Level - Week 1

谁吃了我的flag

描述

呜呜呜，Mki一起床发现写好的题目变成这样了，是因为昨天没有好好关机吗T_T hint: 据当事人回忆，那个夜晚他正在用vim编写题目页面，似乎没有保存就关机睡觉去了,现在就是后悔，十分的后悔。

URL http://118.25.111.31:10086/index.html

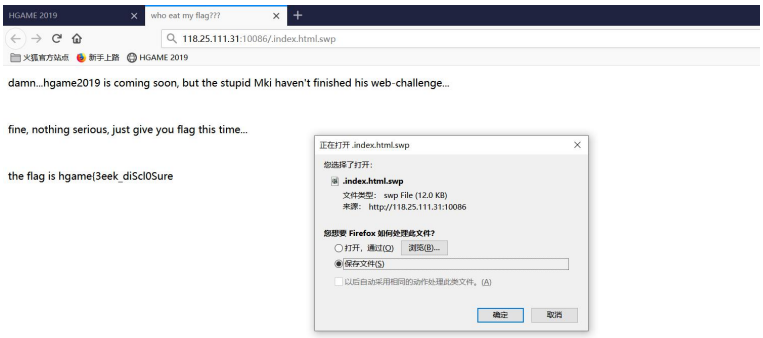
基准分数 50

当前分数 50

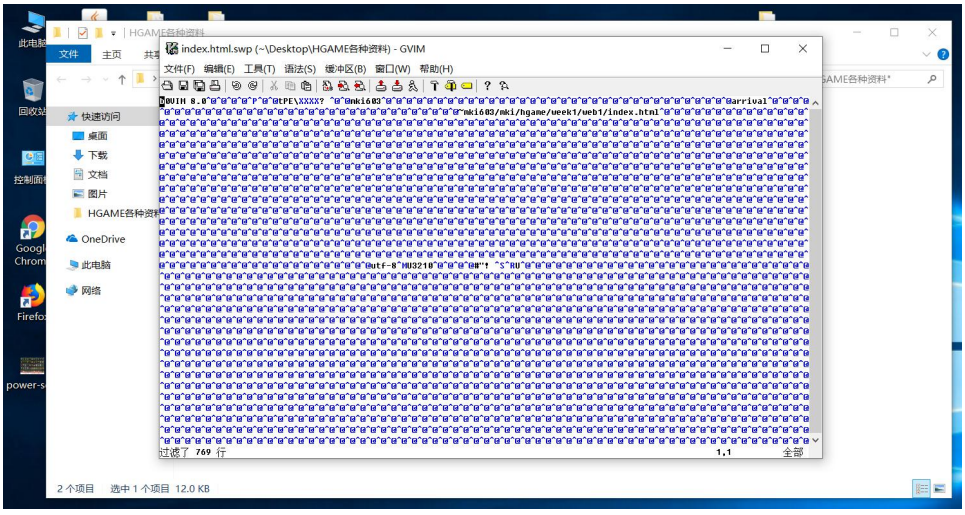
完成人数 250

Emmm 审题审题（不要管学长有没有被学弟交流 哈哈哈大快人心）

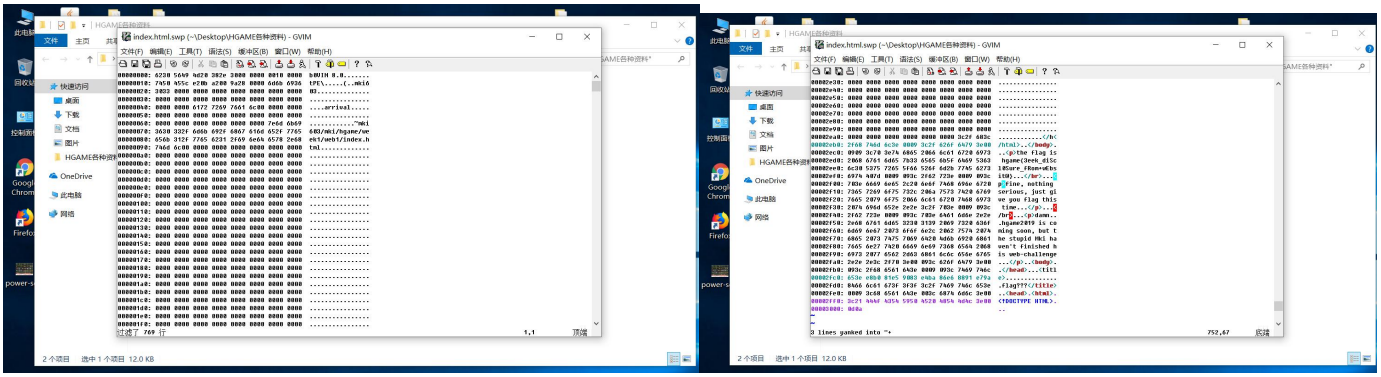
看到重点了 Vim 百度百度 大概了解了 Vim 泄露



加个/.index.html.swp 偷到个文件



Emmm 看不懂。。。 再次百度 ing



转化为十六进制再次寻找 flag

然后 hgame{3eek_diScl0Sure_fRom+wEbsit@}

换头大作战

描述

想要flag嘛工具: burpsuite postman hackbar 怎么用去百度，相信你可以的

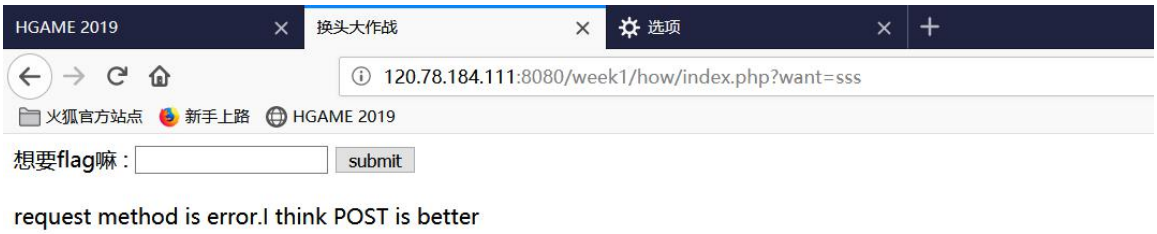
URL http://120.78.184.111:8080/week1/how/index.php

