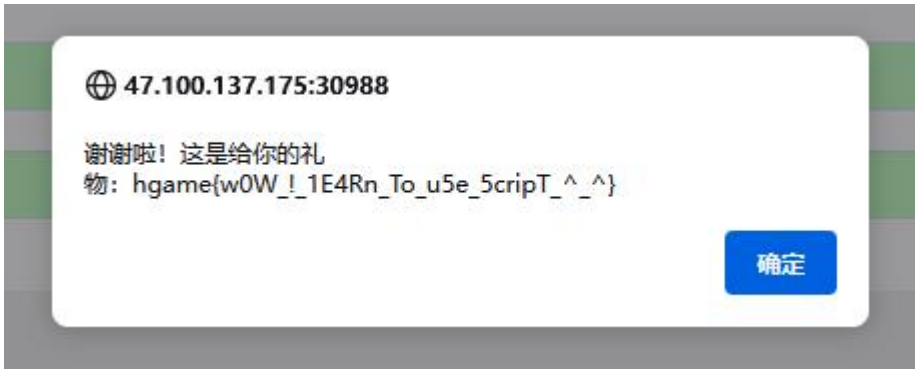
Hgame2023 week1 wp

WEB

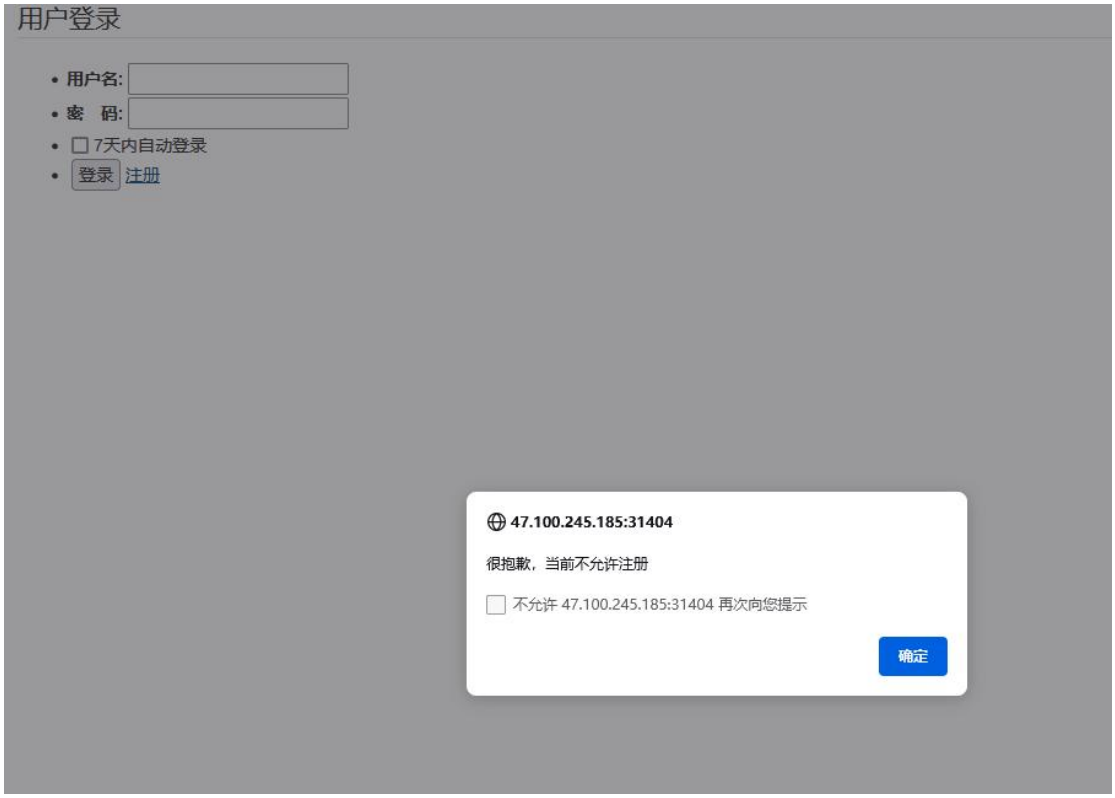
题目：Select Courses
做题人：R4inb0w
解题步骤：
1.一开始漫无目的的尝试没有找到有什么切入点，然后疯狂点击选课没想到成功了。然后猜想这题其实就是提交足够次数的选课就能成功的
2.编写一个脚本用于重复提交选课信息（水平有限所以设置了点击一下提交2000次并且每次需要更改课程id号）

```python
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)
```

