WEEK 1

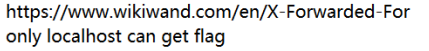
{Web}

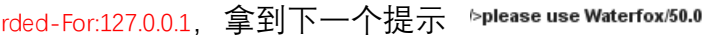
[谁吃了我的 flag]

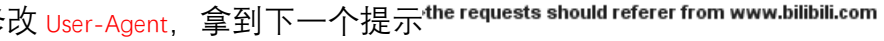
根据半个 flag 里的【3eek_diScl0Sure】和后来的 vim 提示，可以知道应该是没正常退出产生了一个.swp 文件的泄露。直接访问 http://118.25.111.31:10086/.index.html.swp，获得文件。在 vim 里打开，发现 flag。

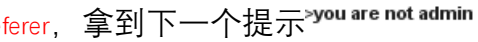
[换头大作战]

先随便输入一个试试，发现 

request method is error.I think POST is better 在开发者工具里把 method 改成等于 post。 

再用 burpsuite 拦截。根据提示加入 X-Forwarded-For:127.0.0.1，拿到下一个提示 

修改 User-Agent，拿到下一个提示 

，修改 Referer，拿到下一个提示 

，把 admin 的值改为 1，成功获取 flag

hgame{hTTp_HeaDeR_iS_Ez}

[very easy web]

代码审计题，关键代码如下：

```
if(strpos("vidar",$_GET['id'])!==FALSE)
    die("<p>干巴爹</p>");

$_GET['id'] = urldecode($_GET['id']);
if($_GET['id'] === "vidar")
{
    echo $flag;
}
```

即要求输入的字符串不等于 vidar，但在一次 url 解密之后等于 vidar，所以可以直接对字符 v 加密两次。在原网址后面加上 get?id=%2576idar，获得 flag

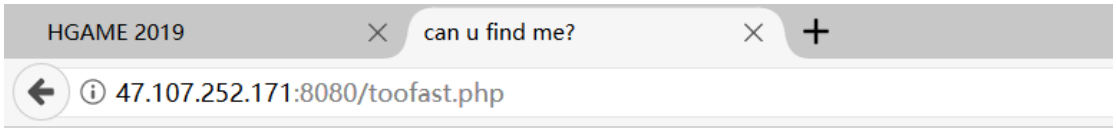
hgame{urlDecode_Is_GoOd}

[can u find me?]

先用开发者工具查看代码，发现一个 f12.php。访问它，要求我们

please post password to me! I will open the gate for you!

用 burpsuite 拦截。在消息头里把 GET 改成 POST，消息体里加上 password=woyaoflag（不要加空格和换行），最后不要忘记在消息头里增加一条 Content-Type: application/x-www-form-urlencoded。成功发送之后出现一个链接，点击后跳转



aoh,your speed is sososo fast,the flag must have been left in somewhere

根据提示可以知道应该是 302 跳转。然后再在 burpsuite 里拦截查看，找到第一次的页面，发现 flag

{Re}

[brainfxxker]

虽然没有学过 c++，但可以逐步调试感受一下程序的走向，理解之后就是

```
x-100+2  b
x-81-1   R
x-49-3   4
x-36+3   !
x-80+2   N
x-100-2  f
x-80-5   U
x-100+1  c
x-72-3   K
```

一点点计算了。，加上 hgame{}就是所要求的 flag 了。

[HelloRe]

我是下载完文档直接打开来，发现是乱码拖着看了一下，看见了 flag

Please input your key: hgame{Welc0m3_t0_R3_World!} success failed..

