Web

换头大作战

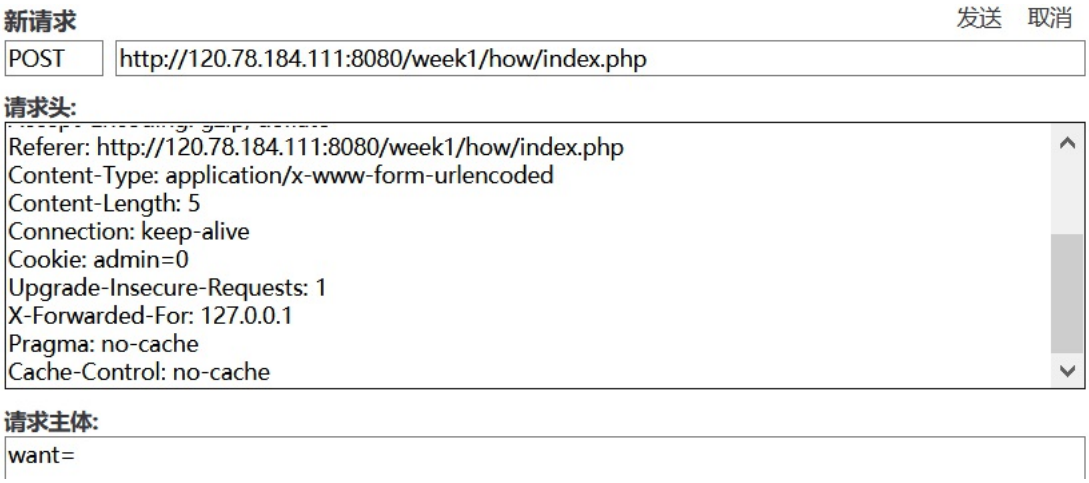
提示要用post，把源码里的method="get"改成method="post"。

得到提示

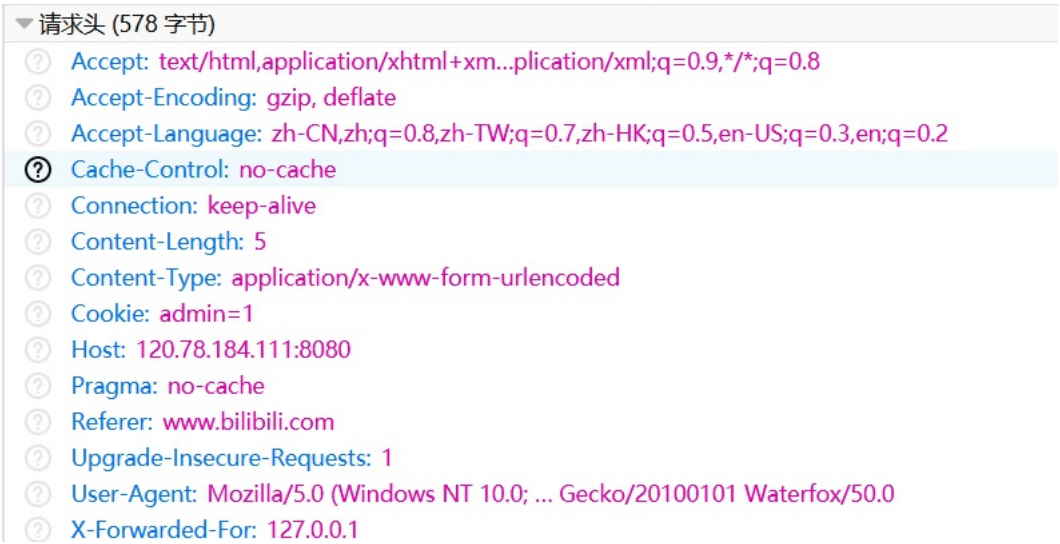
https://www.wikiwand.com/en/X-Forwarded-For
only localhost can get flag