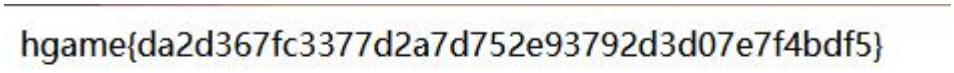
3.最后我们把所有课程都选上后提交就可以拿到flag了



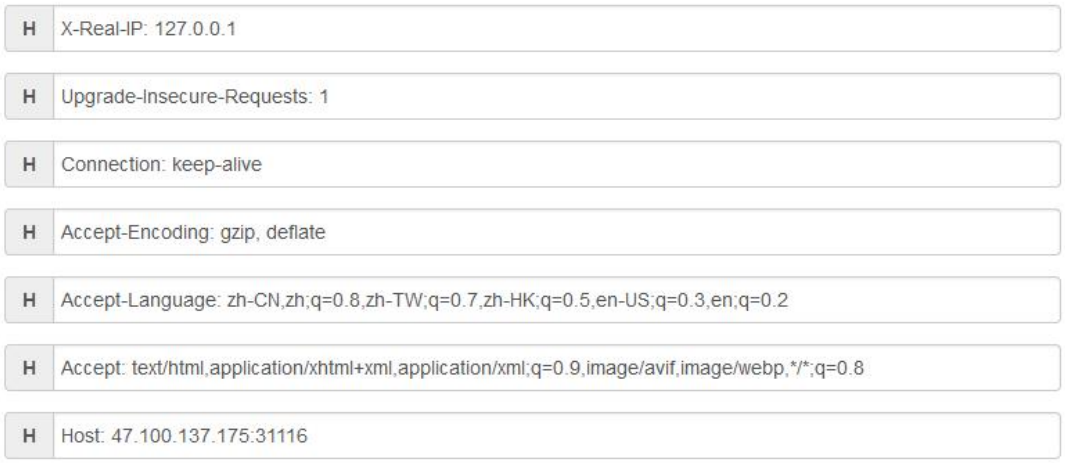
题目：Bypass it
做题人：R4inb0w
解题步骤：
1.一开始在题目页面就提示我们这个网页需要 js 才能正常运行。



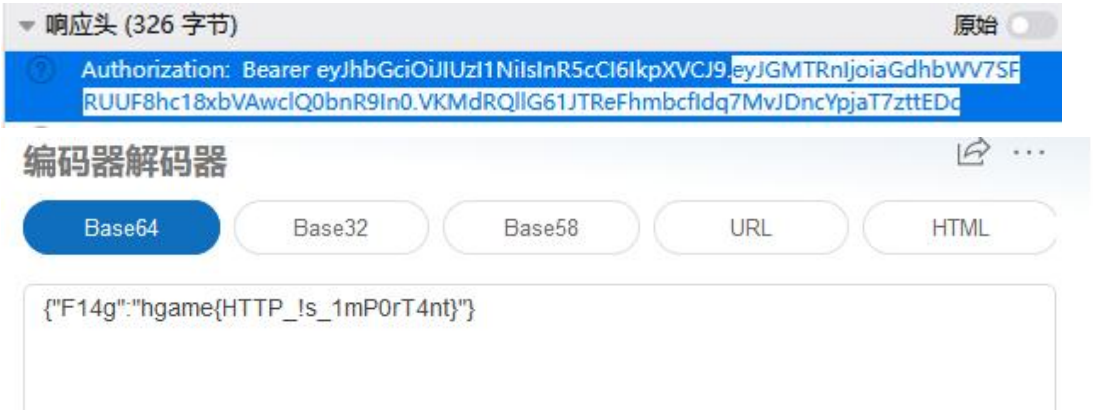
2.在我们没有拦截 js 之前我们是进不去注册页面的。
3.使用 web 开发者工具的拦截 js 功能后我们就可以正常的注册登录然后就拿到 flag 了



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



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。



MISC

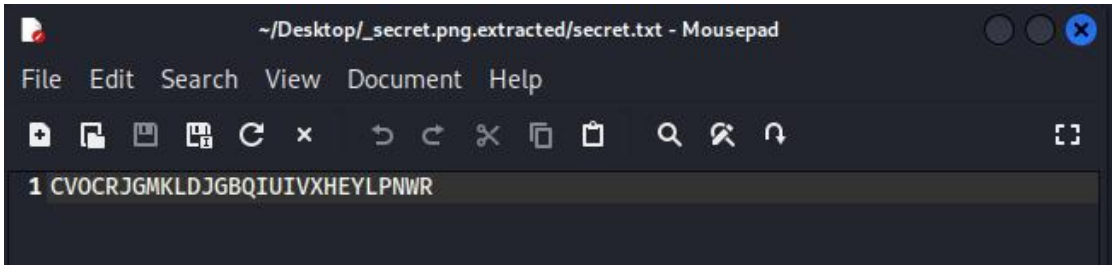
题目：SignIn
做题人：R4inb0w
解题步骤：
1.把图片丢到 word 里面拉伸一下就好了

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 ARCHRP 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

