HGAME-WEEK1-WP

小霸哥xiaobug

注：曾经有一个写wp的良机摆在我面前，但我没有珍惜，等到失去了我才后悔莫及，尘世间最痛苦的事莫过于此。如果上天可以给我再来一次的机会，我会对那个hgame说：“我会解一道题写一篇wp。”如果非要在这份wp前加一个限制的话，我希望是一万字。

web 宝藏走私者

看了一眼hint，难不成只是伪造本地登录？（当时这题还不止50分）试了一下，X-Forwarded-For: 127.0.0.1，不行。看了一眼资料

5.1.1 使用CL-TE绕过前端服务器安全控制

Lab地址：https://portswigger.net/web-security/request-smuggling/exploiting/lab-bypass-front-end-controls-cl-te

实验的最终目的是获取admin权限并删除用户carlos

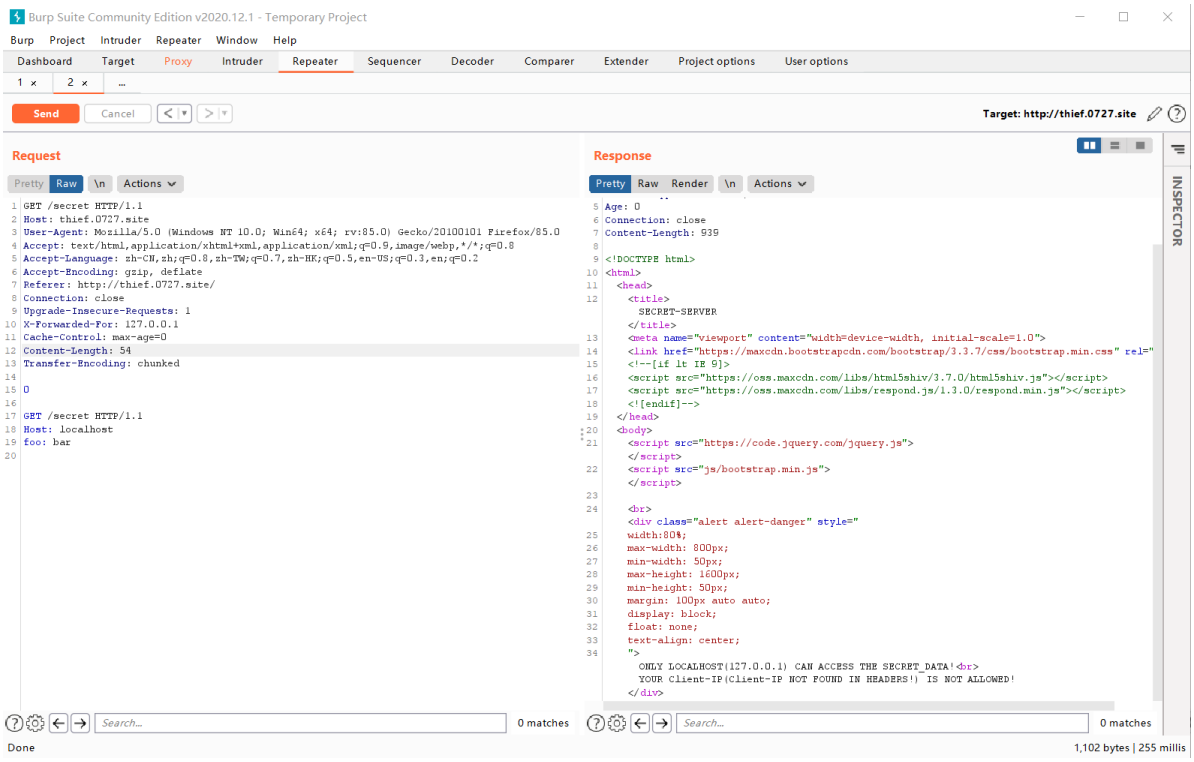
我们直接访问`/admin`，会返回提示`Path /admin is blocked`，看样子是被前端服务器阻止了，根据题目的提示`CL-TE`，我们可以尝试构造数据包

```
POST / HTTP/1.1
Host: ac1b1f991edef1f1802323bc00e10084.web-security-academy.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:56.0) Gecko/20100101 Firefox
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: session=Iegl0O4SGnwlddlFQzxduQdt8NwqWsKI
Content-Length: 38
Transfer-Encoding: chunked

0

GET /admin HTTP/1.1
foo: bar
```