查阅资料得知需在请求头中加入

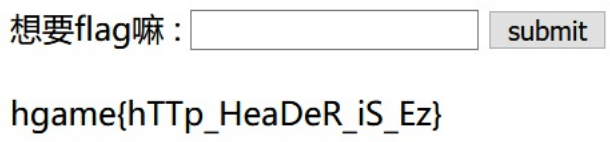
X-Forwarded-For: 127.0.0.1



得到提示要更改User_agent。把User_agent项最后Firefox/64.0改为WaterFox/50.0就好了
得到提示要更改referer。改成w w w.bilibili.com。
然后要改cookie 把admin的值改为1。



得到flag



hgame{hTTp_HeaDeR_iS_Ez}

very easy Web

先看代码

```
<?php
error_reporting(0);
```

```
include("flag.php");

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

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

emmmm...不会php，不过百度一下就基本知道了

strpos() 函数查找字符串在另一字符串中第一次出现的位置。
$_GET会自动进行一次URL解码

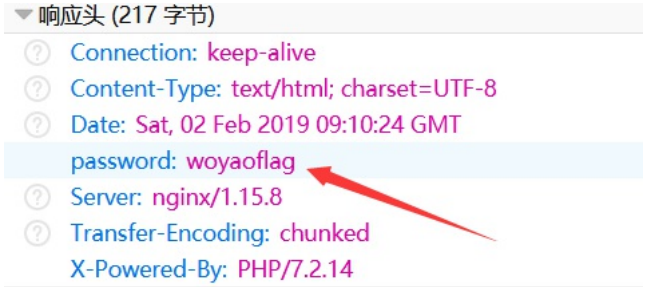
大概意思就是get方法上传的参数进行第一次解码之后不等于"vidar"
而经过 `urldecode($_GEt['id'])` 的两次解码之后等于"vidar"
所以就把"vidar"URL编码两次上传就好出flag了。
在线URL编码

can u find me?

f12看源代码

点进去

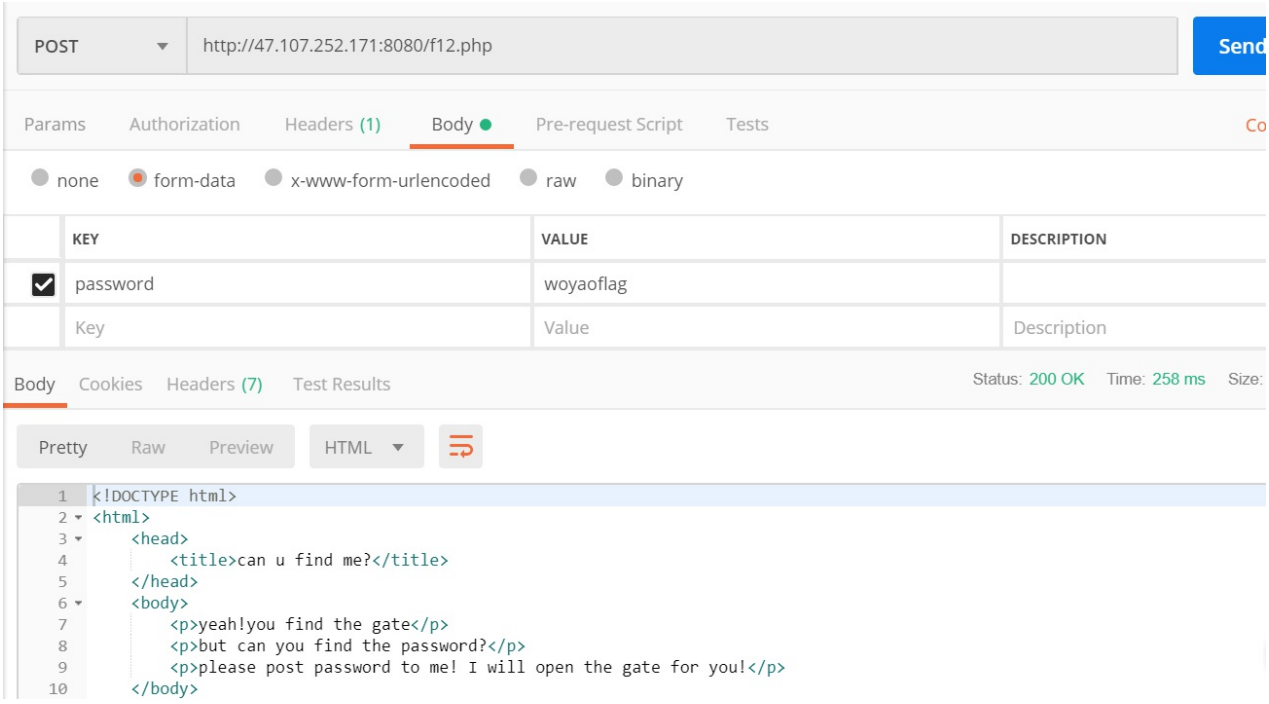
提示找password，找啊找，找到一个password 藏在响应头里



