BugkuCTF-Web-变量1

原创

烟雨天青色 于 2018-12-19 19:57:32 发布 1898 收藏 7
分类专栏： CTF 文章标签： BugkuCTF

打开解题链接发现是一段PHP代码，虽然还没正儿八经学PHP，但是，一顿乱分析之后还是能发现一点问题的，哈哈哈哈哈哈哈哈

接下来我们来分析一下源码：

```
flag In the variable ! <?php


error_reporting(0);          // 关闭php错误显示
include "flag1.php";         // 引入flag1.php文件代码
highlight_file(__file__);
if(isset($_GET['args'])){    // 通过get方式传递 args变量才能执行if里面的代码
    $args = $_GET['args'];
    if(!preg_match("/^\w+$/",$args)){
    // 这个正则表达式的意思是匹配任意 [A-Za-z0-9_] 的字符，就是任意大小写字母和0到9以及下划线组成
        die("args error!");
    }
    eval("var_dump($$args);");// 这边告诉我们这题是代码审计的题目
}
?>
```

根据最后一句代码：var_dump（）可知，这是代码审计。。于是。。。于是。。。我想起了PHP里面的一个超级全局变量GLOBALS。

提示说flag在变量里面，经分析只要运行 eval("var_dump($$args);");，falg很有可能就会出来

$$args====>我们可以猜想$args很有可能是一个数组，应该想到的就是超全局变量$GLOBALS

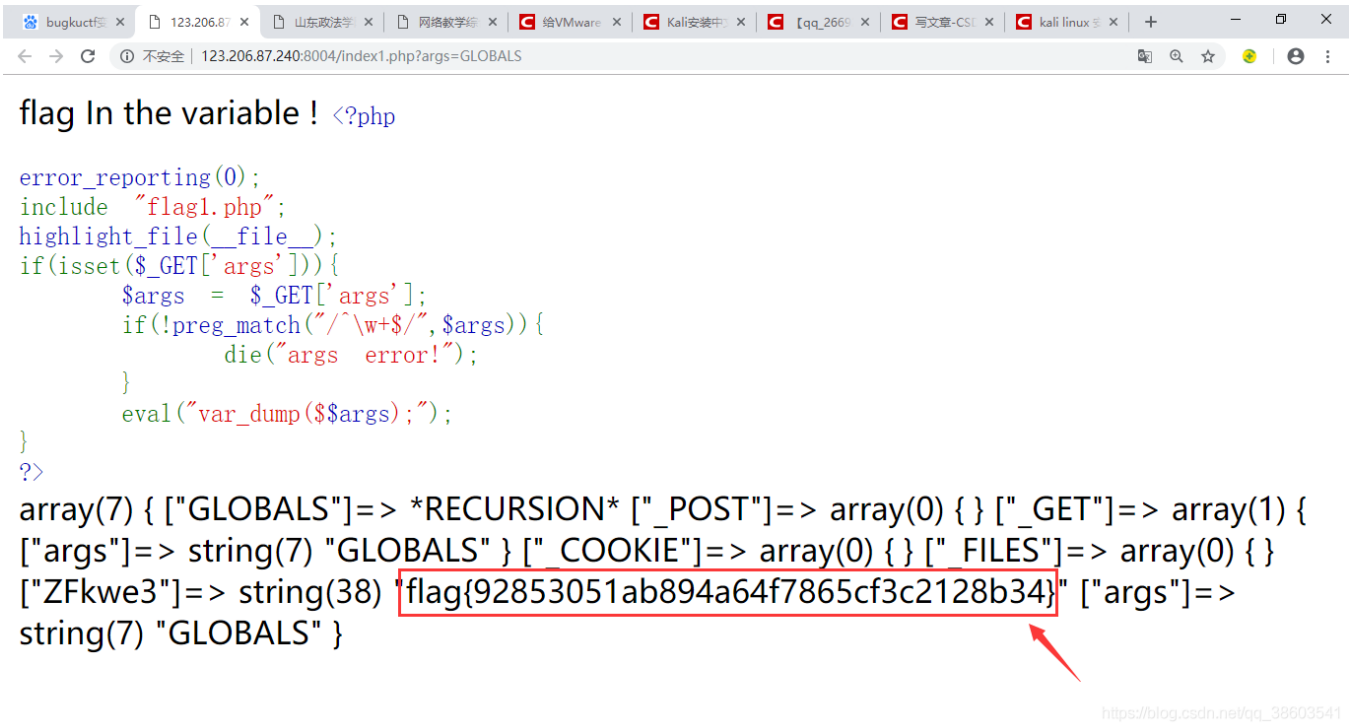
他是用存储全局变量的，全局变量的值在这个超级全局变量里面是一个键值，先当于hashmap的键值对

全局变量可以通过变量名在$GLOBALS找到相对应的值。

eval()这个函数的作用是字符串里面的php代码按正常的php代码被执行

通过构造一个GET参数，直接传GET一个全局变量即可

http://123.206.87.240:8004/index1.php?args=GLOBALS



构造之后，直接在浏览器中运行，网页爆出了flag。