基准分数 100

当前分数 100

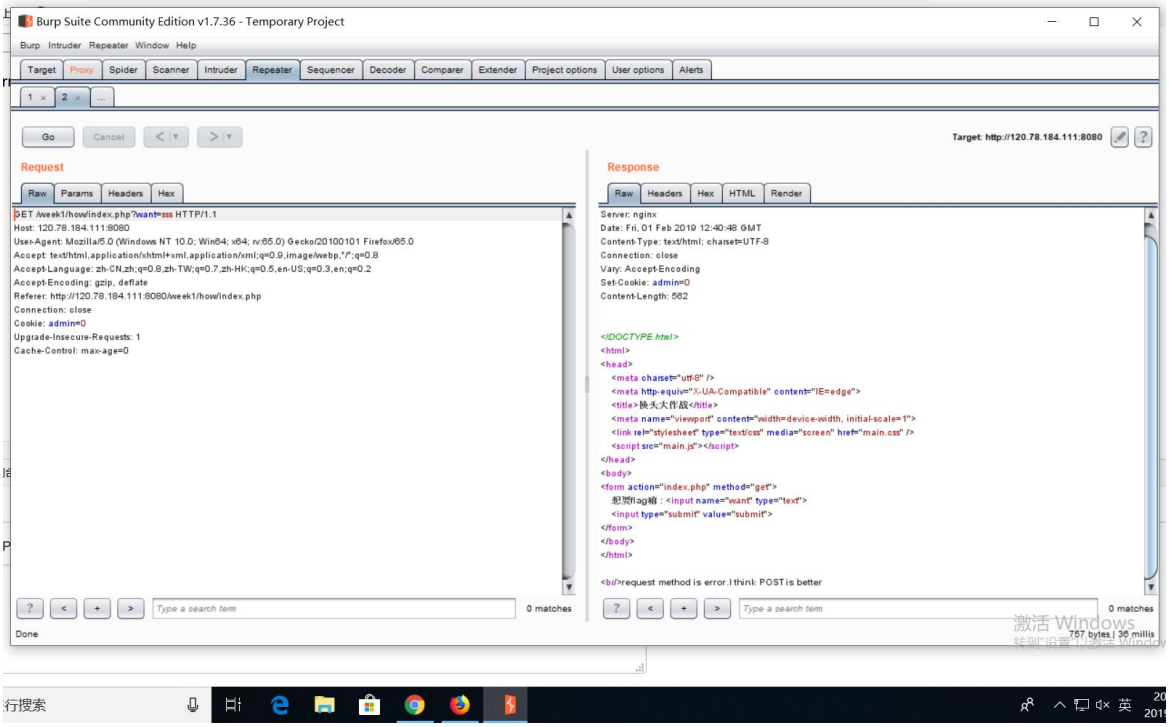
完成人数 267

看到提示不知道学长是不是又被 PY 了 直接下载工具接百度

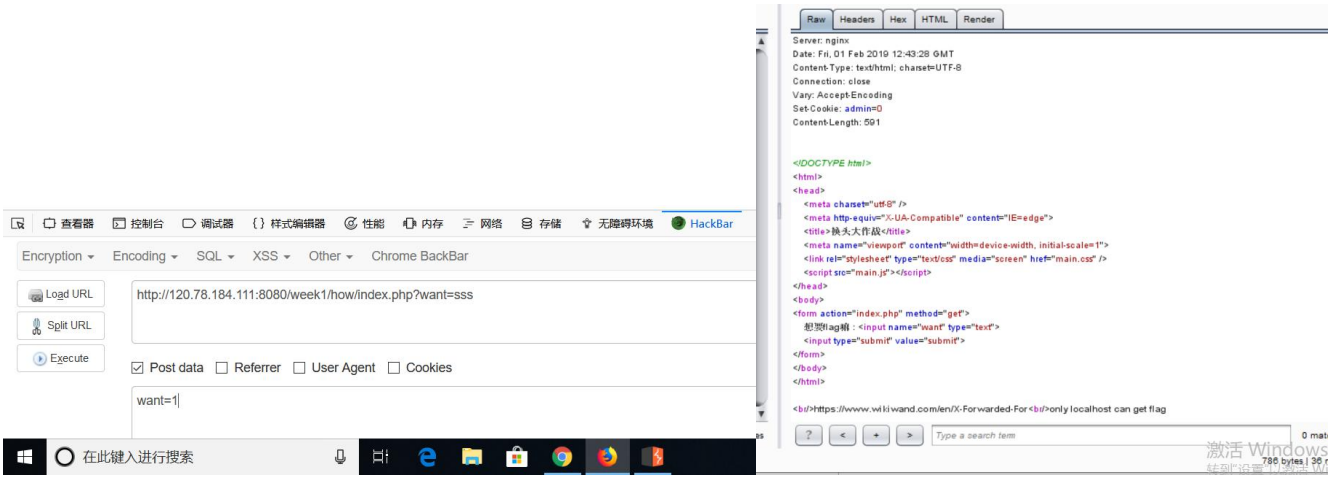


小试一下 发现了 POST 百度先

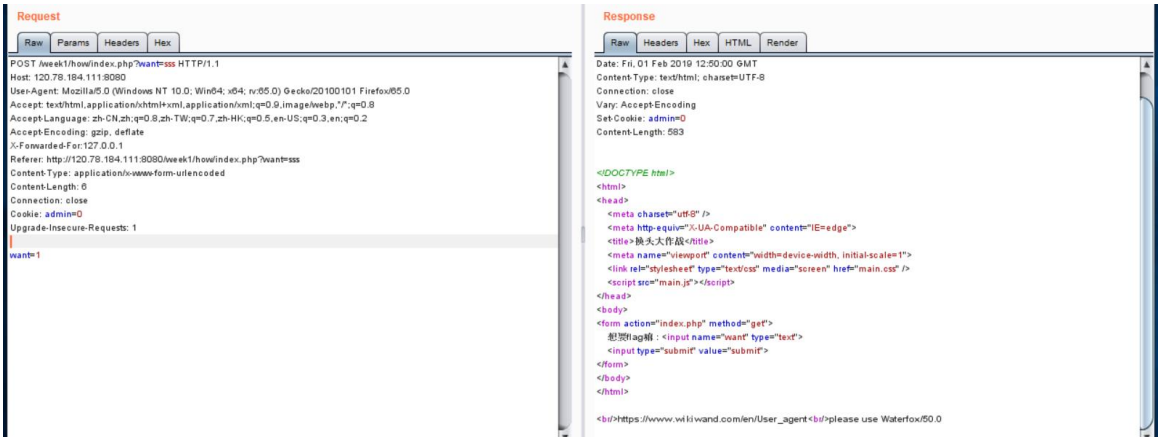
然后

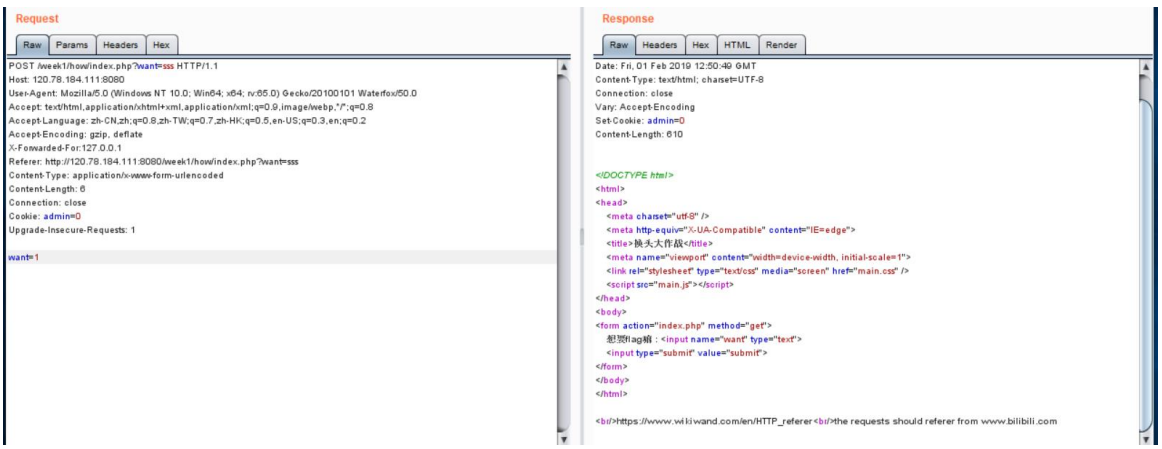


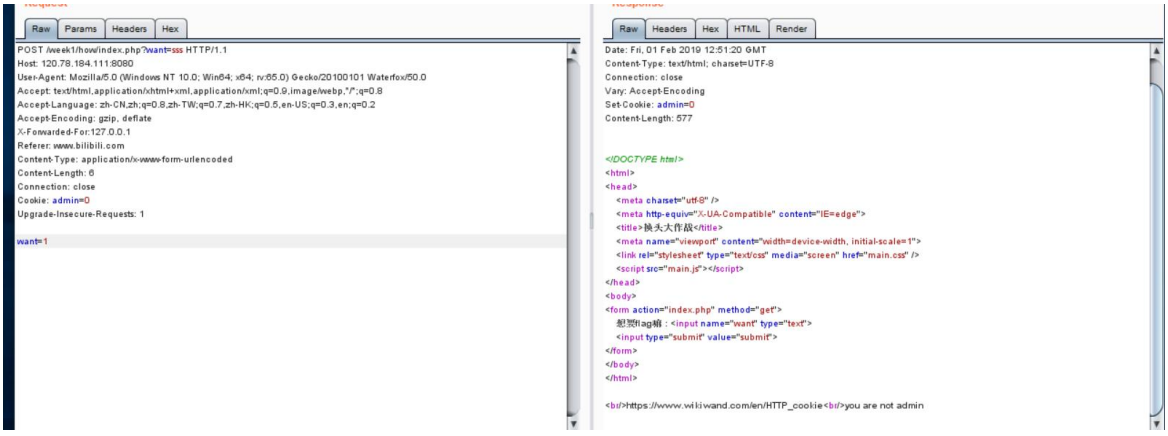
抓个包先 随缘分析一波（百度）

