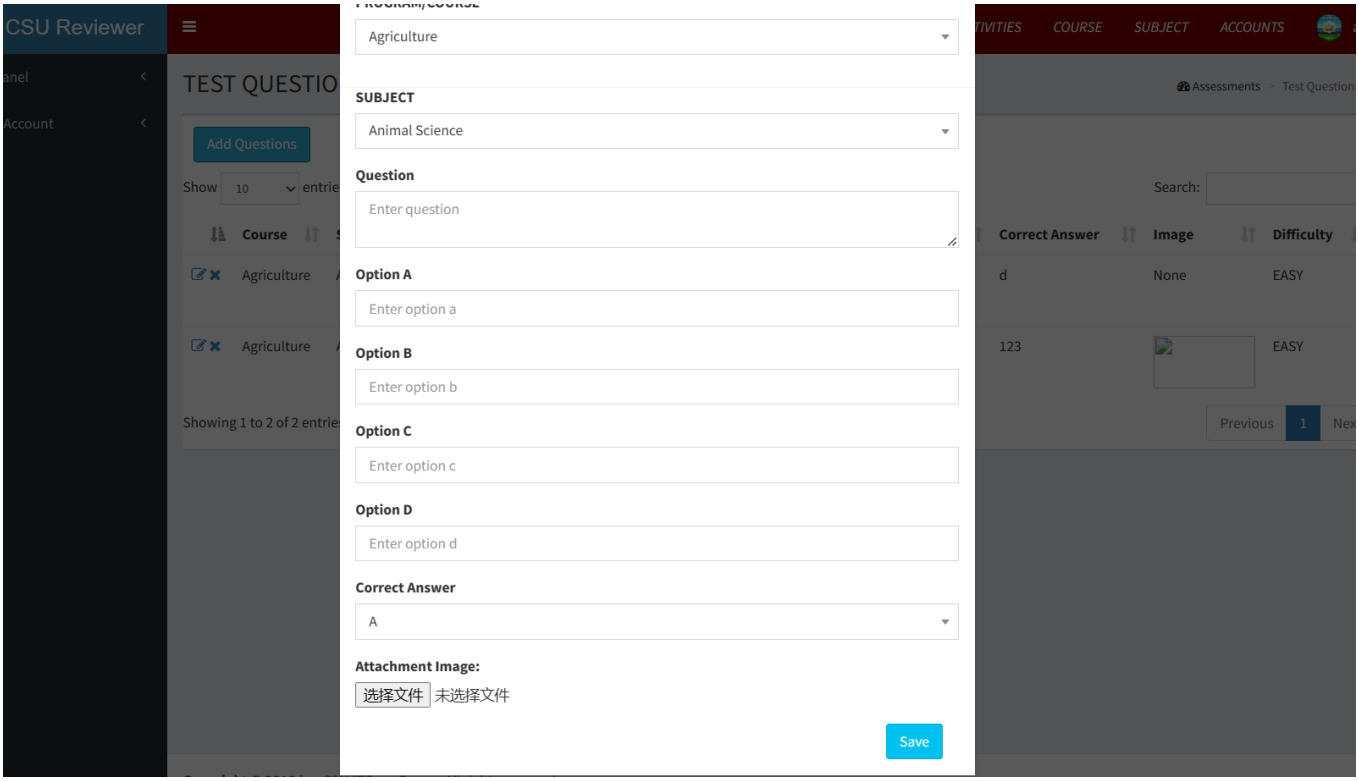
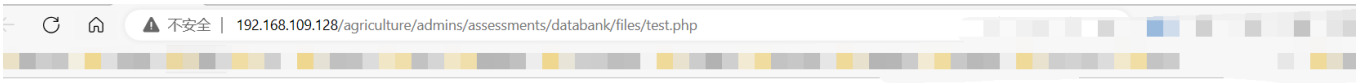
Agro-School Management System has a file upload (RCE) vulnerability

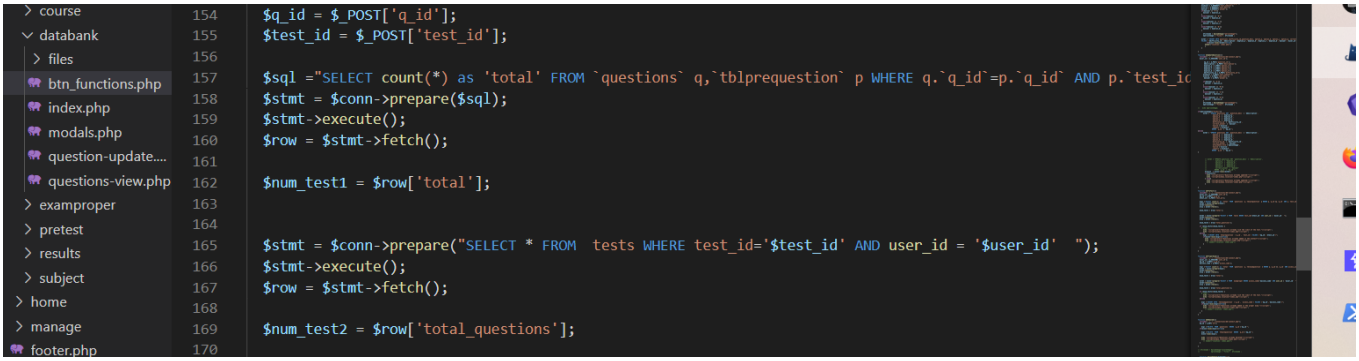
There is a file upload (RCE) vulnerability in the agricultural school management system. The vulnerability exists in the btn_functions.php file, which can upload any file format and execute any code to access the server.





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)




```php
$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");
    }
```