VDB-355351 · CVE-2026-5606 · GCVE-100-355351

PHPGURUKUL ONLINE SHOPPING PORTAL PROJECT 2.1 PARAMETER /ORDER-DETAILS.PHP ORDERID SQL INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
6.1	$0-$5k	1.84

Summary

A vulnerability has been found in PHPGurukul Online Shopping Portal Project 2.1 and classified as critical. The impacted element is an unknown function of the file */order-details.php* of the component *Parameter Handler*. This manipulation of the argument *orderid* causes sql injection. This vulnerability is handled as CVE-2026-5606. The attack can be initiated remotely. There is not any exploit available.

Details

A vulnerability has been found in PHPGurukul Online Shopping Portal Project 2.1 and classified as critical. Affected by this vulnerability is an unknown part of the file */order-details.php* of the component *Parameter Handler*. The manipulation of the argument `orderid` with an unknown input leads to a sql injection vulnerability. The CWE definition for the vulnerability is 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. As an impact it is known to affect confidentiality, integrity, and availability.

It is possible to read the advisory at github.com. This vulnerability is known as CVE-2026-5606. The exploitation appears to be easy. The attack can be launched remotely. Technical details of the vulnerability are known, but there is no available exploit. The pricing for an exploit might be around USD $0-$5k at the moment (estimation calculated on 04/05/2026). The attack technique deployed by this issue is T1505 according to MITRE ATT&CK.

By approaching the search of inurl:order-details.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-355410, VDB-355422, VDB-355423 and VDB-355424.

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: 6.1

VulDB Base Score: 6.3
VulDB Temp Score: 6.1
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: 🔒
Status: Not defined
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
04/05/2026	+1 days	VulDB entry last update

Sources

Vendor: phpgurukul.com

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5606 (🔒)
GCVE (CVE): GCVE-0-2026-5606
GCVE (VulDB): GCVE-100-355351
See also: 🔒

Entry

Created: 04/04/2026 07:41 PM
Updated: 04/05/2026 04:08 PM
Changes: 04/04/2026 07:41 PM (52), 04/05/2026 04:08 PM (2)
Complete: 🔍
Cache ID: 20:842:179

Submit

Accepted

- Submit #784009: PHPGurukul Online Shopping Portal Project 2.1 SQL Injection (by github.com)

Discussion

No comments yet. Languages: en.

Please log in to comment.