[Pro 的 Python 教室(一)]

阅读代码，得知 flag 一共有三个部分，要求我们输入三个部分经过处理后与给出的三个字符串一致。第一部分没有处理，输入等于 enc1，即 hgame{ 。第二部分的输入被 base64 加密过一次之后要与 enc2 相等，说明应该是 enc2 的 base64 解密，百度解密一下得到 Here_1s_3asy_。第三部分我有点奇怪，看上去是经过 base32 解码之后与 enc3 相等，应该是 enc3 的 base32 加密，但加密之后是乱码。所以我直接拿 enc3 来试了试，发现 flag 就是 hgame{Here_1s_3asy_Pyth0n}。

{Pwn}

[aaaaaaaaaa]

用 IDA f5 得到 c 语言的代码

```c
int __cdecl main(int argc, const char **argv, const char **envp)
{
  signed int v3; // eax
  signed int v5; // [rsp+Ch] [rbp-4h]

  setbuf(_bss_start, 0LL);
  signal(14, handle);
  alarm(0xAu);
  puts("Welcome to PWN'world!let us aaaaaaaaaa!!!");
  v5 = 0;
  while ( 1 )
  {
    v3 = v5++;
    if ( v3 > 99 )
      break;
    if ( getchar() != 97 )
      exit(0);
  }
  system("/bin/sh");
  return 0;
}
```

发现只要输入 100 个 a 就好，在 linux 连接服务器，输入好多 a，然后可以直接

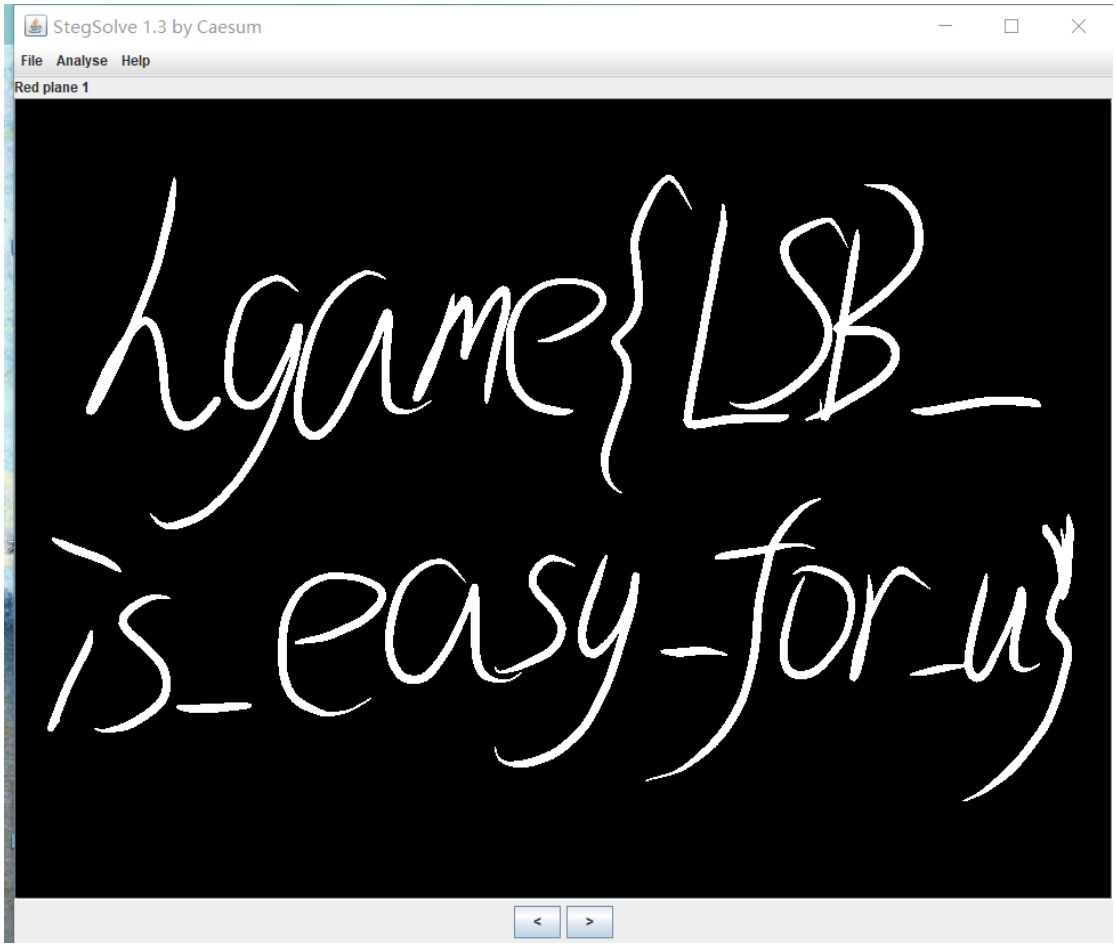
ls 了，再用 cat flag 提取 flag

```
hrh@hrh-study: ~
File Edit View Search Terminal Help
hrh@hrh-study:~$ nc 118.24.3.214 9999
Welcome to PWN'world!let us aaaaaaaaaa!!!
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
ls
aaaaaaaaaa
bin
dev
flag
lib
lib64
run.sh
cat flag
hgame{Aa4_4aA_4a4aAAA}
```

