



CVE-2006-3063

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2006-3063
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-06-19 10:02:00 UTC
Updated	2017-07-20 01:32:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in myPHP Guestbook 1.x through 2.0.0-r1 and before 2.0.1 RC5 allow remote users to inject arbitrary HTML and JavaScript code into the pages of other users. The vulnerabilities exist in the search, login, and registration functions. The search function is vulnerable to a stored XSS attack. The login function is vulnerable to a reflected XSS attack. The registration function is vulnerable to a stored XSS attack. The vulnerabilities exist in the search, login, and registration functions. The search function is vulnerable to a stored XSS attack. The login function is vulnerable to a reflected XSS attack. The registration function is vulnerable to a stored XSS attack.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Myphp Guestbook	Myphp Guestbook	1.0	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	1.8	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	1.8.3	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	1.9	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	1.9.2	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.0	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.0-r1	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.0_alpha	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.0_beta	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.0_rc1	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.0_rc2	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.0_rc3	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.0_rc4	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.1_beta	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.1_rc1	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.1_rc2	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.1_rc3	All	All	All

Application	Myphp Guestbook	Myphp Guestbook	2.0.1_rc4	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	1.0	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	1.8	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	1.8.3	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	1.9	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	1.9.2	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.0	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.0-r1	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.0_alpha	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.0_beta	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.0_rc1	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.0_rc2	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.0_rc3	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.0_rc4	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.1_beta	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.1_rc1	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.1_rc2	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.1_rc3	All	All	All
Application	Myphp Guestbook	Myphp Guestbook	2.0.1_rc4	All	All	All

References

Reference	Source	Link	Tags
MyPHP Guestbook Multiple Cross Site Scripting Vulnerabilities	BID	www.securityfocus.com	
404 Not Found	CONFIRM	www.networkarea.ch	
Secunia - Advisories - myPHP Guestbook Cross-Site Scripting Vulnerabilities	SECUNIA	secunia.com	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report