i春秋-web-爆破-1

转载

大千SS 于 2018-11-12 16:54:56 发布 560 收藏 1
分类专栏： i春秋 文章标签： web


i春秋 专栏收录该内容
13 篇文章 0 订阅
订阅专栏

题目内容：flag就在某六位变量中。
题目

```
include "flag.php";
$a = @$_REQUEST['hello'];
if(!preg_match('/^\w*$/',$a )){//正则表达式^匹配一行的开头，$表示结束。\w表示匹配包括下划线的任何单词字符，等价于'[A-
  die('ERROR');
}
eval("var_dump($$a);");//var_dump — 打印变量的相关信息
show_source(__FILE__);//__FILE__当前运行文件的完整路径和文件名。
?>
```

这个代码的作用是如果匹配正则表达式`/^\w*$/`，就打印变量`$$a`
`$a`是hello，`$$a`是六位变量`$hello`
由于`$a`在函数中，所以函数之外无法访问。如果要访问，将hello修改为超全局变量GLOBALS。
在URL后加`?hello=GLOBALS`，将参数hello修改为Globals
实际执行语句：

```
eval("var_dump($$a);")
eval("var_dump($hello);")
eval("var_dump($GLOBALS);")
```

$GLOBALS的作用：引用全局作用域中可用的全部变量。就可以导出所有的变量
这样就会打印出当前定义的所有变量，也包括 include 的文件中的变量，flag 也存在在这些变量中。

参考：PHP 全局变量 - 超全局变量
超全局变量
$GLOBALS
百度杯-二月场(Misc-Web)爆破-1

转载自简书：https://www.jianshu.com/p/f7055d3f3bb0