{Misc}

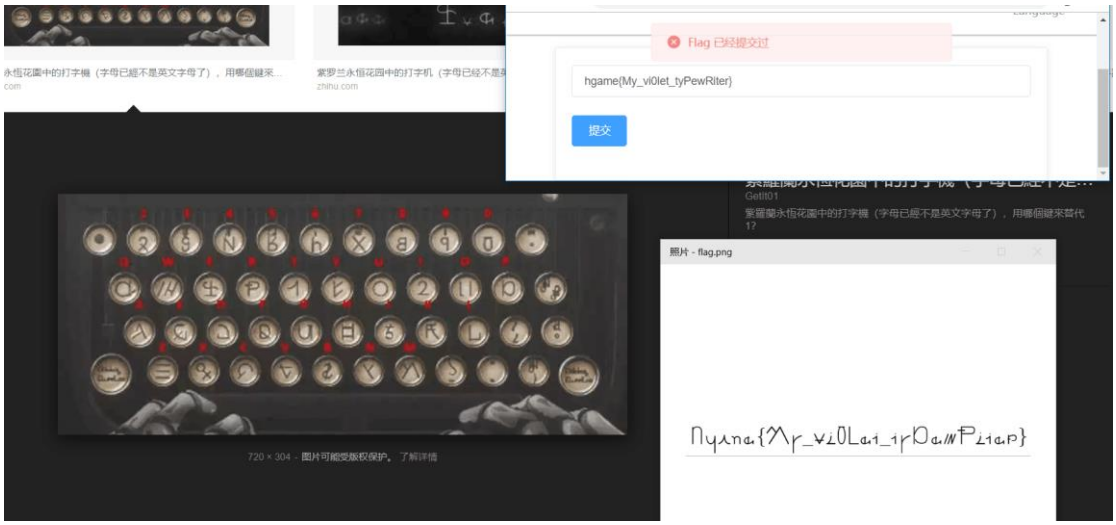
[Hidden Image in LSB]

根据提示，下载 LSB，打开图片。直接可以看到 flag



[打字机]