就再试了一下



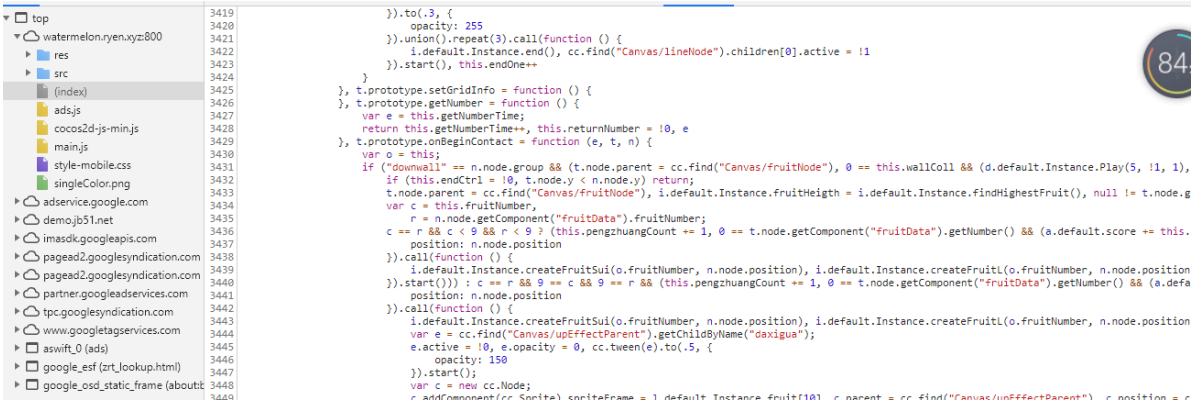
当时send了两次就出来了，但后来不知道怎么也刷不出来了，还请大佬教育

flag:hgame{HtTp+sMUg9l1nG^i5~r3al1y-d4nG3r0Us!}

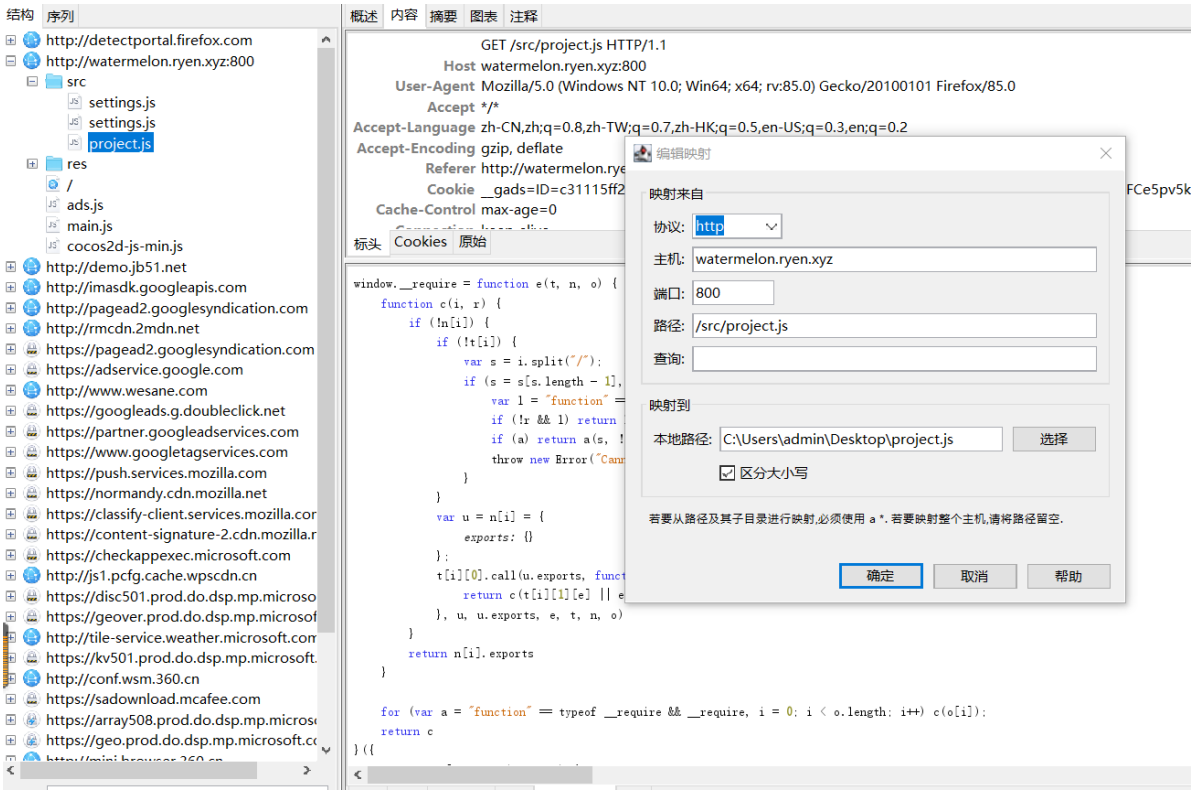
web watermelon

一开始不晓得这题要干嘛，恶心死我了。后来还是在群里看到的，没玩下去就拿不到hint，水群还是有必要的。然后开始玩大西瓜，发现连一个大西瓜都合不出来

猜测就是要改分喽。然后去网上找改大西瓜的教程



先找到源码，再用一手Charles



