



VDB-355296 · CVE-2026-5543 · GCVE-100-355296

# PHPGURUKUL USER REGISTRATION & LOGIN AND USER MANAGEMENT SYSTEM YESTERDAY-REG-USERS.PHP SQL INJECTION

CVSS Meta Temp Score ⓘ

5.7

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

3.78-

## Summary

A vulnerability was found in [PHPGurukul User Registration & Login and User Management System 3.3](#) and classified as *critical*. The impacted element is an unknown function of the file `/admin/yesterday-reg-users.php`. The manipulation of the argument `ID` results in sql injection. This vulnerability is identified as [CVE-2026-5543](#). The attack can be executed remotely. Additionally, an exploit exists.

## Details

A vulnerability, which was classified as critical, was found in [PHPGurukul User Registration & Login and User Management System 3.3](#). Affected is an unknown code of the file `/admin/yesterday-reg-users.php`. The manipulation of the argument `id` with an unknown input leads to a sql injection vulnerability. CWE is classifying the issue as [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. This is going to have an impact on confidentiality, integrity, and availability.

The advisory is shared for download at [github.com](#). This vulnerability is traded as [CVE-2026-5543](#). The exploitability is told to be easy. It is possible to launch the attack remotely. Technical details and a public exploit are known. The MITRE ATT&CK project declares the attack technique as [T1505](#).

The exploit is shared for download at [github.com](#). It is declared as proof-of-concept. By approaching the search of [inurl:admin/yesterday-reg-users.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.

Entry connected to this vulnerability is available at [VDB-317572](#).

## Product

### Vendor

- [PHPGurukul](#)

### Name

- [User Registration & Login and User Management System](#)

### Version

- [3.3](#)

### License

- [free](#)

### Website

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

## CPE 2.3

- 

## CPE 2.2

- 

## CVSSv4

VuIDB Vector: 

VuIDB Reliability: 

## CVSSv3

VuIDB Meta Base Score: 6.3

VuIDB Meta Temp Score: 5.7

VuIDB Base Score: 6.3

VuIDB Temp Score: 5.7

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

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

## Sources

**Vendor:** [phpgurukul.com](https://phpgurukul.com)

**Advisory:** [github.com](https://github.com)

**Status:** Not defined

**CVE:** [CVE-2026-5543](#) (🔒)

**GCVE (CVE):** [GCVE-0-2026-5543](#)

**GCVE (VulDB):** [GCVE-100-355296](#)

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

**See also:** 🔒

## Entry

**Created:** 04/04/2026 08:58 AM

**Changes:** 04/04/2026 08:58 AM (55)

**Complete:** 🔍

**Cache ID:** 20:0B0:179

## Submit

### Accepted

- [Submit #782246](#): PHPGurukul User Registration & Login and User Management System With admin panel 3.3 SQL Injection (by [github.com](https://github.com))

## Discussion

No comments yet. Languages: en.

Please log in to comment.