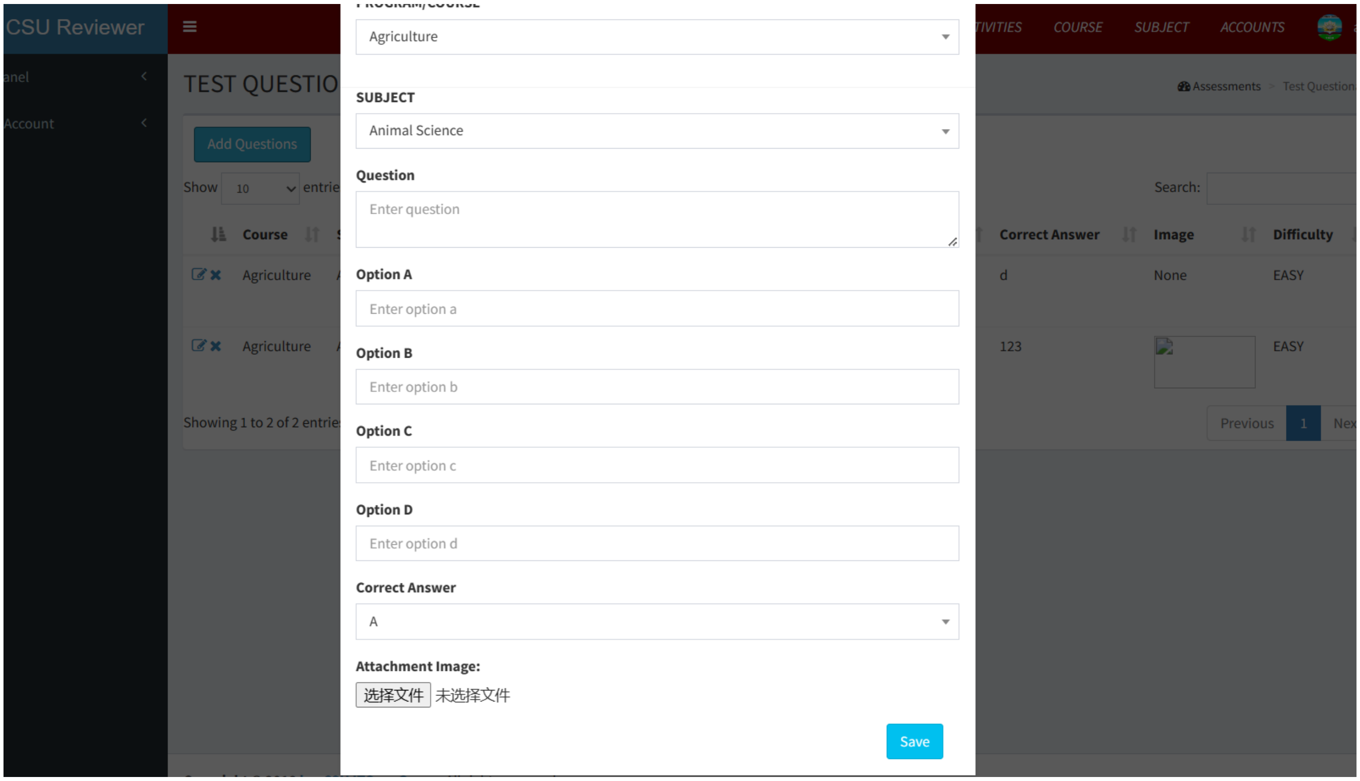
Agro-School Management System has a file upload (RCE) vulnerability

```
Agro-School Management System has a file upload (RCE) vulnerability,
vulnerability exists in btn_functions.php file, can upload any format
of the file, and execute any code, the function of the file name
timestamp confusion, but can be predicted, can be used by malicious
users to upload any file execution code, access to the server.
```



