



CVE-2021-39473

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

Summary

CVE	CVE-2021-39473
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-04 19:15:00 UTC
Updated	2023-09-11 22:15:00 UTC
Description	Saibamen HotelManager v1.2 is vulnerable to Cross Site Scripting (XSS) due to improper sanitization of comment and cont

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hotelmanager Project	Hotelmanager	1.2	All	All	All

References

Reference	Source	Link
HotelManager v1.2 is vulnerable to Cross Site Scripting (XSS). · Issue #49 · Saibamen/HotelManager · GitHub	MISC	github.com
GitHub - BrunoTeixeira1996/CVE-2021-39473	MISC	github.com
GitHub - Saibamen/HotelManager: Web app for managing hotel written in Laravel	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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