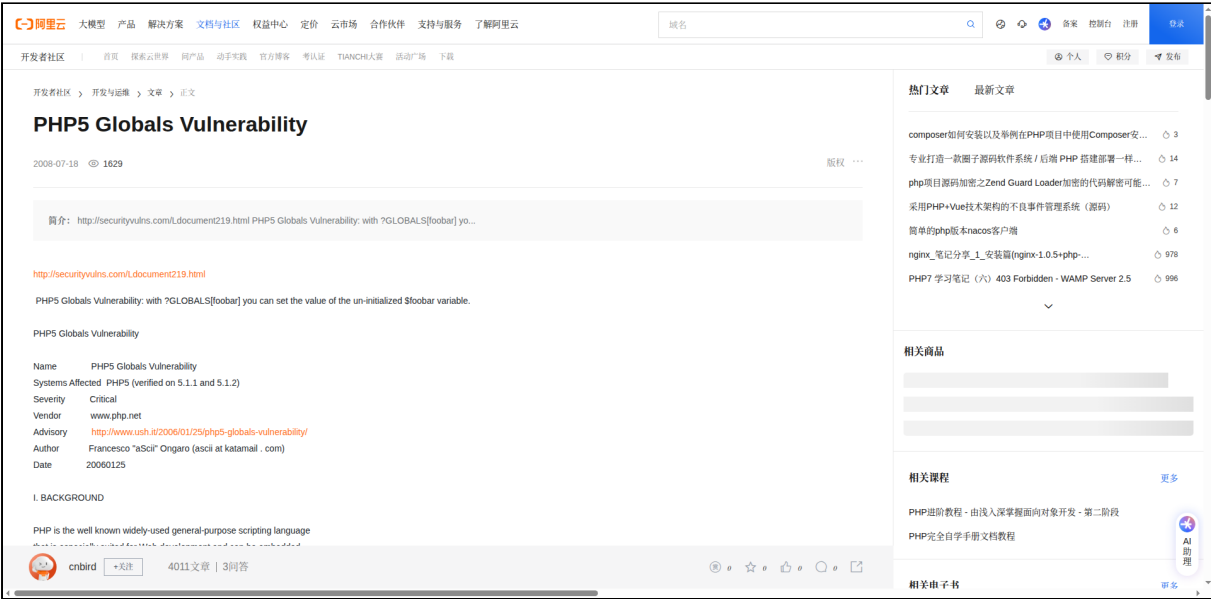


# PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

Source URL:	https://developer.aliyun.com/article/453193
Archived Date:	August 15, 2025 at 15:21
Published:	July 18, 2008
Document Type:	Web Page Archive
Wayback Machine:	https://web.archive.org/web/*/https://developer.aliyun.com/article/453193

## Page Screenshot



阿里云APP

查看产品优惠，实时监控云资源

阿里云

开发者社区

打开APP

个人

2009-07-18 1629

PHP5 Globals Vulnerability

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

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

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

PHP5 Globals Vulnerability

Name	PHP5 Globals Vulnerability
Systems Affected	PHP5 (verified on 5.1.1 and 5.1.2)
Severity	Critical
Vendor	www.php.net
Advisory	<a href="http://www.ussh.it/2006/01/25/php5-globals-vulnerability/">http://www.ussh.it/2006/01/25/php5-globals-vulnerability/</a>
Author	Francesco "aSci" 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 i.e. the global

> variable \$foo [...] by supplying a GPC variable called

> ?GLOBALS[foo]?

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.ussh.it/2006/01/24/pmwiki-multiple-vulnerabilities/) (<http://www.ussh.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 <= 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 (*GLOBALScanbeoverrittenviaGPCwhenregister\_globalsisenabled*). (Ilia)5.1.0FixedpossibleGLOBALSGlobalVariableoverridewhenregister\_globalsareON. (Ilia, Stefan)IfGLOBALScanoverrideGLOBALSthoughETorset\$ESSE cat > foo.php < EOF

<?php echo

foo;? > EOFThenqueryfoo.php?GLOBALS[foo]=HELLO!IfthepocprintsoutHELLOyourPHPversionisvulnerable.Heretheresultscollected: Branch4,register\_globalsON:fixedandnoeffect5.0.5win,register\_globalsON: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(\$\_FILES['GLOBALS'])||isset(\$\_GET['GLOBALS'])||isset(\$\_COOKIE['GLOBALS'])||isset(\$\_SERVER['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 ussh.it)

20060127 Initial release (only on sikuzezza.org)

20060128 Public release

IX. CREDIT

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

koba (who committed the VA on PmWiki, [sikurezza.org](mailto:sikurezza.org))  
Stefano Di Paola (testing on multiple vers. and poc, [wisec.it](mailto:wisec.it))  
Patrick R. Michaud (testing on 5.1.2, the PmWiki vendor)  
Ethan (testing 5.1.1)  
Saidone (testing 5.1.2)

Copyright (c) 2005 Francesco "aScii" Ongaro

Disclaimer: The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

关键词: PHP GLOBALS PHP vulnerability

## 相关文章

PHP SGLOBALS  global

卡尔特斯 90 阅读

技术小甜 1366 阅读

根据官方的解释是\$GLOBALS[*var*] 是外部的全局变量*var*本身。global *var* 是外部*var*的同名引用或者指针。(错误：是个别名引用而已，非指针！！) 举例说明一下：php纯技术探讨交流群：323899029\*\*\* 探讨（一）\*\*\*\*\*很多人都认为global和\$GLOBALS[]只是写法上面的差...

An attacker can exploit this issue by enticing an unsuspecting user to follow a malicious URI.

cnbird 778 阅读

<http://www.securityfocus.com/bid/54721/exploit>

cnbird 574 阅读

\_\_\_\_\_|||V\_\_||||||\_|||/...

cnbird 890 阅读

[ SecurityReason.com PHP 5.2.6 (error\_log) safe\_mode bypass ] Author: Maksymilian Arciemowicz (cXib8O3)securityreason.

cnbird 1247 阅读

The following proof-of-concept PHP code is available: `var_dump(curl_exec(curl_init("file://safe_mode_bypass/x00&quot;`

cnbird 844 阅读

以上就是查看Linux、Apache、MySQL、PHP版本信息的方法，希望这些信息能帮助你更好地理解和使用你的LAMP技术栈。

蓝易云 237 阅读

通过以上步骤，你可以成功地在台Linux服务器上从源码编译并安装LAMP环境，并配置一个BBS论坛（Discuz!）。这些步骤涵盖了从安装依赖、下载源代码、配置编译到安装完成的所有细节。每个命令的解释确保了过程的透明度，使即使是非专业人士也能够理解整个流程。

蓝易云 118 阅读

composer如何安装以及举例在PHP项目中使用Composer安装TCPDF库-优雅草卓伊凡

2 专业打造一款圈子源码软件系统 / 后端 PHP 搭建部署一样实现利益化

### 3 php项目源码加密之Zend Guard Loader加密的代码解密可能性很小-优雅草卓伊凡

#### 4 采用PHP+Vue技术架构的不良事件管理系统（源码）

## 5 简单的php版本nacos客户端

PHP进阶教程 - 由浅入深掌握面向对象开发 - 第二阶段

PHP完全自学手册文档教程

[更多](#)

阿里云栖开发者沙龙PHP技术专场-深入浅出网络编程与swoole内核-吴镇宇

## PHP安全开发:从白帽角度做安全



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