# i春秋之爆破-1

原创

金 帛 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

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



打开连接，是段php代码，审计一下代码

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



@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$a匹配正则表达式/^\w*$\/，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