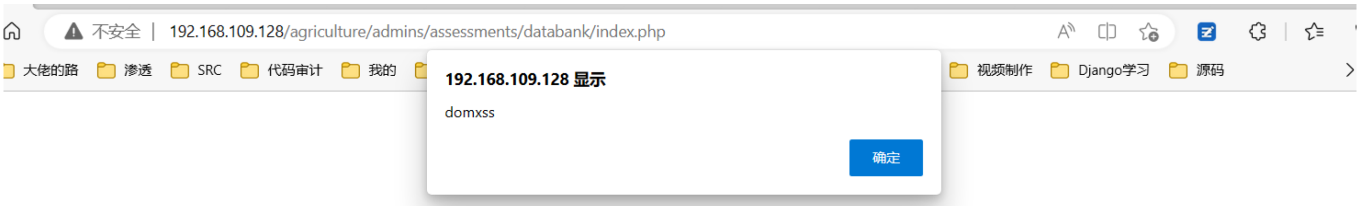
# agricultural school management system has cross-site script vulnerability

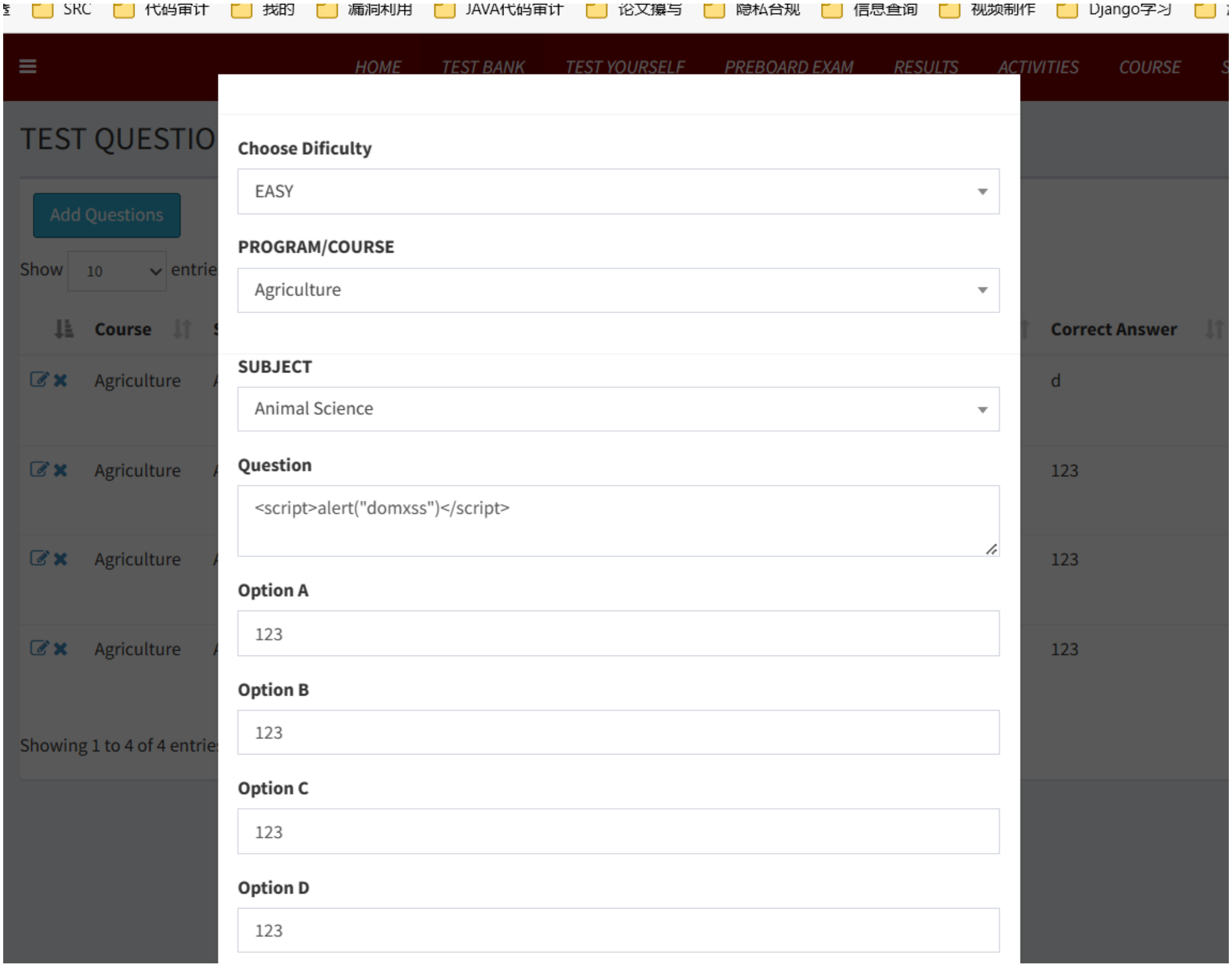
There is a stored cross-site script vulnerability in the agricultural school management system. The vulnerability exists in the btn_functions.php file, which is caused by insufficient filtering of user input by the Web application. Attackers take advantage of website vulnerabilities to inject malicious script code (usually including HTML code and client-side Javascript script) into web pages. When other users browse these pages, the malicious code will be executed, and the victim may take Cookie data theft, session hijacking, phishing, and other attacks.