趁这西瓜不注意，偷摸给它换了芯子，刷新一手，合成一个直接23333，得到flag：

hgame{do_you_know_cocos_game?}

web 智商检测鸡

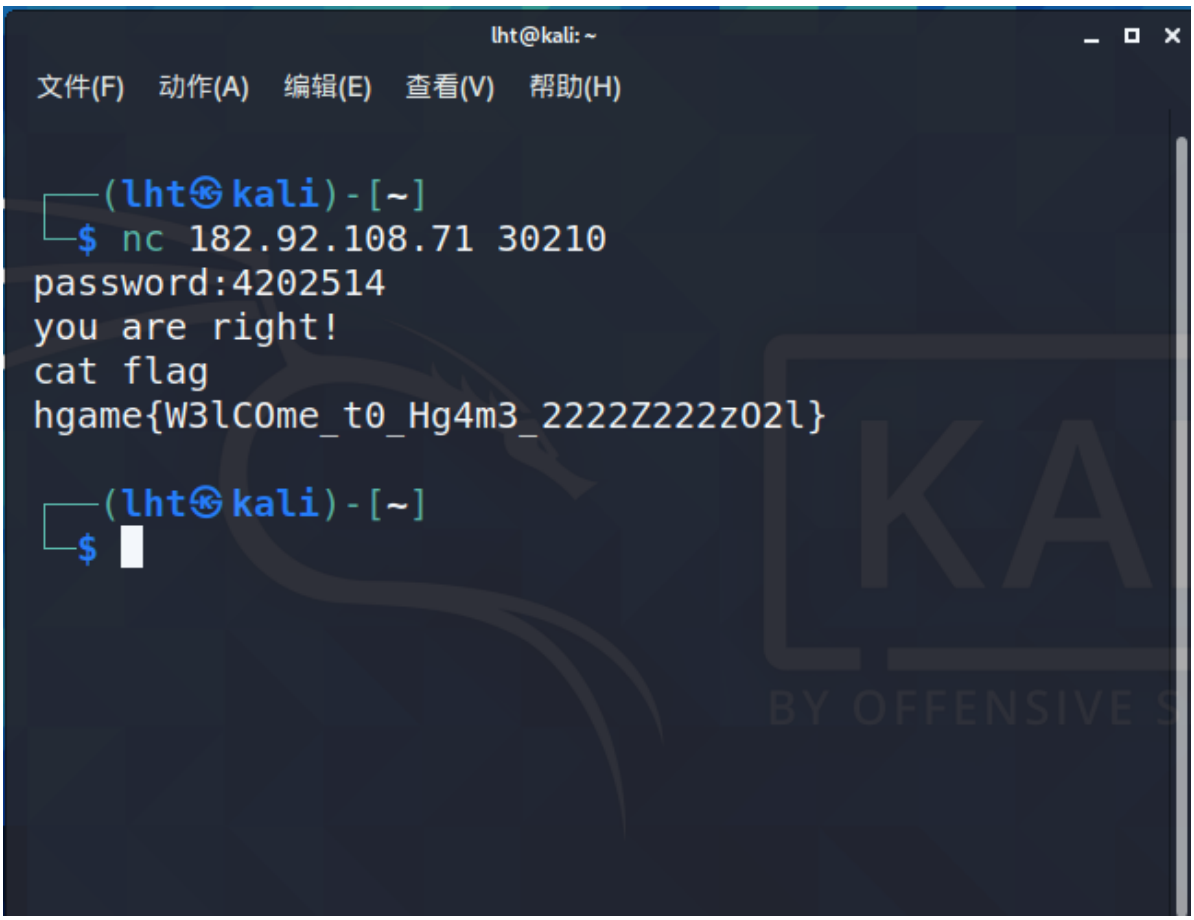
第一天晚上用火狐打开这题，中间是没显示定积分题目的（匪夷所思），所以以为这题是注入，结果就是怎么也做不出
第二天打开一看，出现了题目（直接想到以前做到过的题，要不是我做过，我还真肯定做不出），还是100道，多半就是写脚本，脚本一时写不出就去翻了以前那道题的wp，那道题叫“秋名山老司机”，两秒钟算出一大串式子，然后post结果，就可以拿到flag

