变量1 writeup

原创

ctf小菜鸡 于 2020-02-08 17:11:01 发布 57 收藏

10.变量1

这是一道代码审计。

```
flag In the variable ! <?php

error_reporting(0);
include "flag1.php";
highlight_file(file);
if(isset($_GET['args'])){
$args = $_GET['args'];
if(!preg_match("/^\w+$/",$args)){
die("args error!");
}
eval("var_dump($$args);");
}
?>
```

抓住两个地方，一个是正则表达式匹配，不匹配则直接die，该正则表达式应该是匹配都是字母的串。然后最关键的是最后的KaTeX parse error: Can't use function '$' in math mode at position 21: …这是**可变变量**的意思，如$args的值是另一个变量的变量…args就代表另一个变量。所以我们就给args赋值一个变量名，那么PHP的九大全局变量，一个一个试。

```
$_POST [用于接收post提交的数据]
$_GET [用于获取url地址栏的参数数据]
$_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]
SERVER[是预定义服务器变量的一种，所有SERVER[是预定义服务器变量的一种，所有_SERVER [是预定义服务器变量的一种，所有_SERVER开头的都
$GLOBALS [一个包含了全部变量的全局组合数组]
$_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]
```

当args=GLOBALS时，flag出现。

array(7) { [“GLOBALS”]=> RECURSION ["_POST"]=> array(0) { } ["_GET"]=> array(1) { [“args”]=> string(7) “GLOBALS” } ["_COOKIE"]=> array(0) { } ["_FILES"]=> array(0) { } [“ZFkwe3”]=> string(38) “flag{92853051ab894a64f7865cf3c2128b34}” [“args”]=> string(7) “GLOBALS”
所以 flag flag{92853051ab894a64f7865cf3c2128b34}

可变变量

3.5.3 可变变量

可变变量是一种独特的变量，它允许动态改变一个变量名称。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“$”。

【例 3.16】 下面使用可变变量动态改变变量的名称。首先定义两个变量$change_name 和$trans，并且输出变量$change_name 的值，然后使用可变变量来改变变量$change_name 的名称，最后输出改变名称后的变量值，实例代码如下：（**实例位置：光盘\TM\sl\3\16**）

```
<?php
$change_name = "trans";          //声明变量$change_name
$trans = "You can see me!";      //声明变量$trans
echo $change_name ;              //输出变量$change_name
echo "<br>" ;
echo $$change_name ;             //通过可变变量输出$trans 的值
?>
```

结果为：

```
trans
You can see me!
```