VDB-355429 · CVE-2026-5641 · GCVE-100-355429

PHPGURUKUL ONLINE SHOPPING PORTAL PROJECT 2.1 PARAMETER /ADMIN/UPDATE-IMAGE1.PHP FILENAME SQL INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
5.7	$0-$5k	2.02-

Summary

A vulnerability marked as critical has been reported in PHPGurukul Online Shopping Portal Project 2.1. This affects an unknown function of the file */admin/update-image1.php* of the component *Parameter Handler*. This manipulation of the argument *filename* causes sql injection. The identification of this vulnerability is CVE-2026-5641. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.

Details

A vulnerability classified as critical was found in PHPGurukul Online Shopping Portal Project 2.1. Affected by this vulnerability is an unknown code of the file */admin/update-image1.php* of the component *Parameter Handler*. The manipulation of the argument `filename` 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.

The advisory is shared at github.com. This vulnerability is known as CVE-2026-5641. The exploitation appears to be easy. The attack can be launched remotely. Technical details and also a public exploit are known. MITRE ATT&CK project uses the attack technique T1505 for this issue.

It is possible to download the exploit at github.com. It is declared as proof-of-concept. By approaching the search of inurl:admin/update-image1.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.

The entries VDB-355451, VDB-355452, VDB-355453 and VDB-355454 are related to this item.

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

04/05/2026		Advisory disclosed
04/05/2026	+0 days	VulDB entry created
04/05/2026	+0 days	VulDB entry last update

Sources

Vendor: phpgurukul.com

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5641 (🔒)
GCVE (CVE): GCVE-0-2026-5641
GCVE (VulDB): GCVE-100-355429
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/05/2026 10:36 PM
Changes: 04/05/2026 10:36 PM (57)
Complete: 🔍
Cache ID: 68:12C:179

Submit

Accepted

- Submit #785993: PHPGurukul Online Shopping Portal Project 2.1 SQL Injection (by github.com)

Discussion

No comments yet. Languages: en.

Please log in to comment.