学着他的样子写，得到flag: hgame{3very0ne_H4tes_Math}

听完有人是直接算积分的，我就哭了，可能比我这样做还快

pwn whitegave

kali就是啥都给你装好了，好喜欢啊，这道题我还是愿意再做一次的，不多讲了



crypto Transformer

这描述我都看不懂在干嘛，就下载文件先看看呗。我去，两个文件夹一个文件，大工程啊，真对的起这么长的描述。咦？才50分？想起解另一道密码题时了解到的爆破（感谢大佬），爆破了一下那个txt里面的内容，得到：

Mhe lift bridge console system has only used password login since 2003,the password is "hgame{ea5y_f0r_fun^3nd&he11o_},Yon't forget to add the year at the end.

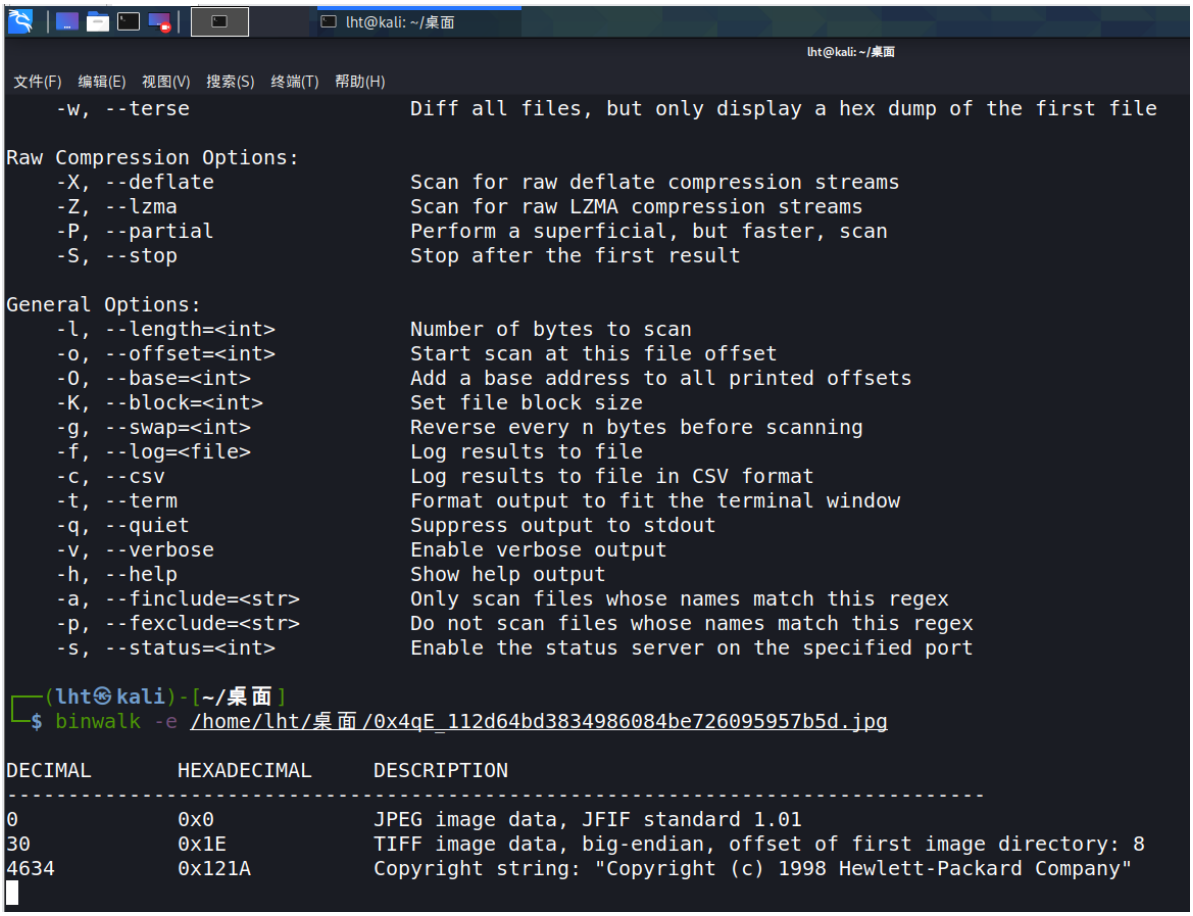
这段英文后半句应该是让我把年份加上，试了试2003和2021，结果2021对了，不过我感觉正解不是这样，请大佬指正

