEB3t4n/ppZfMOeecY+bMmel
r6q5XgpZdeypnvRUI7Rd59911blXvvySezYx8AAAAAYk67K0eMGOGuMtrr73MDTfcYLbckkv3CgDkx:
JKBRwbbLCBjesqvqu1g+K96Yo5yvPyty/TdTSBiOIDAFck1B51xlgR7iozVft279/fdOrUyZ7rhclSrja1fb
KBxD8AAEVm8eLFZuHche4qvSBnOSEe6tevb/r27Wtefvllle0QDZz4CAAAAAAAAYeatWrXcz1BmiBgD/
YHfz40Nmgs/eqrr/41D9GYWadOHft50pi/66672s9SFOPn0qVL/54z6fOvr1fXuu9XVXbeVErzy0zKey5l
nkETvulC12TEdziRtvvLFkYr5AEKUULyilXh9xlvFfAZ/EvwYGVdY9/PDDpn///u7V8OhmUkvgl488MrETf
J6dmpXt/6N+ZyD6s/W81nPaf2dYXwGShnPdGg80vfi9ttvt2sg3ccauwuRCBTN5TWma4zUer/YxkeER+
sf6rmoTSJ6/7Q2J4FVGPPMKA6iOaovJf3VYlmdswDRfax4IRLsihvFKXYpqck9JHazLI9ixZobab1G3ARBc
kFfno2xHkXjBbzSsAMGDCAxfwqeKYjqTSuJ604CqVHzx6tO+PyLFe8SMcGxm2TSCnQZ0CfBd9ER9Wq
NjcrYJAt2/HTt2OPzDjvskHZ81t+nAJkCukoi5nlEh6psu3TpYtZdd133SmEouKOK9kwBtkKMbykvfSSu
WoKKyQgZO4TdpUaHT++ed7Bws0rqjqVc/XMMYYYPbdmzZplA6jJUTzuVgplFJN/B933HFpCxEl1mrE
3d2bTnzHdhaTZzdBWN6r3JVHyqRM/ll18eaqcaPfv1/dduimwKJiXfuy/jmvjnmY7yBJnn6/3Wmls7cPR:
l/ff6VdC90e/g4l14AkPivklKtukHLoyoqtXnUQiTsCYwCUUeo0oArQbCYuqlpWZVE+KWGZKVFZnlTyUpX
Fk6o8//uiUUEqUfFdxinZ1FSLBlajxS2OW5jo+9OzUkY35pPFEXQp96b5X8l2bYPKx7s1E3z+dkb3NNtu
mnYGnmzJl5e5YrVqROHUHPI07R168gfFJ32kdNyYDHH3/cJvB96WiDfB/DieTRRjLfzV66j7VDWc/PqCl
PfONFnW0dY+MYzdbxB3BJaWlf4jvNlno8++sj07Nkz8HiuPJUKbhjHgyFekJkKn4N0X9WGkHxsAkR+E
A6uzcs+ty89dZbgXctKMmmlok4FBf57pzVYjLsooLV26NHBLbnXEiEvi/+OPP/betQKkKOikBVRUhZf
jmloQCHiXPfY5w0nrHt6NGPmidw3EoxUtx1F69epmXXnrJvZKe1r5nnXVW3uN3xYR4gT/IUYIUI+hYIAI
h2jfNMB4DS4NsZMmnJwqgp8Xj77bcHXt+laJ2npBltoRGE5p4+8zatG5RITxLNyX029mIX7U8//eSuCk
N20EEHmSOPPNK9kp6S/1o/af6hrw/xQuK/Aqol9N25IW9RnOfis4hM0gSIWNsmaeEvVK7o8ePdo8
NPWzWtYAXHAJQ2FWoSTEYcldp8hGc68kU7pNXtSAkxFTjXq1fPJfVvvlmkvulDc1HNQY+/fTT5vjji7dE
```

4. 丢去 cyberchef 跑一下就出来了

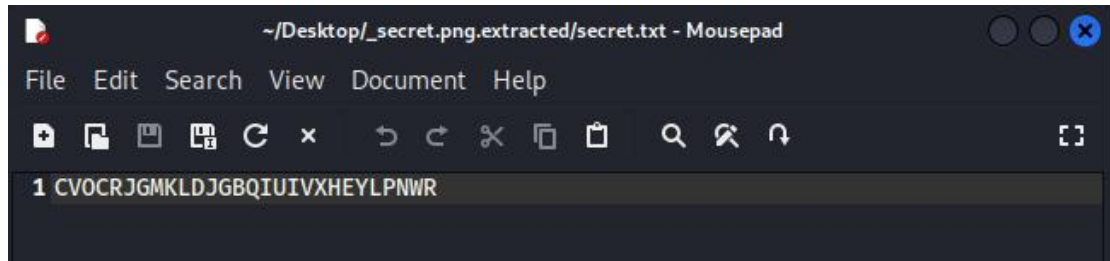
hgame{s1mple_attack_for_zip}

题目：希儿希儿希尔

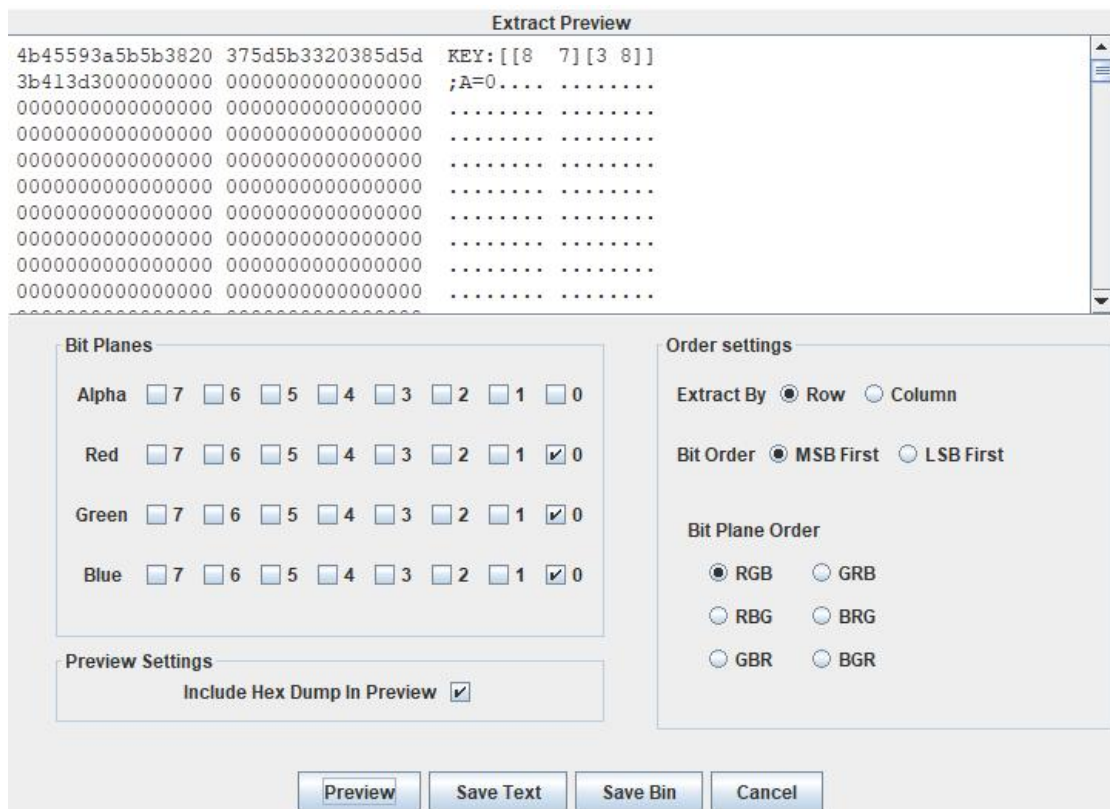
做题人：R4inb0w

解题步骤：

1. 一开始我们会得到一张打开不了的图片，将它丢到 kali 里面 binwalk 一下我们可以得到一段密文



2. 将图片的宽高修复后我们丢到 stegsolve 里面 data analysis 可以发现希尔密码对应的密钥



3. 解密得到 flag



题目：签到

做题人：R4inb0w

解题步骤：

1. 微信公众号发一下“HGAME2024”即可

PWN

题目：EzSignIn

做题人：R4inb0w

解题步骤：

1. NC 一下就好了

