

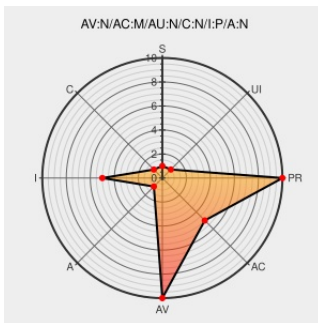


CVE-2006-1034

Published on: 03/07/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:59 PM UTC

CVE-2006-1034

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Multiple cross-site scripting (XSS) vulnerabilities in Woltlab Burning Board (wBB) allow remote attackers to inject arbitrary web script or HTML via (1) the username parameter to galerie_index.php and possibly (2) galerie_onfly.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. The second vector might not be XSS.

CVE-2006-1034 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Woltlab Burning Board Multiple Cross-Site Scripting Vulnerabilities	Exploit cve.report (archive) text/html	🌐 BID 16843

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	1.1.1	All	All	All
Application	Woltlab	Burning Board	2.0_beta_3	All	All	All
Application	Woltlab	Burning Board	2.0_beta_4	All	All	All
Application	Woltlab	Burning Board	2.0_beta_5	All	All	All
Application	Woltlab	Burning Board	2.0_rc1	All	All	All
Application	Woltlab	Burning Board	2.0_rc2	All	All	All
Application	Woltlab	Burning Board	2.2.2	All	All	All
Application	Woltlab	Burning Board	2.3.1	All	All	All
Application	Woltlab	Burning Board	2.3.3	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
Application	Woltlab	Burning Board	1.1.1	All	All	All
Application	Woltlab	Burning Board	2.0_beta_3	All	All	All
Application	Woltlab	Burning Board	2.0_beta_4	All	All	All
Application	Woltlab	Burning Board	2.0_beta_5	All	All	All
Application	Woltlab	Burning Board	2.0_rc1	All	All	All
Application	Woltlab	Burning Board	2.0_rc2	All	All	All
Application	Woltlab	Burning Board	2.2.2	All	All	All
Application	Woltlab	Burning Board	2.3.1	All	All	All
Application	Woltlab	Burning Board	2.3.3	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:1.1.1:*****.*:						
cpe:2.3:a:woltlab:burning_board:2.0_beta_3:*****.*:						
cpe:2.3:a:woltlab:burning_board:2.0_beta_4:*****.*:						
cpe:2.3:a:woltlab:burning_board:2.0_beta_5:*****.*:						
cpe:2.3:a:woltlab:burning_board:2.0_rc1:*****.*:						

No vendor comments have been submitted for this CVE

Next ID→

