New issue

Jump to bottom

The CraigMS has a Command execution in craigms/main.php #1

Open HLHai opened this issue on Jan 23, 2019 · 0 comments

HLHai commented on Jan 23, 2019

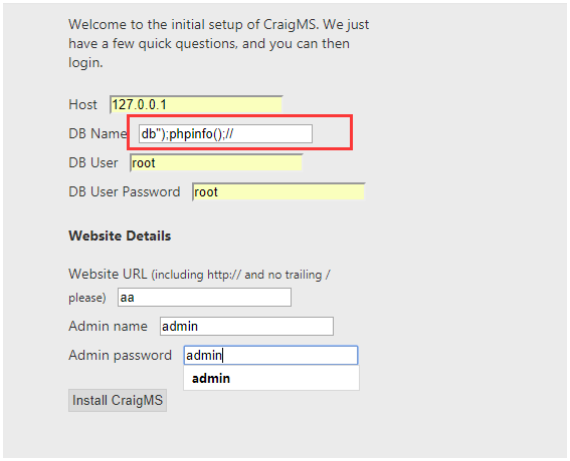
In craigms/main.php line 74

```
73      $f = fopen('includes/database.php', 'w') or die("can't open file");
74      fwrite($f, '<?php  mysql_connect("'.$host.'", "'.$dbuser.'", "'.$
            password.'") ;
75      mysql_select_db("'.$dbname.'") ;
```

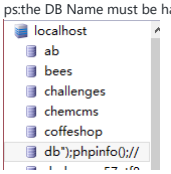
No filtering at post

```
35  <?php
36  $host = $_POST["host"];
37  $dbuser = $_POST["dbuser"];
38  $password = $_POST["password"];
39  $dbname = $_POST["dbname"];
40
41  $weburl = $_POST["weburl"];
42  $adminname = $_POST["adminuser"];
43  $adminpassword = $_POST["adminpass"];
44  $encrypt_password=md5($adminpassword);
45
```

open http://127.0.0.1/Craigcms/craigms/main.php and input exp



ps:the DB Name must be hava in mysql database.



open http://127.0.0.1/Craigcms/craigms/admin/check_login.php

PHP Version 5.2.17

System	Windows NT HAI 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\x86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" "--without-pi3web"
Server API	Apache 2.4 Handler - Apache Lounge
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\windows
Loaded Configuration File	F:\phpStudy\php\php-5.2.17\php.ini
Scan this dir for additional .ini files	(none)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant