

Hgame-Vidar 2021 week1


20-啥也不会-小九

Web

顺风车

发现“我要搭顺风车”指向的地址和实际跳转的地址并不相同

hitchhiker42.0727.site:42420/HitchhikerGuide.php

 hitchhiker42.0727.site:42420/index.php

用 Burp Suite 抓取 HitchhikerGuide.php 丢到 repeater 里

405 Method Not Allowed

改 GET 为 POST

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

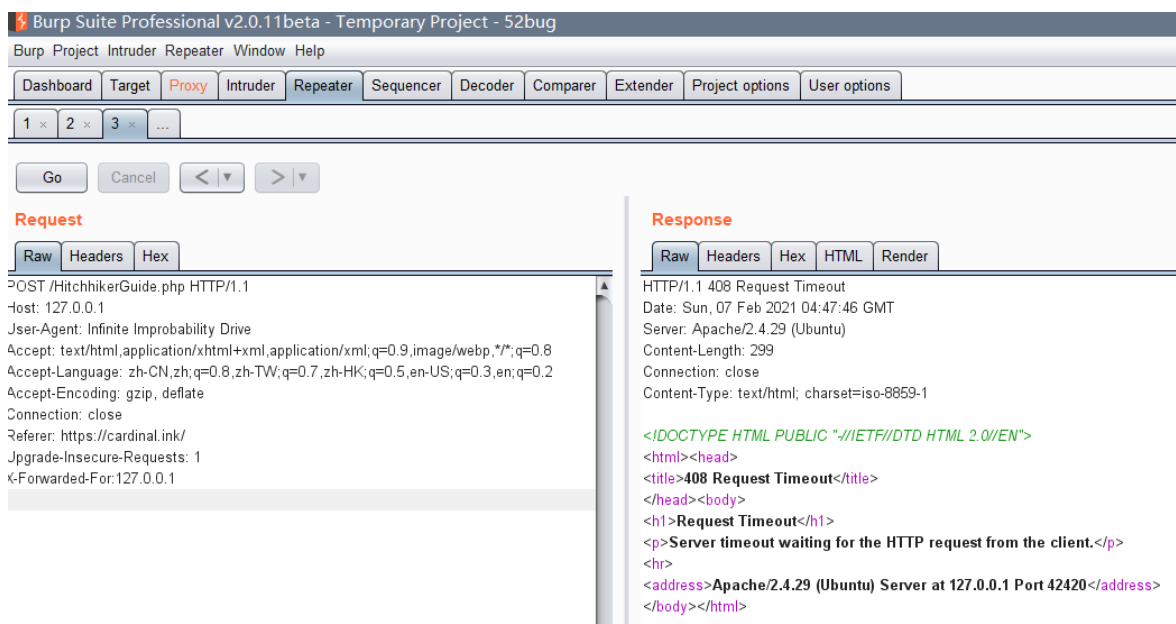
改 User-Agent 为 Infinite Improbability Drive

你知道吗？茄子特别要求：你得从他的[Cardinal](https://cardinal.ink/)过来

改 Referer 为<https://cardinal.ink/>

flag 仅能通过本地访问获得

添加 X-Forwarded-For:127.0.0.1 语句得到flag



Burp Suite Professional v2.0.11beta - Temporary Project - 52bug

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 x 3 x ...

Go Cancel < >

Request

Raw Headers Hex

POST /HitchhikerGuide.php HTTP/1.1
Host: 127.0.0.1
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/
Jpgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1

Response

Raw Headers Hex HTML Render

HTTP/1.1 408 Request Timeout
Date: Sun, 07 Feb 2021 04:47:46 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 299
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>408 Request Timeout</title>
</head><body>
<h1>Request Timeout</h1>
<p>Server timeout waiting for the HTTP request from the client.</p>
<hr>
<address>Apache/2.4.29 (Ubuntu) Server at 127.0.0.1 Port 42420</address>
</body></html>

复现的时候一直超时 emmmmm 做题的时候好像也出现过

watermelon

合就完事了，第三次就上了2000分

(Firefox 控制台拖动改元素大小好像可以把水果卡到界面下面快速上分)

