Hgame 2021-Writeup-Week1

Web

1.Hitchhiking_in_the_Galaxy
描述
第一次在银河系里搭顺风车，要准备啥，在线等，挺急的

题目地址
http://hitchhiker42.0727.site:42420

解题步骤
打开链接，点击”我要搭顺风车”，发现网页没有变化，通过 f12 发现是跳转至
http://hitchhiker42.0727.site:42420/HitchhikerGuide.php

后被重定向至
http://hitchhiker42.0727.site:42420/index.php

在命令行中使用 curl 命令查看，发现 hint

将请求改为 POST 方法，后显示

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

尝试将 ua 改为 Infinite Improbability Drive ，后显示

你知道吗？茄子特别要求：你得从他的Cardinal过来

查询资料，将 Referer 一项改为：
Referer:https://cardinal.ink

显示如下：

flag仅能通过本地访问获得

此时添加 X-Forward-For:127.0.0.1
来是服务器认为我们在本地访问，得到 flag：
hgame{s3Cret_0f_HitCHhiking_in_the_GAl@xy_i5_dOnT_p@nic!}

收获：初步了解了关于 http 请求 的一些基础知识

2.watermelon
描述

简单且上头的游戏
题目地址
http://watermelon.ryen.xyz:800/

解题步骤
玩了一次大西瓜之后发现打到两千分即可获取 flag，既然能玩那为什么还要做呢（bushi
查看源文件后发现，游戏的主要代码存在于 ***project.js*** 中，游戏分数的存储变量是 ***a.default.score*** 将 ***project.js*** 下载至本地，将 ***a.default.score*** 变量赋初值为 666666
通过 Chrome 浏览器插件 ReRes 拦截原 js 并替换为修改后的 ***project.js***
开了金手指就能愉快的玩耍了

3.宝藏走私者
描述

hint: 注意留意服务器信息

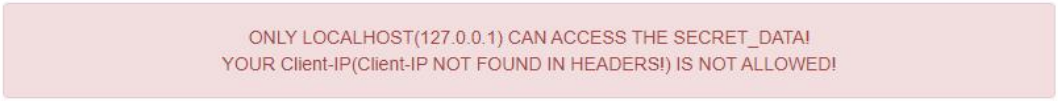
资料：https://paper.seebug.org/1048/

宝藏走私者 Switch 喜欢偷盗并将奇特的宝藏走私到一些黑市商家手中。
为了阻止其继续作恶，警探 Liki 奉命将 Switch 抓捕归案。
调查过程中，Liki 发现 Switch 将一个秘密藏在了一个私人服务器中。
这或许会成为后续追查 Switch 的重大线索，你能找到这个秘密吗？

题目地址
http://thief.0727.site:80

解题步骤

本题出现非预期状况，原本的考点为 http 走私 ，
进入秘密服务器，提示



通过 Client-Ip: 127.0.0.1 伪造后得到 flag，但由于
这是非预期的方法，在写 writeup 时已经无法复现

修复后的题目为第五题

4.智商检测鸡

描述
又有谁不爱高数呢？反正我不爱（请使用 firefox 浏览器打开题目）

题目地址
http://r4u.top:5000/

我爱高数，我写了 100 道，是男人就来写定积分，格式都一样（学长别锤我）

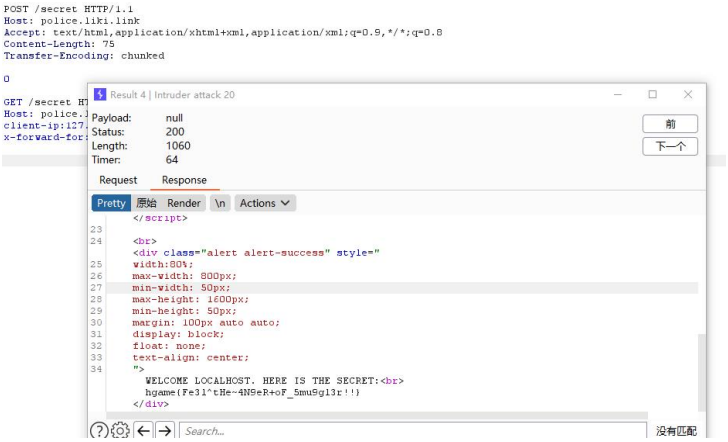
5.走私者的愤怒
描述

本题为宝藏走私者的更改版本，考点相同，请先做出宝藏走私者

Liki 日记：
2020 年 2 月 2 日：
今天警局寄来一封信，是走私者 Switch 寄来的，信里只有一句话
“我最讨厌顺风车，我将带来我的愤怒”
真是让人摸不着头脑……
我看不懂，但我大受震撼。

