CVE LIST of 192:168:0:102

https https : CRITICAL EXPOSURE

|_ Apache Tomcat 6.0.16 - 'HttpServletResponse.sendError()' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/32138

|_ BugHunter HTTP Server 1.6.2 - 'httpsv.exe' GET 404 Remote Denial of Service CVE_ID: CVE-2007-3340

|___|_ URL: https://www.exploit-db.com/exploits/9478

|_ Cybrotech CyBroHttpServer 1.0.3 - Cross-Site Scripting CVE_ID: CVE-2018-16134

|___|_ URL: https://www.exploit-db.com/exploits/45309

|_ Cybrotech CyBroHttpServer 1.0.3 - Directory Traversal CVE_ID: CVE-2018-16133

|___|_ URL: https://www.exploit-db.com/exploits/45303

|_ GeoHttpServer - Remote Denial of Service URL: https://www.exploit-db.com/exploits/12531

|_ GeoVision (GeoHttpServer) Webcams - Remote File Disclosure URL: https://www.exploit-db.com/exploits/37258

|_ HttpServer 1.0 - Directory Traversal URL: https://www.exploit-db.com/exploits/41638

|_ Mabry Software HTTPServer/X 1.0 0.047 - File Disclosure URL: https://www.exploit-db.com/exploits/22892

|_ MailEnable Enterprise & Professional - https Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/952

|_ MiniHTTPServer Web Forum & File Sharing Server 4.0 - Add User CVE_ID: CVE-2006-5597

|___|_ URL: https://www.exploit-db.com/exploits/2651

|_ MiniHTTPServer Web Forums Server 1.x/2.0 - Directory Traversal URL: https://www.exploit-db.com/exploits/22795

|_ Novell eDirectory - HTTPSTK Login Stack Overflow URL: https://www.exploit-db.com/exploits/10163

|_ Novell eDirectory 8.x - iMonitor HTTPSTK Buffer Overflow (1) URL: https://www.exploit-db.com/exploits/28835

|_ Novell eDirectory 8.x - iMonitor HTTPSTK Buffer Overflow (2) URL: https://www.exploit-db.com/exploits/28836

|_ Novell eDirectory 8.x - iMonitor HTTPSTK Buffer Overflow (3) URL: https://www.exploit-db.com/exploits/28837

|_ Novell Netware 6.0 / eDirectory 8.7 - HTTPSTK.NLM Remote Abend URL: https://www.exploit-db.com/exploits/22749

|_ Python CGIHTTPServer - Encoded Directory Traversal URL: https://www.exploit-db.com/exploits/33894

|_ Sunway Force Control SCADA 6.1 SP3 - 'httpsrv.exe' Remote Overflow URL: https://www.exploit-db.com/exploits/17721

MySQL MySQL : CRITICAL EXPOSURE

|_ Active Calendar 1.2 - '/data/mysqlevents.php?css' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/29653

|_ Advanced Poll 2.0 - 'mysql_host' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/33972

|_ Agora 1.4 RC1 - 'MysqlfinderAdmin.php' Remote File Inclusion CVE_ID: CVE-2006-7194

|___|_ URL: https://www.exploit-db.com/exploits/2726

|_ Asterisk 'asterisk-addons' 1.2.7/1.4.3 - CDR_ADDON_MYSQL Module SQL Injection URL: https://www.exploit-db.com/exploits/30677

|_ Banex PHP MySQL Banner Exchange 2.21 - 'admin.php' Multiple SQL Injections URL: https://www.exploit-db.com/exploits/28307

|_ Banex PHP MySQL Banner Exchange 2.21 - 'members.php?cfg_root' Remote File Inclusion URL: https://www.exploit-db.com/exploits/28308

|_ Banex PHP MySQL Banner Exchange 2.21 - 'signup.php?site_name' SQL Injection URL: https://www.exploit-db.com/exploits/28306

|_ Cholod MySQL Based Message Board - 'Mb.cgi' SQL Injection URL: https://www.exploit-db.com/exploits/27464

|_ Cisco Firepower Threat Management Console 6.0.1 - Hard-Coded MySQL Credentials CVE_ID: CVE-2016-6434