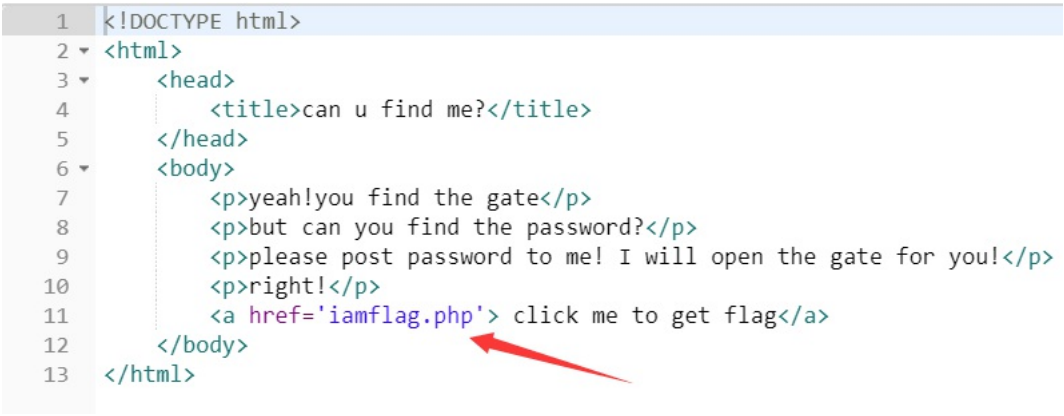
提示要把password POST给他，so

postman登场

(本菜鸡觉得用postman简单，嗯，只会用postman)



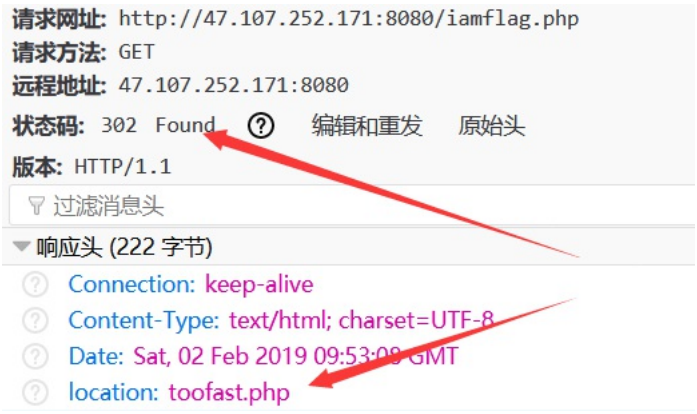
返回结果



点进去

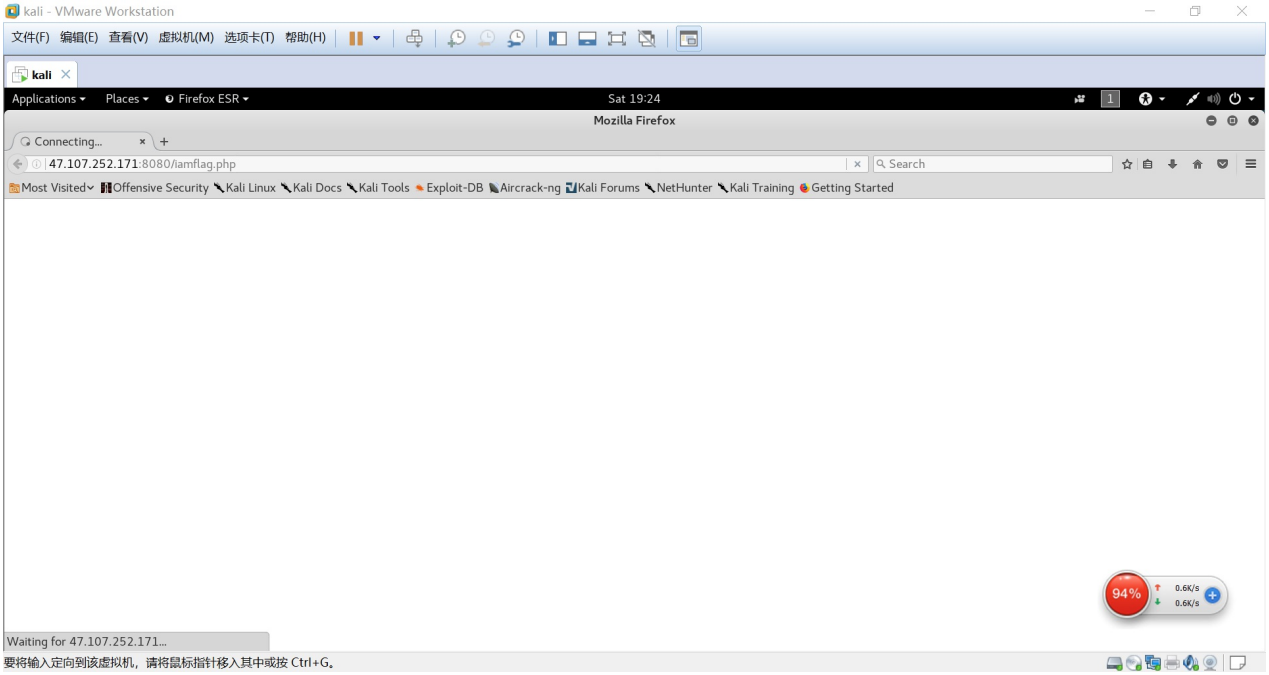
哇塞！惊呆了

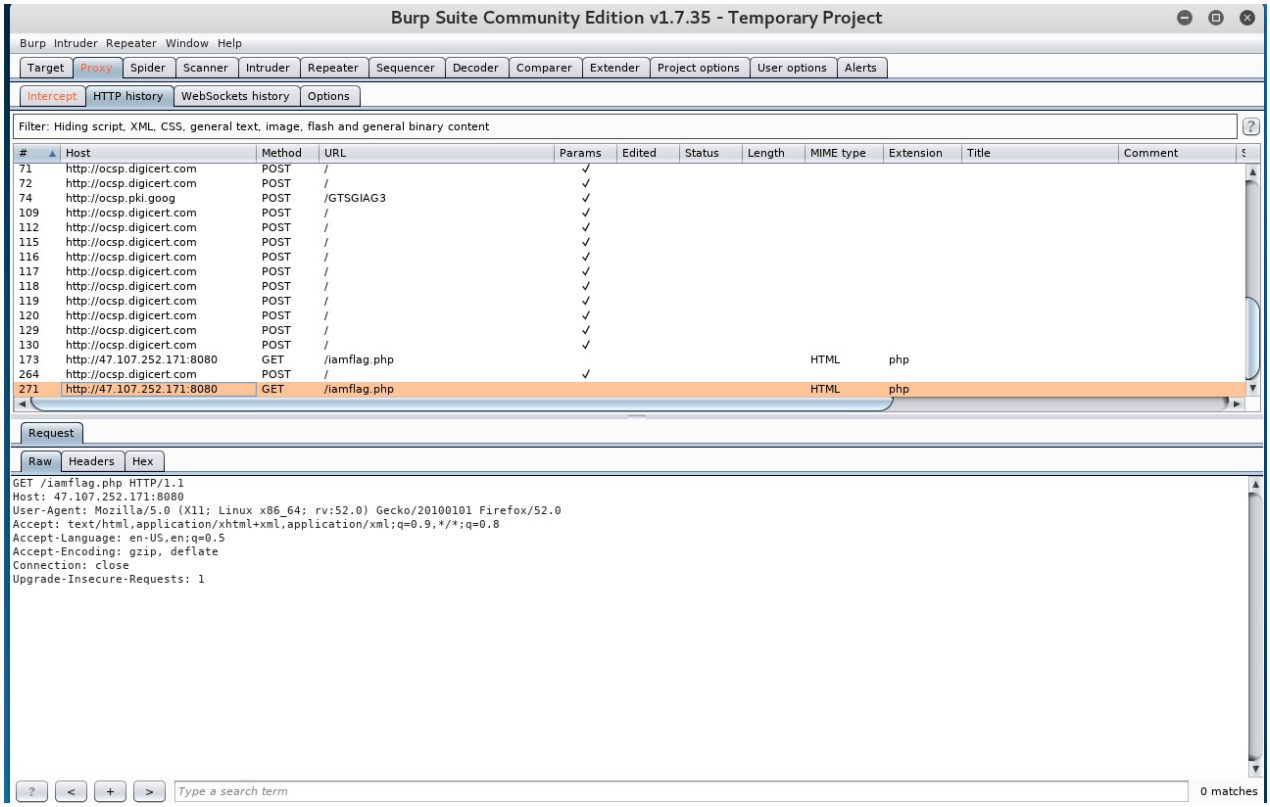
嗯。。。根据提示和资料可知是302跳转



然后 brupsuit 启动!

（不知道咋回事，虚拟机就是连不上，网络是正常的，然后就没有响应报文，然后就没有截图了）





然后拿到flag就行。。。

Re

brainfxxer

这题就改一下程序就好了