题目地址
http://police.liki.link

解题步骤：构造一个 http 走私数据包（本人构造存在问题，大概十出一，抽卡非酋），但 Liki 说很稳定



MISC

1 Base 全家福

描述
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

本次比赛为招新赛，请各位选手不要在当周比赛进行期间至结束后 24 小时内发布当周比赛题目的 writeup

解答：
base64，base32，base16 三次解密

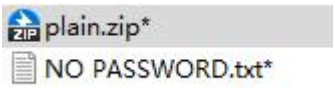
2.不起眼压缩包的养成的方法

描述
0x4qE 给了张图给我，说这图暗藏玄机，你能帮我找出来吗？

题目地址
https://1.oss.hgame2021.vidar.club/0x4qE_112d64bd3834986084be726095957b5d.jpg

一张加藤惠的图片

题目名中含关键字 压缩包
扔进 foremost，分离出照片和一个压缩包
内含两个加密文件

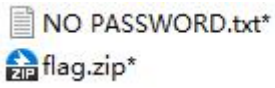


注释如下

Picture ID+二次元图片=Pixiv
在 P 站搜图后获得 id：70415155

解压后获得这两个文件

打开 plain.zip



发现里面存在与之前得到的文件同名的 txt 文件，两个文件的 crc 校验值相同。且压缩包文件名为 plain ，这是一个 hint ，提示我们本题将会用到 zip 明文攻击 。
将先前得到的 NO PASSWORD.txt 以存储方式压缩为同名 zip 文件，使用 AZPR 软件进行明文攻击。

获得密码：C8uvP$DP

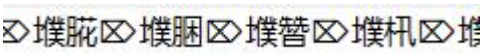
Akira 学长 提供的补充资料：https://www.freebuf.com/articles/network/255145.html

解压后获得 flag.zip

除了之前的文本文件名为 NO PASSWORD ，本题没有其他的提示，要么暴力跑字典，要么就是伪加密。显然后者可能性极大

使用 Hxd 软件将 全局方式位标记 改为 00 00 后保存、解压未出错，得到 flag.txt

打开后是乱码



可能是编码方式不对，在 Hxd 中打开后如右图所示
是熟悉的 ascii 码，转换一下得到 flag

```
&#x68;&#x67;&#x6
1;&#x6D;&#x65;&#
x7B;&#x32;&#x49;
&#x50;&#x5F;&#x6
9;&#x73;&#x5F;&#
x55;&#x73;&#x65;
&#x66;&#x75;&#x3
1;&#x5F;&#x61;&#
x6E;&#x64;&#x5F;
&#x4D;&#x65;&#x3
9;&#x75;&#x6D;&#
x69;&#x5F;&#x69;
&#x35;&#x5F;&#x5
7;&#x30;&#x72;&#
x31;&#x64;&#x7D;
```

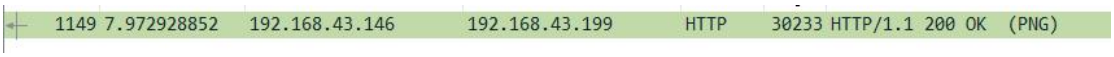
hgame{2IP_is_Usefu1_and_Me9umi_i5_W0r1d}

3 Galaxy

描述
Akira 的信物：用于提升 Akira 的潜能。一张藏着秘密的星空壁纸，不幸的是似乎在某次行动
中遗失了。

题目地址
https://1.oss.hgame2021.vidar.club/galaxy_a123bd9c2edcc8439575cacdf2afe352.pcapng

