变量1-writeup

打开题目

点击访问链接

得到一串php代码提示

```
<?php
error_reporting(0);  //关闭错误报告（报错不显示）
include "flag1.php";  //引用flag1.php文件代码
highlight_file(__file__);  //语法高亮
if(isset($_GET['args'])){  //检查变量是否声明
    $args = $_GET['args'];  //赋值给变量$args
    if(!preg_match("/^\w+$/",$args)){
//!preg_match 不匹配，^匹配字符串的开始，\w匹配字母或数字或下划线或汉字等价于'[^A-Za-z0-9_]',$匹配字符串的结束 这里达到过滤作用。
        die("args error!");   //输出args error!并退出当前脚本
    }
```

```
    eval("var_dump($$args);");
//eval()将字符串作为php代码执行,var_dump()函数 打印变量的相关信息,显示关于一个或多个表达式的结构信息，包括表达式的类型与值。数组将递归展开值，通过缩进显示其结构。$$args可变变量
}
?>
```

可变变量（Variable variables）
可变变量是一种独特的变量，他允许动态改变一个变量的名称。其工作原理是该变量的名称由另外一个变量的值来确定，实现过程就是在变量的前面再多加一个美元符号“$”。
下面举一个例子，实例代码如下：

```
<?php
$args = "xiaowei";  //声明变量$args
$xiaowei = "www.axiaowei.cn";  //声明变量$xiaowei
echo $args;  //输出变量$args
echo "\n";   //换行
echo $$args; //通过可变变量输出$xiaowei的值
?>
```

再看提示的第一句话flag in the variable! （#flag在变量中）
上述的可变变量简单来说$args的值是另一个变量的变量名。那么$$args就代表另一个变量。所以我们就给args赋值一个变量名
我们测试php的中的超全局变量，将其变量名传入

超全局变量 – 超全局变量是在全部作用域中始终可用的内置变量
超全局变量:
$GLOBALS：[一个包含了全部变量的全局组合数组]
$_SERVER:[是预定义服务器变量的一种,所有$_SERVER开头的都是预定义服务变量]
$_GET：[用于获取url地址栏的参数数据]
$_POST： [用于接收post提交的数据]
$_FILES：[用于文件就收的处理img 最常见]
$_COOKIE： [用于获取与setCookie()中的name 值]
$_SESSION： [用于存储session的值或获取session中的值]
$_REQUEST：[具有get,post的功能，但比较慢]
$_ENV：[是一个包含服务器端环境变量的数组。它是PHP中一个超级全局变量，我们可以在PHP 程序的任何地方直接访问它]

直接构造payload：?args=BLOBLAS