VDB-355316 · CVE-2026-5552 · GCVE-100-355316

PHPGURUKUL ONLINE SHOPPING PORTAL PROJECT 2.1 PARAMETER /SUB-CATEGORY.PHP PID SQL INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
5.7	$0-$5k	3.29-

Summary

A vulnerability labeled as critical has been found in PHPGurukul Online Shopping Portal Project 2.1. Impacted is an unknown function of the file */sub-category.php* of the component *Parameter Handler*. Such manipulation of the argument *pid* leads to sql injection. This vulnerability is documented as CVE-2026-5552. The attack can be executed remotely. Additionally, an exploit exists.

Details

A vulnerability was found in PHPGurukul Online Shopping Portal Project 2.1 and classified as critical. Affected by this issue is an unknown part of the file */sub-category.php* of the component *Parameter Handler*. The manipulation of the argument `pid` with an unknown input leads to a sql injection vulnerability. Using CWE to declare the problem leads to CWE-89. The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component. Impacted is confidentiality, integrity, and availability.

The advisory is shared for download at github.com. This vulnerability is handled as CVE-2026-5552. The exploitation is known to be easy. The attack may be launched remotely. Technical details as well as a public exploit are known. The MITRE ATT&CK project declares the attack technique as T1505.

The exploit is available at github.com. It is declared as proof-of-concept. By approaching the search of inurl:sub-category.php it is possible to find vulnerable targets with Google Hacking.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

Entries connected to this vulnerability are available at VDB-355328, VDB-355330, VDB-355334 and VDB-355335.

Product

Type

- Project Management Software

Vendor

- PHPGurukul

Name

- Online Shopping Portal Project

Version

- 2.1

License

- free

Website

- Vendor: https://phpgurukul.com/

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 6.3
VulDB Meta Temp Score: 5.7

VulDB Base Score: 6.3
VulDB Temp Score: 5.7
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Sql injection
CWE: CWE-89 / CWE-74 / CWE-707
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Download: 🔒
Google Hack: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

04/04/2026		Advisory disclosed
04/04/2026	+0 days	VulDB entry created
04/04/2026	+0 days	VulDB entry last update

Sources

Vendor: phpgurukul.com

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5552 (🔒)
GCVE (CVE): GCVE-0-2026-5552
GCVE (VulDB): GCVE-100-355316
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/04/2026 03:40 PM
Changes: 04/04/2026 03:40 PM (57)
Complete: 🔍
Cache ID: 74:9A1:179

Submit

Accepted

- Submit #782864: PHPGurukul Online Shopping Portal Project 2.1 SQL Injection (by github.com)

Discussion

No comments yet. Languages: en.

Please log in to comment.

© 1997-2026 vuldb.com · cc by-nc-sa

v20.2.0