# HGAME 2021 WEEK 2 WRITE UP


HGAME 2021 WEEK 2 WRITE UP
- WEB
  - Liki的生日礼物
- MISC
  - Tools
  - Telegraph：1601 6639 3459 3134 0892
  - Hallucigenia
  - DNS


# WEB

## Liki的生日礼物

注册登陆，发现余额只能购买50张兑换券；兑换switch需要52张。根据hint，这题为条件竞争漏洞。查看网页，综合分析猜测为代码逻辑漏洞，先给兑换券再扣款。使用`BurpSuite`抓取兑换的封包，右键发送至`Intruder`，并发请求，成功拿到52张兑换券。

复现时发现成功率很低，于是找到了第二种并发请求方式。打开侦听拦截封包，浏览器多次点击兑换，所有封包被拦截。点击关闭侦听，队列中的封包一起被释放，达成并发目的。此方法成功率远高于`Intruder`（可能是我方式不对）

# MISC

## Tools

下载后解压，得到`Matryoshka.jpg`和有密码的`F5.7z`。查看`Matryoshka.jpg`的文件详细信息，发现一段代码`!LyJJ9bi&M7E72*JyD`。直接作为密码或尝试解码都失败。根据压缩包名字，找到了F5隐写。将图片详细信息的代码作为密钥，从`Matryoshka.jpg`中获得隐写内容，作为密码成功解压`F5.7z`，得到`01.jpg`和`Steghide.7z`。

梅开二度，用`01.jpg`的代码、`Steghide`隐写方式获得`Steghide.7z`的密码，解压出`02.jpg`和`Outguess.7z`

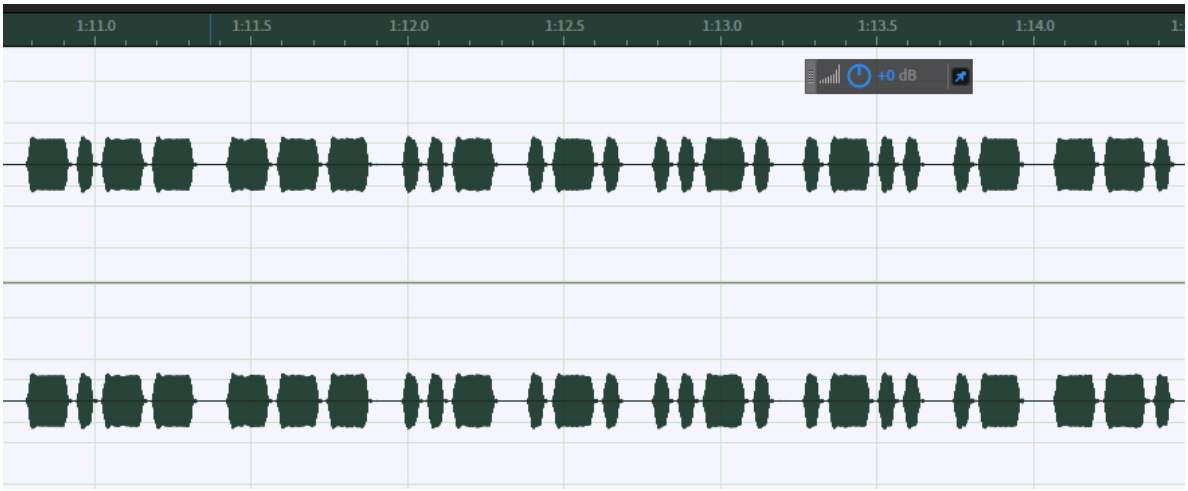
梅开三度，获得`03.jpg`和`JPHS.7z`

梅开四度，获得`04.jpg`

将`01.jpg`、`02.jpg`、`03.jpg`、`04.jpg`拼成同一张图，获得完整的二维码，扫码获得Flag。

## Telegraph：1601 6639 3459 3134 0892

听一遍音乐，发现在大约1:10-1:35有电报声；音乐频谱图中有850Hz字样。使用`Audition`科学滤波器，参数如下，获得清晰的摩斯电码波形。


（部分波形）

记录下摩斯电码

> -.-- --- ..- .-. ..-. .-.. .-- --. .. ... ---... ....- --. ----- ----- -.. ... ----- -. --. -... ..- - -. ----- - ....- --. ----- ----- -.. -- .- -. ----- ...-- ----. ...-- .---- ----- -.- ..