|___|_ URL: https://www.exploit-db.com/exploits/40465

|_ CMSQLite / CMySQLite 1.3 - Cross-Site Request Forgery URL: https://www.exploit-db.com/exploits/14096

|_ CMSQLite 1.2 / CMySQLite 1.3.1 - Remote Code Execution URL: https://www.exploit-db.com/exploits/14654

|_ cPanel 10.8.x - 'cpwrap' via MySQLAdmin Privilege Escalation (PHP) URL: https://www.exploit-db.com/exploits/2554

|_ cPanel 10.8.x - cpwrap via MySQLAdmin Privilege Escalation URL: https://www.exploit-db.com/exploits/2466

|_ cPanel 11 - PassWDMySQL Cross-Site Scripting URL: https://www.exploit-db.com/exploits/29572

|_ CSP MySQL User Manager 2.3.1 - Authentication Bypass CVE_ID: CVE-2018-10757

|___|_ URL: https://www.exploit-db.com/exploits/44589

|_ Froxlor Server Management Panel 0.9.33.1 - MySQL Login Information Disclosure URL: https://www.exploit-db.com/exploits/37725

|_ GEDCOM_TO_MYSQL - '/PHP/index.php?nom_branche' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/31731

|_ GEDCOM_TO_MYSQL - '/PHP/info.php' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/31732

|_ GEDCOM_TO_MYSQL - '/PHP/prenom.php' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/31730

|_ JSPMySQL Administrador - Multiple Vulnerabilities URL: https://www.exploit-db.com/exploits/38098

|_ KBVault MySQL 0.16a - Arbitrary File Upload CVE_ID: CVE-2017-9602

|___|_ URL: https://www.exploit-db.com/exploits/42184

|_ Keld PHP-MySQL News Script 0.7.1 - 'login.php' SQL Injection URL: https://www.exploit-db.com/exploits/32143

|_ Linkster - PHP/MySQL SQL Injection URL: https://www.exploit-db.com/exploits/10450

|_ miniMySQLAdmin 1.1.3 - Cross-Site Request Forgery (SQL Execution) URL: https://www.exploit-db.com/exploits/39912

|_ MyBlog: PHP and MySQL Blog/CMS software - Remote File Inclusion CVE_ID: CVE-2007-1968

|___|_ URL: https://www.exploit-db.com/exploits/3685

|_ MyBlog: PHP and MySQL Blog/CMS software - SQL Injection / Cross-Site Scripting CVE_ID: CVE-2008-2962 CVE-2008-2963 CVE-2008-6193

|___|_ URL: https://www.exploit-db.com/exploits/5913

|_ MySQL (Linux) - Database Privilege Escalation URL: https://www.exploit-db.com/exploits/23077

|_ MySQL (Linux) - Heap Overrun (PoC) CVE_ID: CVE-2012-5612

|___|_ URL: https://www.exploit-db.com/exploits/23076

|_ MySQL (Linux) - Stack Buffer Overrun (PoC) CVE_ID: CVE-2012-5611

|___|_ URL: https://www.exploit-db.com/exploits/23075

|_ MySQL - 'Stuxnet Technique' Windows Remote System URL: https://www.exploit-db.com/exploits/23083

|_ MySQL - Authentication Bypass CVE_ID: CVE-2012-2122

|___|_ URL: https://www.exploit-db.com/exploits/19092

|_ MySQL - Denial of Service (PoC) URL: https://www.exploit-db.com/exploits/23078

|_ MySQL - Remote User Enumeration URL: https://www.exploit-db.com/exploits/23081

|_ MySQL - yaSSL CertDecoder::GetName Buffer Overflow (Metasploit) URL: https://www.exploit-db.com/exploits/16850

|_ MySQL / MariaDB - Geometry Query Denial of Service URL: https://www.exploit-db.com/exploits/38392

|_ MySQL / MariaDB / PerconaDB 5.5.51/5.6.32/5.7.14 - Code Execution / Privilege Escalation CVE_ID: CVE-2016-6662

