bugku web 8 （文件包含）wp

原创

hfhqhkyyzyq 于 2021-02-25 19:43:33 发布 129 收藏

文章标签： php

本文链接：https://blog.csdn.net/yanfangjie/article/details/111127132

bugku web 8（文件包含） writeup

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

$_REQUEST[ ]

默认情况下包含了 ET、_POST、$_COOKIE的数组；

1、$_REQUEST可以接收_GET、POST、POST、_COOKIE发送的数据；

2、由于$_REQUEST 中的变量通过 GET、POST、和 COOKIE 输入机制传递给脚本文件，因此可以被远程用户篡改而并不可信，这个数组的项目及其顺序依赖于PHP的 variables_order 指令的配置。

这里的意思是可采用post和get两种方式将表域名为hello的数据赋值给变量$a
eval() 函数计算 JavaScript 字符串，并把它作为脚本代码来执行。

如果参数是一个表达式，eval() 函数将执行表达式。如果参数是Javascript语句，eval()将执行 Javascript 语句。

var_dump()
void var_dump (mixed expression [, mixed expression [, …]])
var_dump()方法是判断一个变量的类型与长度,并输出变量的数值,如果变量有值输的是变量的值并回返数据类型.
此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。
这里是将变量a的值打印到界面中。

这题有两种思路：
直接将flag.php文件读入变量hello中，然后让var_dump打印到界面中。

所以payload可为：?hello=get_file_contents(‘flag.php’)或者?hello=file('flag.php)

根据最基本注入''引号闭合的思路，很容易就想到了利用括号，毕竟，eval中是执行的代码段

最基本的，再利用eval()会将括号内的字符串当作php内部的代码来执行这一漏洞，构造payload ?
hello=);print_r(file(%22./flag.php%22));//

eval函数中，"“内部为代码，//只在代码中起作用，相当于只注释了；（在URL中%22指的是一个”）

由于eval()会将括号内的字符串当成php代码，所以会形成var_dump();print_r(file(%22./flag.php%22));//)这个程序，执行后得到flag的值。