PROGRAM/COURSE
Agriculture

SUBJECT
Animal Science

Question
Enter question

Option A
Enter option a

Option B
Enter option b

Option C
Enter option c

Option D
Enter option d

Correct Answer
A

Attachment Image:
选择文件 未选择文件

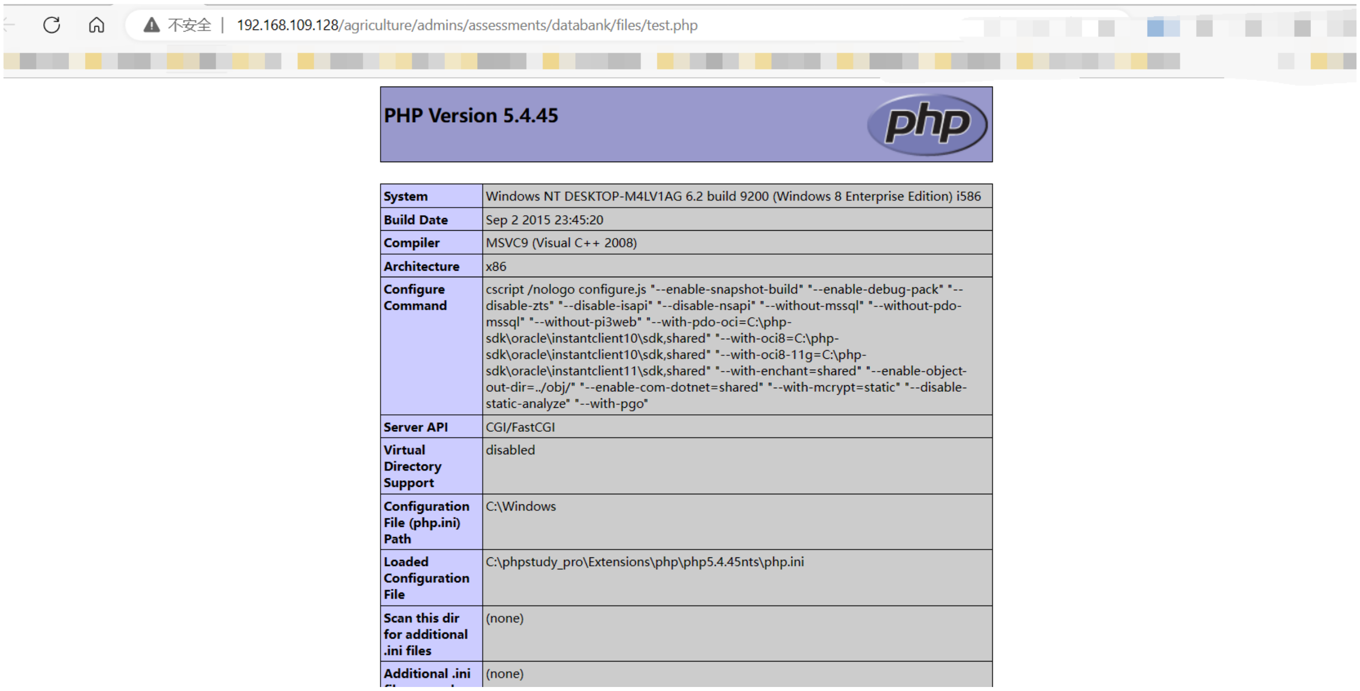
Save

Show 10 entrie

	Course		Correct Answer	Image	Difficulty
	Agriculture		d	None	EASY
	Agriculture		123		EASY

Showing 1 to 2 of 2 entrie

Previous 1 Nex

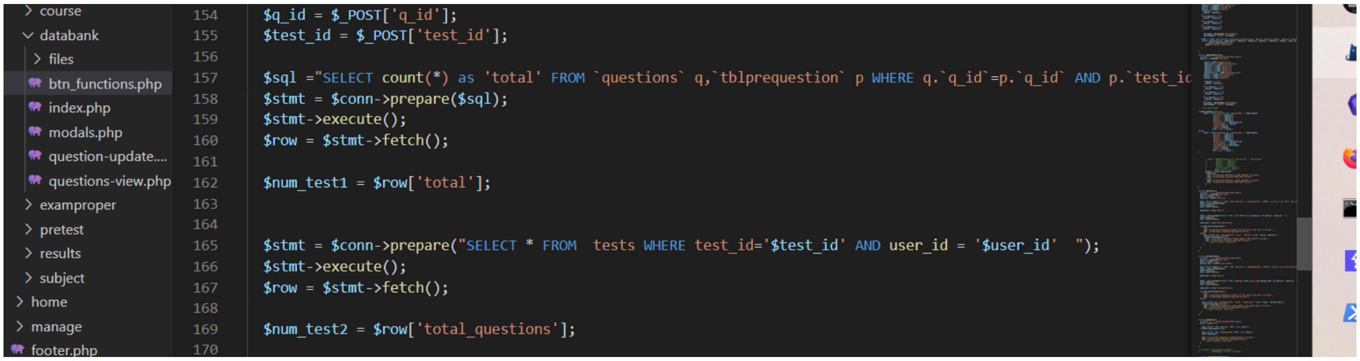


192.168.109.128/agriculture/admins/assessments/databank/files/test.php

[redacted]

PHP Version 5.4.45

System	Windows NT DESKTOP-M4LV1AG 6.2 build 9200 (Windows 8 Enterprise Edition) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\phpstudy_pro\Extensions\php\php5.4.45nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini	(none)