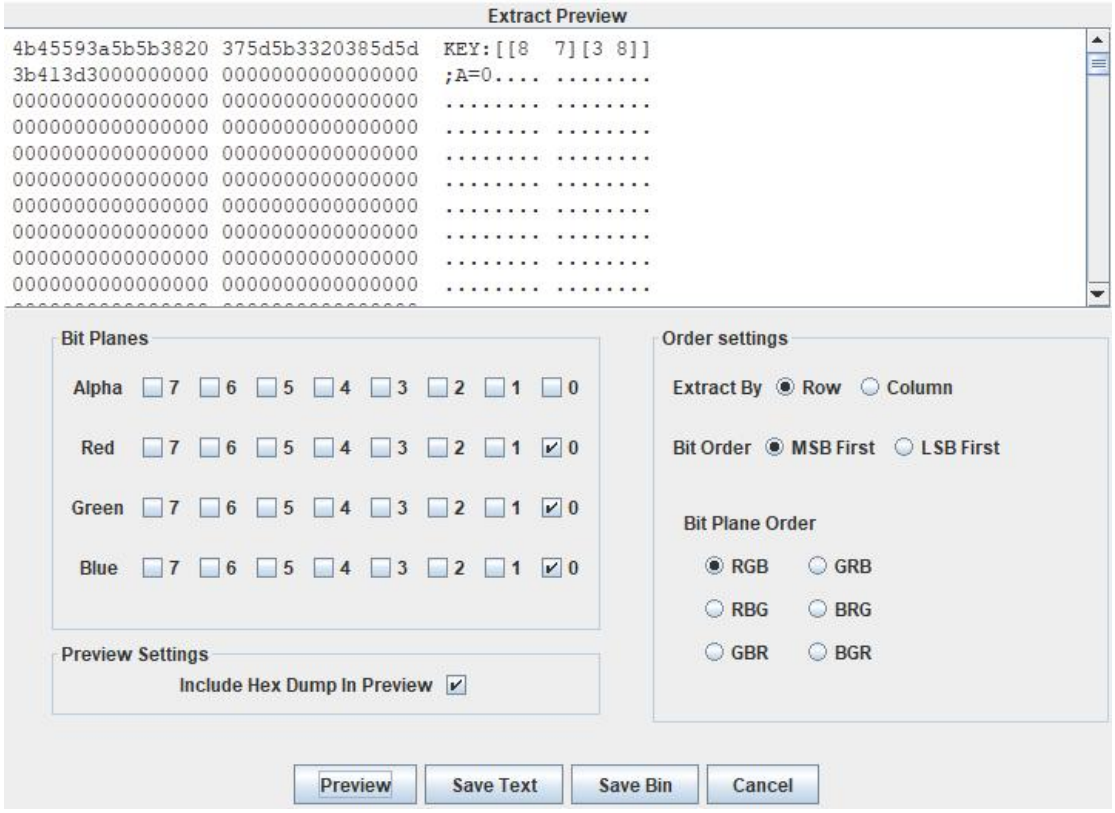
4.丢去 cyberchef 跑一下就出来了

hgame{s1mple_attack_for_zip}

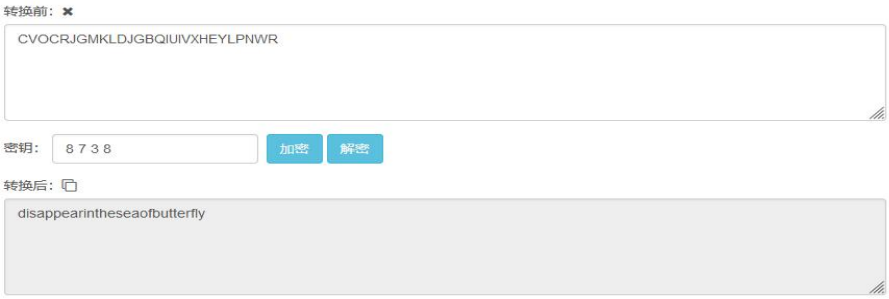
题目：希儿希儿希尔
做题人：R4inb0w
解题步骤：
1.一开始我们会得到一张打开不了的图片，将它丢到 kali 里面 binwalk 一下我们可以得到一段密文



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



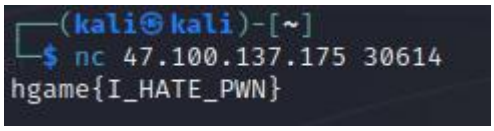
3.解密得到 flag



题目：签到
做题人：R4inb0w
解题步骤：
1.微信公众号发一下“HGAME2024”即可

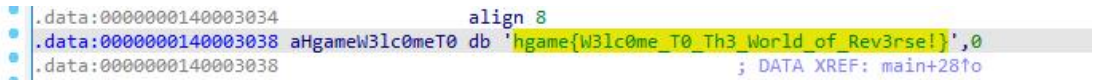
PWN

题目：EzSignIn
做题人：R4inb0w
解题步骤：
1.NC 一下就好了

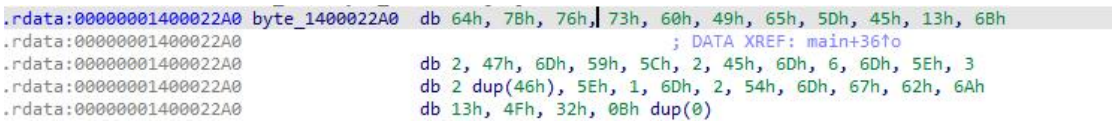


REVERSE

题目：EzSignIn
做题人：R4inb0w
解题步骤：
1.用 idapro 打开给的附件就出了



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



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