# CVE LIST of 192:168:0:103

vsftpd 2.3.4 vsftpd 2.3.4 : CRITICAL EXPOSURE

|_ vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) URL: https://www.exploit-db.com/exploits/17491

Linux telnetd  Linux telnetd : CRITICAL EXPOSURE

|_ netkit-telnet-0.17 telnetd (Fedora 31) - 'BraveStarr' Remote Code Execution URL: https://www.exploit-db.com/exploits/48170
|_ TelnetD encrypt_keyid - Function Pointer Overwrite CVE_ID: CVE-2011-4862
|___|_ URL: https://www.exploit-db.com/exploits/18280

rpcbind 2 rpcbind 2 : CRITICAL EXPOSURE

|_ rpcbind - CALLIT procedure UDP Crash (PoC) URL: https://www.exploit-db.com/exploits/26887
|_ RPCBind / libtirpc - Denial of Service CVE_ID: CVE-2017-8779
|___|_ URL: https://www.exploit-db.com/exploits/41974
|_ Wietse Venema Rpcbind Replacement 2.1 - Denial of Service URL: https://www.exploit-db.com/exploits/20376

login  login : CRITICAL EXPOSURE

|_ (GREEZLE) Global Real Estate Agent Login - Multiple SQL Injections URL: https://www.exploit-db.com/exploits/34111
|_ 4x CMS - 'login.php' Multiple SQL Injections URL: https://www.exploit-db.com/exploits/33914
|_ 68 Classifieds 4.1 - 'login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/33198
|_ Absolute Form Processor XE 1.5 - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/32898
|_ AckerTodo 4.2 - 'login.php' Multiple SQL Injections URL: https://www.exploit-db.com/exploits/28767
|_ Active News Manager - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/25703
|_ Activedition - '/activedition/aelogin.asp' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/34397
|_ AdMentor - Admin Login SQL Injection URL: https://www.exploit-db.com/exploits/29533
|_ AdminLog 0.5 - 'valid_login' Authentication Bypass URL: https://www.exploit-db.com/exploits/9075
|_ Adobe ColdFusion Server 8.0.1 - '/wizards/common/_logintowizard.cfm' Query String Cross-Site Scripting URL: https://www.exploit-db.com/exploits/33169
|_ Advanced Login 0.7 - 'root' Remote File Inclusion CVE_ID: CVE-2007-1766
|___|_ URL: https://www.exploit-db.com/exploits/3608
|_ AfterLogic MailBee WebMail Pro 3.x - 'login.php?mode' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/30641
|_ AIOCP 1.3.x - 'cp_login.php' SQL Injection URL: https://www.exploit-db.com/exploits/28931
|_ Airties - login-cgi Buffer Overflow (Metasploit) CVE_ID: CVE-2015-2797
|___|_ URL: https://www.exploit-db.com/exploits/37170
|_ Alisveristr E-Commerce Login - Multiple SQL Injections URL: https://www.exploit-db.com/exploits/26707
|_ allocPSA 1.7.4 - '/login/login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/35754
|_ AlphAdmin CMS 1.0.5_03 - 'aa_login' Cookie Authentication Bypass URL: https://www.exploit-db.com/exploits/32102
|_ Ampache 3.4.3 - 'login.php' Multiple SQL Injections URL: https://www.exploit-db.com/exploits/33421
|_ Ampache 3.5.4 - 'login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/35716
|_ aoblogger 2.3 - 'login.php?Username' SQL Injection URL: https://www.exploit-db.com/exploits/27105
|_ APBook 1.3 - Admin Login Multiple SQL Injections URL: https://www.exploit-db.com/exploits/34705
|_ AppIntellect SpotLight CRM - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/29271
|_ AppleFileServer (OSX) - LoginExt PathName Overflow (Metasploit) URL: https://www.exploit-db.com/exploits/16863
|_ AppleFileServer 10.3.3 (OSX) - LoginEXT PathName Overflow (Metasploit) URL: https://www.exploit-db.com/exploits/9931
|_ ARISg 5.0 - 'wflogin.jsp' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/33678
|_ Article Dashboard - '/admin/login.php' Multiple SQL Injections URL: https://www.exploit-db.com/exploits/31028
|_ Article Directory - 'login.php' SQL Injection URL: https://www.exploit-db.com/exploits/33409
|_ ASPired2Protect Login Page - SQL Injection URL: https://www.exploit-db.com/exploits/31070
|_ ASPThai Forums 8.0 - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/27142
|_ ATutor 1.5.1 - 'login.php?course' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/26170
|_ BandSite CMS 1.1 - 'login_header.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/28622
|_ Bandwebsite 1.5 - 'LOGIN' Remote Add Admin CVE_ID: CVE-2006-6722
|___|_ URL: https://www.exploit-db.com/exploits/2938

|_ Banking@Home 2.1 - 'login.asp' Multiple SQL Injections URL: https://www.exploit-db.com/exploits/32797
|_ Battleaxe Software BTTLXE Forum - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/22529
|_ bbPress 0.8.1 - 'BB-login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/30175
|_ BEA WebLogic 7.0/8.1 - Administration Console LoginForm.jsp Cross-Site Scripting URL: https://www.exploit-db.com/exploits/25738
|_ Beck IPC GmbH IPC@CHIP - TelnetD Login Account Brute Force URL: https://www.exploit-db.com/exploits/20881
|_ Belkin N750 - 'jump?login' Remote Buffer Overflow CVE_ID: CVE-2014-1635
|___|_ URL: https://www.exploit-db.com/exploits/35184
|_ BestWebApp Dating Site - 'login_form.asp?msg' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/29081
|_ BestWebApp Dating Site Login Component - Multiple Field SQL Injections URL: https://www.exploit-db.com/exploits/29080
|_ BibORB 1.3.2 Login Module - Multiple SQL Injections URL: https://www.exploit-db.com/exploits/25121
|_ Bloginator 1a - Cookie Bypass / SQL Injection CVE_ID: CVE-2009-1049 CVE-2009-1050
|___|_ URL: https://www.exploit-db.com/exploits/8243
|_ Bloginator 1a - SQL Injection / Command Injection (via Cookie Bypass ) CVE_ID: CVE-2009-1049
|___|_ URL: https://www.exploit-db.com/exploits/8244
|_ Boutique SudBox 1.2 - Cross-Site Request Forgery (Changer Login et Mot de Passe) URL: https://www.exploit-db.com/exploits/12419
|_ BrowserCRM 5.100.1 - 'login[]' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/36454
|_ BSD/OS 2.1 / DG/UX 4.0 / Debian 0.93 / Digital UNIX 4.0 B / FreeBSD 2.1.5 / HP-UX 10.34 / IBM AIX 4.1.5 / NetBSD 1.0/1.1 / NeXTstep 4.0 / SGI IRIX 6.3 /
|_ BT Home Hub 6.2.2.6 - Login procedure Authentication Bypass URL: https://www.exploit-db.com/exploits/30740
|_ Cacti 0.8.7 - '/index.php/sql.php?Login Action login_username' SQL Injection URL: https://www.exploit-db.com/exploits/31161
|_ Campsite 2.6.1 - 'LoginAttempts.php?g_documentRoot' Remote File Inclusion URL: https://www.exploit-db.com/exploits/29986
|_ CartWIZ 1.10 - 'login.asp' Message Argument Cross-Site Scripting URL: https://www.exploit-db.com/exploits/25520
|_ CartWIZ 1.10 - 'login.asp' Redirect Argument Cross-Site Scripting URL: https://www.exploit-db.com/exploits/25516
|_ Ceica-GW - 'login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/34155
|_ Check Point Connectra R62 - '/Login/Login' Arbitrary Script Injection URL: https://www.exploit-db.com/exploits/33234
|_ Check Point VPN-1 UTM Edge NGX 7.0.48x - Login Page Cross-Site Scripting URL: https://www.exploit-db.com/exploits/31340
|_ Chris LaPointe Download Center 1.2 - login Action Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/31389
|_ CI User Login and Management 1.0 - Arbitrary File Upload URL: https://www.exploit-db.com/exploits/45757
|_ Cisco Network Assistant 6.3.3 - 'Cisco Login' Denial of Service (PoC) URL: https://www.exploit-db.com/exploits/45275
|_ Cisco Secure ACS 2.3 - 'LoginProxy.cgi' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/28030
|_ Citrix Metaframe Web Manager - 'login.asp' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/31286
|_ CMtextS 1.0 - '/users_logins/admin.txt' Credentials Disclosure CVE_ID: CVE-2006-4897
|___|_ URL: https://www.exploit-db.com/exploits/2388
|_ Codice CMS - 'login.php' SQL Injection URL: https://www.exploit-db.com/exploits/31099
|_ ColdFusion Server 2.0/3.x/4.x - Administrator Login Password Denial of Service URL: https://www.exploit-db.com/exploits/19996
|_ Commercial Interactive Media SCOOP! 2.3 - 'account_login.asp' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/26942
|_ Community Link Pro - 'login.cgi?File' Remote Command Execution URL: https://www.exploit-db.com/exploits/25920
|_ ContentBoxx - 'login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/27688
|_ ContentLion Alpha 1.3 - 'login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/36870
|_ Cool Cafe Chat 1.2.1 - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/25839
|_ CoolForum 0.5/0.7/0.8 - 'register.php?login' SQL Injection URL: https://www.exploit-db.com/exploits/25240
|_ CoolShot E-Lite POS 1.0 - Login SQL Injection URL: https://www.exploit-db.com/exploits/30803
|_ cPanel 5/6/7/8/9 - Login Script Remote Command Execution URL: https://www.exploit-db.com/exploits/23807
|_ CS-Guestbook 0.1 - Login Credentials Information Disclosure URL: https://www.exploit-db.com/exploits/30581
|_ CubeCart 3.0.20 - '/admin/login.php?goto' Arbitrary Site Redirect URL: https://www.exploit-db.com/exploits/36686
|_ Cuteflow Bin 1.5.0 - 'login.php' Local File Inclusion CVE_ID: CVE-2008-1493
|___|_ URL: https://www.exploit-db.com/exploits/5296
|_ CyberBuild - 'login.asp?sessionid' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/27815
|_ CyberBuild - 'login.asp?sessionid' SQL Injection URL: https://www.exploit-db.com/exploits/27813
|_ Cyphor 0.19 - 'footer.php?t_login' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/26339
|_ Cyrus IMAPD 1.4/1.5.19/2.0.12/2.0.16/2.1.9/2.1.10 - Pre-Login Heap Corruption URL: https://www.exploit-db.com/exploits/22061
|_ D-Link Airspot DSA-3100 Gateway - 'Login_error.SHTML' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/27923
|_ D-Link DIR-Series Routers - HNAP Login Stack Buffer Overflow (Metasploit) CVE_ID: CVE-2016-6563
|___|_ URL: https://www.exploit-db.com/exploits/40805

