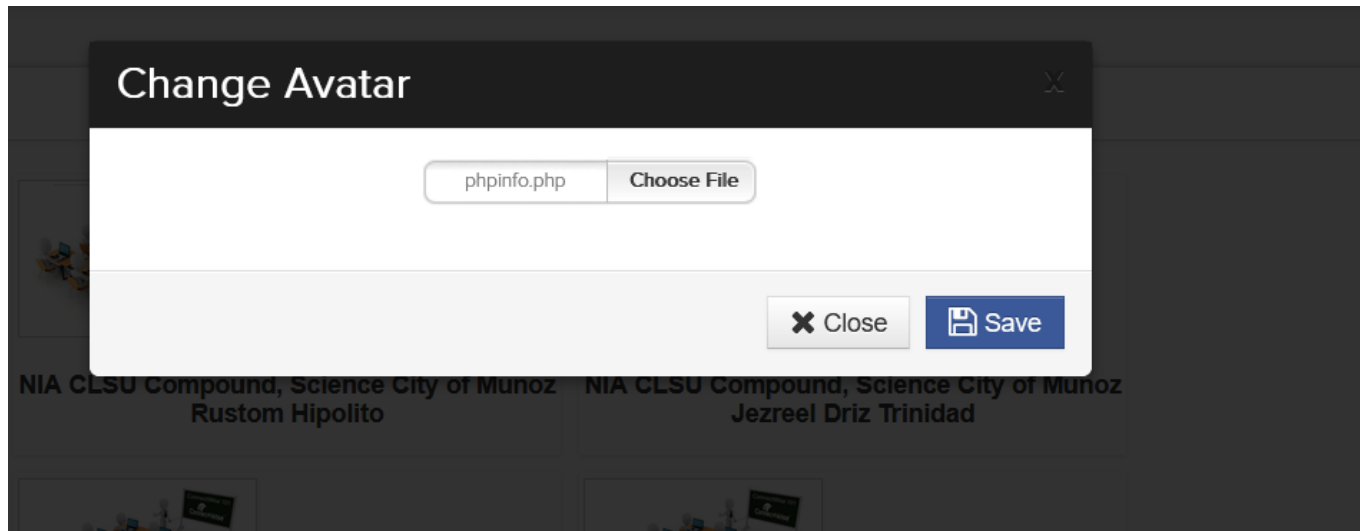


# Engineers Online Portal System has a file upload (RCE) vulnerability

Engineers Online Portal System has a file upload (RCE) vulnerability, vulnerability exists in student\_avatar.php file, Can upload any format of the file, and there is no limit, the file name is the file name when uploaded, developers should limit the type of file uploaded by users, otherwise it will lead to users to obtain server permissions, steal sensitive data, serious or even lead to server crash, a large number of user privacy disclosure.

```
if (isset($_POST['change'])) {  
  
    $image = addslashes(file_get_contents($_FILES['image']['tmp_name']));  
    $image_name = addslashes($_FILES['image']['name']);  
    $image_size = getimagesize($_FILES['image']['tmp_name']);  
  
    move_uploaded_file($_FILES["image"]["tmp_name"], "admin/uploads/" . $_FILES["image"][$  
    $location = "uploads/" . $_FILES["image"]["name"];  
  
    mysqli_query($conn,"update student set location = '$location' where student_id = '$  
  
    ?>  
  
    <script>  
    window.location = "dashboard_student.php";  
    </script>  
  
    <?php    }    ?>
```

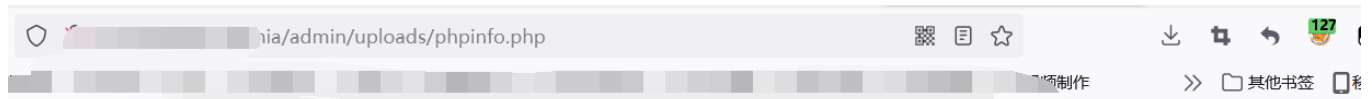


Access user profile picture

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<?php
echo phpinfo();

?>
```



## PHP Version 5.4.45



System	Windows NT DESKTOP-M4LV1... (Windows 8 Enterprise Edition) i586
Build Date	See below
Compiler	Visual C++
Architecture	
Configure Command	configure '--enable-debug-pack' '--disable-zts' '--with-instantclient10\jdk,shared' '--with-oci8-11g=C:\php-sdk\oracle\instantclient11\jdk,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	disabled
Configuration File (php.ini) Path	
Loaded Configuration File	
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20090924
PHP Extension	20090924
Zend Extension	220100525
Zend Extension	