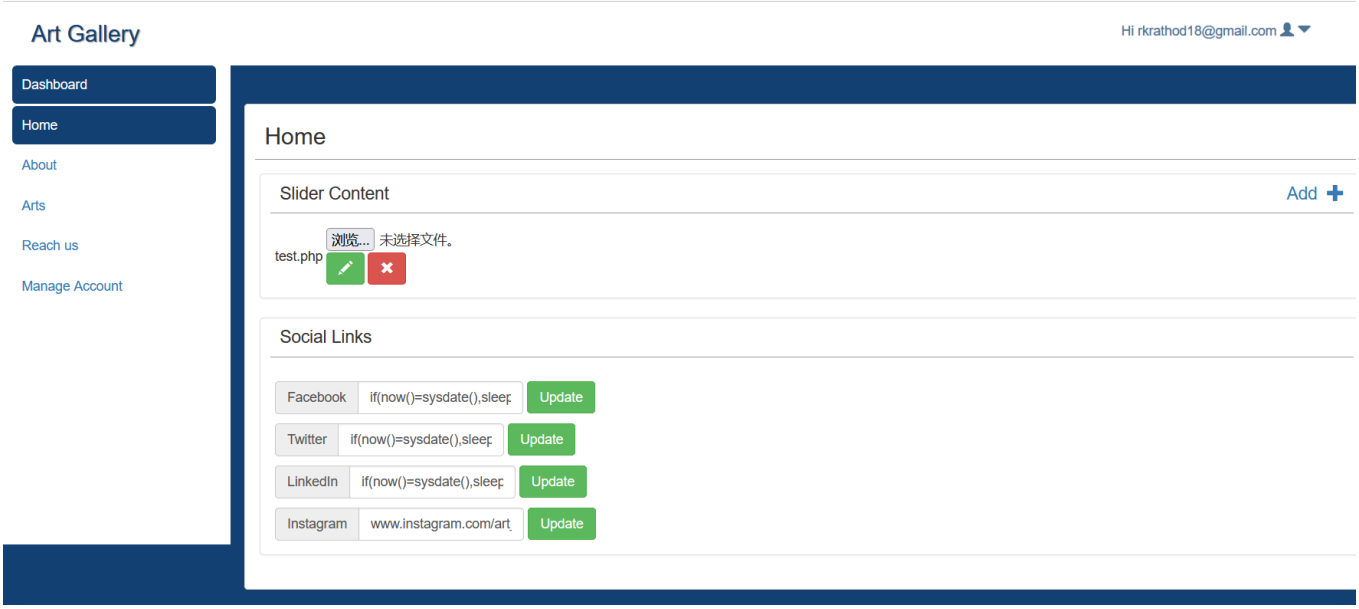
SIMPLE ART GALLERY system has a file upload (RCE) vulnerability

SIMPLE ART GALLERY system has a file upload (RCE) vulnerability

Simple Art Gallery system has a file upload (rCE) vulnerability

The sliderPicSubmit function in the adminHome.php file, The attacker can upload any file for remote code execution command after logging in to the background.




```
32
33
34      if(isset($_POST['sliderPicSubmit']))
35      {
36          $nm=$_FILES['sliderpic']['name'];
37          $target = "../images/Slider".$_FILES['sliderpic']['name'];
38          $datatarget = "images/Slider".$_FILES['sliderpic']['name'];
39          if(!move_uploaded_file($_FILES['sliderpic']['tmp_name'],$target))
40          {
41              echo "Sorry can't upload file....";
42          }
43          else
44          {
45              $query="update slider set img_nm='$nm',path='$datatarget'";
46              mysqli_query($link,$query) or die("Error updating data.".mysqli_error($link));
47          }
48      }
```

PHP Version 7.3.4

System	Windows NT DESKTOP-M4LV1AG 10.0 build 19042 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--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\php7.3.4nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS,VC15
PHP Extension Build	API20180731,NTS,VC15
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled