bugku.welcome to the bugkuctf

原创

林夕林@ 于 2019-09-25 19:05:19 发布 190 收藏

分类专栏： bugku

本文链接：https://blog.csdn.net/qq_44598397/article/details/101380317

这里记录我花了一整天才理清题目意思的题目，因为接触CTF时间还不长，水平还停留在各个方面都稍有了解，但是涉及的知识稍微深入一些就没有思路了，这道题目涉及了php的代码审计，php的伪协议，php的序列化，php魔术方法。

因为我是小白一个，所以这道题目稍微把一些细节的地方说多一点，万一有些朋友看到其他writeup没看懂，看到我说的一些地方有可能就懂了。。。。

```
you are not the number of bugku !

<!--
$user = $_GET["txt"];
$file = $_GET["file"];
$pass = $_GET["password"];

if(isset($user)&&(file_get_contents($user,'r')==="welcome to the bugkuctf")){
    echo "hello admin!<br>";
    include($file); //hint.php
}else{
    echo "you are not admin ! ";
}
 -->
```


首先打开题目查看源代码以后：

从上面的代码可以看出以下信息：

通过get方法传递三个值：txt,file,password

读取$user文件的内容，并且文件内容要与‘welcome to the bugkuctf’相同

$file经提示应该为hint.php

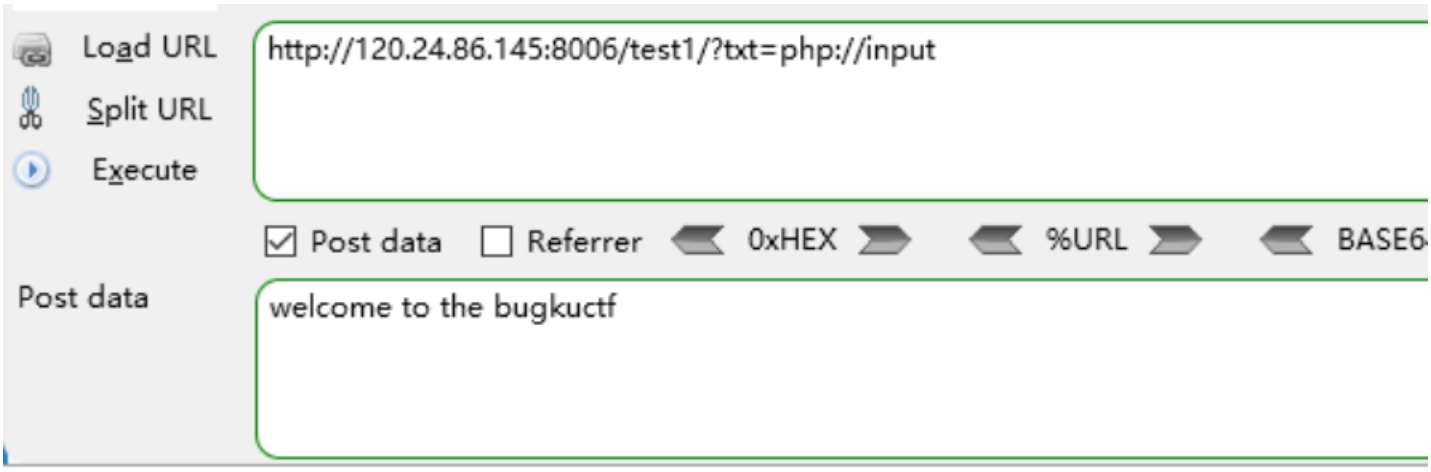
因为file_get_contents(

$user, r$)这个函数的意思是将 user这个文件的内容写到字符串里去，就是说$user$文件里的内容会变成一

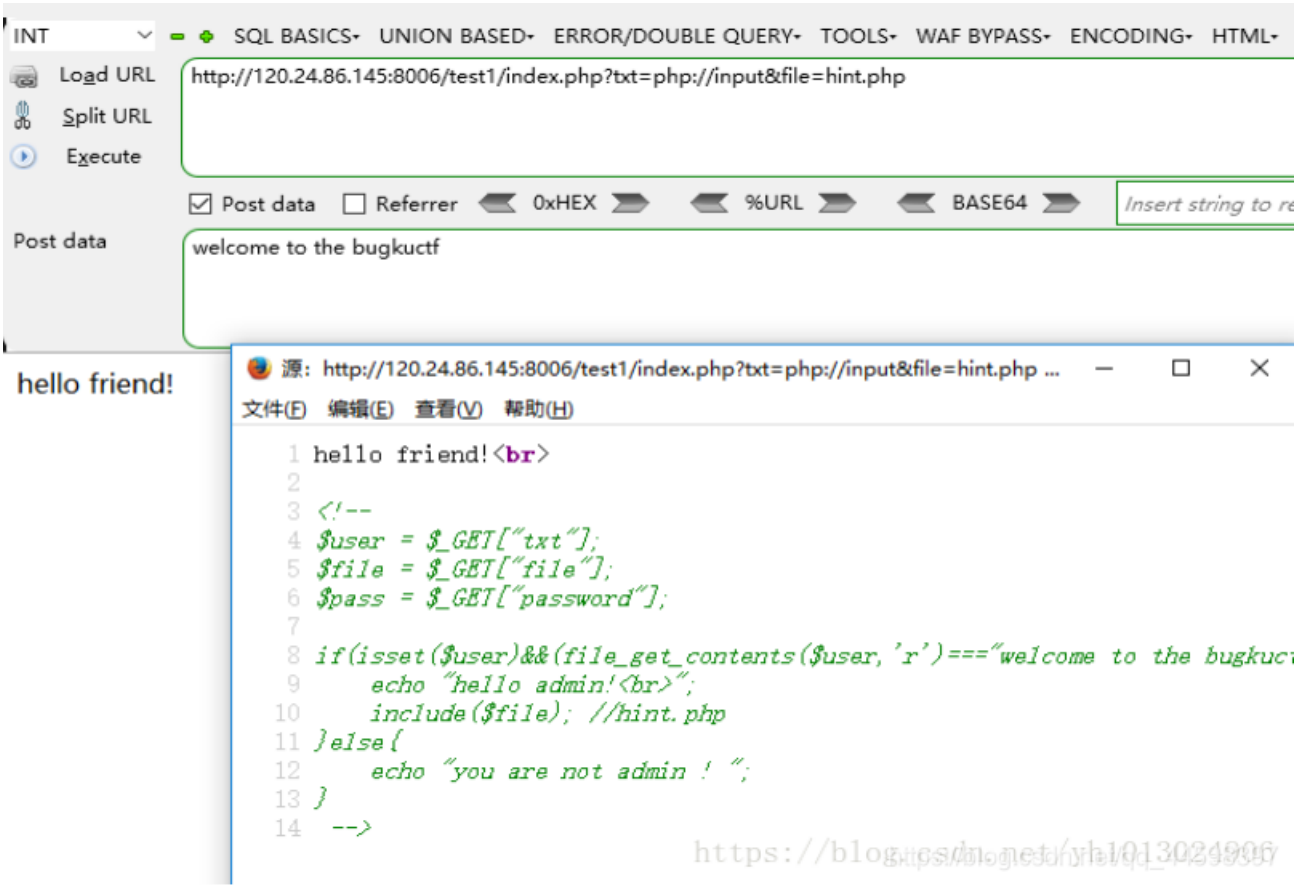
这里就涉及到一个php伪协议，就是php://input，它的大概意思就是可以读取我们post传递的数据。它的详解在这篇文章中有很好的解释 https://blog.csdn.net/qq_27682041/article/details/73326435。