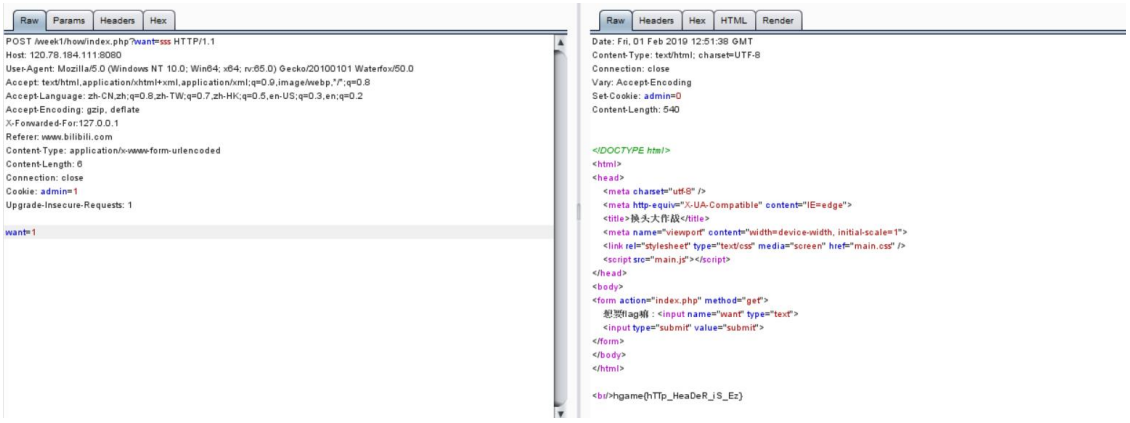


感觉就是这样的我也不知道为什么 然后发现代码最后不大一样

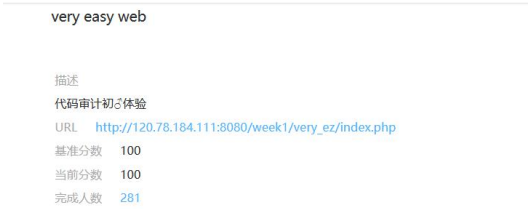


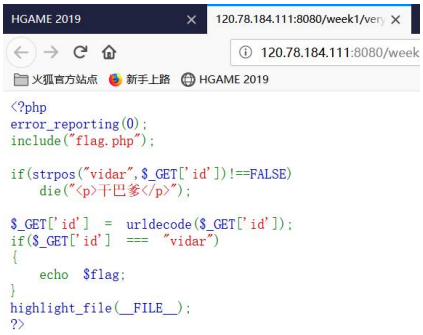






就这样边蒙边猜边百度得到了 hgame{hTTp_HeaDeR_iS_Ez}

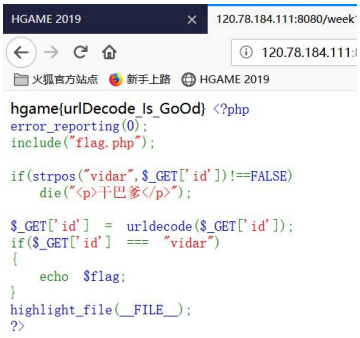




打开题目这是啥。。。 继续百度开始边蒙边猜

Id 经过两次 url 解码得到 vidar 开始寻找 id 解码前是啥 百度:在线编译器

