

PHP中register_globals引发的问题 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/167/2021_2022_PHP_E4_B8_ADregi_c103_167245.htm 前几天要命了。。因为偷懒，服信建材拿tg的代码来复用了一下，，本地测试完，传到新开的虚拟主机上去。。不能登录，phpinfo().看了一下，果然是register_globals没开。。要信诺立给开是不可能了。。如何有效地改最少的代码，让全部程序正常地跑起来呢。。刚学PHP的时候，官方文档上demo建议用户关闭全局变量并且用\$_REQUEST["XXX"]、\$_POST["XXX"]等方式获得表单传送过来的数据，当时也没有深究究竟为什么要这么做，惯性的力量真的是比较强大。。后来看myg(就用缩写了，省得待会儿又被他用so361.com[广告]什么的搜出来。。)写的程序看得多了，我也就跟着全部用全局变量传递表单提交的数据。没想到这下碰到了钉子。先重新回头去看看register_globals究竟工作原理是怎样。。开起来有什么不好。。其实在相当一段时间内，PHP作为应用的最广泛的服务器端脚本语言的最大卖点之一就是会为从表单提交的值自动建立一个全局变量。方便多个资源跳转时数据的共享。我们通常这样来写一个身份验证程序：
\$authorized = false. //稍微小心一点的程序员还会将其初始化为false
if (frm_username == "\$v_username" amp.
\$frm_password! = "\$v_password") \$authorized = ture.
if (\$authorized == false) { . // 通过验证用户在这里显示的内容 }
else { . // 未授权的用户将在这里给予提示 那么，用户只要在请求验证程序的时候在url后面添加一个?\$authorized=false就可以成功突破安全限制，从而获得访问权力了，恐怖。所以

在4.1.*之后，php.ini中的register_globals选项默认为关闭，以防止此类事情发生。。因此EGPCS值将不会被作为全局变量来创建。但他们可以通过各自一个系统指定的数组来访问，他们被称为超全局变量：\$_ENV、\$_GET、\$_POST、\$_COOKIE和\$_SERVER。至于他们分别在什么时候用。。从名字就可以看出来。其实我们最常用的也就是\$_POST了。要让上面的程序跑起来。。我们只需要在上面的程序里添两行代码：\$frm_username = \$_POST[frm_username]. \$frm_password = \$_POST[frm_password]. 还有一点好处就是以前当register_globals开启时，我们需要增加一行代码以在函数中获取\$frm_username和\$frm_password等变量的值 global \$frm_username, \$frm_password, ... 即使是使用\$HTTP_POST_VARS数组以获得表单提交传递过来的值，但是我们还是需要从全局范围导入这个数组：global \$HTTP_POST_VARS. \$frm_username = \$HTTP_POST_VARS[frm_username]. \$frm_password = \$HTTP_POST_VARS[frm_password]. 但是在PHP 4.1及以后的版本中，特殊的\$_POST变量(以及上面提到的其它变量)则完全不必那么麻烦地做，EGPCS值可以在所有范围内使用而不需要先先在函数中申明了，而且特殊的\$_SESSION数组的引入实际上也大大简化了session代码。我们完全不必将session变量申明为全局变量，然后再去留意哪些变量是否被注册了，我们现在可以简单地从\$_SESSION[varname]中引用所有的session变量。需要修改的代码也十分十分的简单。。 session_start(). if (frm_username == "\$v_username" amp. \$frm_password! = "\$v_password") \$_SESSION[authorized] = true. 我们只需要直接

在\$_SESSION数组中设置authorized变量，然后用同样的方法使用它。这样程序变得更短了，而且对于全局变量中是否有重名也不会引起混乱了。。就这么简单，想想还不就那么回事嘛。。前两天绞尽脑汁想有什么简单点的方法避免修改全部代码。。就是想不出来。。今天问孟誉国死活要了一份他的解决方案：//全局变量设置

```
function globals() { global
$HTTP_SESSION_VARS, $HTTP_POST_VARS,
$HTTP_GET_VARS, $HTTP_COOKIE_VARS. while
(list($tmp_key, $tmp_value) = each($HTTP_SESSION_VARS)) {
$name = $tmp_key. global $$name. $$name = $tmp_value. } while
(list($tmp_key, $tmp_value) = each($HTTP_POST_VARS)) {
$name = $tmp_key. global $$name. $$name = $tmp_value. } while
(list($tmp_key, $tmp_value) = each($HTTP_GET_VARS)) {
$name = $tmp_key. global $$name. $$name = $tmp_value. } while
(list($tmp_key, $tmp_value) = each($HTTP_COOKIE_VARS)) {
$name = $tmp_key. global $$name. $$name = $tmp_value. } }
```

拿到之后一拍脑脑袋。。不是自己就能写嘛。。。而且代码可以更简单：

```
if(!empty($_GET)) extract($_GET).
if(!empty($_POST)) extract($_POST). if(!empty($_COOKIE))
extract($_GET). if(!empty($_SESSION)) extract($_POST).
```

检查变量是否为空，如果非空，去掉数组头，导入到当前符号表。或者用foreach遍历数组的同时转换掉格式，

```
if(!ini_get(register_globals)) foreach ($_POST as $key => $value)
unset($GLOBALS[$key]). ... ..
```

100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com