HGAME 2022 Week1 writeup by Northward

[TOC]

REVERSE

WEB

easy_auth

打开开发者工具，在login.js中发现这一段

```
if (data.code !== 2000) {
        alert(data.message)
    } else {
        localStorage.setItem("token", data.data[0].token)
        console.log(localStorage)
        window.location.href = "/"
    }
```

尝试注册了一个账号并登录后，在开发者工具的本地存储中发现token 试着用burp的编码器解码了一下，前两段内容是base64编码的，后面一段被加密

查找教程大概了解了一下JWT，然后尝试了几种网上教程里的方法，改alg头为none、用jwtcrack爆破密钥等，未果。

之后尝试在jwt头中添加 `"kid":1`，把username和id分别改为admin和1，最后用jwt.io重新生成密钥，通过burpsuit发送请求，得到flag

蜘蛛

进去点了几下，应该需要写个爬虫，但以前其实连python都没学过，临时去学了下，但大概是因为我把hgame作为关键词在查找目标，最后到了这个页面

`<h1>你这key有毒啊！</h1>`

`<p>红豆泥私密马赛，我忘记我把flag丢在哪一关了，下面有个按钮让你前往下一关，慢慢找叭~XD</p>`

`<a href="https://hgame.vidar.club/">点我试试</a>`

之后其实是看着源码手点了一百关过的……

Tetris plus

小游戏网站，试了下抓包，没东西，去看JS源码 在checking.js中发现了注释里的表达式 复制进控制台，得到flag

Fujiwara Tofu Shop

根据每一步的提示，分别将referer,User-Agent,cookie中的flavor，Gasoline改为指定内容

最后一步提示让请求从本地出发，尝试添加X-Forwarded-For:127.0.0.1，结果没有得到flag，好像也没有下一步的提示了，之后去问了学长才知道是xff被ban了 于是查了资料把分别尝试其他几种指定本地ip的头部（X-Forwarded-For， X-Forward-For， X-Remote-IP， X-Originating-IP， X-Remote-Addr， X-Client-IP ），得到了flag

MISC

压缩包

第一层没给什么提示，直接尝试爆破，成功打开

第二层给了一个字典，爆破打开

第三层通过查看CRC32确定提示文本和压缩包内的txt是相同文件，将README.txt用store方式压缩，通过ARCHPR进行明文攻击

最后得到了一张图片，试着用binwalk分析了一下，发现隐藏的压缩包，没有其他提示，猜测是伪加密，修改压缩源文件的全局方式位标记后解压成功，得到flag

好康的流量

用wireshark打开流量包，导出imf，得到eml文件，用firefoxmail打开得到龙女仆图片

根据邮件里的提示，应该是LSB隐写，用stegsolve分别查看各个通道，发现一张条形码，扫描得到flag前半部分

之后尝试用binwalk，得到了一个zlib文件，不知道怎么处理，之后问学长才知道这个应该是binwalk的识别问题，图片里没藏文件

改用zsteg，发现了后半段的flag

CRYPTO

IoT