```
(kali@kali)-[~]  
$ nc 47.100.137.175 30614  
hgame{I_HATE_PWN}
```

REVERSE

题目：EzSignIn

做题人：R4inb0w

解题步骤：

1. 用 idapro 打开给的附件就出了

```
.data:0000000140003034 align 8  
.data:0000000140003038 aHgameW3lc0meT0 db 'hgame{W3lc0me_T0_Th3_World_of_Rev3rse!}',0  
.data:0000000140003038 ; DATA XREF: main+28fo
```

题目：ezUPX

做题人：R4inb0w

解题步骤：

1. 得到的文件先用 UPX 对他进行脱壳
2. 然后丢到 ida 里面就可以发现一连串 16 位的数字

```
.rdata:00000001400022A0 byte_1400022A0 db 64h, 78h, 76h, 73h, 60h, 49h, 65h, 5Dh, 45h, 13h, 68h  
.rdata:00000001400022A0 ; DATA XREF: main+36fo  
.rdata:00000001400022A0 db 2, 47h, 6Dh, 59h, 5Ch, 2, 45h, 6Dh, 6, 6Dh, 5Eh, 3  
.rdata:00000001400022A0 db 2 dup(46h), 5Eh, 1, 6Dh, 2, 54h, 6Dh, 67h, 62h, 6Ah  
.rdata:00000001400022A0 db 13h, 4Fh, 32h, 08h dup(0)
```

3. 将上面的结合伪代码的判断条件与 0x32 进行异或回去即可

VIDAR{Wow!Y0u_kn0w_4_l1ttl3_of_UPX!}