```
#include <iostream>
#include <cctype>

// Orz... I haven't learnt C++ before.
// It seems like my brain was fxxked by these codes...

// Notice:
// 1. the answer is your input when nothing strange was printed
// 2. that is, wrong inputs will encounter with the part "[+.]"
// 3. [!!!] REMEMBER TO WRAP YOUR ANSWER WITH "hgame{" AND "}"
//    [!!!] BEFORE YOU SUBMITTED IT

// oyiadin, Jan 18, 2019
// enjoy it! ;)
uint8_t data[100];
int ptr;
int* p;
namespace bf {

    class Parser {
    public:
        Parser() = default;
        ~Parser() = default;
        void execute(const std::string &buf);

//    protected:
//        data[100] = { 0 };
//        ptr = 0;
//        p = data;
    };


    void Parser::execute(const std::string &buf) {
        for (auto i = buf.cbegin(); i != buf.cend(); ++i) {
            switch (*i) {
            case '>':
                ++ptr;
                break;
            case '<':
                --ptr;
                break;
            case '+':
                ++data[ptr];
                break;
            case '-':
                --data[ptr];
                break;
            case '.':
                putchar(data[ptr]);
```

```
                break;
            case ',':
                while ((data[ptr] = getchar()) == '\n');
                break;
            case '[':
                if (!data[ptr]) {
                    while (*i++ != ']') continue;
                    --i;
                }
                break;
            case ']':
                if (data[ptr]) {
                    while (*(i - 1) != '[') --i;
                    --i;
                }
                break;
            default:
                break;
            }
        }
    }

}


int main() {
    bf::Parser parser;
    for (int i = 0; i < 127; i++)
    {
        data[ptr] = i;
        parser.execute(">+++++++++[<-------->-]<---");
        if (data[ptr] == 0)printf("%c", i);
    }

    getchar();
    return 0;
}

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

（就把最后几行注释的一行一行的带到程序里，就可以一个字一个字的出flag了！ 注意把","
和"[+.]"去掉）
嗯，下一题。

HelloRe

把文件用ida打开，发现flag

```
rax, 1
[rbp+rax+s], 0
rax, [rbp+s]
esi, offset s2  ; "hgame{Welc0m3_t0_R3_World!}"
rdi, rax        ; s1
_strcmp
eax, eax
```

