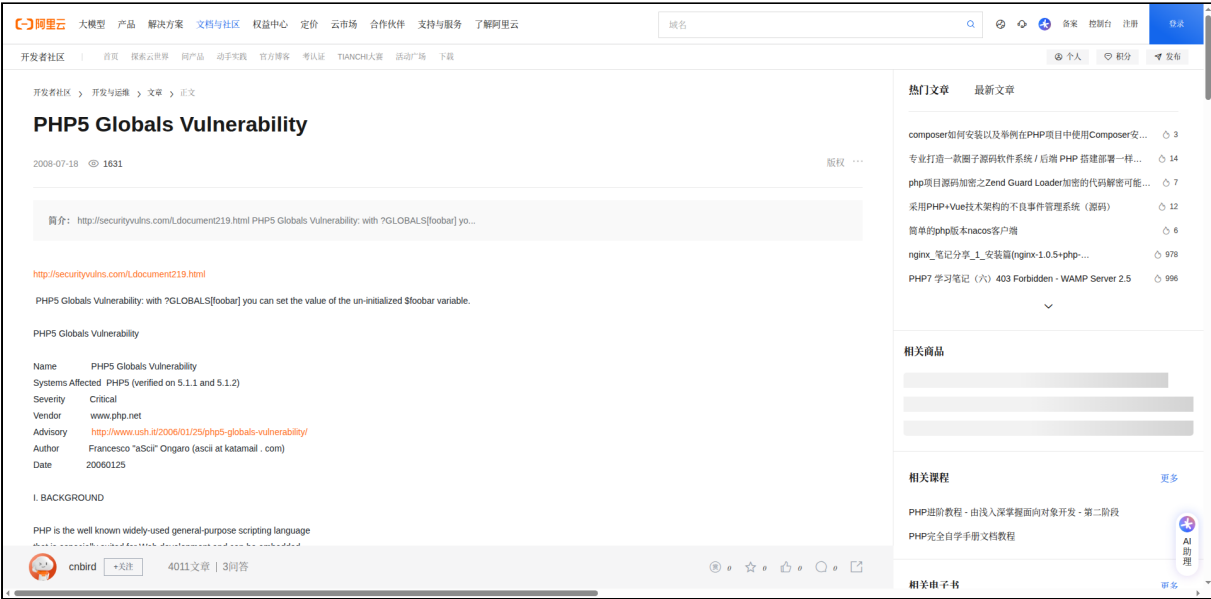


# PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

|                  |                                                                           |
|------------------|---------------------------------------------------------------------------|
| Source URL:      | https://developer.aliyun.com/article/453193                               |
| Archived Date:   | August 15, 2025 at 15:22                                                  |
| Published:       | July 18, 2008                                                             |
| Document Type:   | Web Page Archive                                                          |
| Wayback Machine: | https://web.archive.org/web/*/https://developer.aliyun.com/article/453193 |

## Page Screenshot



## PHP5 Globals Vulnerability

2008-07-18 © 1631

版权 ...

简介: <http://securityvulns.com/Ldocument219.html> PHP5 Globals Vulnerability: with ?GLOBALS[foobar] yo...

<http://securityvulns.com/Ldocument219.html>

PHP5 Globals Vulnerability: with `?GLOBALS[foobar]` you can set the value of the un-initialized `$foobar` variable.

## PHP5 Globals Vulnerability

|                  |                                                                                                                                 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Name             | PHP5 Globals Vulnerability                                                                                                      |
| Systems Affected | PHP5 (verified on 5.1.1 and 5.1.2)                                                                                              |
| Severity         | Critical                                                                                                                        |
| Vendor           | <a href="http://www.php.net">www.php.net</a>                                                                                    |
| Advisory         | <a href="http://www.ush.it/2006/01/25/php5-globals-vulnerability/">http://www.ush.it/2006/01/25/php5-globals-vulnerability/</a> |
| Author           | Francesco "aScii" Ongaro (ascii at katamail . com)                                                                              |
| Date             | 20060125                                                                                                                        |

## I. BACKGROUND

PHP is the well known widely-used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML.

