



CVE-2005-3369

Published on: 10/29/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:23 PM UTC

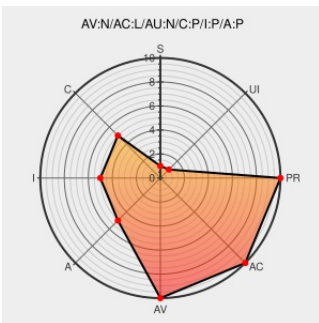
CVE-2005-3369

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Burning Board](#) from [Woltlab](#) contain the following vulnerability:

Multiple SQL injection vulnerabilities in the Info-DB module (info_db.php) in Woltlab Burning Board 2.7 and earlier allow remote attackers to execute arbitrary SQL commands and possibly upload files via the (1) fileid and (2) subkatid parameters.

CVE-2005-3369 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access Vector

NETWORK

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

PARTIAL

Integrity Impact

PARTIAL

Availability Impact

PARTIAL

CVE References

Description

Tags

Link

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[www.vupen.com](#)
[text/html](#)

[VUPEN ADV-2005-2224](#)

Secunia - Advisories - Woltlab Burning Board Database Module SQL Injection Vulnerabilities

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[SECUNIA 17347](#)

'Woltlab Burning Board info_db.php multiple SQL injection' - MARC

[marc.info](#)
[text/html](#)

[BUGTRAQ 20051026 Woltlab Burning Board info_db.php multiple SQL injection](#)

Woltlab Burning Board info_db.php multiple SQL injection - CXSecurity.com

[securityreason.com](#)
[text/html](#)

[SREASON 119](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 20330](#)

Inactive Link **Not Archived**

IBM X-Force Exchange

exchange.xforce.ibmcloud.com
XF wbb-infodb-sql-injection(22887)
text/html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Woltlab	Burning Board	2.4	All	All	All
Application	Woltlab	Burning Board	2.5	All	All	All
Application	Woltlab	Burning Board	2.6	All	All	All
Application	Woltlab	Burning Board	2.7	All	All	All
Application	Woltlab	Burning Board	2.4	All	All	All
Application	Woltlab	Burning Board	2.5	All	All	All
Application	Woltlab	Burning Board	2.6	All	All	All
Application	Woltlab	Burning Board	2.7	All	All	All
cpe:2.3:a:woltlab:burning_board:2.4:*:*:*:*:*:						
cpe:2.3:a:woltlab:burning_board:2.5:*:*:*:*:*:						
cpe:2.3:a:woltlab:burning_board:2.6:*:*:*:*:*:						
cpe:2.3:a:woltlab:burning_board:2.7:*:*:*:*:*:						
cpe:2.3:a:woltlab:burning_board:2.4:*:*:*:*:*:						
cpe:2.3:a:woltlab:burning_board:2.5:*:*:*:*:*:						
cpe:2.3:a:woltlab:burning_board:2.6:*:*:*:*:*:						
cpe:2.3:a:woltlab:burning_board:2.7:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)