不安全 | 192.168.109.128/agriculture/admins/assessments/databank/index.php
大佬的路
渗透
SRC
代码审计
我的
视频制作
Django学习
源码

192.168.109.128 显示

domxss

确定



Choose Dificulty: EASY

PROGRAM/COURSE: Agriculture

SUBJECT: Animal Science

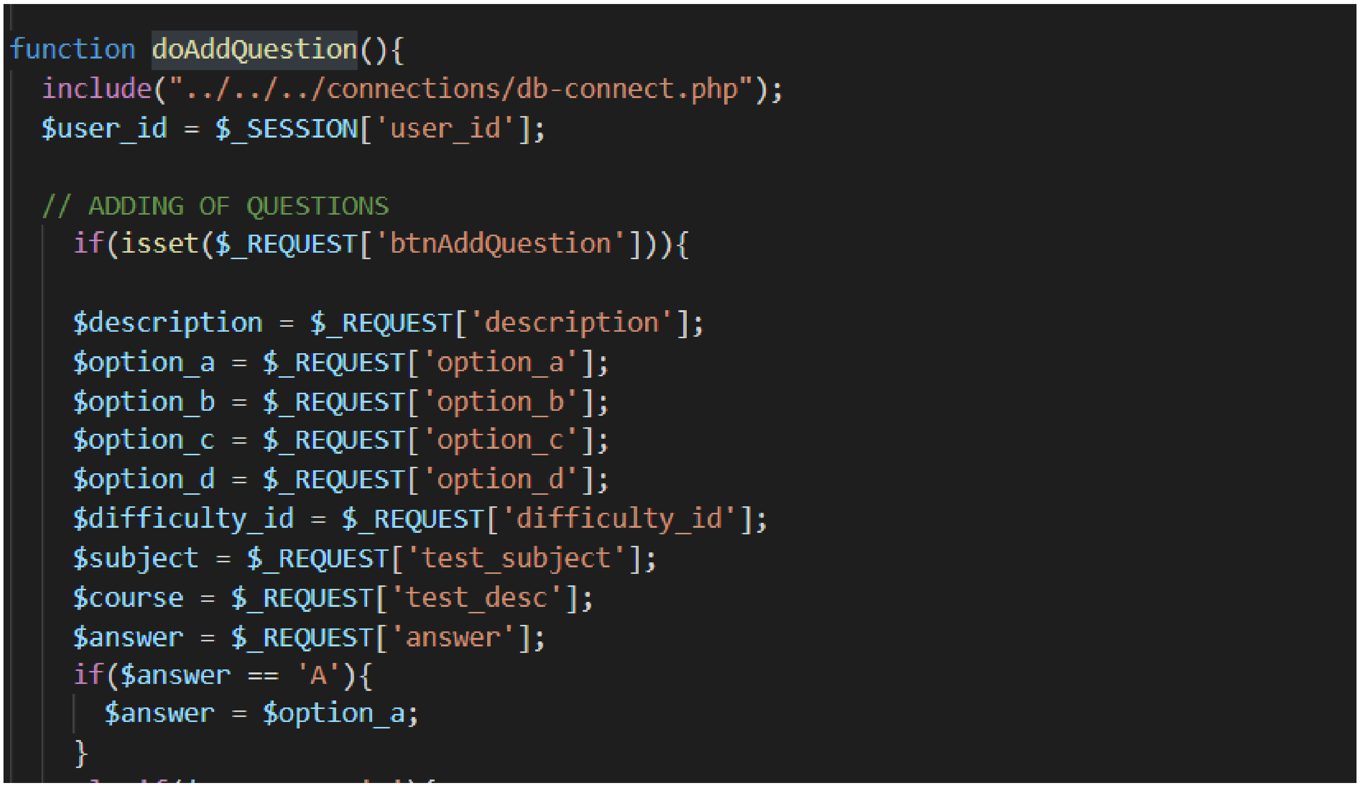
Question: <script>alert("domxss")</script>

