HGAME 2021 WEEK 1 WRITE UP

WEB

Hitchhiking_in_the_Galaxy

点开网页，多次点击`我要搭顺风车!`，浏览器始终访问`index.php`；该按钮指向URL为`HitchhikerGuide.php`，猜测被跳转。

对`HitchhikerGuide.php`页面尝试GET和POST，发现POST请求后得到

> 只有使用"无限非概率引擎"(Infinite Improbability Drive)才能访问这里～

猜测应修改请求header内容。经查询和测试，发现将`User-Agent`（常用于标识用户浏览器信息）的值修改为`Infinite Improbability Drive`后返回以下内容

> 你知道吗？茄子特别要求：你得从他的Cardinal过来

经查询，HTTP常用请求头中`Referer`字段可表示用户来源

> Referer：包含一个URL，用户从该URL代表的页面出发访问当前请求的页面。提供了Request的上下文信息的服务器，告诉服务器我是从哪个链接过来的

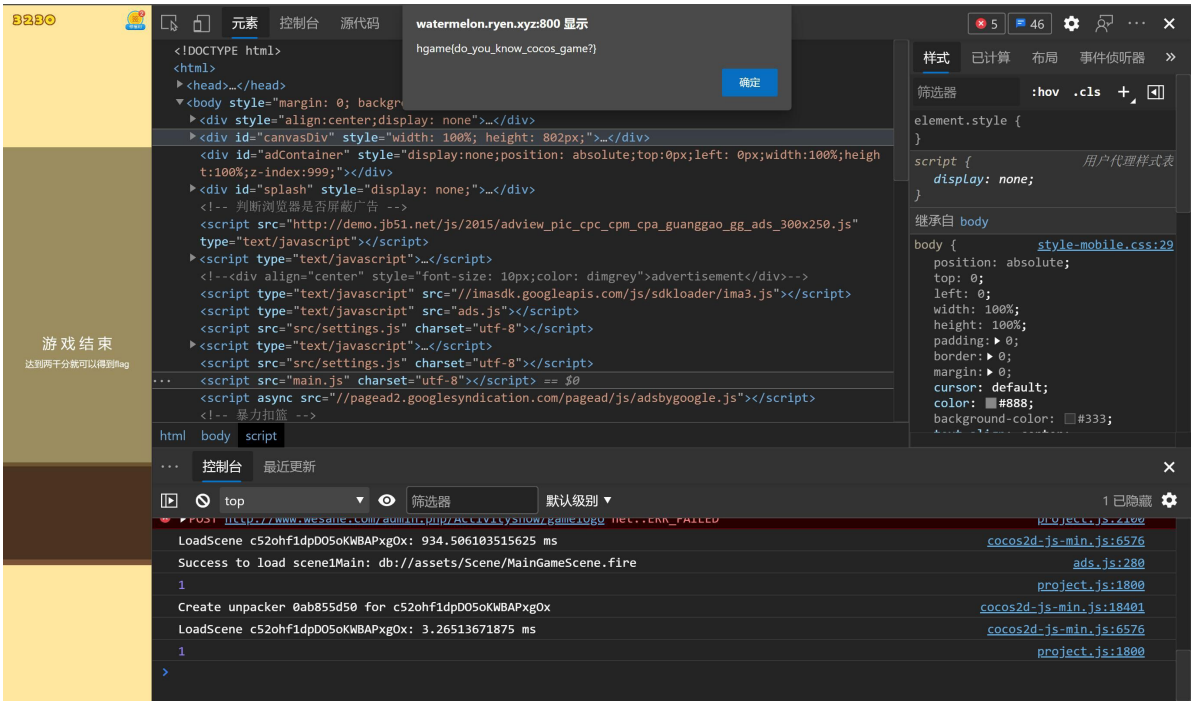
修改`Referer`的值为`https://cardinal.ink/`后，获得以下内容

> flag仅能通过本地访问获得

HTTP常用请求头中`X-Forwarded-For`字段可表示用户IP。尝试修改为127.0.0.1后，成功获得Flag

watermelon

合成大西瓜，早有耳闻第一次实操。调整浏览器，用控制台拉长游戏界面，上头亿会儿……诶怎么flag就出来了



这样偷，这样骗，我觉得不好。查询资料得知，源代码中`index/project.js`为游戏的核心代码。观察代码，发现了加分相关代码。

```
this.targetScore = e, this.scoreChangeValue = Math.abs(this.targetScore -
this.currentScore)
```