|_ Daffodil CRM 1.5 - 'Userlogin.asp' SQL Injection URL: https://www.exploit-db.com/exploits/27151
|_ DaLogin - Multiple Vulnerabilities CVE_ID: CVE-2010-5012
|___|_ URL: https://www.exploit-db.com/exploits/13830
|_ DaLogin 2.2 - 'FCKeditor' Arbitrary File Upload URL: https://www.exploit-db.com/exploits/13835
|_ Dark Age CMS 2.0 - 'login.php' SQL Injection URL: https://www.exploit-db.com/exploits/32724
|_ Dark Hart Portal - 'login.php' Remote File Inclusion URL: https://www.exploit-db.com/exploits/12553
|_ Darxite 0.4 - Login Buffer Overflow URL: https://www.exploit-db.com/exploits/20159
|_ DCP-Portal 6.0 - 'login.php?Username' SQL Injection URL: https://www.exploit-db.com/exploits/28573
|_ Debian - Symlink In Login Arbitrary File Ownership CVE_ID: CVE-2008-5394
|___|_ URL: https://www.exploit-db.com/exploits/7313
|_ DELTAScripts PHP Classifieds 6.20 - 'Member_Login.php' SQL Injection URL: https://www.exploit-db.com/exploits/27214
|_ DeskPro 2.0.1 - 'login.php' HTML Injection URL: https://www.exploit-db.com/exploits/29828
|_ Dick Lin ZetaMail 2.1 - Login Denial of Service URL: https://www.exploit-db.com/exploits/19636
|_ Digital Scribe 1.4 - Login SQL Injection URL: https://www.exploit-db.com/exploits/26262
|_ Disk Pulse Enterprise 9.0.34 - 'Login' Remote Buffer Overflow (Metasploit) URL: https://www.exploit-db.com/exploits/40758
|_ Disk Pulse Enterprise 9.0.34 - 'Login' Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/40452
|_ Disk Pulse Enterprise 9.1.16 - 'Login' Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/40835
|_ Disk Savvy Enterprise 9.0.32 - 'Login' Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/40459
|_ Disk Savvy Enterprise 9.1.14 - 'Login' Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/40834
|_ Disk Sorter Enterprise 9.0.24 - 'Login' Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/40458
|_ Disk Sorter Enterprise 9.1.12 - 'Login' Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/40833
|_ DMXReady Secure Login Manager 1.0 - '/applications/SecureLoginManager/inc_secureloginmanager.asp?sent' SQL Injection URL: https://www.exploit-db.co
|_ DMXReady Secure Login Manager 1.0 - 'content.asp?sent' SQL Injection URL: https://www.exploit-db.com/exploits/29359
|_ DMXReady Secure Login Manager 1.0 - 'login.asp?sent' SQL Injection URL: https://www.exploit-db.com/exploits/29358
|_ DMXReady Secure Login Manager 1.0 - 'members.asp?sent' SQL Injection URL: https://www.exploit-db.com/exploits/29360
|_ Dotclear 2.4.1.2 - '/admin/auth.php?login_data' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/36888
|_ DragDropCart - 'login.php?redirect' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/34734
|_ Dragon Internet Events Listing 2.0.01 - 'admin_login.asp' Multiple Field SQL Injections URL: https://www.exploit-db.com/exploits/29044
|_ DRZES Hms 3.2 - 'login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/26758
|_ DSLogin 1.0 - 'index.php' Multiple SQL Injections URL: https://www.exploit-db.com/exploits/27485
|_ DUforum 3.x - Login Form 'Password' SQL Injection URL: https://www.exploit-db.com/exploits/24673
|_ Dup Scout Enterprise - 'Login' Buffer Overflow (Metasploit) URL: https://www.exploit-db.com/exploits/43339
|_ Dup Scout Enterprise 10.0.18 - 'Login' Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/43145
|_ Dup Scout Enterprise 9.0.28 - 'Login' Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/40457
|_ Dup Scout Enterprise 9.1.14 - 'Login' Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/40832
|_ dvbbs 8.2 - 'login.asp' Multiple SQL Injections URL: https://www.exploit-db.com/exploits/31861
|_ Dynamic Biz Website Builder 'QuickWeb' 1.0 - '/login.asp' Multiple Field SQL Injections / Authentication Bypass URL: https://www.exploit-db.com/exploits/388
|_ Dynamic Biz Website Builder (QuickWeb) 1.0 - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/25914
|_ E-lokaler CMS 2 - Admin Login Multiple SQL Injections URL: https://www.exploit-db.com/exploits/35027
|_ E-Smart Cart - 'Members Login' Multiple SQL Injection Vulnerabilities URL: https://www.exploit-db.com/exploits/31059
|_ E-Smart Cart 1.0 - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/30564
|_ e-Soft24 PTC Script 1.2 - 'login.php' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/34652
|_ Easebay Resources Login Manager - Multiple Input Validation Vulnerabilities URL: https://www.exploit-db.com/exploits/29498
|_ Easy POS System - 'login.php' SQL Injection URL: https://www.exploit-db.com/exploits/31145
|_ Easylogin Pro 1.3.0 - 'Encryptor.php' Unserialize Remote Code Execution CVE_ID: CVE-2018-15576
|___|_ URL: https://www.exploit-db.com/exploits/45227
|_ ECommPro 3.0 - 'Admin/login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/25466
|_ EsContacts 1.0 - 'login.php?msg' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/31664
|_ Evandor Easy notesManager 0.0.1 - 'login.php?Username' SQL Injection URL: https://www.exploit-db.com/exploits/28878
|_ Expinion.net News Manager Lite 2.5 - 'NEWS_LOGIN?admin' Cookie Authentication Bypass URL: https://www.exploit-db.com/exploits/23863
|_ eXtremail 2.1.1 - 'LOGIN' Remote Stack Overflow CVE_ID: CVE-2007-5466
|___|_ URL: https://www.exploit-db.com/exploits/4533
|_ Extreme Mobster - 'login' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/33650