所以看完了这篇文章的话，你应该就知道file_get_contents()函数里面放的不止文件名哦，还可以放php的伪协议，如果把这个

php://input作为文件名放进去的话，这个函数发现是一个伪协议，那作为一个“文件”，它里面肯定是没有内容的吧，那要怎么把它的内容变成一个字符串呢，它会读取我们post传递的数据作为它的”文件内容“，然后再变成一个字符串。
如说我们现在有这么一句 file_get_contents(“php://input”)，然后我们又post传递了一个数据的话，那这个数据就会被php://input读取到，然后file_get_contents又把它变成字符串。
所以我们构造txt=php://input，并且post一个"welcome to the bugkuctf"试试看



网页变了，但是为什么是一个hello friend!呢。。。。我也不知道，不过我们代码中的第一层已经解开了，再往下看吧。有一个include($file);//hint.php，首先我们知道include(file)是动态读取文件名，然后又提示我们hint.php，那岂不是说我们可以直接让file=hint.php就可以得到下一步信息了！



果然还是没有那么简单。。。不然怎么引出我们第二个php伪协议呢？php://filter 这个协议现在我只知道可

以用来读取网页base64编码后的源代码。用这句 file=php://filter/read=convert.base64-encode/resource=hint.php

就可以得到hint.php这个网页的base64编码后的源代码了。

```php
<?php

class Flag{//flag.php
    public $file;
    public function __tostring(){
        if(isset($this->file)){
            echo file_get_contents($this->file);
            echo "<br>";
        return ("good");
        }
    }
}
?>
```

光看这个代码是不是感觉信息不是很够呢，要不我们再看看index.php这个文件的源代码。

```php
<?php
$txt = $_GET["txt"];
$file = $_GET["file"];
$password = $_GET["password"];

if(isset($txt)&&(file_get_contents($txt,'r')==="welcome to the bugkuctf")){
    echo "hello friend!<br>";
    if(preg_match("/flag/",$file)){
        echo "不能现在就给你flag哦";
        exit();
    }else{
        include($file);
        $password = unserialize($password);
        echo $password;
    }
}else{
    echo "you are not the number of bugku ! ";
}