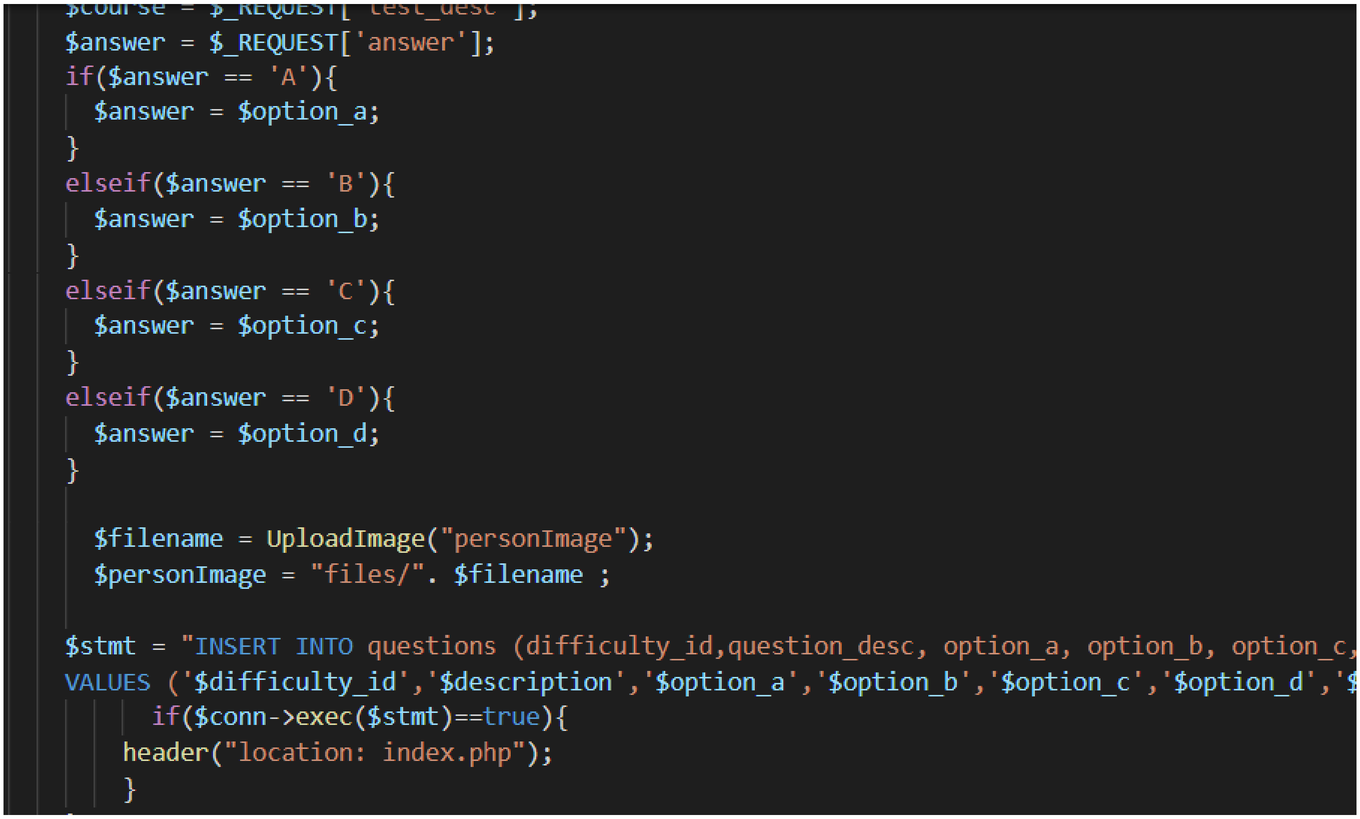
```
$q_id = $_POST['q_id'];
$test_id = $_POST['test_id'];

$sql ="SELECT count(*) as 'total' FROM `questions` q,`tblprequestion` p WHERE q.`q_id`=p.`q_id` AND p.`test_ic
$stmt = $conn->prepare($sql);
$stmt->execute();
$row = $stmt->fetch();

$num_test1 = $row['total'];


$stmt = $conn->prepare("SELECT * FROM  tests WHERE test_id='$test_id' AND user_id = '$user_id'  ");
$stmt->execute();
$row = $stmt->fetch();

$num_test2 = $row['total_questions'];
```



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

  $filename = UploadImage("personImage");
  $personImage = "files/". $filename ;

$stmt = "INSERT INTO questions (difficulty_id,question_desc, option_a, option_b, option_c,
VALUES ('$difficulty_id','$description','$option_a','$option_b','$option_c','$option_d','$
      if($conn->exec($stmt)==true){
    header("location: index.php");
    }
```