Week1

Web

Hitchhiking_in_the_Galaxy

2021版的**接头霸王**

要你自定义请求方式为`POST`

User-Agent为`Infinite Improbability Drive`

Referer为`https://cardinal.ink/`

X-Forwarded-For为`localhost`

最后的http请求为：

```
POST /HitchhikerGuide.php HTTP/1.1
Host: 5a2b415114.hitchhiker42.0727.site:42420
User-Agent: Infinite Improbability Drive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: https://cardinal.ink/
Upgrade-Insecure-Requests: 1
X-Forwarded-For:localhost
```

用Burpsuite抓包再改或者直接发包就行了。

得到flag：`hgame{s3Cret_0f_HitCHhiking_in_the_GAl@xy_i5_dOnT_p@nic!}`

watermelon

F12，改掉property.js里的一句话

```
a.default.score += this.fruitNumber + 1
//改为下面的
a.default.score += this.fruitNumber + 1000
```

然后努力输掉这个游戏就可以了。

flag弹窗获得：`hgame{do_you_know_cocos_game?}`

Misc

Base全家福

```
R1k0RE1OWldHRTNFSU5SVkc1QkRLTlpXR1VaVENOUlRHTVlETVJCV0dVMlVNTlpVR01ZREtSUlVIQTJE
T01aVUdSQ0RHTVpWSVlaVEVNWlFHTVpER01KWElRPT09PT09
```

这玩意 先 Base64解码 再Base32解码 再Base16解码就能得到flag：`hgame{We1c0me_t0_HG4M3_2021}`

不起眼的压缩包的养成的方法

图片是图种，后缀名改成zip，密码是70415155（网上去搜图）

解压得到一个NO PASSWORD.txt 和 一个有密码压缩包

把txt用7zip纯Store方法压缩成zip，然后用ARCHPR明文攻击得flag.zip

直接丢HxD或者WinHex可以看到

```
&#x68;&#x67;&#x61;&#x6D;&#x65;&#x7B;&#x32;&#x49;&#x50;&#x5F;&#x69;&#x73;&#x5F;&#
x55;&#x73;&#x65;&#x66;&#x75;&#x31;&#x5F;&#x61;&#x6E;&#x64;&#x5F;&#x4D;&#x65;&#x3
9;&#x75;&#x6D;&#x69;&#x5F;&#x69;&#x35;&#x5F;&#x57;&#x30;&#x72;&#x31;&#x64;&#x7D;
```

把它去掉无关字符可以得到：

```
6867616D657B3249505F69735F5573656675315F616E645F4D6539756D695F69355F57307231647D
```

16进制转字符，得到flag：`hgame{2IP_is_Usefu1_and_Me9umi_i5_W0r1d}`