?id=%2576%2569%2564%2561%2572 啊真香



hgame{urlDecode_Is_GoOd}

can u find me?

描述

为什么不问问神奇的十二姑娘和她的小伙伴呢

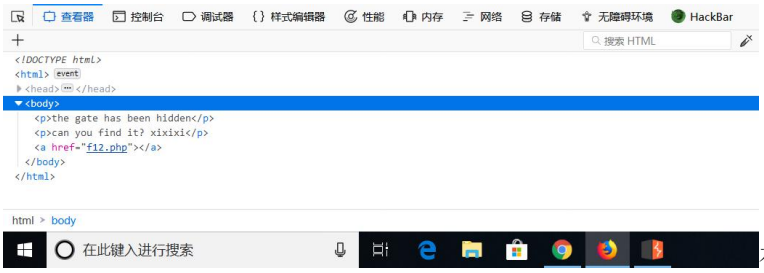
学习资料:

https://www.cnblogs.com/yaoyaojing/p/9530728.html

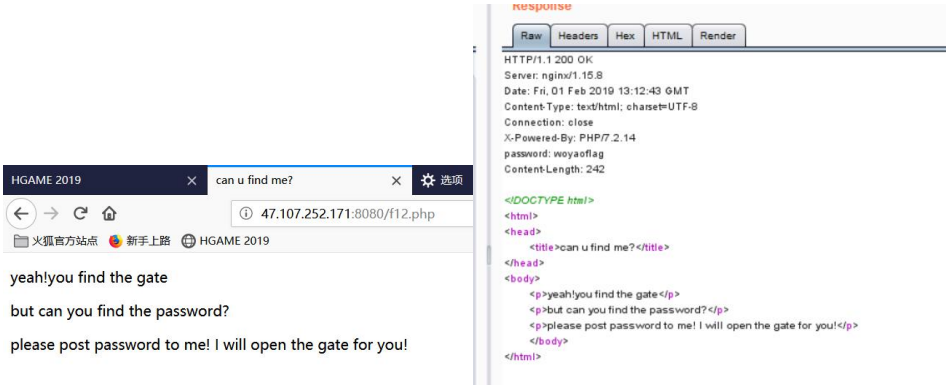
https://www.cnblogs.com/logsharing/p/8448446.html