|_ Facebook for Android - 'LoginActivity' Information Disclosure URL: https://www.exploit-db.com/exploits/38170
|_ Farsinews 2.1 - 'Loginout.php' Remote File Inclusion URL: https://www.exploit-db.com/exploits/27154
|_ FlatFile Login System - Remote Password Disclosure URL: https://www.exploit-db.com/exploits/11515
|_ FotoWeb 6.0 - 'Login.fwx?s' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/32782
|_ Free File Hosting System 1.1 - 'login.php?AD_BODY_TEMP' Remote File Inclusion URL: https://www.exploit-db.com/exploits/29773
|_ FreeBSD 4.3/4.4 - Login Capabilities Privileged File Reading URL: https://www.exploit-db.com/exploits/21114
|_ Freeway 1.4.1.171 - '/templates/Freeway/boxes/loginbox.php?language' Traversal Local File Inclusion URL: https://www.exploit-db.com/exploits/32268
|_ Freewebscriptz Online Games Login - Multiple SQL Injections URL: https://www.exploit-db.com/exploits/34230
|_ Friendly Technologies TR-069 ACS 2.8.9 - Login SQL Injection URL: https://www.exploit-db.com/exploits/33731
|_ Froxlor Server Management Panel 0.9.33.1 - MySQL Login Information Disclosure URL: https://www.exploit-db.com/exploits/37725
|_ FunkyASP AD Systems 1.1 - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/25705
|_ Game-Panel 2.6 - 'login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/27364
|_ Gate Pass Management System 2.1 - 'login' SQL Injection URL: https://www.exploit-db.com/exploits/45766
|_ GAzie 5.10 - 'Login' Multiple Vulnerabilities URL: https://www.exploit-db.com/exploits/16183
|_ GNU Mailman 2.0.x - Admin Login Cross-Site Scripting URL: https://www.exploit-db.com/exploits/21480
|_ GNU Mailman 2.0.x - Admin Login Variant Cross-Site Scripting URL: https://www.exploit-db.com/exploits/21642
|_ Gravity Board X 1.1 - Login SQL Injection URL: https://www.exploit-db.com/exploits/26106
|_ Guestbara 1.2 - Change Admin Login and Password CVE_ID: CVE-2007-1553
|___|_ URL: https://www.exploit-db.com/exploits/3506
|_ H-Sphere WebShell 2.x - 'login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/28815
|_ Hero Framework - '/users/login?Username' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/38461
|_ Hero Framework - users/login 'Username' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/38142
|_ Home of MCLogin System - Authentication Bypass CVE_ID: CVE-2010-5000
|___|_ URL: https://www.exploit-db.com/exploits/13766
|_ Horde Framework 3.1.3 - 'login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/29745
|_ HotPlug CMS 1.0 - 'Login1.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/28031
|_ HP Data Protector - DtbClsLogin Buffer Overflow (Metasploit) URL: https://www.exploit-db.com/exploits/23290
|_ HP StorageWorks P4000 Virtual SAN Appliance - Login Buffer Overflow (Metasploit) URL: https://www.exploit-db.com/exploits/27555
|_ Iatek PortalApp 3.3/4.0 - 'login.asp' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/34221
|_ IBD Micro CMS 3.5 - 'microcms-admin-login.php' Multiple SQL Injections URL: https://www.exploit-db.com/exploits/31781
|_ IBM (Multiple Products) - Login Page Cross-Site Scripting URL: https://www.exploit-db.com/exploits/33675
|_ IBM AIX 3.2.5 - 'login(1)' Privilege Escalation URL: https://www.exploit-db.com/exploits/19348
|_ IBM Bladecenter Advanced Management Module 1.42 - Login 'Username' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/32894
|_ IBM ENOVIA SmarTeam - 'LoginPage.aspx' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/33728
|_ IceWarp Web Mail 5.3 - login.html 'Username' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/25068
|_ ImageVue 2.0 - Remote Admin Login URL: https://www.exploit-db.com/exploits/10630
|_ Indexu 5.0/5.3 - 'login.php?Error_msg' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/29489
|_ INFINICART - 'login.asp' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/28991
|_ Infoblox NetMRI 6.2.1 - Admin Login Page Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/36299
|_ InstantSoftwares Dating Site - Login SQL Injection URL: https://www.exploit-db.com/exploits/30963
|_ IntelliTamper 2.07/2.08 - 'ProxyLogin' Local Stack Overflow CVE_ID: CVE-2008-5868
|___|_ URL: https://www.exploit-db.com/exploits/7608
|_ International TeleCommunications WebBBS 2.13 - login & Password Buffer Overflow URL: https://www.exploit-db.com/exploits/19623
|_ IntranetApp 3.3 - 'login.asp?ret_page' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/26928
|_ Invision Power Board 1.3.1 - 'login.php' SQL Injection URL: https://www.exploit-db.com/exploits/1036
|_ Invision Power Board 2.0.3 - 'login.php' SQL Injection (Tutorial) URL: https://www.exploit-db.com/exploits/1014
|_ Invision Power Board 2.0.3 - 'login.php' SQL Injection CVE_ID: CVE-2005-1598
|___|_ URL: https://www.exploit-db.com/exploits/1013
|_ IPortalX - '/forum/login_user.asp' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/30940
|_ Ipswitch WhatsUp Professional 2005 SP1 - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/25874
|_ ISP Site Man - 'admin_login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/27552
|_ Jamroom 3.0.16 - 'login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/28659
|_ Jax Guestbook 3.50 - Admin Login CVE_ID: CVE-2009-4447