```

不要问我为什么知道要看index.php里的，因为这个一般是主页文件，有很重要的信息嘛，嘿嘿嘿嘿嘿嘿嘿。

可以看到这么多代码，虽然很烦，但是先从简单的地方来理解。

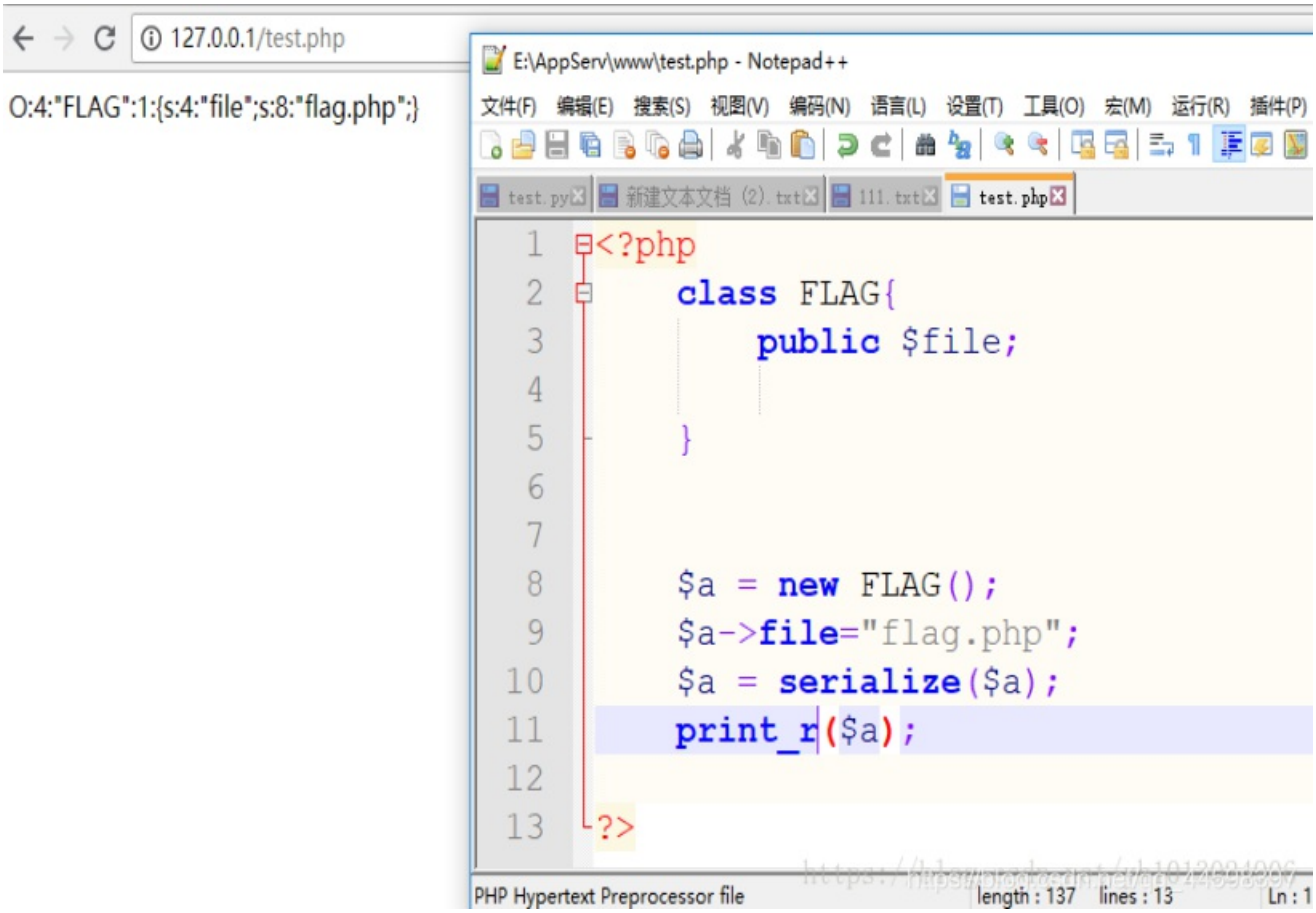
第一张图提示了我们flag.php，但是我们可以看第二张图，如果我们设定的文件名中包含'flag'，那么就会跳出"不能现在就给你flag哦"然后exit（）；

继续看第二张图，第一个if告诉我们，我们之前的大前提并没有改变，但是在这个前提下还附加了一些条件，如果文件名没有"flag"了，就会把这个文件包含进来,然后$password$进行反序列化，再输出password的值。什么是反序列化呢，那就要先知道序列化啦，在PHP中,序列化用于存储或传递 PHP 的值的过程中,同时不丢失其类型和结构（这是百度的）。我们可以把它想成一种编码嘛。

回到第一张图，定义了一个类 FLAG，类里面有一个$file属性，并且有一个魔术方法_tostring()，这个方法的作用就是当调用实例化对象时就会自动执行_tostring（）这个方法。简单来说创造一个这个类的对象就会调用这个方法。魔术方法呢，就是一个很神奇的方法（一本正经的胡说八道），大概就是一种类里面默认的方法，你可以对它进行改造，类似于构造方法。反正大家都要了解的，去百度看看用法和详解吧。

