



CVE-2022-29009

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

Summary

CVE	CVE-2022-29009
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-11 14:15:00 UTC
Updated	2023-10-04 17:36:00 UTC
Description	Multiple SQL injection vulnerabilities via the username and password parameters in the Admin panel of Cyber Cafe Management System Project

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cyber Cafe Management System Project	Cyber Cafe Management System	1.0	All	All	All
Application	Phpgurukul	Cyber Cafe Management System	1.0	All	All	All

References

Reference	Source	Link
Cyber Cafe Management System Project (CCMS) 1.0 - SQL Injection Authentication Bypass - PHP webapps Exploit	MISC	www.exploit-db.com/exploits/48844/
CVE-2022-29009/CVE-2022-29009.txt at main · sudoninja-noob/CVE-2022-29009 · GitHub	MISC	github.com/sudoninja-noob/CVE-2022-29009
CVE Program record	CVE.ORG	www.cve.org/CVE-2022-29009
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2022-29009

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