Submit #566719: projectworlds Student Project Allocation System v1.0 SQL Injection

Title projectworlds Student Project Allocation System v1.0 SQL Injection

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

```bash
《sqlmap.py -r C:\Users\韩旭\Desktop\sqli.txt -p id --batch》
```


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.

Source ⚠️ https://github.com/hhhanxx/attack/issues/3

User attackxu (UID 84219)

Submission 04/28/2025 04:56 PM (12 days ago)

Moderation 05/09/2025 01:46 PM (11 days later)

Status Accepted

VulDB Entry 308197 [Project Worlds Student Project Allocation System 1.0 forgot_password_sql.php Pat_BloodGroup1 sql injection]

Points 20

Notice

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling