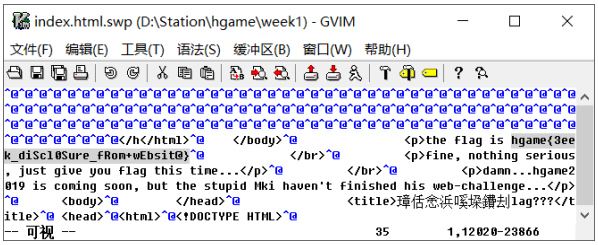
Web

1. 谁吃了我的 flag

   题干 vim 非正常退出，可知可能存在 swp 自动备份文件，请求下载

   后用 vim 即可。



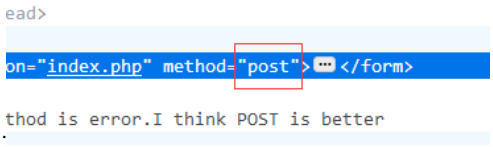
   给自己划的重点： 

←这**的是错的!!!

   默认文件是：.原文件名.swp（前面有点!）即 

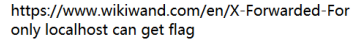
2. 换头大作战

   随便输入点什么，出现提示 request method is error.I think POST is better

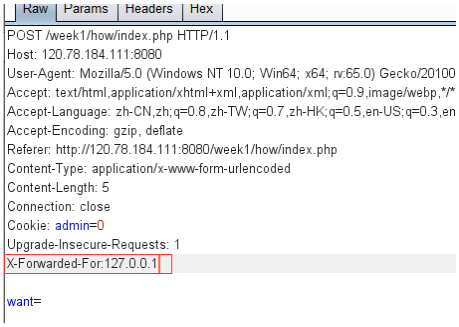


   咱菜鸡照着出题爸爸说的来就是了…

   get 改成 post

   再提交， 

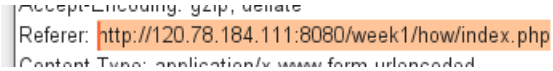
，这网页我没打开，大概被墙了。不过看起来是个 X-Forwarded-For 的维基百科还是啥的…反正查这个就对了。于是在出题爸爸的谆谆指导下我了解了这玩意的用法，大体意思就是放 http 请求头里中转个代理服务器，再根据提示，only localhost can get flag，localhost 即 127.0.0.1，就是要先转到 127.0.0.1 再访问。然后用 burpsuite 在报文里添加 X-Forwarded-For:127.0.0.1



发送后出现新提示 https://www.wikiwand.com/en/User_agent

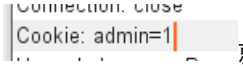
please use Waterfox/50.0 这次是改 User_agent

改成 Waterfox/50.0，当然别忘加上一步的 XFF 头。下一步提示
https://www.wikiwand.com/en/HTTP_referer
the requests should referer from www.bilibili.com，继续改就是了，referer 改成 B 站。

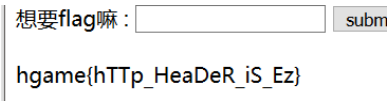


就这个改掉。下一步 https://www.wikiwand.com/en/HTTP_cookie

you are not admin。改 cookie 呗…(出题爸爸你真耐心…)，



就这个，=1 就行，啥原理不大清楚。然后就是结果（终于结束了…这一遍一遍的….）



3. very easy web

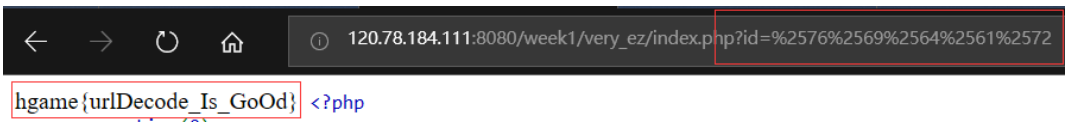
打开就是一脸码。凭 C 的记忆推理…

```php
<?php
error_reporting(0);
include("flag.php");

if(strpos("vidar",$_GET['id'])!==FALSE)  // id 字符串不等于 vidar，否则挂掉
  die("<p>干巴爹</p>");

$_GET['id'] = urldecode($_GET['id']);  // id urldecode 解码
if($_GET['id'] === "vidar")             //   解码后等于 vidar 打印 flag
{
  echo $flag;
}
highlight_file(__FILE__);
?>
```

总之意思就是输入 id=x，x 是 vidar 的 urlencode 的值。

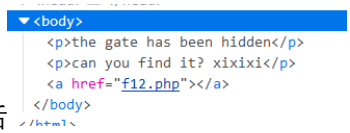
那么问题来了…字母不能 urlencode!!!

查了下原理，硬着头皮把 vidar 转成了 ascll 码然后加上%即%76%69%64%61%72 再 url 编码，得 %2576%2569%2564%2561%2572 。



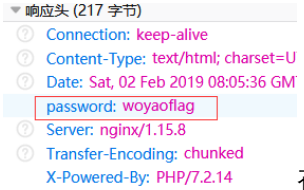
4. can u find me?

出题爸爸说，问 12 姑娘，然后

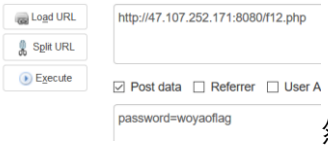


，再 47.107.252.171:8080/f12.php，please

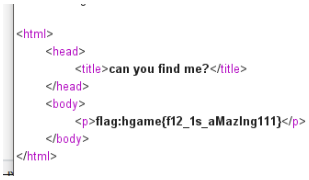
post password to me! I will open the gate for you!