解题步骤
Google 了 pcapng 格式，发现是 Wireshark 软件所捕获信息的存储文件。
将其打开。根据题目，我们所要找的是一张图片，搜索常用的几种格式，发现其中藏有一个 png 文件



将分组字节流导出为 **Galaxy.png**

在使用 Quicklook 查看该文件的时候出现了问题，但是 Windows 的 看图 应用可以正常打开，怀疑是该图片的长宽遭到了修改导致图片显示不正常，有一部分被隐藏。
使用 HxD 修改 png 图片的长宽信息

图片底部藏有 flag（l 和 1 傻傻分不清楚）

4．Word RE:MASTER

描述

timmix 不知所踪，只留下了两个 word 文档，作为 word 专家的你能帮忙找出他的去向吗？

题目地址

https://1.oss.hgame2021.vidar.club/Word_REMASTER_e3c365a2c0edb60fbb7152279a31dafd.zip

解题步骤

解压后获得两个文档

其中 first.docx 未加密

但是其中没有有效的信息，只有音游人的 brainpower

了解到 docx 格式类似于一个压缩包

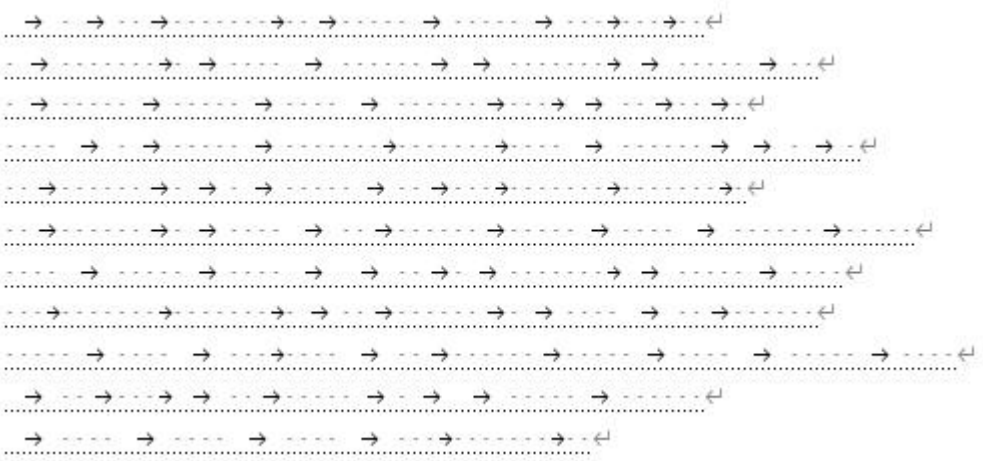
将其后缀名改为 .zip 后发现里面有一个 password.xml

获得 maimai.docx 的密码：

DOYOUKNOWHIDDEN?

打开后只有一张截图

结合上一步的密码，可能存在隐藏文字，在 word 的设置中开启显示隐藏的选项



一开始以为是 摩斯电码 或者是 whitespace 编程语言 ， 但是两个可能性都是错的。后来问了出题的 Akira 学长，hint 是“图片中出现最多的汉字翻译成英文” 百度没有结果，Google 后发现是 Snow 加密 。解密后获得 flag

```
C:\Users\11792\Desktop\snow>snow.exe -C 1.txt
hgame{Challen9e_Whit3_P4ND0R4_P4R4D0XXX}
C:\Users\11792\Desktop\snow>
```

Crypto

1. まひと

描述

hint: flag 的格式为 hgame{xxx}（重要）

大家好，我叫真人，来自咒术回战，你也可以叫我，缝合怪!!

题目地址 https://mix.liki.link

下载文件后打开，摩斯密码解密——ascii 码转字符——base64 解密——维吉尼亚密码秘钥 Liki 解密——栅栏密码每组字数 6 解密——凯撒密码位移 13 解密——编写脚本反序输出

```
}!!Pu~X1m+YhpAr90TpyRc_laC1sS4Lc{emagh
hgame{cL4Ss1Cal_cRypTO9rAphY+m1X~uP!!}
```