



VDB-356261 · CVE-2026-5813 · GCVE-100-356261

PHPGURUKUL ONLINE COURSE REGISTRATION 3.1 /CHECK_AVAILABILITY.PHP CID SQL INJECTION

CVSS Meta Temp Score ⓘ

6.6

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

1.47

Summary

A vulnerability has been found in [PHPGurukul Online Course Registration 3.1](#) and classified as **critical**. This issue affects some unknown processing of the file `/check_availability.php`. The manipulation of the argument `cid` leads to sql injection. This vulnerability is documented as [CVE-2026-5813](#). The attack can be initiated remotely. Additionally, an exploit exists.

Details

A vulnerability was found in [PHPGurukul Online Course Registration 3.1](#) and classified as **critical**. This issue affects an unknown part of the file `/check_availability.php`. The manipulation of the argument `cid` 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 at [github.com](#). The identification of this vulnerability is [CVE-2026-5813](#). The exploitation is known to be easy. The attack may be initiated remotely. No form of authentication is needed for a successful exploitation. Technical details as well as a public exploit are known. MITRE ATT&CK project uses the attack technique [T1505](#) for this issue.

The exploit is available at [github.com](#). It is declared as proof-of-concept. By approaching the search of `inurl:check_availability.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.

Product

Vendor

- [PHPGurukul](#)

Name

- [Online Course Registration](#)

Version

- [3.1](#)

License

- [free](#)

Website

- Vendor: <https://phpgurukul.com/>

CPE 2.3

- 

CPE 2.2

- 

CVSSv4

VuIDB Vector: 

VuIDB Reliability: 

CVSSv3

VuIDB Meta Base Score: 7.3

VuIDB Meta Temp Score: 6.6

VuIDB Base Score: 7.3

VuIDB Temp Score: 6.6

VuIDB Vector: 

VuIDB 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

04/08/2026		Advisory disclosed
04/08/2026	+0 days	VulDB entry created
04/08/2026	+0 days	VulDB entry last update

Sources

Vendor: phpgurukul.com

Advisory: github.com

Status: Not defined

CVE: [CVE-2026-5813](#) (🔒)

GCVE (CVE): [GCVE-0-2026-5813](#)

GCVE (VulDB): [GCVE-100-356261](#)

scip Labs: <https://www.scip.ch/en/?labs.20161013>

Entry

Created: 04/08/2026 05:31 PM

Changes: 04/08/2026 05:31 PM (55)

Complete: 🔍

Cache ID: 20:631:179

Submit

Accepted

- [Submit #787686](#): PHPGurukul Online Course Registration 3.1 SQL Injection (by github.com)

Discussion

No comments yet. Languages: en.

Please [log in](#) to comment.