flag:hgame{ea5y_f0r_fun^3nd&he11o_2021}

misc 不起眼压缩包的养成方法

还好做完题之后的文件我没删，那张原题图片我就不放了，我不配

对着图片上的妹子，想啊想，我能做些什么呢？哈哈，想到了，用binwalk扒光它



然后就在kali桌面得到了zip文件

然后开始套娃的逆操作

99C8B.zip的密码简单，用ARCHPR纯数字爆破，得到密码：70415155

打开后，里面是plain.zip和NO PASSWORD.txt, NO PASSWORD.txt中给了hint，重点是密码是爆破不了的，还有该zip文件是仅储存的，然后不就有思路了？明文攻击，懂？得到密码：C8uvP$DP（有$在里面，能爆破出来？）

打开后得到flag.zip,还是有密码，很明显是最后一层，最后一层有密码又怎样？扒不扒有区别？用透视镜winhex打开，发现字符串flag.txt后面跟着一串有规律的编码，解码就完事了，拿到flag：

hgame{2IP_is_Usefu1_and_Me9umi_i5_W0r1d}

PS：不过还是希望大佬教育一下，flag.txt的密码怎么破解

misc base全家福

一看题目地址，激动了一下，签到题？

然后蠢萌的我把base家族试了个遍，结果没做出来，如下图

流下几滴眼泪：base64+base32+base16

flag:hgame{We1c0me_t0_HG4M3_2021}

misc Word RE:MASTER

拿到两个word，一个有密码，一个没有。

啥也看不出来，只能看到主人公在发烧（骚）。只好再去看描述：啥？word专家？出题人在凡我？肯定有问题。这就百度：word的本质。

然后就会了，无脑加上后缀.zip,打开后，一眼就看到了password.xml, 用记事本打开，一串奇奇怪怪的东西，不过很明确，它就是某种编码！

百度救我！百度：告诉你吧，它就是brainfuck（跟jsfuck有点像）！！！作为没经验的小萌新，总是get到方法才看懂hint，此处又是两滴眼泪，题解两句话，搜索两小时，拿到密码：

DOYOUKNOWHIDDEN?

又是很嘲讽的样子，小萌新又哭了，解开另一个word，什么鬼？一张图？用Stegsolve看了半天，啥也没有。。。还好小萌新还是用过word的，开出隐藏的空格、制表符等等，有了！但是一串箭头和点是什么东西呢？

只好厚着脸皮问出题人，出题人：图片给了hint。看半天，没看出来，难道这一串东西是能翻译的？脸皮渐渐变厚，再问问。出题人：名词。。。好吧，不想讲废话了，下载snow.exe,解密得到：

flag:hgame{Cha11en9e_Whit3_P4ND0R4_P4R4D0XXX}

misc Galaxy

首先得到pcapng文件，用wireshark打开，搜索http，找到图片，导出字节流，奇怪的是win10自带的图片查看器可以直接看图，出题人让我换个软件，我问为啥。出题人说有的软件不会检查CRC。百度一下我就秒懂了，哈哈哈

我猜测出题人的意图，是要根据CRC校验码，爆破出图片长度

但是。。。

我的做法：直接把图片改长，flag就出来了,谁让我的图片查看器不检验CRC呢

没想到最难的居然是肉眼识别图上的flag，不说了，懂的都懂