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' ")
```

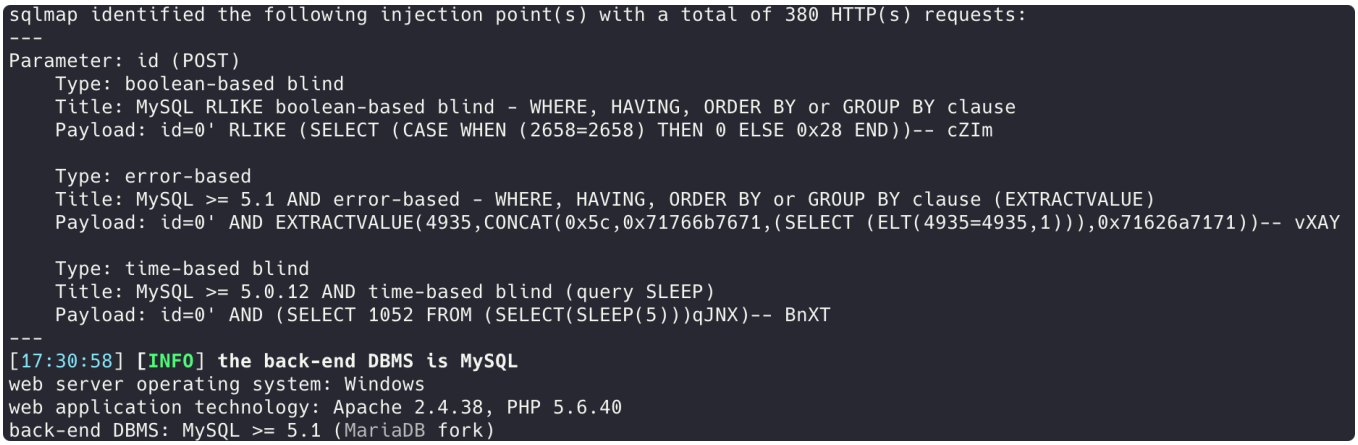
Suggested Fixes:

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



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