宝藏走私者

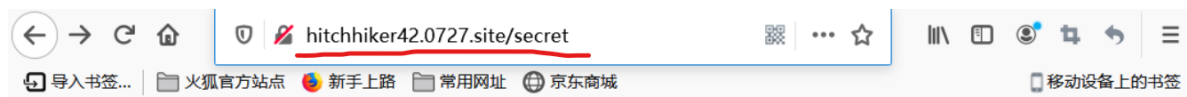
这题我在做顺风车的时候尝试访问顺风车的根域名，提示需要本地 IP 访问

Burp Suite 抓包伪造 IP 访问得到flag

以为是顺风车做好了，结果发现这道题已完成

4qE学长改了域名解析之后同样的方法无法复现，白嫖50分？

```
X-Forwarded-For:127.0.0.1
```



智商检测鸡

打开定积分计算器 Ctrl+c Ctrl+v 100题即可得到flag (bushi

不想再做100题复现了

呜呜呜呜正解在学了在学了

MISC

Base全家福

Base64→Base32→Base16得到 flag

Base16编解码

6867616D657B57653163306D655F74305F4847344D335F323032317D

编码

解码

清空

hgame{We1c0me_t0_HG4M3_2021}

不起眼压缩包的养成的方法

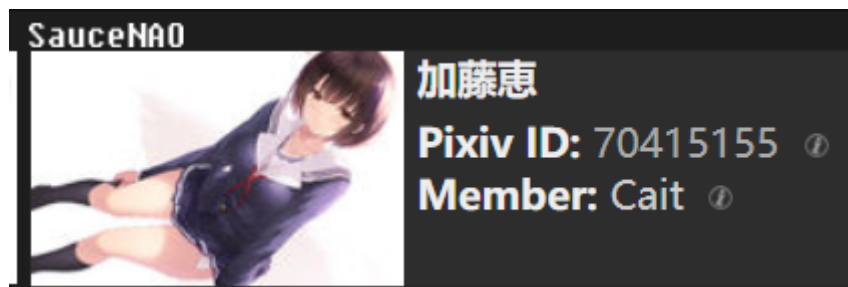
看到题名有“压缩包”想到图种

用 foremost 分离文件 / 直接改后缀，看到备注"Password is picture ID (Up to 8 digits)"

(Github 上找了个 win 版的foremost <https://github.com/raddyfiy/foremost>)

把文件名前8位取出来密码错误之后

作为 Pixiv 老用户，合理猜测为pid。SauceNAO 搜原图获取 pixiv id=70415155 解压出 plain.zip
和 NO PASSWORD.txt