一开始猜测是和键盘对应而且可以通过前四个确定 hgame 几个字符的位置。但它实在太乱了，还不好找。后来提示说是可以谷歌识图就方便了。



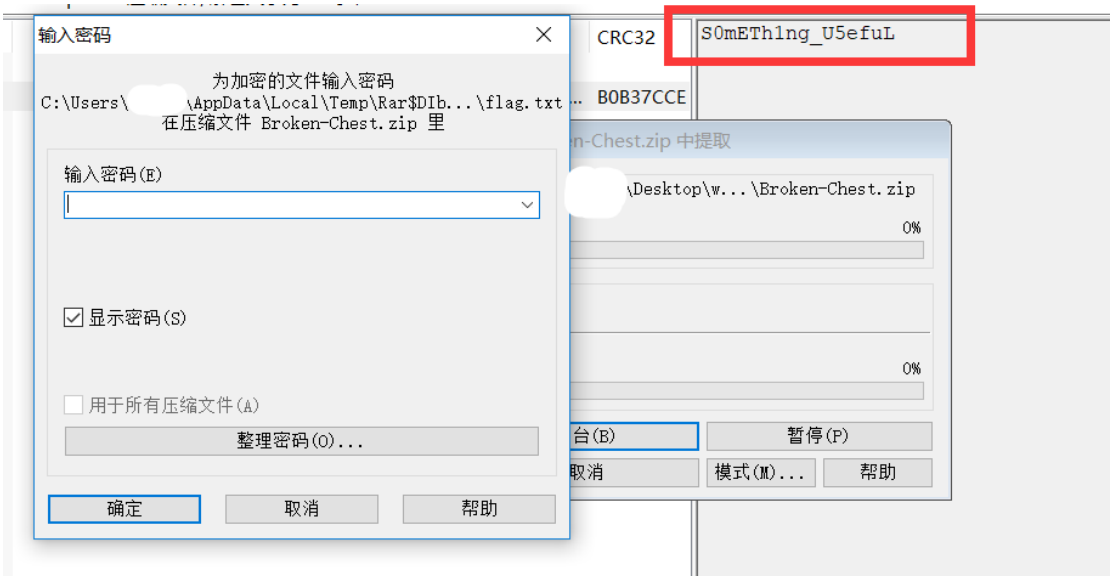
对着一个个找就好了。那些在图里一下找不到的可以先找一些相似的，然后改成它们的小写试试。然后前后相同的符号对照着看看，对着输着试试，错了就改改大小写。

[Broken Chest]

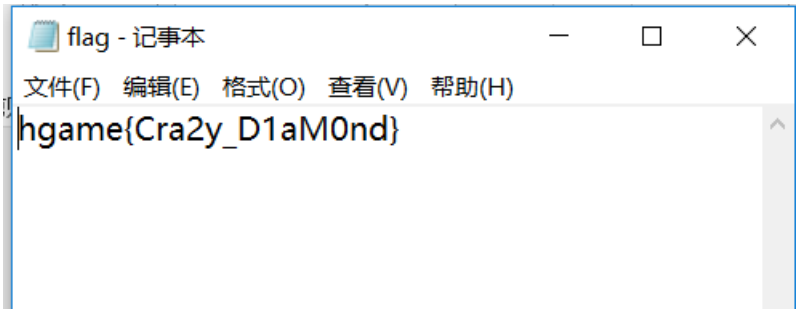
下载压缩文件，打开说文件损坏，用 winhex 打开。根据给出的资料，前面四个应该是 50 4B 03 04，但该文件为

```
4F 4B 03 04 14 00 09 00  08 00 55 BB 35 4E CE 7C  OK□□□□ □□□U□ |
B3 B0 22 00 00 00 14 00  00 00 08 00 00 00 66 6C  □  □□□□□□□□□□fl
61 67 2E 74 78 74 67 49  3F 48 A0 BE 53 8B 38 E4  ag.txtgI?H□  8□
5A 42 49 02 08 5D 55 A6  4A 67 B2 B3 CE B0 6E C1    □□]U□  □  □
0B 85 DC EB 4F 91 4D BF  50 4B 07 08 CE 7C B3 B0    □  □  □□
22 00 00 00 14 00 00 00  50 4B 01 02 1F 00 14 00  "□□□□□□□PK□□ □□□
09 00 08 00 55 BB 35 4E  CE 7C B3 B0 22 00 00 00   □□□U□  |□  □□
14 00 00 00 08 00 24 00  00 00 00 00 00 00 20 00  □□□□□□$□□□□□□□ □
00 00 00 00 00 00 66 6C  61 67 2E 74 78 74 0A 00  □□□□□□flag.txt □
20 00 00 00 00 00 01 00  18 00 3E 2C 76 B6 9D B1   □□□□□□□□□>,v□
D4 01 3E 2C 76 B6 9D B1  D4 01 1D F1 7E C5 9C B1  □>,v□  □ □  □
D4 01 50 4B 05 06 00 00  00 00 01 00 01 00 5A 00    K□□□□□□□□□□Z□
00 00 58 00 00 00 10 00  53 30 6D 45 54 68 31 6E  □□X□□□□□S0mETh1n
67 5F 55 35 65 66 75 4C                           g_U5efuL
```