https://blog.csdn.net/z929118967/article/details/50384529

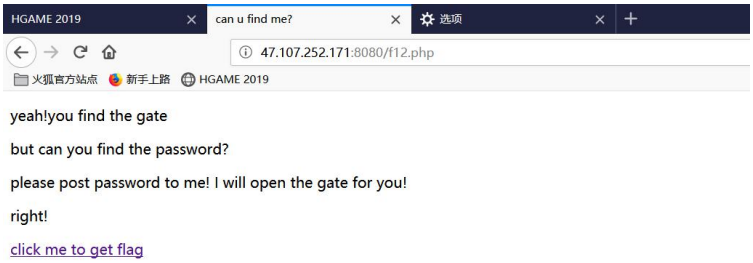
URL http://47.107.252.171:8080/

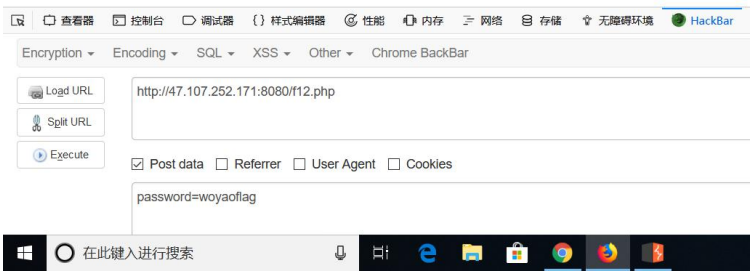


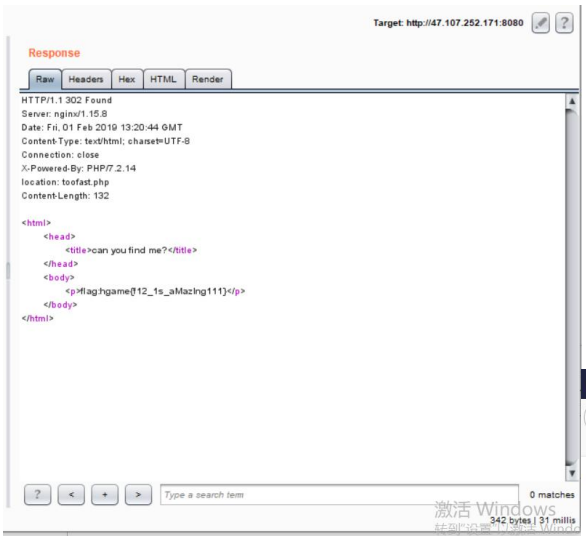
在源代码中发现了/f12.php

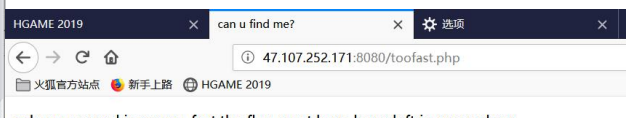


进去了 在抓包时发现了密码









得到了 flag:hgame{f12_1s_aMazIng111} 然后还发现了有趣的事情。。。

描述

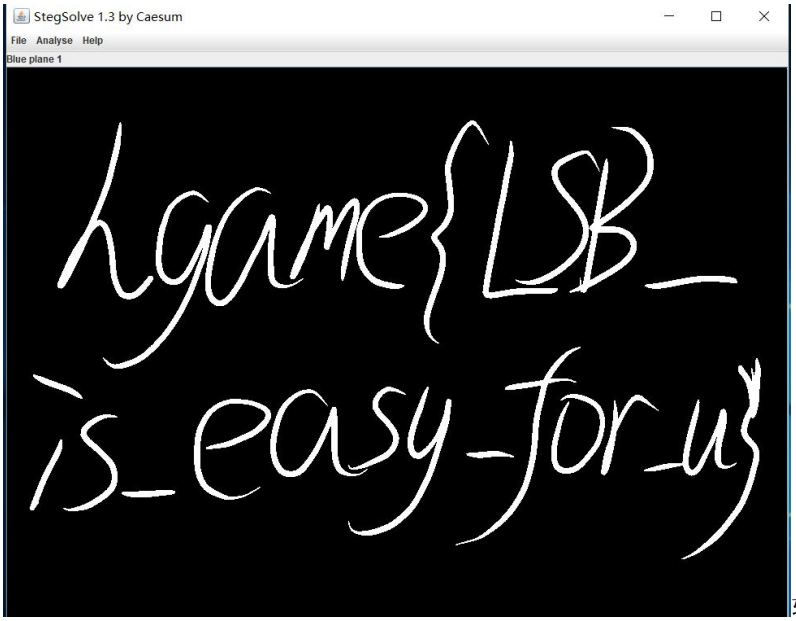
Here are some magic codes which can hide information in an ordinary picture, can you extract the hidden image in the provided picture?