Pro的Python教室(一)

这题么。。。

```
enc1 = 'hgame{'
enc2 = 'SGVyZV8xc18zYXN5Xw=='
enc3 = 'Pyth0n}'
```

你看这架势，吓死个人
enc2用base64解码，然后flag就出来了不是吗？
看不懂对enc3的蜜汁操作。忘记base64.b32encode(enc3)了？

Pwn

aaaaaaaaaa

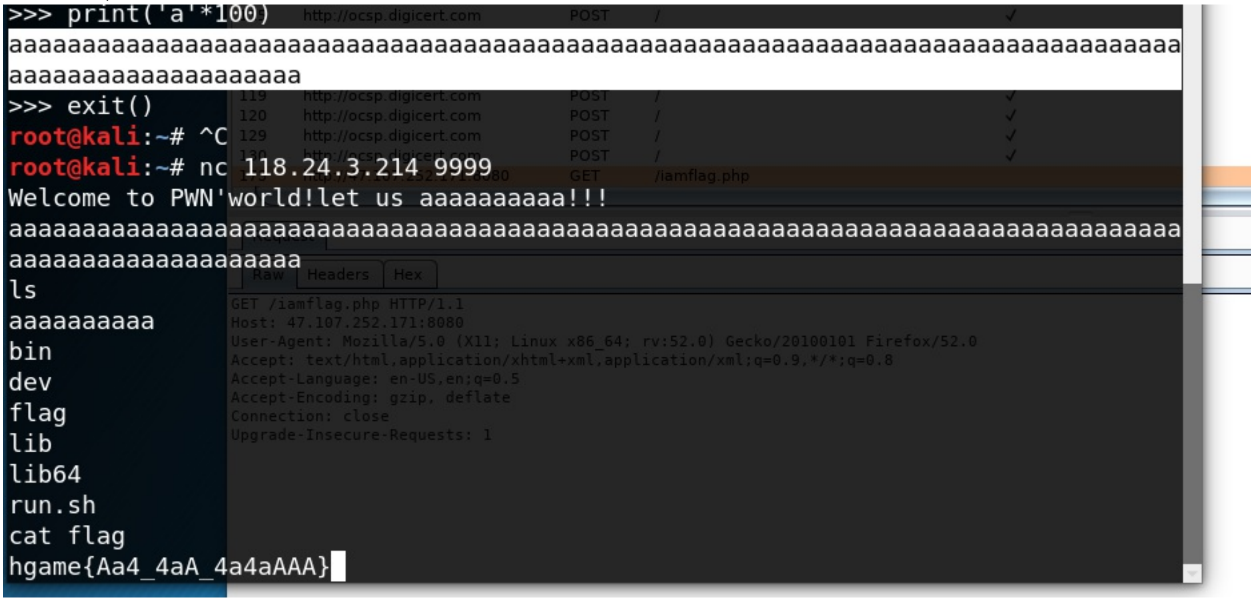
用ida打开，f5

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int v3; // eax MAPDST

  setbuf(_bss_start, 0LL);
  signal(14, (__sighandler_t)handle);
  alarm(0xAu);
```