## II. DESCRIPTION

Everybody knows the GLOBALS vulnerability, this is a serious bug and can leak in a lot of different bugs in applications otherwise secure.

(Text from [http://www.hardened-php.net/advisory\\_202005.79.html](http://www.hardened-php.net/advisory_202005.79.html))

- > In PHP5 <= 5.0.5 it is possible to register f.e. the global
- > variable \$foobar [...] by supplying a GPC variable called
- > \$\_GLOBALS[foobar]?

As I was saying everybody knows this, except me :) While conducting some VA and code review on PmWiki I rediscovered this independently. More details on this can be found in [PmWiki Multiple Vulnerabilities?](http://www.ush.it/2006/01/24/pmwiki-multiple-vulnerabilities/)  
(<http://www.ush.it/2006/01/24/pmwiki-multiple-vulnerabilities/>)

Trying to replicate the PmWiki bug on various PHP versions i discovered it was in reality also a PHP bug (in fact the PmWiki bug itself is PHP version dependent), but while it was supposed to affect only  $\leq 5.0.5$  we reproduced the same results in theoretically safe PHP versions.

!! Note: There has been some updates, read the first comment! !!

Lately we produced a (22 bytes long) POC to test the PHP vulnerability separately and we had the confirm that this bug is still here.

Will this advisory produce a third line in the changelog after these?

5.0.4 Fixed bug #31440 ([GLOBALScan](#)be overwritten via GPC when register\_globals is enabled). (Ilia) 5.1.0 Fixed possible GLOBALS variable override when register\_globals are ON. (Ilia, Stefan) If GLOBALS can override GLOBALS you could inject a variable into \$\_POST by \$\_GET or set \$\_ESS (cat > foo.php < EOF

```
<?php echo
fooBar;? > EOFThenqueryfoo.php?GLOBALS['fooBar'] = HELLO!|the poc prints out HELLO! your PHP version is vulnerable. Here the results collected : Branch4, register_globals ON : fixed and no effect 5.0.5 win, register_globals ON : affected, WORKS! 5.1.
GLOBALS;?>
```

#### IV. DETECTION

PHP 5.1.1 and 5.1.1 is vulnerable (this advisory).  
 PHP <= 4.3.10 should be vulnerable (bug discovered by Stefan Esser).  
 PHP <= 5.0.5 is vulnerable (bug discovered by Stefan Esser).  
 Older version not verified. PHP 5.1.0 not verified.

## V. WORKAROUND

Register global off will fix. This PHP code will mitigate this bug.

```
// put this code before everything
if (isset($_POST['GLOBALS'])) {isset($_POST['GLOBALS']) ||
isset($_POST['FILES']['GLOBALS']) ||isset($_FILES['GLOBALS']) ||
isset($_POST['ETV']['GLOBALS']) ||isset($_GET['GLOBALS']) ||
isset($_POST['COOKIE']['GLOBALS']) ||isset($_COOKIE['GLOBALS']) ||
trigger_error('Is this a GLOBAL GPC hacking attempt?', E_USER_ERROR);
```

For deeper fixage wait for an official patch.

## VI. VENDOR RESPONSE

This is a known bug in PHP <= 5.0.5, that seems to be still effective in PHP 5.1.1 and 5.1.2. I'll wait for official and Stefan Esser responses.

!! Note: There has been some updates, read the first comment! !!

Note:

## VII. CVE INFORMATION

No CVE at this time.

## VIII. DISCLOSURE TIMELINE

20060119 Bug discovered  
20060119 Internal release  
20060125 Initial release (only on ush.it)  
20060127 Initial release (only on sikurezza.org)  
20060128 Public release

## IX. CREDIT

Francesco "aSciì" Ongaro is credited with the discovery of this vulnerability.





联系我们

[文档](#) | [开发者社区](#) | [天池大赛](#) | [培训与认证](#)



[法律声明](#)及[隐私权政策](#) | [Cookies](#)政策

© 2009-2025 Aliyun.com 版权所有

增值电信业务经营许可证: 浙B2-20080101

域名注册服务机构许可: 浙D3-20210002

浙公网安备 3301060200975号浙B2-20080101-4