|___|_ URL: https://www.exploit-db.com/exploits/10626
|_ Jetbox CMS 2.1 - Login Variable Cross-Site Scripting URL: https://www.exploit-db.com/exploits/30068
|_ JibberBook 2.3 - 'Login_form.php' Authentication Bypass URL: https://www.exploit-db.com/exploits/37139
|_ JiRo's (Multiple Products) - '/files/login.asp' Multiple SQL Injections URL: https://www.exploit-db.com/exploits/33361
|_ JiRo's Banner System 2.0 - 'login.asp' Multiple SQL Injections URL: https://www.exploit-db.com/exploits/30775
|_ JiRo's Upload System 1.0 - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/25780
|_ Joomla! Component LoginBox - Local File Inclusion CVE_ID: CVE-2010-1353
|___|_ URL: https://www.exploit-db.com/exploits/12068
|_ JSBoard 2.0.10 - 'login.php?table' Local File Inclusion CVE_ID: CVE-2007-1842
|___|_ URL: https://www.exploit-db.com/exploits/3614
|_ JSBoard 2.0.10/2.0.11 - 'login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/27794
|_ JSPWiki 2.5.139 - 'Login.jsp' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/30612
|_ Juniper Networks Mobility System Software - '/aaa/wba_login.html' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/37429
|_ KB Login Authentication Script 1.1 - Authentication Bypass URL: https://www.exploit-db.com/exploits/41167
|_ Keld PHP-MySQL News Script 0.7.1 - 'login.php' SQL Injection URL: https://www.exploit-db.com/exploits/32143
|_ Kodak InSite 5.5.2 - '/Pages/login.aspx?Language' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/35412
|_ KwsPHP 1.0 - 'login.php' SQL Injection CVE_ID: CVE-2007-4956
|___|_ URL: https://www.exploit-db.com/exploits/4412
|_ LaGarde StoreFront 5.0 Shopping Cart - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/25847
|_ Lantern CMS - '11-login.asp' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/34824
|_ LBreakout2 2.x - Login Remote Format String URL: https://www.exploit-db.com/exploits/22830
|_ LDF - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/32756
|_ Lead Capture - 'login.php' Script Cross-Site Scripting URL: https://www.exploit-db.com/exploits/36647
|_ LedgerSMB1.0/1.1 / SQL-Ledger 2.6.x - 'Login' Local File Inclusion / Authentication Bypass URL: https://www.exploit-db.com/exploits/29761
|_ Liferay Portal 4.1 Login Script - Cross-Site Scripting URL: https://www.exploit-db.com/exploits/30774
|_ Limny 3.0.1 - 'login.php' Script Cross-Site Scripting URL: https://www.exploit-db.com/exploits/36494
|_ Linux PAM 0.77 - Pam_Wheel Module 'getlogin() Username' Spoofing Privilege Escalation URL: https://www.exploit-db.com/exploits/22781
|_ Linux pam_lib_smb < 1.1.6 - '/bin/login' Remote Overflow URL: https://www.exploit-db.com/exploits/89
|_ LiveStreet 0.2 - '/include/ajax/blogInfo.php?asd' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/34446
|_ Livingcolor Livingmailing 1.3 - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/25783
|_ Login-Reg Members Management PHP 1.0 - Arbitrary File Upload URL: https://www.exploit-db.com/exploits/42575
|_ Lootan - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/32758
|_ LucidCMS 2.0 - Login SQL Injection URL: https://www.exploit-db.com/exploits/26307
|_ Magento 1.2 - '/app/code/core/Mage/Admin/Model/Session.php?login['Username']' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/32808
|_ Magic Photo Storage Website - '/user/login.php?_config[site_path]' Remote File Inclusion URL: https://www.exploit-db.com/exploits/29427
|_ Maia Mailguard 1.0.2 - 'login.php' Multiple Local File Inclusions URL: https://www.exploit-db.com/exploits/30277
|_ MailBee WebMail Pro 3.4 - 'Check_login.asp' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/29851
|_ MailEnable IMAPD Professional (2.35) - Login Request Buffer Overflow (Metasploit) URL: https://www.exploit-db.com/exploits/16475
|_ ManageEngine OpUtils 5 - 'Login.DO' SQL Injection CVE_ID: CVE-2010-1044
|___|_ URL: https://www.exploit-db.com/exploits/11330
|_ MatterDaddy Market 1.1 - 'login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/32299
|_ Mercur Messaging 2005 - IMAP Login Buffer Overflow (Metasploit) URL: https://www.exploit-db.com/exploits/16481
|_ Mercury/32 Mail Server 4.0.1 - 'LOGIN' Remote IMAP Stack Buffer Overflow URL: https://www.exploit-db.com/exploits/3561
|_ Mercury/32 Mail Server < 4.01b - LOGIN Buffer Overflow (Metasploit) URL: https://www.exploit-db.com/exploits/16473
|_ MercuryBoard 1.1.5 - 'login.php' Blind SQL Injection CVE_ID: CVE-2008-6632
|___|_ URL: https://www.exploit-db.com/exploits/5653
|_ MGinternet Property Site Manager - 'admin_login.asp' Multiple SQL Injections URL: https://www.exploit-db.com/exploits/29031
|_ Microsoft Outlook 2003 - Web Access Login Form Remote URI redirection URL: https://www.exploit-db.com/exploits/25084
|_ Milw0rm Clone Script 1.0 - '/admin/login.php' Authentication Bypass CVE_ID: CVE-2015-4658
|___|_ URL: https://www.exploit-db.com/exploits/37290
|_ miniBloggie 1.0 - 'login.php' SQL Injection URL: https://www.exploit-db.com/exploits/27125
|_ Miro Broadcast Machine 0.9.9 - 'login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/30751
|_ MoinMoin 1.5.x - 'MOIND_ID' Cookie Login Bypass CVE_ID: CVE-2008-0782

|___|_ URL: https://www.exploit-db.com/exploits/4957
|_ Monstra CMS 1.2.0 - 'login' SQL Injection URL: https://www.exploit-db.com/exploits/38769
|_ MyBace Light - 'login_check.php' Remote File URL: https://www.exploit-db.com/exploits/2285
|_ MyBloggie 2.1.5 - 'login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/29492
|_ MyMail 1.0 - 'login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/28108
|_ myNewsletter 1.1.2 - 'adminLogin.asp' Authentication Bypass URL: https://www.exploit-db.com/exploits/1884
|_ MyPHPim - Login Page pass Field SQL Injection URL: https://www.exploit-db.com/exploits/27068
|_ myPHPscripts Login Session 2.0 - Cross-Site Scripting / Database Disclosure CVE_ID: CVE-2008-5854 CVE-2008-5855
|___|_ URL: https://www.exploit-db.com/exploits/7526
|_ MySQL Eventum 1.5.5 - 'login.php' SQL Injection URL: https://www.exploit-db.com/exploits/1134
|_ MyWeight 1.0 - 'user_login.php' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/34742
|_ Nagios XI - 'login.php' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/34507
|_ Net Clubs Pro 4.0 - 'login.cgi?Password' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/27697
|_ Net-Billetterie 2.9 - 'login' SQL Injection URL: https://www.exploit-db.com/exploits/45863
|_ Netautor Professional 5.5 - 'login2.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/34649
|_ Netgear ProSafe 1.x - VPN Firewall Web Interface Login Denial of Service URL: https://www.exploit-db.com/exploits/22407
|_ NetWin Surgemail 1.8/1.9/2.0 / WebMail 3.1 - Login Form Cross-Site Scripting URL: https://www.exploit-db.com/exploits/24177
|_ NEWSolved 1.1.6 - 'login grabber' Multiple SQL Injections CVE_ID: CVE-2009-2389
|___|_ URL: https://www.exploit-db.com/exploits/9042
|_ NEXTWEB (i)Site - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/25781
|_ NoseRub 0.5.2 - Login SQL Injection CVE_ID: CVE-2007-6602
|___|_ URL: https://www.exploit-db.com/exploits/4805
|_ Noticeware Email Server 4.6 - NG LOGIN Messages Denial of Service URL: https://www.exploit-db.com/exploits/32194
|_ NovaStor NovaNET 12 - 'DtbClsLogin()' Remote Stack Buffer Overflow URL: https://www.exploit-db.com/exploits/32832
|_ Novell eDirectory - HTTPSTK Login Stack Overflow URL: https://www.exploit-db.com/exploits/10163
|_ Nukedit 4.9.x - 'login.asp' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/30402
|_ Nukeviet 2.0 - '/admin/login.php' Cookie Authentication Bypass URL: https://www.exploit-db.com/exploits/32243
|_ OCS Inventory NG Server 1.3.1 - 'LOGIN' Remote Authentication Bypass URL: https://www.exploit-db.com/exploits/12520
|_ Ollance Member Login Script - Multiple Vulnerabilities URL: https://www.exploit-db.com/exploits/17466
|_ Omnicron OmniHTTPd 1.1/2.0 Alpha 1 - 'visiadmin.exe' Denial of Service URL: https://www.exploit-db.com/exploits/20304
|_ oneSCHOOL - 'admin/login.asp' SQL Injection CVE_ID: CVE-2007-6665
|___|_ URL: https://www.exploit-db.com/exploits/4824
|_ Online Work Order Suite - Login SQL Injection URL: https://www.exploit-db.com/exploits/34951
|_ OpenEMR 2.8.2 - 'Login_Frame.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/29557
|_ Openfire 3.5.2 - 'login.jsp' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/32249
|_ Oracle Rapid Install Web Server - Secondary Login Page Cross-Site Scripting URL: https://www.exploit-db.com/exploits/30256
|_ OS4E - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/25751
|_ osCMax 2.5 - '/admin/login.php?Username' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/37038
|_ osCMax 2.5 - '/admin/login.php?Username' SQL Injection URL: https://www.exploit-db.com/exploits/37047
|_ osTicket 1.6 RC4 - Admin Login Blind SQL Injection CVE_ID: CVE-2009-2361
|___|_ URL: https://www.exploit-db.com/exploits/9032
|_ OTRS 2.0 - Login Function 'User' SQL Injection URL: https://www.exploit-db.com/exploits/26550
|_ Outfront Spooky 2.x - Login SQL Query Manipulation Password URL: https://www.exploit-db.com/exploits/21434
|_ PaoBacheca Guestbook 2.1 - 'login_ok' Authentication Bypass CVE_ID: CVE-2009-3421
|___|_ URL: https://www.exploit-db.com/exploits/9293
|_ PaoLiber 1.1 - 'login_ok' Authentication Bypass CVE_ID: CVE-2009-3422
|___|_ URL: https://www.exploit-db.com/exploits/9294
|_ PaoLink 1.0 - 'login_ok' Authentication Bypass CVE_ID: CVE-2009-3423
|___|_ URL: https://www.exploit-db.com/exploits/9292
|_ Parallels H-Sphere 3.0/3.1 - 'login.php' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/32396
|_ Pay Roll Time Sheet and Punch Card Application With Web UI - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/30427
|_ PCPIN Chat 5.0.4 - 'login/language' Remote Code Execution URL: https://www.exploit-db.com/exploits/1697
|_ Pentacle In-Out Board 6.03 - 'login.asp' Remote Authentication Bypass URL: https://www.exploit-db.com/exploits/1529