```
  puts("Welcome to PWN'world!let us aaaaaaaaaa!!!");
  v3 = 0;
  while ( ++v3 <= 99 )
  {
    if ( getchar() != 97 )
      exit(0);
  }
  system("/bin/sh");
  return 0;
}
```

分析程序，开始pw n!

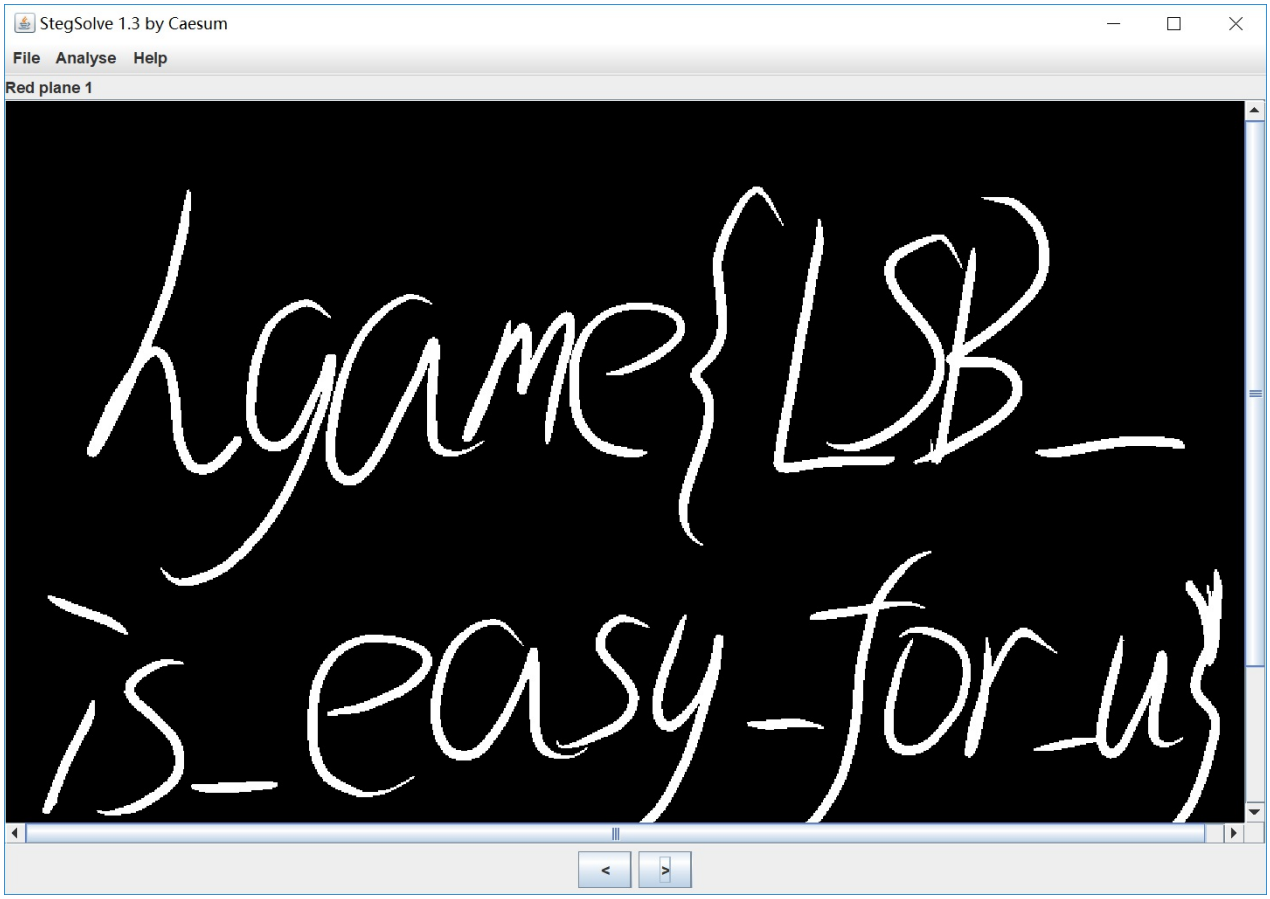


100个a，了解一下

Misc

Hidden Image in LSB

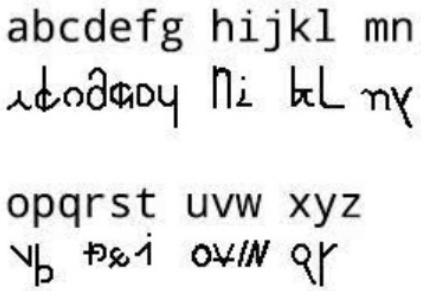
根据提示用StegSolve打开，出flag



打字机

根据提示，用谷歌以图搜图，我找到了这个

至此小写字母终于全部解读完成，得到了小写字母对照表（J Q Z的小写字符并没有出现）：



这就舒服啦，比某张图片舒服，秒出flag

end