用winhex尝试查看隐藏信息无果，用stegsolve尝试查看原图的隐藏信息无果

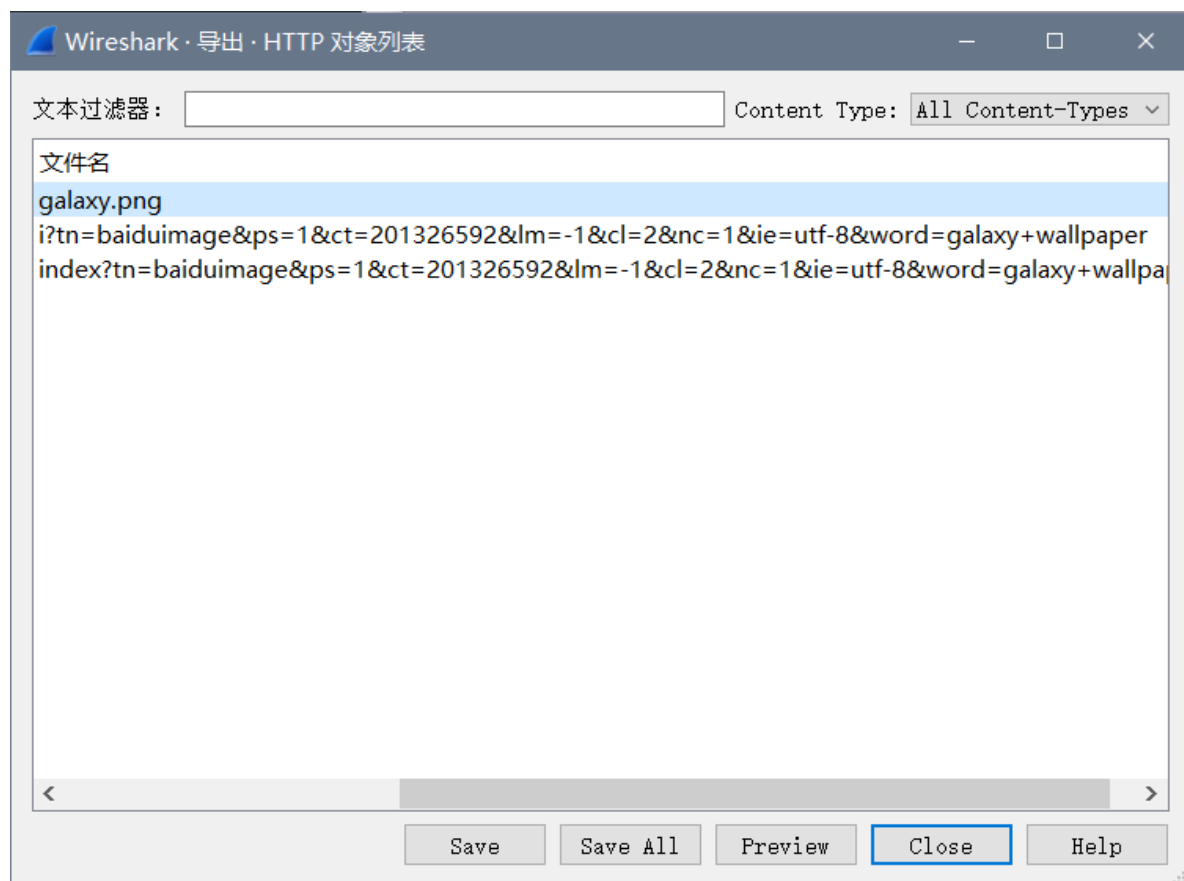
请教Akira学长后得知第二层压缩包名字是hint

没get到，还是想不通，看到No Password.txt的大小相同，CRC值也相同。下载ARCHPR 明文
爆破得到密码

Galaxy

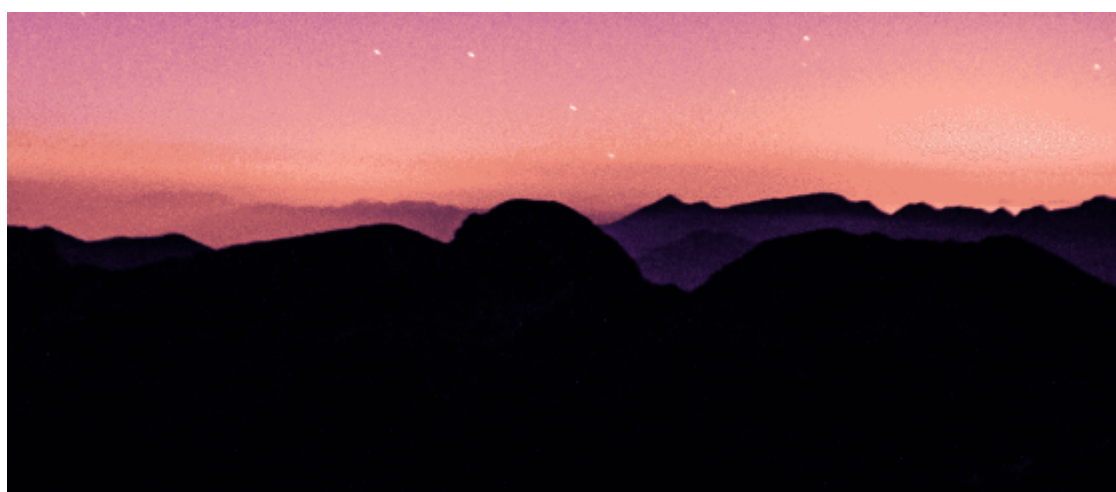
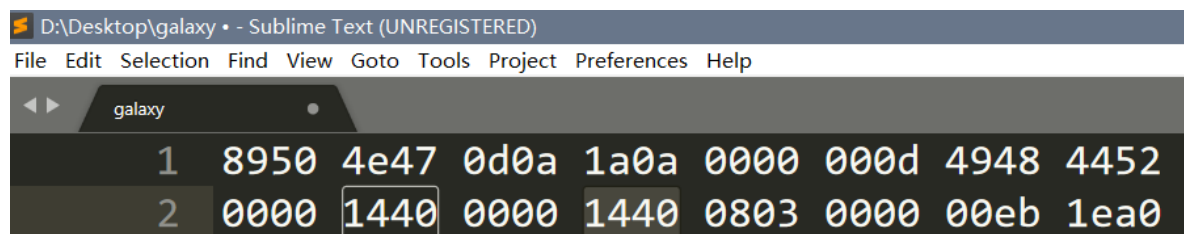
文件为 pcapng，百度得知为流量包文件

Wireshark 打开并导出 HTTP 对象得到 PNG 文件



尝试各种图片隐写，修改图片的高后获得 flag

我找到的winHex修改后保存文件时必闪退，所以实际操作中均使用 Sublime Text 代替 winHex



hgame{Wh4t_A_W0nderfu1_Wa11paper}