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'")
```

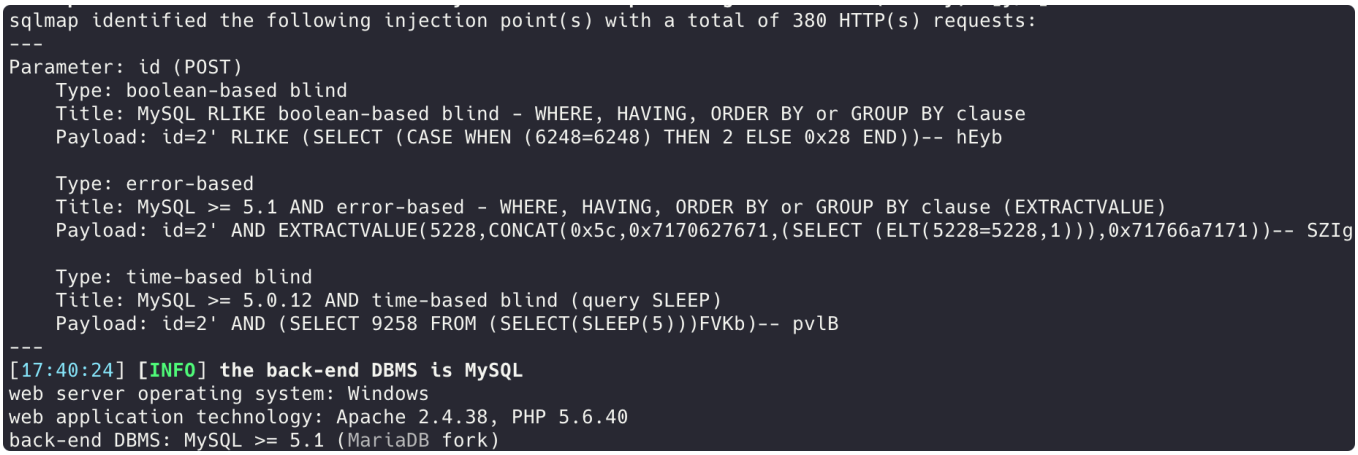
Suggested Fixes:

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



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