|_ People-Trak - Login SQL Injection URL: https://www.exploit-db.com/exploits/32903
|_ Petraware pTransformer ADC < 2.1.7.22827 - Login Bypass URL: https://www.exploit-db.com/exploits/46934
|_ Pheap 2.0 - 'config.php' Pheap_Login Authentication Bypass URL: https://www.exploit-db.com/exploits/30102
|_ Phenotype CMS 2.8 - 'login.php?user' Blind SQL Injection CVE_ID: CVE-2009-3543
|___|_ URL: https://www.exploit-db.com/exploits/9107
|_ Phorum 3.x - 'login.php' HTTP_REFERER Cross-Site Scripting URL: https://www.exploit-db.com/exploits/23819
|_ PHP Address Book - '/addressbook/register/checklogin.php?Username' SQL Injection URL: https://www.exploit-db.com/exploits/38434
|_ PHP Address Book - '/addressbook/register/router.php?BasicLogin' Cookie SQL Injection URL: https://www.exploit-db.com/exploits/38431
|_ PHP Lite Calendar Express 2.2 - 'login.php?cid' SQL Injection URL: https://www.exploit-db.com/exploits/26112
|_ PHPCOIN 1.2 - 'login.php' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/25175
|_ phpCOIN 1.2 - 'login.php?PHPcoinsessid' SQL Injection URL: https://www.exploit-db.com/exploits/25568
|_ PHPEasyData 1.5.4 - '/admin/login.php?Username' SQL Injection URL: https://www.exploit-db.com/exploits/31905
|_ PHPFreeNews 1.x - Admin Login SQL Injection URL: https://www.exploit-db.com/exploits/26061
|_ PHPGedView 2.5/2.6 - 'login.php' Newlanguage Cross-Site Scripting URL: https://www.exploit-db.com/exploits/24831
|_ PHPGedView 2.5/2.6 - 'login.php?URL' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/24829
|_ PHPGedView 2.5/2.6 - 'login.php?Username' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/24830
|_ PHPGedView 4.1 - 'login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/30534
|_ phpHeaven phpMyChat 0.14.5 - 'edituser.php3?do_not_login' Authentication Bypass URL: https://www.exploit-db.com/exploits/24216
|_ PHPOpenChat 2.3.4/3.0.1 - 'poc_loginform.php?phpbb_root_path' Remote File Inclusion URL: https://www.exploit-db.com/exploits/25227
|_ phpPgAdmin 3.x - Login Form Directory Traversal URL: https://www.exploit-db.com/exploits/25938
|_ PHPsFTPd 0.2/0.4 - 'Inc.login.php' Privilege Escalation URL: https://www.exploit-db.com/exploits/25964
|_ phpSQLiteCMS 1 RC2 - '/cms/includes/login.inc.php' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/31824
|_ PHPWCMS 1.2.5 -DEV - 'login.php?form_lang' Traversal Arbitrary File Access URL: https://www.exploit-db.com/exploits/26512
|_ PHPX 3.5.x - 'Admin 'login.php' SQL Injection URL: https://www.exploit-db.com/exploits/26697
|_ PhxContacts 0.93 - 'login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/27512
|_ Pilot Group eTraining - 'courses_login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/33119
|_ Pilot Group eTraining - 'lessons_login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/33121
|_ Plesk 7.5/8.0 - 'login_up.php3' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/29018
|_ plesk 8.1.1 - 'login.php3' Directory Traversal URL: https://www.exploit-db.com/exploits/29898
|_ PonVFTP - 'login.php' SQL Injection URL: https://www.exploit-db.com/exploits/34095
|_ Portail Web PHP 2.5.1 - 'login.php' Remote File Inclusion URL: https://www.exploit-db.com/exploits/31110
|_ PortalApp 3.3/4.0 - 'login.asp' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/26926
|_ PostNuke 0.6 - User Login URL: https://www.exploit-db.com/exploits/21119
|_ Pre ASP Job Board - 'emp_login.asp' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/32630
|_ Pre Hotel and Resorts - 'user_login.asp' Multiple SQL Injection Vulnerabilities URL: https://www.exploit-db.com/exploits/31058
|_ PrestaShop 1.1 - '/admin/login.php?PATH_INFO' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/32647
|_ ProductCart 1.5/1.6/2.0 - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/22865
|_ ProjectApp 3.3 - 'login.asp?ret_page' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/26935
|_ Property Pro 1.0 - 'vir_Login.asp' Remote Authentication Bypass URL: https://www.exploit-db.com/exploits/2774
|_ Property Watch - 'login.php?redirect' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/34474
|_ Prototype of an PHP Application 0.1 - '/ident/loginliste.php?path_inc' Remote File Inclusion URL: https://www.exploit-db.com/exploits/30121
|_ Prototype of an PHP Application 0.1 - '/ident/loginmodif.php?path_inc' Remote File Inclusion URL: https://www.exploit-db.com/exploits/30122
|_ QwikiWiki 1.4/1.5 - 'login.php' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/27410
|_ Race River Integard Home/Pro - LoginAdmin Password Stack Buffer Overflow (Metasploit) URL: https://www.exploit-db.com/exploits/16778
|_ RASPcalendar 1.01 (ASP) - Admin Login URL: https://www.exploit-db.com/exploits/29500
|_ RaXnet Cacti 0.6.x/0.8.x - 'Auth_Login.php' SQL Injection URL: https://www.exploit-db.com/exploits/24375
|_ Real Estate Listing Website Application Template Login Dialog - SQL Injection URL: https://www.exploit-db.com/exploits/30428
|_ RealWin SCADA Server - DATAC Login Buffer Overflow (Metasploit) URL: https://www.exploit-db.com/exploits/17434
|_ Red Mombin 0.7 - 'process_login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/28722
|_ RedCMS 0.1 - 'login.php' Multiple SQL Injections URL: https://www.exploit-db.com/exploits/27539
|_ RSA ClearTrust 4.6/4.7 - Login Page Cross-Site Scripting URL: https://www.exploit-db.com/exploits/22357
|_ School Equipment Monitoring System 1.0 - 'login' SQL Injection URL: https://www.exploit-db.com/exploits/45709
|_ Scout Portal Toolkit 1.3.1 - 'SPT-UserLogin.php' SQL Injection URL: https://www.exploit-db.com/exploits/26783