Option A: 123

Option B: 123

Option C: 123

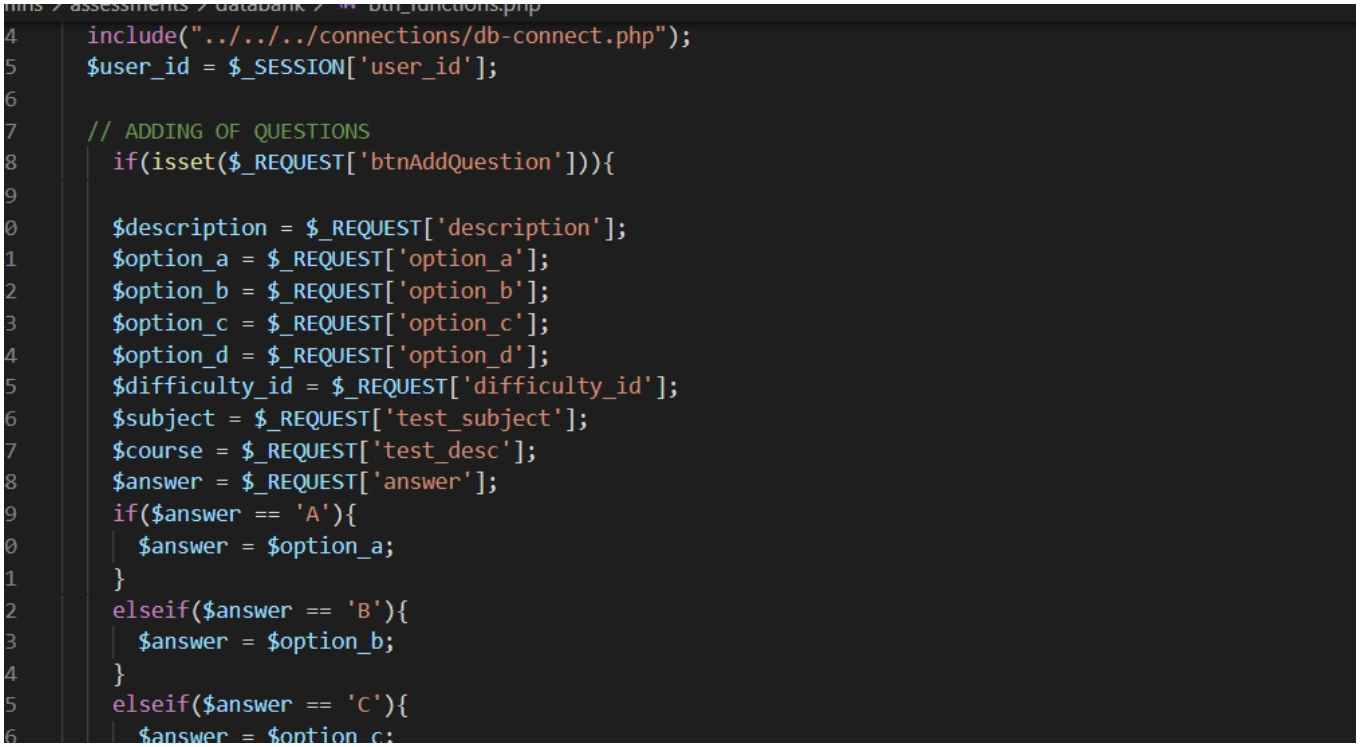
Option D: 123



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

  // ADDING OF QUESTIONS
    if(isset($_REQUEST['btnAddQuestion'])){

    $description = $_REQUEST['description'];
    $option_a = $_REQUEST['option_a'];
    $option_b = $_REQUEST['option_b'];
    $option_c = $_REQUEST['option_c'];
    $option_d = $_REQUEST['option_d'];
    $difficulty_id = $_REQUEST['difficulty_id'];
    $subject = $_REQUEST['test_subject'];
    $course = $_REQUEST['test_desc'];
    $answer = $_REQUEST['answer'];
    if($answer == 'A'){
      $answer = $option_a;
    }
```



mins > assessments > databank > btn_functions.php

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

  // ADDING OF QUESTIONS
    if(isset($_REQUEST['btnAddQuestion'])){

    $description = $_REQUEST['description'];
    $option_a = $_REQUEST['option_a'];
    $option_b = $_REQUEST['option_b'];
    $option_c = $_REQUEST['option_c'];
    $option_d = $_REQUEST['option_d'];
    $difficulty_id = $_REQUEST['difficulty_id'];
    $subject = $_REQUEST['test_subject'];
    $course = $_REQUEST['test_desc'];
    $answer = $_REQUEST['answer'];
    if($answer == 'A'){
      $answer = $option_a;
    }
    elseif($answer == 'B'){
      $answer = $option_b;
    }
    elseif($answer == 'C'){
      $answer = $option_c;
```