

New issue

[Jump to bottom](#)

There is an file inclusion vulnerability() in the template management module in UCMS 1.6. #1

Open luoyangchangan opened this issue on Oct 1 · 0 comments

luoyangchangan commented on Oct 1

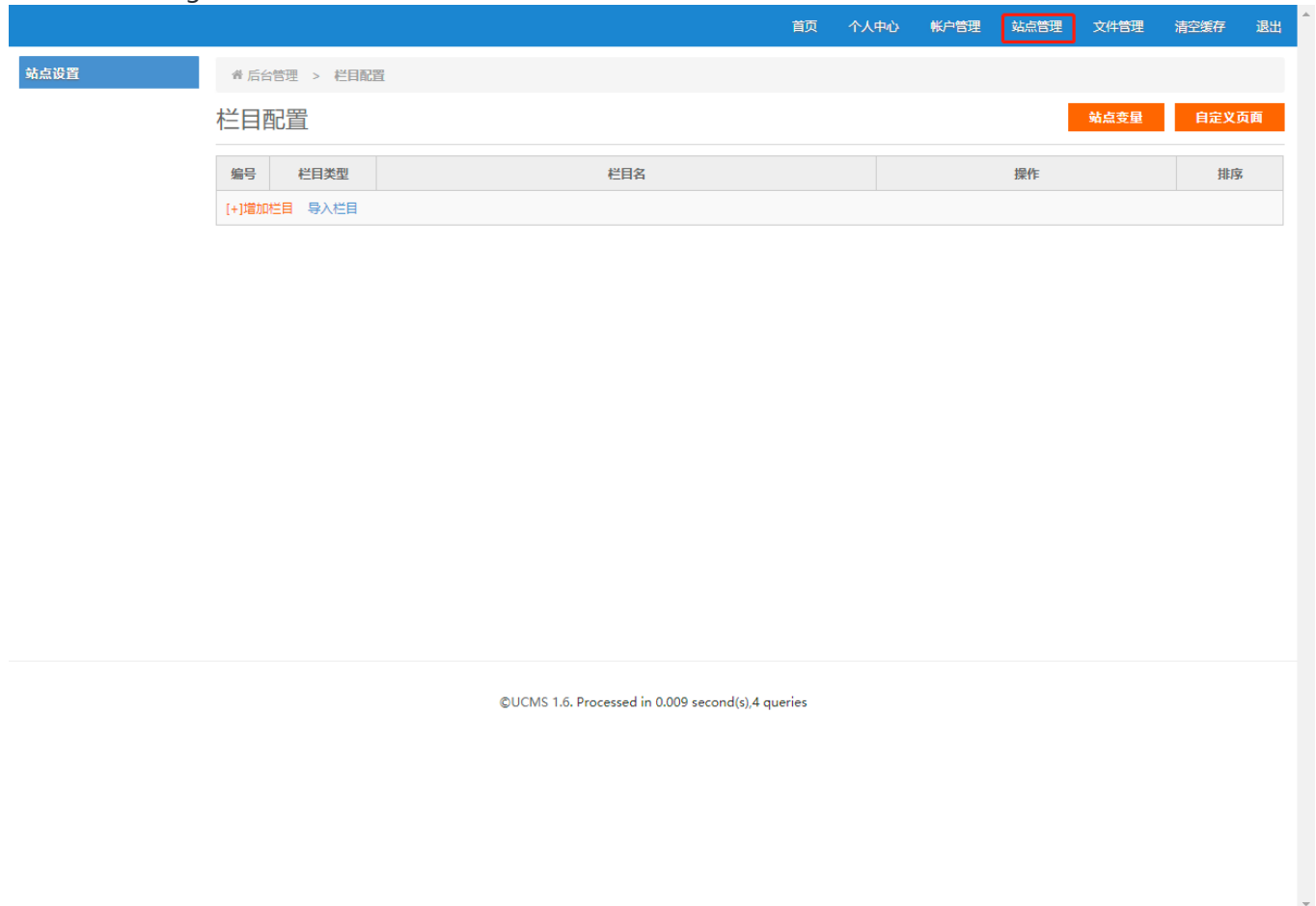
Owner

vendor: <http://uuu.la/>

UCMS 1.6 installation package: http://uuu.la/uploadfile/file/ucms_1.6.zip

After installation, log in to the background

click Site management



click on the Custom page

首页 个人中心 帐户管理 站点管理 文件管理 清空缓存 退出

站点设置

后台管理 > 栏目配置

栏目配置

站点变量

自定义页面

编号	栏目类型	栏目名	操作	排序
<div>[+]增加栏目 导入栏目</div>				

©UCMS 1.6. Processed in 0.009 second(s),4 queries

fiset click Add Page,then click choose

站点设置

首页 个人中心 帐户管理 站点管理 文件管理 清空缓存 退出

自定义页面

页面地址: 页面缓存时间: 0 模板文件:

[+]增加页面

自定义页面帮助

选择 删除

保存

1

2

©UCMS 1.6. Processed in 0.009 second(s),4 queries














click footer.php

站点设置

后台管理 > 文件管理

文件管理 /template/

根目录 最近修改 返回

文件名	文件大小	创建时间	修改时间	操作
 article.php	1.09 KB	2022-09-29 14:58:15	2021-05-20 00:00:00	编辑 重命名 删除
 css		2022-09-29 14:58:15	2022-09-29 14:58:31	打开文件夹 重命名
 footer.php 选择	301 B	2022-09-29 14:58:15	2022-10-01 17:35:13	编辑 重命名 删除
 header.php	549 B	2022-09-29 14:58:15	2021-05-20 00:00:00	编辑 重命名 删除
 images		2022-09-29 14:58:15	2022-09-29 14:58:31	打开文件夹 重命名
 index.php	1.37 KB	2022-09-29 14:58:15	2021-05-20 00:00:00	编辑 重命名 删除
 js		2022-09-29 14:58:15	2021-05-20 00:00:00	打开文件夹 重命名
 list.php	991 B	2022-09-29 14:58:15	2021-05-20 00:00:00	编辑 重命名 删除
 m		2022-09-29 14:58:15	2022-09-29 14:58:31	打开文件夹 重命名
 page.php	676 B	2022-09-29 14:58:15	2021-05-20 00:00:00	编辑 重命名 删除
 right_ad.php	258 B	2022-09-29 14:58:15	2021-05-20 00:00:00	编辑 重命名 删除
 right_article.php	435 B	2022-09-29 14:58:15	2021-05-20 00:00:00	编辑 重命名 删除
 right_channel.php	268 B	2022-09-29 14:58:15	2021-05-20 00:00:00	编辑 重命名 删除

新建文件夹:

提交

新建文件:

提交

上传文件:

选择文件

 未选择任何文件

上传

总数:13

Add shellcode ,then click save it

[首页](#) [个人中心](#) [帐户管理](#) [站点管理](#) [文件管理](#) [清空缓存](#) [退出](#)

站点设置

后台管理 > 文件修改

文件管理 /template/footer.php

[根目录](#) [模板制作助手](#) [返回](#)

```
1 <!-- 底部--><?php if(!defined('ucms'))exit, ?> -->
2 <div class="clear"></div>
3 <div class="footer wrap">
4 <div>
5 <?php phpinfo();?>
6 {{Z(首页)}} {{Z(联系我们)}}
7 </div>
8
```

保存

©UCMS 1.6. Processed in 0.011 second(s),3 queries

The image is a screenshot of a web browser displaying the UCMS website. The browser's address bar at the top shows the URL '127.0.0.1:8002/index.php'. The website's header features the 'UCMS' logo on the left and a banner on the right that reads 'UCMS模板制作指南' (UCMS Template Making Guide) with a subtext '如何用UCMS制作各类网站,详情点击uuu.la' (How to use UCMS to make various websites, click uuu.la for details). Below the header is a blue navigation bar with the link '首页' (Home). On the left side, there is a sidebar with the text '当前位置: 首页' (Current location: Home). The main content area is divided into three sections: '最新文章' (Latest Articles), '广告位' (Advertisement Position), and '友情链接' (Friendly Links). The '广告位' section contains a large 3D orange 'WWW' graphic, the text 'uuu.la', and 'UCMS在线交流' (UCMS Online Communication) with a QQ group number '83626361'. The '友情链接' section includes links like '自己动手,丰衣足食' (Do it yourself, have plenty to eat and drink), '学习如何搭建友情链接栏目→' (Learn how to build a friendly link column →), and '如何自定义LOGO、广告位图片→' (How to customize LOGO, advertisement position image →).

```
}  
if(!$templist[3][$key] && substr($thisTemp, offset: 0, length: 5)=='file ') {  
    $thisOtherTemp=substr($thisTemp, offset: 5);  
    $templist[3][$key]=1;  
    if(strpos($thisOtherTemp, needle: '.')===false) {  
        $thisOtherTemp.='.php';  
    }  
    $templist[1][$key]='@include(\''.include_template($thisOtherTemp,0).'\');';  
}  
if(!$templist[3][$key]) {  
    $thisNewTemp=escape_temp_char($thisTemp, encode: 1);
```

No one assigned

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

