



Home > Submit > 782877

# Submit #782877: PHPGurukul Online Shopping Portal Project 2.1 SQL Injection

<b>Title</b>	PHPGurukul Online Shopping Portal Project 2.1 SQL Injection
<b>Description</b>	A SQL injection vulnerability was identified within the "pending-orders.php" file of the "Online Shopping Portal Project" project. The root cause lies in the fact that attackers can inject malicious code via the parameter "id". This input is then directly utilized in SQL queries without undergoing proper sanitization or validation processes. As a result, attackers are able to fabricate input values, manipulate SQL queries, and execute unauthorized operations.
<b>Source</b>	<a href="https://github.com/f1rstb100d/CVE/issues/11">https://github.com/f1rstb100d/CVE/issues/11</a>
<b>User</b>	Anonymous User
<b>Submission</b>	03/19/2026 10:19 AM (17 days ago)
<b>Moderation</b>	04/04/2026 03:50 PM (16 days later)
<b>Status</b>	Accepted
<b>VulDB entry</b>	<a href="#">VUL-2026-1000</a> [PHPGurukul PHPGurukul Online Shopping Portal Project up to 2.1 Parameter /pending-orders.php ID sql injection]
<b>Points</b>	20

## Community Content

Submissions are made by [VulDB community users](#). VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

## Documentation

- [Submission Policy](#)
- [Data Processing](#)
- [CVE Handling](#)