



CVE-2009-2783

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

Summary

CVE	CVE-2009-2783
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-08-17 16:30:00 UTC
Updated	2013-08-14 06:04:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in XOOPS 2.3.3 allow remote attackers to inject arbitrary web script or HTL

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xoops	Xoops	2.3.3	All	All	All
Application	Xoops	Xoops	2.3.3	All	All	All

References

Reference	Source
56638	OSVDB
Page Not Found Sense of Security	MISC
404 Not Found	CONFIRMED
'XOOPS Multiple Cross-Site Scripting Vulnerabilities - Security Advisory - SOS-09-005' - MARC	BUGTRAQ
XOOPS 'op' Parameter Multiple Cross Site Scripting Vulnerabilities	BID
404 Not Found	CONFIRMED
XOOPS "op" Cross-Site Scripting Vulnerability - Advisories - Community	SECURITY
SecurityTracker.com Archives - XOOPS Input Validation Flaws in 'viewpmsg.php' and 'user.php' Permit Cross-Site Scripting Attacks	SECTOP
CVE Program record	CVE.O
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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](#)