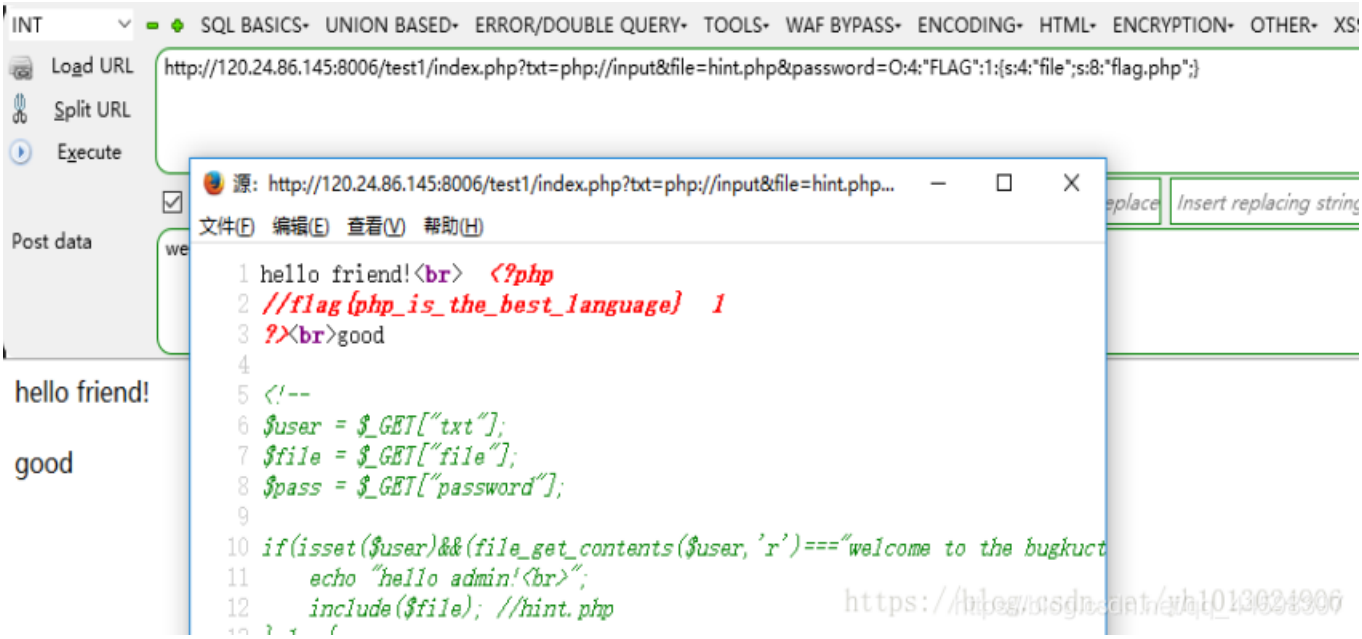
_tostring（）方法里面又定义了如果$file这个属性有赋值的话，那么就会输出这个文件的内容（输出成一个字符串）。

所以根据上面的这些条件，我们可以让$password为FLAG类型，并且让FLAG中的file就等于flag.php，这样我们就可以得到flag.php的内容了，不过要记得，前面$password进行了反序列化的操作，所以我们要先把它序列化。写一个php脚本吧！



在本地的服务器跑一下，我们就可以得到序列化的一个FLAG类咯。大家如果还没有搭本地服务器的话，推荐先自己学习一下怎么搭建环境，在本地可以自己试验各种php代码，可以自己了解数据库一些操作等等。下一个APPSERV就可以啦，这是一个合集，也是有中文的，网上都有教程的，很简单。

那最后我们就给$password赋值吧！



得到了flag啦。

感谢您的观看，这是我的第一篇文章，没有什么写作的经验，而且自己现在的技术没有多高，就是一个刚入门的小白，因为经常在**writeup**上看不懂，所以我会用自己理解的方式做下笔记，方便自己以后查看的时候能够看懂，在一些名词的解释方面可能不太正确，推荐大家去看看大佬们的解释，我只是用自己的方式记忆。。。。如果文章中有哪里出错，希望您可以指出让我改进，如果有和我一样刚入门的小白想知道**bugku**上其他一些题目的思路也可以告诉我，如果我会的话，会尽力写一篇**writeup**讲解的，再次感谢！

以下自己的过程：