|_ Scriptme SmE 1.21 - File Mailer Login SQL Injection URL: https://www.exploit-db.com/exploits/29474
|_ Sell@Site PHP Online Jobs Login - Multiple SQL Injections URL: https://www.exploit-db.com/exploits/34146
|_ SGI IRIX - '/bin/login' Local Buffer Overflow URL: https://www.exploit-db.com/exploits/336
|_ SGI IRIX 6.4 - 'login' Local Privilege Escalation URL: https://www.exploit-db.com/exploits/19310
|_ ShopWeezle 2.0 - 'login.php?itemID' SQL Injection URL: https://www.exploit-db.com/exploits/27612
|_ SIAP CMS - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/29180
|_ Silentum LoginSys 1.0 - Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/32337
|_ Silentum LoginSys 1.0.0 - Insecure Cookie Handling CVE_ID: CVE-2008-6763
|___|_ URL: https://www.exploit-db.com/exploits/7601
|_ SilverStripe CMS - 'MemberLoginForm.php' Information Disclosure URL: https://www.exploit-db.com/exploits/38689
|_ Simple OS CMS 0.1c_beta - 'login.php' SQL Injection URL: https://www.exploit-db.com/exploits/31098
|_ Simple Text-File Login script (SiTeFiLo) 1.0.6 - File Disclosure / Remote File Inclusion CVE_ID: CVE-2008-5762 CVE-2008-5763
|___|_ URL: https://www.exploit-db.com/exploits/7444
|_ SimpleLoginSys 0.5 - Authentication Bypass CVE_ID: CVE-2009-4733
|___|_ URL: https://www.exploit-db.com/exploits/9336
|_ SiteEnable 3.3 - 'login.asp' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/26927
|_ SOA School Management - 'access_login' SQL Injection URL: https://www.exploit-db.com/exploits/44037
|_ Social Oauth Login PHP - Authentication Bypass URL: https://www.exploit-db.com/exploits/44036
|_ Soitec SmartEnergy 1.4 - SCADA Login SQL Injection / Authentication Bypass URL: https://www.exploit-db.com/exploits/35529
|_ Solaris /bin/login (SPARC/x86) - Remote Code Execution URL: https://www.exploit-db.com/exploits/346
|_ Solaris 2.5.1/2.6/7/8 rlogin (SPARC) - '/bin/login' Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/716
|_ Solaris 2.x/7.0/8 - Derived 'login' Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/21179
|_ Sophos UTM 9.410 - 'loginuser' 'confd' Service Privilege Escalation URL: https://www.exploit-db.com/exploits/44246
|_ SPIP 1.8.3 - 'Spip_login.php' Remote File Inclusion URL: https://www.exploit-db.com/exploits/27589
|_ SPIP 2.1 - 'var_login' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/34388
|_ Spooky 2.7 - 'login/register.asp' SQL Injection URL: https://www.exploit-db.com/exploits/29373
|_ SpotLight CRM 1.0 - 'login.asp' SQL Injection CVE_ID: CVE-2006-6543
|___|_ URL: https://www.exploit-db.com/exploits/2907
|_ SSH2 3.0 - Short Password Login URL: https://www.exploit-db.com/exploits/21021
|_ SudBox Boutique 1.2 - 'login.php' Authentication Bypass URL: https://www.exploit-db.com/exploits/22625
|_ Sun Java System Identity Manager 6.0/7.0/7.1 - '/idm/login.jsp' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/31004
|_ SWSoft Plesk 8.2 - 'login.php3' PLESKSESSID Cookie SQL Injection URL: https://www.exploit-db.com/exploits/30577
|_ SWsoft Plesk Reloaded 7.1 - 'Login_name' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/24405
|_ Symantec pcAnywhere 12.5.0 - 'Login' / 'Password' Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/19407
|_ Symantec Sygate Management Server - 'LOGIN' SQL Injection (Metasploit) URL: https://www.exploit-db.com/exploits/1680
|_ Sync Breeze Enterprise 8.9.24 - 'Login' Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/40456
|_ Sync Breeze Enterprise 9.1.16 - 'Login' Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/40831
|_ SynConnect Pms - 'index.php?loginid' SQL Injection CVE_ID: CVE-2013-2690
|___|_ URL: https://www.exploit-db.com/exploits/24898
|_ System V Derived /bin/login - Extraneous Arguments Buffer Overflow (Metasploit) URL: https://www.exploit-db.com/exploits/16928
|_ System V Derived /bin/login - Extraneous Arguments Buffer Overflow (modem based) (Metasploit) URL: https://www.exploit-db.com/exploits/10036
|_ TeamPass 2.1.5 - 'login' HTML Injection URL: https://www.exploit-db.com/exploits/37087
|_ TestLink 1.8.5 - 'order_by_login_dir' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/33534
|_ TGS Content Management 0.3.2r2 - 'login.php' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/32023
|_ The Don 1.0.1 - 'login' SQL Injection URL: https://www.exploit-db.com/exploits/45812
|_ TR News 2.1 - 'login.php' Remote Authentication Bypass URL: https://www.exploit-db.com/exploits/6991
|_ TRUC 0.11 - 'login_reset_password_page.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/33679
|_ TWiki 5.0 - bin/login Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/34843
|_ Tyger Bug Tracking System 1.1.3 - 'login.php?PATH_INFO' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/29704
|_ UBBCentral UBB.Threads 6.2.3/6.5 - 'login.php?Cat' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/24826
|_ UeberProject 1.0 - '/login/secure.php' Remote File Inclusion CVE_ID: CVE-2006-5539
|___|_ URL: https://www.exploit-db.com/exploits/2640
|_ Ultimate PHP Board 2.0b1 - '/chat/login.php' Code Execution URL: https://www.exploit-db.com/exploits/2999

|_ User Login and Management - Multiple Vulnerabilities URL: https://www.exploit-db.com/exploits/42584
|_ VBZoom 1.0/1.11 - 'login.php?UserID' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/26050
|_ VEGO Links Builder 2.0 Login Script - SQL Injection URL: https://www.exploit-db.com/exploits/27001
|_ VideoDB 3.0.3 - 'login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/33619
|_ Virtual Hosting Control System 2.2/2.4 - 'login.php?check_login()' Authentication Bypass URL: https://www.exploit-db.com/exploits/27205
|_ VisionGate 1.6 - 'login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/33463
|_ VisualShapers EZContents 2.0.3 - 'Loginreq2.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/28465
|_ Vizra - 'A_Login.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/27855
|_ VX Search Enterprise 9.0.26 - 'Login' Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/40455
|_ VX Search Enterprise 9.1.12 - 'Login' Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/40830
|_ W-Agora 4.1.6a - 'login.php?loginuser' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/24652
|_ WebChat 0.78 - 'login.php?rid' SQL Injection CVE_ID: CVE-2007-3534
|___|_ URL: https://www.exploit-db.com/exploits/4125
|_ Webeveyn Whomp! Real Estate Manager 2005 - Login SQL Injection URL: https://www.exploit-db.com/exploits/27169
|_ WEBInsta FM 0.1.4 - 'login.php' absolute_path Remote File Inclusion CVE_ID: CVE-2007-2181
|___|_ URL: https://www.exploit-db.com/exploits/3778
|_ WebspotBlogging 3.0 - 'login.php' SQL Injection URL: https://www.exploit-db.com/exploits/27114
|_ Wecodex Hotel CMS 1.0 - 'Admin Login' SQL Injection URL: https://www.exploit-db.com/exploits/44729
|_ Wecodex Restaurant CMS 1.0 - 'Login' SQL Injection URL: https://www.exploit-db.com/exploits/44730
|_ Whale Communications e-Gap Security Appliance 2.5 - Login Page Source Code Disclosure URL: https://www.exploit-db.com/exploits/23545
|_ WinWebMail 3.7.3 - IMAP Login Data Handling Denial of Service URL: https://www.exploit-db.com/exploits/31635
|_ WordPress Core 1.2 - 'wp-login.php' HTTP Response Splitting URL: https://www.exploit-db.com/exploits/24667
|_ WordPress Core 1.2 - 'wp-login.php' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/24641
|_ WordPress Plugin Limit Login Attempts Reloaded 2.7.4 - Login Limit Bypass URL: https://www.exploit-db.com/exploits/46672
|_ WordPress Plugin Login Widget With ShortCode 3.1.1 - Multiple Vulnerabilities CVE_ID: CVE-2014-6312
|___|_ URL: https://www.exploit-db.com/exploits/34762
|_ WordPress Plugin Pie Register - 'wp-login.php' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/38643
|_ WordPress Plugin Simple Gmail Login - Stack Trace Information Disclosure URL: https://www.exploit-db.com/exploits/38111
|_ WordPress Plugin User Login Log 2.2.1 - Cross-Site Scripting URL: https://www.exploit-db.com/exploits/41484
|_ WordPress Plugin zM Ajax Login & Register 1.0.9 - Local File Inclusion CVE_ID: CVE-2015-4153
|___|_ URL: https://www.exploit-db.com/exploits/37200
|_ WWWeb Concepts Events System 1.0 - 'login.asp' SQL Injection URL: https://www.exploit-db.com/exploits/25790
|_ WzdFTPD 0.1 rc5 - Login Remote Denial of Service URL: https://www.exploit-db.com/exploits/23169
|_ XP Book 3.0 - login Admin URL: https://www.exploit-db.com/exploits/10621
|_ XRms 1.99.2 - 'login.php?target' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/32318
|_ XtremeASP PhotoGallery 2.0 - 'Adminlogin.asp' SQL Injection URL: https://www.exploit-db.com/exploits/23547
|_ YaBB 1.40/1.41 - Login Cross-Site Scripting URL: https://www.exploit-db.com/exploits/21950
|_ Yosemite Backup 8.70 - 'DtbClsLogin()' Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/32578
|_ Your Articles Directory - Login Option SQL Injection URL: https://www.exploit-db.com/exploits/33908
|_ Ziteman CMS - Login Page SQL Injection URL: https://www.exploit-db.com/exploits/38786
|_ ZKTeco ZKBioSecurity 3.0 - 'visLogin.jsp' Local Authentication Bypass URL: https://www.exploit-db.com/exploits/40327
|_ Zyxel ZyWall 310 / ZyWall 110 / USG1900 / ATP500 / USG40 - Login Page Cross-Site Scripting CVE_ID: CVE-2019-9955
|___|_ URL: https://www.exploit-db.com/exploits/46706