把 4F 改成 50，可以打开。但解压要求密码，发现旁边有串字符



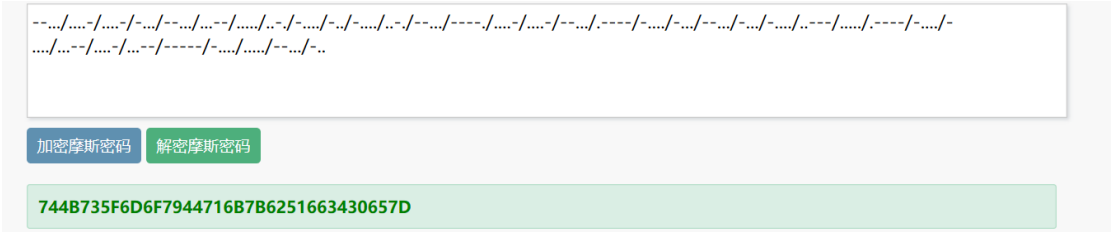
输入得到 flag



{Crypto}

[Mix]

URL 没什么用，题目在提示里。是一串.-/组成的，猜测是摩斯密码。网上在线解码



得到一串数字和字母，数字从 0-9，字母只有 B,D,F，猜测是十六进制，用 HEX 转码

tKs_moyDqk{bQf40e}

UTF-8 GB2312 编码 解码

感觉是栅栏密码，但没有开头的 hgame，先用凯撒密码移位试试，得到结果

tKs_moyDqk{bQf40e}

解密 使用英文字典智能分析

第2次解密:sjr_lnxcpj{ape40d}
第3次解密:riq_kmwboi{zod40c}
第4次解密:qhp_jlvanh{ync40b}
第5次解密:pgo_ikuzmg{xmb40a}
第6次解密:ofn_hjtylf{wla40z}
第7次解密:nem_gisxke{vkz40y}
第8次解密:mdl_fhrwjd{ujy40x}
第9次解密:lck_egqvic{tix40w}
第10次解密:kbj_dfpuhb{shw40v}
第11次解密:jai_ceotga{rgv40u}
第12次解密:izh_bdnsfz{qfu40t}
第13次解密:hyg_acmrey{pet40s}
第14次解密:gxf_zblqdx{ods40r}
第15次解密:fwe_yakpcw{ncr40q}
第16次解密:evd_xzjobv{mbq40p}
第17次解密:duc_wyinau{lap40o}
第18次解密:ctb_vxhmzt{kzo40n}
第19次解密:bsa_uwglys{jyn40m}
第20次解密:arz_tvfkxr{ixm40l}
第21次解密:zqy_suejwq{hwl40k}
第22次解密:ypx_rtdivp{gvk40j}
第23次解密:xow_qschuo{fuj40i}
第24次解密:wnv_prbgtn{eti40h}
第25次解密:vmu_oqafsm{dsh40g}
第26次解密:ult_npzerl{crg40f}

看上去符合要求，用栅栏密码解密试试

栅栏密码

hyg_acmrey{pet40s}

输入每栏的字符数(100内的整数且必须是字符总数的因数)

加密↓ 暴力解密↓

2字一栏：hgame{e4sy_crypt0}
3字一栏：h_mye0yar{tsgcep4}
6字一栏：hmeyrtge4_y0a{scp}
9字一栏：hyy{gp_eatc4m0rse}

看上去很对，但提交之后是错的，怎么试都是错的。。。开始怀疑人生，后来发现，在凯撒解密的时候大写字母全部被替换成了小写字母，导致错误，找到几个大写字母的位置，修改后得到正确的 flag