在报文里能找到。用 hackbar Post 过去



然后出现链接，点开被 304 转走了，回头，用 Burpsuite 拦下中间网页。



，结了。

RE

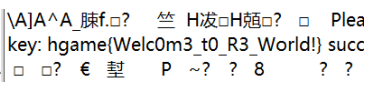
1. brainfxxker

```
,>++++++++++[<---------->-]<++[+.]
,>+++++++++[<---------->-]<-[+.]
,>+++++++[<------->-]<---[+.]
,>++++++[<------>-]<+++[+.]
,>++++++++[<---------->-]<++[+.]
,>++++++++++[<---------->-]<--[+.]
,>++++++++++[<--------->-]<-----[+.]
,>++++++++++[<---------->-]<+[+.]
,>+++++++++[<--------->-]<---[+.]
```

九个输入，要求输出没乱码。就是 ascll 码++--的，第一行是 x-10*10+2=x-98，不出乱码就得跳过[+.]结构，否则…ascll 码加一下输出一个，不乱码才怪了啊…即第一个数 ascll 码为 98，就是 b，后同，我就先不算了。

2. HelloRe

记事本里瞅一瞅…



3. Pro 的 Python 教室(一)

```
enc1 = 'hgame{'
enc2 = 'SGVyZV8xc18zYXN5Xw=='
enc3 = 'Pyth0n}'
secend = base64.b64encode(secend)
```

base64 一波出答案。

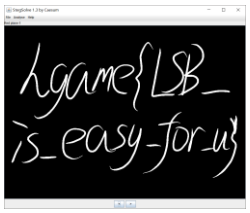
PWN

我！一道都没做出来…有大佬收倒水工吗…?

MISC

1. Hidden Image in LSB

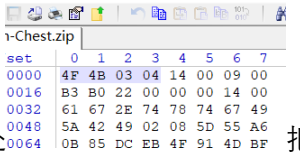
   明示十分到位…出题爸爸爱鸡人士(咳咳..我说的是菜鸡)



2. 打字机

   就是键盘(还是京紫的…)，一个字母一个字母对上去，艹蛋的是大小写。

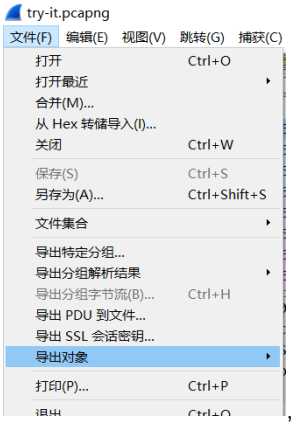
3. Broken Chest



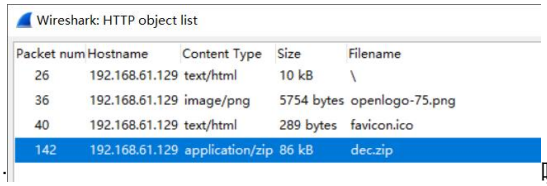
Zip 包坏了，根据提(ming)示，打开 winhex，此处 把文件头标识改成 504B0304，解压即可。

4. Try

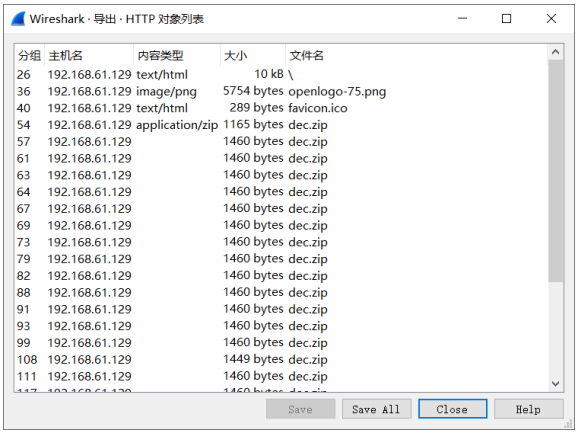
给了一个 pcapng 文件，wireshark 打开，



，没对象没关系，咱可以导出嘛…HTTP 的对象…



嗯，zip，就这玩意导出来。当然，如果你的 Wireshark 出现了这种情况：



请立刻将它删掉再下一个…别问我是咋知道的…挺悲伤的…

好的，得到了 dec.zip 解压，出了一个带密码的 zip，以及一个 txt，hgame********,其实我也不懂啥意思…弄了好久才知道要掩码爆破掉…

解压出了个 1.jpg，哦吼？搞了这一两天就给看个妹子…?(……)
查资料把…各种查…行吧，似乎是叫伪加密，改后缀名，再用 winrar 修复一下就行了，里面是个 word，复制不出来，因为上了“隐藏“属性，关掉，最熟练的复制粘贴结束。

CRYPTO

1. Mix
   咱没 URL 就别挂成吗…我感觉有点小悲伤…
   --.../....-/....-/-.../--.../...--/...../..-./-..../-../-..../..-./--.../----./....-/....-/--.../.----/-..../-.../--.../-.../-..../..---/...../.----/-..../-..../...--/....-/...--/-----/-..../...../--.../-.. 莫尔斯电码就是了，找个工具翻一下，744B735F6D6F7944716B7B6251663430657D，这应该是段 Base16，数字+A-F，翻一下，tKs_moyDqk{bQf40e}，然后凯撒(key=14，试到 14 刚好出现字母 h g a m e 这五个)再栅栏换位一波就出来了。

2. Base 全家
   开局一件 txt，翻译全靠手。
   最初一大串是 64（有小写就 64），翻啊翻，翻到全是数，那就 16（数字+A-F），有 F 之后的大写字母还没小写的给 32，之后来回倒腾，越来越短越来越短，最后出来了一段 base58，翻一波结束。
   此题翻的次数比较少能用手翻…至于写脚本…学艺不精的我试了一试，然后 python 炸了…嗯…炸了…到死未响应…哪写坏了吧…
   其次，手翻的难点是…找工具…!