BugKu-web8-文件包含

原创

这个bug我写过 于 2021-03-11 22:13:41 发布 269 收藏 4

分类专栏： CTF-web 文章标签： php include 文件包含

本文链接：https://blog.csdn.net/m0_51641607/article/details/114680018

~~不做writeup，只写新手详解~~

每处解析

include" "

$_REQUEST

\@？$

eval()

var_dump()

show_source(__FILE__);

print_r（）

flag

审代码

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

include" "

include文件包含是解题关键，漏洞

PHP include 和 require 语句

通过 include 或 require 语句，可以将 PHP 文件的内容插入另一个 PHP 文件（在服务器执行它之前）。

include 和 require 语句是相同的，除了错误处理方面：

require 会生成致命错误（E_COMPILE_ERROR）并停止脚本
include 只生成警告（E_WARNING），并且脚本会继续
因此，如果您希望继续执行，并向用户输出结果，即使包含文件已丢失，那么请使用 include。否则，在框架、CMS 或者复杂的 PHP 应用程序编程中，请始终使用 require 向执行流引用关键文件。这有助于提高应用程序的安全性和完整性，在某个关键文件意外丢失的情况下。

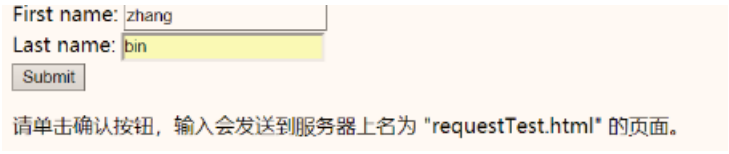
包含文件省去了大量的工作。这意味着您可以为所有页面创建标准页头、页脚或者菜单文件。然后，在页头需要更新时，您只需更新这个页头包含文件即可。

链接: include变量用法

$_REQUEST

PHP $_REQUEST 用于收集HTML表单提交的数据。
php中$_REQUEST可以获取以POST方法和GET方法提交的数据，缺点：速度比较慢 。

```php
<?php
            $fn=$_REQUEST["fname"];
            $ln=$_REQUEST["lname"];
            echo $fn.$ln;
            ?>
```



@？$

@ 屏蔽掉出错信息,有@时就算连接出错,也不会报错的
防止别人根据错误提示信息来推测出你的数据库结构进行注入攻击一类的黑客行为

$a表示变量a

？：
连接作用：
http://www.xxx.com/Show.asp?id=77&nameid=2905210001&page=1

清除缓存:
http://www.xxxxx.com/index.html
http://www.xxxxx.com/index.html?test123123
两个url打开的页面一样，但是后面这个有问号，说明不调用缓存的内容，而认为是一个新地址，重新读取。

eval()

eval() 函数用来执行一个字符串表达式，并返回表达式的值。
eval 函数的功能就是讲一个字符串当作 php 的代码进行执行

```
a = 1
b = 2
eval("a + b")
>>>3
```

就是说这里会执行
var_dump($a)

var_dump()

php的输出语句

show_source(FILE);

将此php以代码高亮的形式展现

~~新手理解请斧正~~

print_r（）

print_r：打印复合类型 如数组 对象等，打印关于变量的易于理解的信息。

flag

?hello=$a);print_r(file("./flag.php"));