



CVE-2021-43451

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2021-43451
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-01 19:15:00 UTC
Updated	2023-09-25 16:46:00 UTC
Description	SQL Injection vulnerability exists in PHPGURUKUL Employee Record Management System 1.2 via the Email POST param

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Employee Record Management System Project	Employee Record Management System	1.2	All	All	All
Application	Phpgurukul	Employee Record Management System	1.2	All	All	All

References

Reference

- [CVE-2021-43451](#)
- [Employee Record Management System 1.2 - 'empid' SQL injection \(Unauthenticated\) - PHP webapps Exploit](#)
- [CVE-nu11secur1ty/vendors/PHPGURUKUL/ANUJ KUMAR/Employee-Record-Management-System-SQL-Injection at main · nu11secur1ty/CV](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

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