nfs 2-4 nfs 2-4 : CRITICAL EXPOSURE

|_ Linux Kernel < 2.6.31-rc4 - 'nfs4_proc_lock()' Denial of Service URL: https://www.exploit-db.com/exploits/10202
|_ NfSen < 1.3.7 / AlienVault OSSIM < 5.3.6 - Local Privilege Escalation CVE_ID: CVE-2017-6970
|___|_ URL: https://www.exploit-db.com/exploits/42305

VNC  VNC : CRITICAL EXPOSURE

|_ AMX Corp. VNC ActiveX Control - 'AmxVnc.dll 1.0.13.0' Remote Buffer Overflow CVE_ID: CVE-2007-3536
|___|_ URL: https://www.exploit-db.com/exploits/4123
|_ Chicken of the VNC 2.0 - 'NULL-pointer' Remote Denial of Service CVE_ID: CVE-2007-0756

|___|_ URL: https://www.exploit-db.com/exploits/3257
|_ EchoVNC Viewer - Remote Denial of Service URL: https://www.exploit-db.com/exploits/27292
|_ QEMU 0.9 / KVM 36/79 - VNC Server Remote Denial of Service URL: https://www.exploit-db.com/exploits/32675
|_ RealVNC - Authentication Bypass (Metasploit) URL: https://www.exploit-db.com/exploits/17719
|_ RealVNC 3.3.7 - Client Buffer Overflow (Metasploit) URL: https://www.exploit-db.com/exploits/16489
|_ RealVNC 4.1.0 < 4.1.1 - VNC Null Authentication Bypass (Metasploit) URL: https://www.exploit-db.com/exploits/1794
|_ RealVNC 4.1.0 < 4.1.1 - VNC Null Authentication Bypass URL: https://www.exploit-db.com/exploits/1791
|_ RealVNC 4.1.0 < 4.1.1 - VNC Null Authentication Scanner URL: https://www.exploit-db.com/exploits/1799
|_ RealVNC 4.1.0/4.1.1 - Authentication Bypass URL: https://www.exploit-db.com/exploits/36932
|_ RealVNC 4.1.2 - 'vncviewer.exe' RFB Protocol Remote Code Execution (PoC) URL: https://www.exploit-db.com/exploits/7943
|_ RealVNC 4.1.3 - 'ClientCutText' Message Remote Denial of Service URL: https://www.exploit-db.com/exploits/33924
|_ RealVNC Server 4.0 - Remote Denial of Service URL: https://www.exploit-db.com/exploits/24412
|_ RealVNC Windows Client 4.1.2 - Remote Denial of Service Crash (PoC) CVE_ID: CVE-2008-3493
|___|_ URL: https://www.exploit-db.com/exploits/6181
|_ SmartCode ServerX VNC Server ActiveX 1.1.5.0 - 'scvncsrvx.dll' Denial of Service URL: https://www.exploit-db.com/exploits/14634
|_ SmartCode VNC Manager 3.6 - 'scvncctrl.dll' Denial of Service CVE_ID: CVE-2007-2526
|___|_ URL: https://www.exploit-db.com/exploits/3873
|_ Sun SunPCi II VNC Software 2.3 - Password Disclosure URL: https://www.exploit-db.com/exploits/21592
|_ ThinVNC 1.0b1 - Authentication Bypass URL: https://www.exploit-db.com/exploits/47519
|_ TightVNC - Authentication Failure Integer Overflow (PoC) CVE_ID: CVE-2009-0388
|___|_ URL: https://www.exploit-db.com/exploits/8024
|_ Ultr@VNC 1.0.1 - 'client Log::ReallyPrint' Buffer Overflow (PoC) CVE_ID: CVE-2006-1652
|___|_ URL: https://www.exploit-db.com/exploits/1643
|_ Ultr@VNC 1.0.1 - 'client Log::ReallyPrint' Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/1664
|_ Ultr@VNC 1.0.1 - VNCLog::ReallyPrint Remote Buffer Overflow (PoC) CVE_ID: CVE-2006-1652
|___|_ URL: https://www.exploit-db.com/exploits/1642
|_ UltraVNC 1.0.1 - Client Buffer Overflow (Metasploit) URL: https://www.exploit-db.com/exploits/16490
|_ UltraVNC 1.0.1 - Multiple Remote Error Logging Buffer Overflow Vulnerabilities (1) URL: https://www.exploit-db.com/exploits/27568
|_ UltraVNC 1.0.1 - Multiple Remote Error Logging Buffer Overflow Vulnerabilities (2) URL: https://www.exploit-db.com/exploits/27569
|_ UltraVNC 1.0.2 Client - 'vncviewer.exe' Remote Buffer Overflow (Metasploit) CVE_ID: CVE-2008-0610
|___|_ URL: https://www.exploit-db.com/exploits/18666
|_ UltraVNC 1.0.8.2 - DLL Loading Arbitrary Code Execution URL: https://www.exploit-db.com/exploits/34542
|_ UltraVNC Launcher 1.2.2.4 - 'Path' Denial of Service (PoC) URL: https://www.exploit-db.com/exploits/46703
|_ UltraVNC Launcher 1.2.4.0 - 'Password' Denial of Service (PoC) URL: https://www.exploit-db.com/exploits/48290
|_ UltraVNC Launcher 1.2.4.0 - 'RepeaterHost' Denial of Service (PoC) URL: https://www.exploit-db.com/exploits/48288
|_ UltraVNC Viewer 1.2.2.4 - 'VNC Server' Denial of Service (PoC) URL: https://www.exploit-db.com/exploits/46702
|_ UltraVNC Viewer 1.2.4.0 - 'VNCServer' Denial of Service (PoC) URL: https://www.exploit-db.com/exploits/48291
|_ UltraVNC/TightVNC (Multiple VNC Clients) - Multiple Integer Overflows (PoC) CVE_ID: CVE-2009-0388
|___|_ URL: https://www.exploit-db.com/exploits/7990
|_ Vino VNC Server 3.7.3 - Persistent Denial of Service URL: https://www.exploit-db.com/exploits/28338
|_ VNC Keyboard - Remote Code Execution (Metasploit) URL: https://www.exploit-db.com/exploits/37598
|_ WinVNC Web Server 3.3.3r7 - GET Overflow (Metasploit) URL: https://www.exploit-db.com/exploits/16491

