



CVE-2023-2973

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

Summary

CVE	CVE-2023-2973
State	PUBLIC
Assigner	cna@vuldb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-30 11:15:00 UTC
Updated	2023-11-07 04:13:00 UTC
Description	A vulnerability, which was classified as problematic, has been found in SourceCodester Students Online Internship Timesheet System Project. The attack can be performed by exploiting a cross site scripting (XSS) vulnerability. The vulnerability is located in the login page. The attack can be performed by sending a malicious request to the login page. The attack can be performed by sending a malicious request to the login page. The attack can be performed by sending a malicious request to the login page.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Exclude
Application	Students Online Internship Timesheet System Project	Students Online Internship Timesheet System	1.0	All	All

References

Reference	Source	Link	Tags
VulnerabilityReport/XSS.md at main · ShallowDream888/VulnerabilityReport · GitHub	MISC	github.com	
CVE-2023-2973: SourceCodester Students Online Internship Timesheet System cross site scripting	MISC	vuldb.com	
Login required	MISC	vuldb.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, archived

No vendor comments have been submitted for this CVE.

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

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