Hgame2024 week1 WP

MakaRi

1.2048*16: F12，设置为不能暂停，关闭断点，查看 js 文件，虽然被混淆了，但是还是发现包含应该是 flag 的一段字符串的关键代码

```
g[h(432)][h(469)] = function(x) {
    var n = h
      , e = x ? "game-won" : n(443)
      , t = x ? s0(n(439), "V+g5LpoEej/fy0nPNivz9SswHIhGaDOmU8CuXb72dB1xYMrZFRAl=QcTq6JkWK4t3") : n(453);
    this[n(438)][n(437)].add(e),
    this[n(438)][n(435)]("p")[-1257 * -5 + 9 * 1094 + -5377 * 3].textContent = t
  }
```

不知道我这里编辑不了前端 js，但是题目所有内容都在前端，因此直接把所有文件下载下来，自己起个服务运行，然后修改代码即可，将 x 改为 true，直接出。

2. Bypass it: 点击注册发现不行，bp 截包，发现不允许注册的弹窗处带有 js 代码将网站定向到初始页面。所以关闭 js 再进入注册页，进入后在开启 js，注册后登录即可。

3. Select Courses:写脚本抢课即可，截一下抢课的请求包内容，反复发送该包。我这里的 id 是每一次抢课成功后都手动改的。

```
import requests


# 请求的URL和头部信息
url = "http://47.102.130.35:30026/api/courses"
headers = {
    "Content-Length": "8",
    "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.51 Safari/537.36",
    "Content-Type": "application/json",
    "Accept": "*/*",
    "Origin": "http://47.102.130.35:30026",
    "Referer": "http://47.102.130.35:30026/",
    "Accept-Encoding": "gzip, deflate",
    "Accept-Language": "zh-CN,zh;q=0.9",
    "Connection": "close"
}
data = {"id": 1}
response = requests.post(url, headers=headers, json=data)
first_response = response.text
```

```
while True:
    response = requests.post(url, headers=headers, json=data)
    if response.text != first_response:
        print("已抢到")
        break
```

4. ezHTTP：加 Referer 头，改 UA 头，加 X-Real-IP 头（改 XFF 头发现不行），最后解密一下响应头里的密文就行。

5. ezASM: 原理是将用户输入的每一个字符异或之后与 flag 对比。写个脚本即可。

```
c=[74, 69, 67, 79, 71,89,99,113, 111, 125, 107, 81, 125, 107, 79,82, 18, 80, 86, 22, 76, 86, 125, 22, 125, 112,
71, 84, 17, 80, 81, 17, 95,34]
flag=''.join(chr(byte ^ 0x22) for byte in c)
print(flag)
```

6. ezUPX：用 exeinfo 查壳发现是 UPX 壳，在 kali upx -d 脱壳后放 IDA 看，F5 反编译，只有一个数组 byte_1400022A0 不知道，双击进去就知道了。

```
b=[0x64, 0x7B, 0x76, 0x73, 0x60, 0x49, 0x65, 0x5D, 0x45, 0x13, 0x6B,2, 0x47, 0x6D, 0x59, 0x5C, 2, 0x45, 0x6D,
6, 0x6D, 0x5E, 3,0x46,0x46, 0x5E, 1, 0x6D, 2, 0x54, 0x6D, 0x67, 0x62, 0x6A,0x13, 0x4F, 0x32]


def reverse_flag(ar):
    return ''.join(chr(b ^ 0x32) for b in ar)
flag = reverse_flag(b)
print("Flag:", flag)
```

7. ezIDA：文件放 IDA 里，出。

8. EzSignIn：nc 监听一下就出了。

9. SignIn：图片拉拉长，压压扁。

10. simple_attack：疑似明文攻击，先用 bandizip 压缩外面的图片，发现 CRC 一样，用 ARCHRP 解密压缩包。打开 photo.txt 发现是 base64 的图片，解密出 flag。

11.希儿希儿希尔：binwalk 解析图片发现包含了压缩包，用 foremost 分离出来发现 secret.txt，发现不是 flag。Stegsolve 解析图片，发现有效最低位有隐藏信息，鉴定为希尔密码，从网上搬个脚本，将 secret.txt 的内容作为密文，KEY 的值以 A=0 作为密钥矩阵，解出明文，验证为 flag。