其实本来想让大家写写代码，后来干脆就送分了

有个神器叫 stegsolve，利用它可以直接提取本题 flag

URL http://plir4axuz.bkt.clouddn.com/hgame2019/lsb.zip

不说了先下个软件为敬



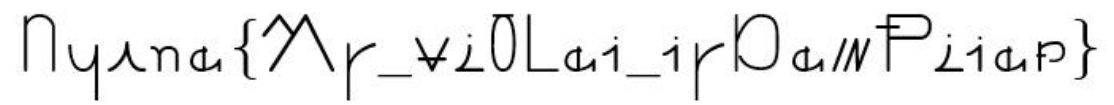
软件一开 百度一开一顿操作

得 hgame{LSB_is_easy_for_u}

Aris(划掉)牌打字机，时尚时尚最时尚~

hint:谷歌有个以图搜图功能很不错，百度识图好垃圾的。。。

URL http://plps4kyke.bkt.clouddn.com/打字机.zip



这个是啥。。。 照着键盘 跟着百度 大小写随缘

得 hgame{My_vi0let_tyPewRiter}

Broken Chest

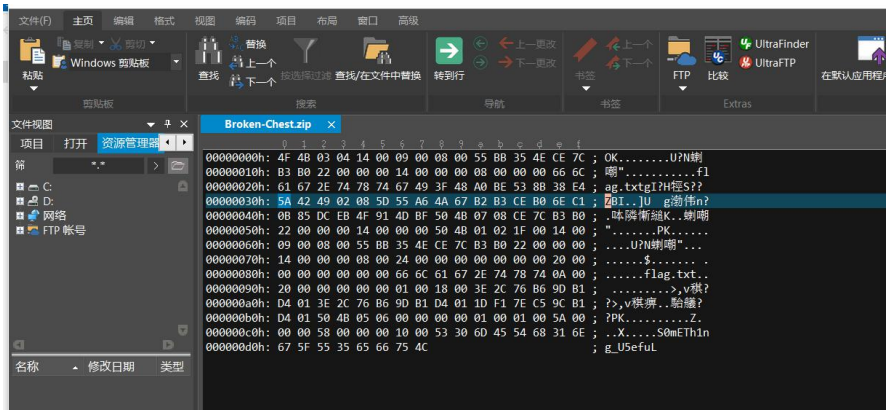
描述

这个箱子坏掉了！快用你无敌的[疯狂钻石]想想办法啊！

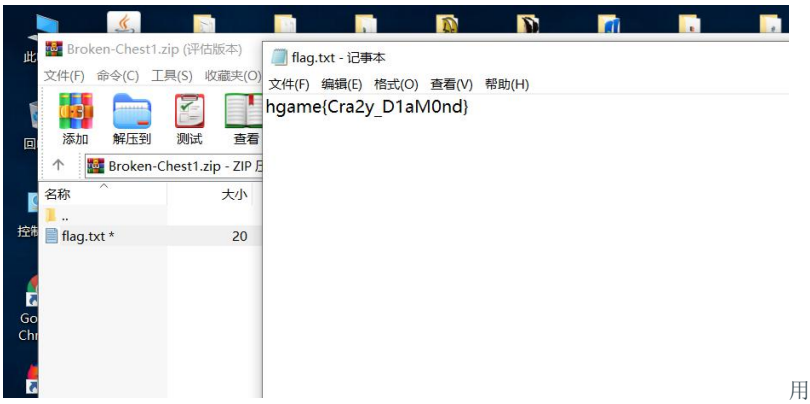
更新一波学习资料https://ctf-wiki.github.io/ctf-wiki/misc/archive/zip/