修改`scoreChangeValue`发现无效果；修改`targetScore`后，游戏界面左上角数字成功变化，但结算界面仍为原分数，未弹出Flag。修改该段代码失败，尝试寻找结算界面相关代码，发现如下：

```
update: function (e) {
                this.gameOverGoToOVer()
            },
            gameOverGoToOVer: function () {
                this.gameOveEndBool && (this.gameOverNum++, this.gameOverNum >=
900 && (this.gameOverNum = 0, this.gameOveEndBool = !1))
            },
            SetScore: function (e) {
                o.gameScore = e
            },
            RestartGame: function () {
                o.GAME_OVER_BOOL = !0, o.gameScore = 0, o.publicGameBool ||
adBreak({
                    type: "next",
                    name: "restart-game"
                }), c.loadingScene("MainGameScene")
            },
            SetGameEndScore: function () {
                a.gameOverShowText(o.gameScore, 1)
            },
            GetGameEndInfo: function () {
                return a.endHttpShowInfo
            }
```

修改`o.gameScore`为9999，再次进行游戏，结束后成功弹出Flag.

智商检测鸡

是我讨厌的高数。

> (积分式全部为ax+b的形式)，可以方便的写出定积分公式。写一个python脚本，获取积分上下限、积分式，并自动提交。

我如是想

> 掏出手机，打开微软数学，选择扫描。对准屏幕拍照，约5s后得到结果。重复以上过程100次，总用时小于30分钟。

我如是做

MISC

Base全家福

> 新年即将来临之际，Base家族也团聚了，他们用他们特有的打招呼方式向你问了个好，你知道他们在说什么吗?
> R1k0RE1OWldHRTNFSU5SVkc1QkRLTlpXR1VaVENOUlRHTVlETVJCV0dVMlVNTlpVR01ZREtSUlVIQTJET01aVUdSQ0RHTVpWSVlaVEVNWlFHTVpER01KWElRPT09PT09

一段编码，大小写字母、数字都有。结合`Base全家福`，应该是Base64没错了。解码后得到

> GY4DMNZWGE3EINRVG5BDKNZWGUZTCNRTGMYDMRBWGU2UMNZUGMYDKRRUHA2DOMZUGRCDGMZVIYZTEMZQGMZDGMJXIQ======

只剩大写字母和数字了，结尾还有多个`=`。尝试Base32，得到

> 6867616D657B57653163306D655F74305F4847344D335F323032317D

字母只剩D和F了，估计是Base16编码，解码后成功得到Flag

不起眼压缩包的养成的方法

下载文件，是一张JPG格式的图片。用二进制查看器打开，在文件末尾发现`NO PASSWORD.txt`和`plain.zip`字样。结合标题，应该是利用JPG文件结构，把图片和压缩包数据叠加的隐写方式。将图片后缀改为`zip`，成功打开压缩包。

发现压缩包有密码，压缩包注释如下

> Password is picture ID (Up to 8 digits)

研究了好久`picture ID`为何物，最终决定暴力破解。最多八位数字，几秒钟搞定。解压后发现`plain.zip`也是加密压缩包，内有`NO PASSWORD.txt`和`flag.zip`

查询资料后，发现两个`NO PASSWORD.txt`原大小一致，大概率采用明文攻击方式破解密码。尝试将`NO PASSWORD.txt`以相同方式加密。尝试Bandizip中所有加密方式，均不同。查询后，使用7zip工具，逐个尝试，发现为BZip2压缩方法。使用ARCHPR工具进行明文破解，得到`plain.zip`压缩包密码，解压。

不出所料，`flag.zip`仍为加密压缩包。经尝试，该压缩包是伪加密。使用`ZipCenOp`，成功解压`flag.zip`，拿到Flag。

Galaxy

下载文件，用Wireshark打开，查看HTTP包。

```
HTTP        460 GET /galaxy.png HTTP/1.1
HTTP      30233 HTTP/1.1 200 OK  (PNG)
HTTP       1105 GET /i?tn=baiduimage&ps=1&ct=201326592&lm=-1&cl=2&nc=1&ie=utf-8&word=galaxy+wallpape
HTTP        469 HTTP/1.1 301 Moved Permanently  (text/html)
HTTP       1167 GET /search/index?tn=baiduimage&ps=1&ct=201326592&lm=-1&cl=2&nc=1&ie=utf-8&word=gala
HTTP        491 HTTP/1.1 301 Moved Permanently  (text/html)
```

结合题干，这个`galaxy.png`应该就是我们要找的。右键 - 追踪流 - TCP流，发现下方有PNG图片文件的文件头`.PNG`。大概率对了，另存这段内容，用WinHex删除HTTP包的信息后，发现无法打开。仔细观察文件的二进制内容与Wireshark中不吻合。多次尝试后，发现将内容以二进制方式复制（`Copy as Raw Binary`），粘贴到WinHex中，保存。成功得到PNG图片。

修改PNG图片二进制信息，调大尺寸，发现原图片下方即为Flag。