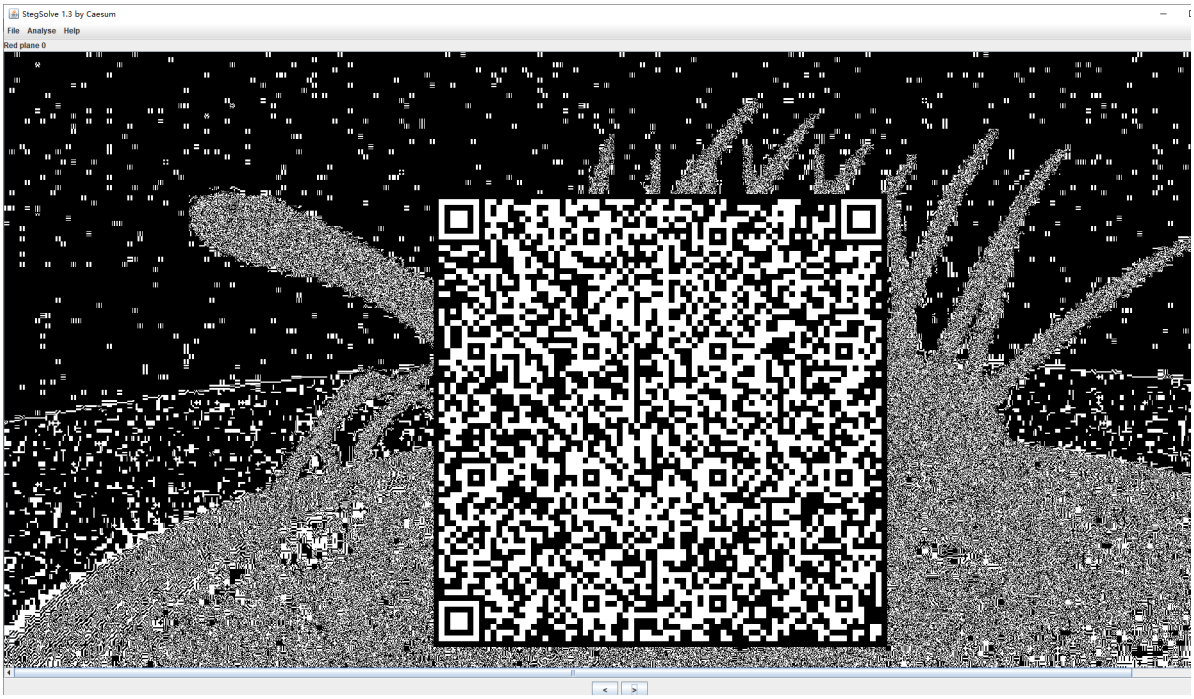
翻译后得到

> yourflagis:4g00ds0ngbutn0t4g00dman039310ki

将`：`后的文本转换为全大写，填入`hgame{ }`，成功拿到Flag

## Hallucigenia

下载图片，用Stegsolve打开，查看各图层信息。发现在`plane 0`图层有二维码。




反色处理后，扫描二维码，得到

> gmBCrkRORUkAAAAA+jrgsWajaq0BeC3IQhCEIQhCKZw1MxTzSlNKnmJpivW9IHVPrTjvkkuI3sP7bWAEdIHWCbDsGsRkZ9IUJC9AhfZFbpqrmZBtI+ZvptWC/KCPrL0gFeRPOcI2WyqjndfUWlNj+dgWpe1qSTEcdurXzMRAc5EihsEflmIN8RzuguWq61JWRQpSI51/KHHT/6/ztPZJ33SSKbieTa1C5koONbLcf9aYmsVh7RW6p3SpASnUSb3JuSvpUBKxscbyBjiOpOTq8jcdRsx5/IndXw3VgJV6iO1+6jl4gjVpWouViO6ih9ZmybSPkhaqyNUxVXpV5cYU+Xx5sQTfKystDLipmqaMhxIcgvplLqF/LWZzIS5PvwbqOvrSlNHVEYchCEIQISICSZJijwu50rRQHDyUpaF0y///p6FEDCCDFsuW7YFoVEFEST0BAACLgLOrAAAAAggUAAAAtAAAAFJESEkNAAAAChoKDUdOUIk=

这段密文极有可能经过base64加密。但许多网站提示解码失败。多次尝试后，有部分网站解码出一段乱码。

```
`BDNEI□□□□:oj□x-Â□!□B)53□JSJbi uO8□↗m`□t:욄dgЭ$/@Enm#聒ᄀ □睨¶[*ㄇZSc◆1□vᛋĀs"_b
□□뒖E
R# (qʁl')MB扜5ŝ핹t□)ㄲɹ+鎊U□8頂7□Fد
ے◆9x5iZ□ᵡ□ŭ1UzU舋|y□ᆍ-□□e. -fs!.O□꺨Эs□!□B□!"□Ib□ЏP□<tᵢD □.큨TADI=□□□□□□□□□□□□□□□□RDHI
□□□
□
```

GNP

思索再三，发现结尾为倒序的PNG，结合“我们不仅弄错了他的上下，还颠倒了它的左右。”，大胆猜测这是一段倒序的PNG文件。将解码出的内容以十六进制复制，粘贴到WinHex中、保存、打开，获得Flag图片。左右、上下颠倒后即为Flag。

## DNS

打开下载的`.pcapng`文件，根据题目提示寻找DNS封包。共有三组DNS封包，均指向`flag.hgame2021.cf`。直接访问，提示`Flag is here but not here`。查看源代码，发现注释`Do you know SPF?`。搜索SPF，发现为防晒系数。感觉不太对，调整关键词，找到查询SPF记录的方法

> 1.打开CMD/Powershell 输入nslookup
>
> 2.set type=txt

> 3.输入要查询SPF记录的域名

查询`flag.hgame2021.cf`的SPF记录，拿到Flag。