X11  X11 : CRITICAL EXPOSURE

|_ ASUS DSL-X11 ADSL Router - DNS Change URL: https://www.exploit-db.com/exploits/40373
|_ BSD/OS 2.1 / DG/UX 7.0 / Debian 1.3 / HP-UX 10.34 / IBM AIX 4.2 / SGI IRIX 6.4 / Solaris 2.5.1 - '/usr/bin/X11/xlock' Local Privilege Escalation (2) URL: http
|_ Eterm 0.8.10 / rxvt 2.6.1 / PuTTY 0.48 / X11R6 3.3.3/4.0 - Denial of Service URL: https://www.exploit-db.com/exploits/19984
|_ Gnome 1.0/1.1 / Group X 11.0 / XFree86 X11R6 3.3.x/4.0 - Denial of Service URL: https://www.exploit-db.com/exploits/20023
|_ SCO Open Server 5.0.5 / IRIX 6.2 ibX11/X11 Toolkit/Athena Widget Library - Local Buffer Overflow URL: https://www.exploit-db.com/exploits/19684
|_ Slackware Linux 3.1 - '/usr/X11/bin/SuperProbe' Local Buffer Overflow URL: https://www.exploit-db.com/exploits/19283
|_ Solaris 5.5.1 X11R6.3 - xterm '-xrm' Local Privilege Escalation URL: https://www.exploit-db.com/exploits/338
|_ Tor (Linux) - X11 Linux Sandbox Breakout URL: https://www.exploit-db.com/exploits/42626
|_ X 11.0/3.3.3/3.3.4/3.3.5/3.3.6/4.0 - libX11 '_XAsyncReply()' Stack Corruption URL: https://www.exploit-db.com/exploits/20045

|_ X.Org X11 (X11R6.9.0/X11R7.0) - Local Privilege Escalation URL: https://www.exploit-db.com/exploits/1596

|_ X.Org xorg-x11-xfs 1.0.2-3.1 - Local Race Condition CVE_ID: CVE-2007-3103

|___|_ URL: https://www.exploit-db.com/exploits/5167

|_ X11R6 3.3.3 - Symlink URL: https://www.exploit-db.com/exploits/19257

|_ X11R6 < 6.4 XKEYBOARD (sco x86) - Local Buffer Overflow URL: https://www.exploit-db.com/exploits/2332

|_ X11R6 < 6.4 XKEYBOARD (solaris x86) - Local Buffer Overflow URL: https://www.exploit-db.com/exploits/2331

|_ X11R6 < 6.4 XKEYBOARD (Solaris/SPARC) - Local Buffer Overflow (1) URL: https://www.exploit-db.com/exploits/2330

|_ X11R6 < 6.4 XKEYBOARD (Solaris/SPARC) - Local Buffer Overflow (2) URL: https://www.exploit-db.com/exploits/2360

|_ XFree86 X11R6 3.3 XDM - Session Cookie Guessing URL: https://www.exploit-db.com/exploits/20993

|_ XFree86 X11R6 3.3.2 XMan - ManPath Environment Variable Buffer Overflow URL: https://www.exploit-db.com/exploits/21010

|_ XFree86 X11R6 3.3.5/3.3.6/4.0 Xserver - Denial of Service URL: https://www.exploit-db.com/exploits/19950

|_ XFree86 X11R6 3.3.x - Font Server Remote Buffer Overrun URL: https://www.exploit-db.com/exploits/22036

|_ Xorg X11 Server (AIX) - Local Privilege Escalation CVE_ID: CVE-2018-14665

|___|_ URL: https://www.exploit-db.com/exploits/45938

|_ Xorg X11 Server - Local Privilege Escalation (Metasploit) URL: https://www.exploit-db.com/exploits/47701

|_ Xorg X11 Server - SUID privilege escalation (Metasploit) CVE_ID: CVE-2018-14665

|___|_ URL: https://www.exploit-db.com/exploits/45908

|_ xorg-x11-server 1.20.3 - Privilege Escalation CVE_ID: CVE-2018-14665

|___|_ URL: https://www.exploit-db.com/exploits/45742

|_ xorg-x11-server < 1.20.1 - Local Privilege Escalation CVE_ID: CVE-2018-14665

|___|_ URL: https://www.exploit-db.com/exploits/45832

|_ xorg-x11-server < 1.20.3 (Solaris 11) - 'inittab Local Privilege Escalation CVE_ID: CVE-2018-14665

|___|_ URL: https://www.exploit-db.com/exploits/46142

|_ xorg-x11-server < 1.20.3 - 'modulepath' Local Privilege Escalation CVE_ID: CVE-2018-14665

|___|_ URL: https://www.exploit-db.com/exploits/45922

|_ xorg-x11-server < 1.20.3 - Local Privilege Escalation CVE_ID: CVE-2018-14665

|___|_ URL: https://www.exploit-db.com/exploits/45697

UnrealIRCd UnrealIRCd : CRITICAL EXPOSURE

|_ UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit) URL: https://www.exploit-db.com/exploits/16922

|_ UnrealIRCd 3.2.8.1 - Local Configuration Stack Overflow URL: https://www.exploit-db.com/exploits/18011

|_ UnrealIRCd 3.2.8.1 - Remote Downloader/Execute CVE_ID: CVE-2010-2075

|___|_ URL: https://www.exploit-db.com/exploits/13853

|_ UnrealIRCd 3.x - Remote Denial of Service URL: https://www.exploit-db.com/exploits/27407

UnrealIRCd UnrealIRCd : CRITICAL EXPOSURE

|_ UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit) URL: https://www.exploit-db.com/exploits/16922

|_ UnrealIRCd 3.2.8.1 - Local Configuration Stack Overflow URL: https://www.exploit-db.com/exploits/18011

|_ UnrealIRCd 3.2.8.1 - Remote Downloader/Execute CVE_ID: CVE-2010-2075

|___|_ URL: https://www.exploit-db.com/exploits/13853

|_ UnrealIRCd 3.x - Remote Denial of Service URL: https://www.exploit-db.com/exploits/27407

status 1 status 1 : CRITICAL EXPOSURE

|_ Accellion FTA - getStatus verify_oauth_token Command Execution (Metasploit) CVE_ID: CVE-2015-2857

|___|_ URL: https://www.exploit-db.com/exploits/37597

|_ Apache 2.4.7 mod_status - Scoreboard Handling Race Condition CVE_ID: CVE-2014-0226

|___|_ URL: https://www.exploit-db.com/exploits/34133

|_ Apache mod_perl - 'Apache::Status' / 'Apache2::Status' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/9993

|_ Apple Safari 1.2 Web Browser - TABLE Status Bar URI Obfuscation URL: https://www.exploit-db.com/exploits/24716

|_ Apple Safari Web Browser 1.x - HTML Form Status Bar Misrepresentation URL: https://www.exploit-db.com/exploits/24843

|_ Centreo 19.10.8 - 'DisplayServiceStatus' Remote Code Execution URL: https://www.exploit-db.com/exploits/48256

|_ Dell SonicWALL Scrutinizer 9.0.1 - 'statusFilter.php?q' SQL Injection CVE_ID: CVE-2012-2962

|___|_ URL: https://www.exploit-db.com/exploits/20033

|_ Dicshunary 0.1a - 'check_status.php' Remote File Inclusion URL: https://www.exploit-db.com/exploits/2808

|_ Google Chrome 3.0195.38 - Status Bar Obfuscation URL: https://www.exploit-db.com/exploits/10879

|_ HP Insight Diagnostics Online Edition 8.4 - 'idstatusframe.php' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/34544

|_ HP Network Node Manager (NMM) i 9.10 - 'nnm/protected/statuspoll.jsp?nodename' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/36356

|_ Huawei eSpace 1.1.11.103 - 'ContactsCtrl.dll' / 'eSpaceStatusCtrl.dll' ActiveX Heap Overflow