



CVE-2022-47131

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

Summary

CVE	CVE-2022-47131
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-03 01:15:00 UTC
Updated	2023-02-09 17:18:00 UTC
Description	A Cross-Site Request Forgery (CSRF) in Academy LMS before v5.10 allows an attacker to arbitrarily create a page.

Risk And Classification

Problem Types: CWE-352 | CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Creativeitem	Academy Lms	All	All	All	All

References

Reference	Source	Link	Tags
Academy LMS < 5.10 CSRF + XSS Stored - XPsec Security	MISC	xpsec.co	
XSS vs CSRF Web Security Academy	MISC	portswigger.net	
What is CSRF (Cross-site request forgery)? Tutorial & Examples Web Security Academy	MISC	portswigger.net	
Cross-Site Scripting (XSS)	MISC	blog.hackingforce.com.br	
Vinicius Alves - Minas Gerais, Brazil Professional Profile LinkedIn	MISC	www.linkedin.com	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

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