



CVE-2021-43137

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-43137
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-01 20:15:00 UTC
Updated	2023-11-14 16:36:00 UTC
Description	Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) vulnerability exists in hostel management system 2.1 via

Risk And Classification

Problem Types: CWE-352 | CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hostel Management System Project	Hostel Management System	2.1	All	All	All
Application	Phpgurukul	Hostel Management System	2.1	All	All	All

References

Reference	Source
PHPGurukul Hostel Management System 2.1 - Cross-site request forgery (CSRF) to Cross-site Scripting (XSS) - PHP webapps Exploit	MIS
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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](#)