URL http://plqfgjy5a.bkt.clouddn.com/Broken-Chest.zip

发现了学习 赶紧资料学习一波



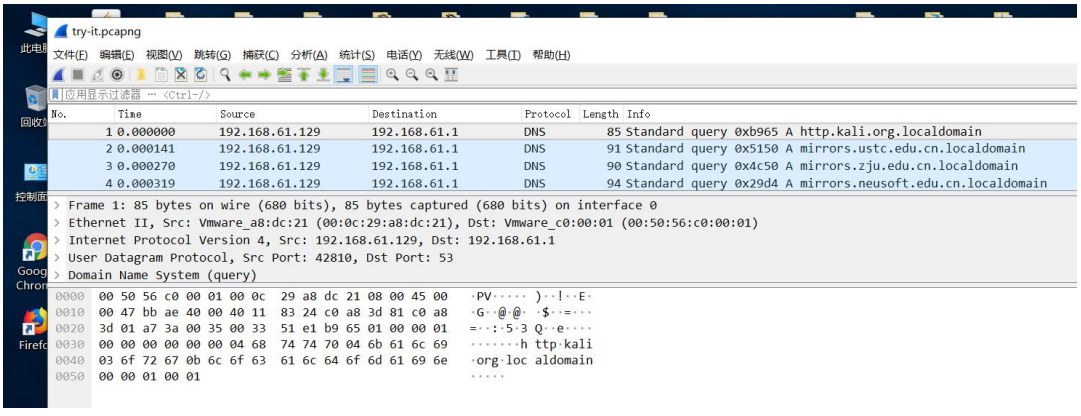
文件头错误改回 50 4B 03 04



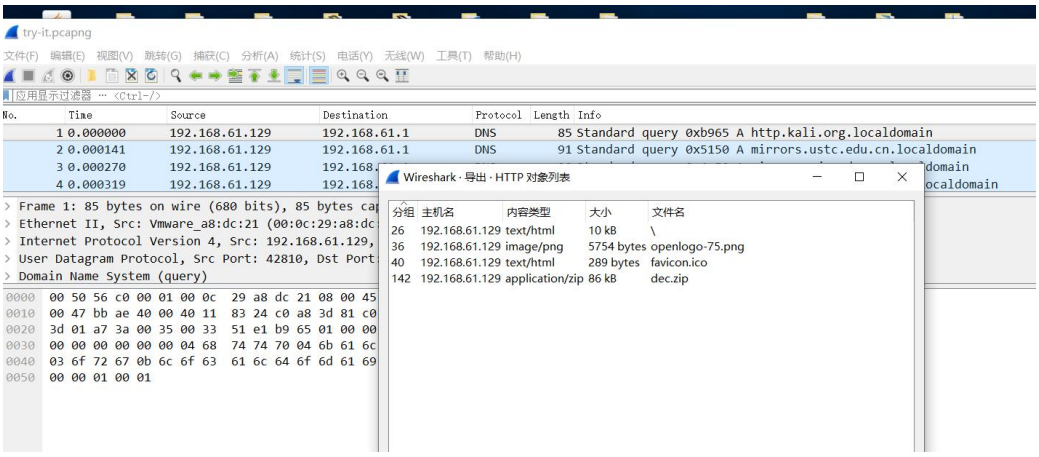
用注释里面的解压密码得到压缩文件

hgame{Cra2y_D1aM0nd}

百度寻找打开文件的工具



发现可以这么打开



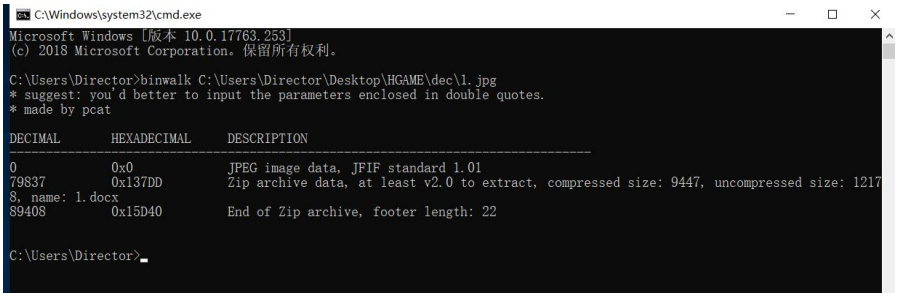
导出对象 得到一堆乱七八糟的东西最后发现只有压缩包是有用的

解压得到又一个压缩包（这是个套娃吗？）发现居然还有解压密码格式，我还以为是 flag 太令人失望了

知道密码格式那就暴力一点 嘿嘿嘿

