



CVE-2020-28173

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

Summary

CVE	CVE-2020-28173
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-31 13:15:00 UTC
Updated	2021-04-02 18:17:00 UTC
Description	Simple College Website 1.0 allows a user to conduct remote code execution via /alumni/admin/ajax.php?action=save_settin

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Simple College Project	Simple College	1.0	All	All	All

References

Reference	Source	Link
dl.packetstormsecurity.net/2010-exploits/simplecollegewebsite10-sqlexec.txt	MISC	dl.packetstormsecurity.net/2010-exploits/simplecollegewebsite10-sqlexec.txt
poc-dump/sqli_rce.py at main · yunaranyancat/poc-dump · GitHub	MISC	github.com
Simple College Website using HTML/PHP/MySQLi with Source Code Free Source Code Projects and Tutorials	MISC	www.sourcecodester.com
www.sourcecodester.com/sites/default/files/download/oretnom23/simple-college-website...	MISC	www.sourcecodester.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.

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