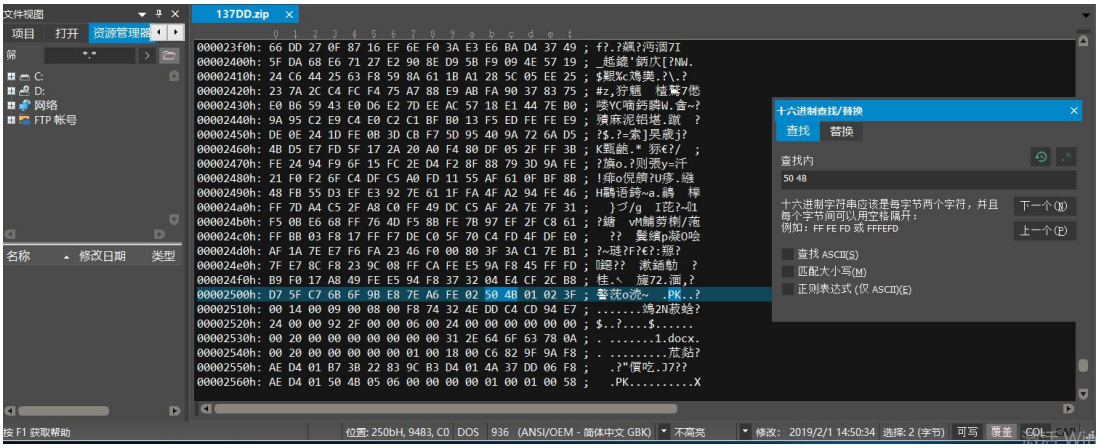
得到了一个小姐姐的图片 wow

先拿着 StegSolve 一顿分析发现啥都没有。。。 老老实实的百度。。。



用 binwalk 分析一下发现还有一个压缩文件 顺便就将其分离

压缩包又有密码但是没有格式此处必有问题 先理性分析一波



百度得这玩意是伪密码 来修改一下 09 为 00 就可以打开压缩包得到 真・无字天书 word 的选项勾选 隐藏文字

Flag：

这是个摩斯电码 来在线翻译一下

744B735F6D6F7944716B7B6251663430657D

这个初步猜测是十六进制对应 ASCII 码

再次翻译一下 tKs_moyDqk{bQf40e} 感觉还有排序一下 试了很多发现是栅栏密码 tsmyq{Q4eK_oDkbf0}

将前面改为 hgame 后对应一下发现规律应该为凯撒密码 hgame{E4sY_cRypt0}