|___|_ URL: https://www.exploit-db.com/exploits/40360

|_ MySQL / MariaDB / PerconaDB 5.5.x/5.6.x/5.7.x - 'mysql' System User Privilege Escalation / Race Condition CVE_ID: CVE-2016-6663

|___|_ URL: https://www.exploit-db.com/exploits/40678

|_ MySQL / MariaDB / PerconaDB 5.5.x/5.6.x/5.7.x - 'root' System User Privilege Escalation CVE_ID: CVE-2016-6664

|___|_ URL: https://www.exploit-db.com/exploits/40679

|_ MySQL 3.20.32 a/3.23.34 - Root Operation Symbolic Link File Overwriting URL: https://www.exploit-db.com/exploits/20718

|_ MySQL 3.20.32/3.22.x/3.23.x - Null Root Password Weak Default Configuration (1) URL: https://www.exploit-db.com/exploits/21725

|_ MySQL 3.20.32/3.22.x/3.23.x - Null Root Password Weak Default Configuration (2) URL: https://www.exploit-db.com/exploits/21726

|_ MySQL 3.22.27/3.22.29/3.23.8 - GRANT Global Password Changing URL: https://www.exploit-db.com/exploits/19721

|_ Mysql 3.22.x/3.23.x - Local Buffer Overflow URL: https://www.exploit-db.com/exploits/20581

|_ MySQL 3.23.x - 'mysqld' Local Privilege Escalation URL: https://www.exploit-db.com/exploits/22340

|_ MySQL 3.23.x/4.0.x - 'COM_CHANGE_USER' Password Length Account URL: https://www.exploit-db.com/exploits/22084

|_ MySQL 3.23.x/4.0.x - COM_CHANGE_USER Password Memory Corruption URL: https://www.exploit-db.com/exploits/22085

|_ MySQL 3.23.x/4.0.x - Password Handler Buffer Overflow URL: https://www.exploit-db.com/exploits/23138

|_ MySQL 3.23.x/4.0.x - Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/98

|_ MySQL 3.x/4.0.x - Weak Password Encryption URL: https://www.exploit-db.com/exploits/22565

|_ MySQL 3.x/4.x - ALTER TABLE/RENAME Forces Old Permission Checks URL: https://www.exploit-db.com/exploits/24669

|_ MySQL 4.0.17 (Linux) - User-Defined Function (UDF) Dynamic Library (1) URL: https://www.exploit-db.com/exploits/1181

|_ MySQL 4.1.18/5.0.20 - Local/Remote Information Leakage URL: https://www.exploit-db.com/exploits/1742

|_ MySQL 4.1/5.0 - Authentication Bypass URL: https://www.exploit-db.com/exploits/24250

|_ MySQL 4.1/5.0 - Zero-Length Password Authentication Bypass URL: https://www.exploit-db.com/exploits/311

|_ MySQL 4.x - CREATE FUNCTION Arbitrary libc Code Execution URL: https://www.exploit-db.com/exploits/25209

|_ MySQL 4.x - CREATE FUNCTION mysql.func Table Arbitrary Library Injection URL: https://www.exploit-db.com/exploits/25210

|_ MySQL 4.x - CREATE Temporary TABLE Symlink Privilege Escalation URL: https://www.exploit-db.com/exploits/25211

|_ MySQL 4.x/5.0 (Linux) - User-Defined Function (UDF) Dynamic Library (2) URL: https://www.exploit-db.com/exploits/1518

|_ MySQL 4.x/5.0 (Windows) - User-Defined Function Command Execution URL: https://www.exploit-db.com/exploits/3274

|_ MySQL 4.x/5.x - Server Date_Format Denial of Service URL: https://www.exploit-db.com/exploits/28234

|_ MySQL 4/5 - SUID Routine Miscalculation Arbitrary DML Statement Execution URL: https://www.exploit-db.com/exploits/28398

|_ MySQL 4/5/6 - UDF for Command Execution URL: https://www.exploit-db.com/exploits/7856

|_ MySQL 5 - Command Line Client HTML Special Characters HTML Injection URL: https://www.exploit-db.com/exploits/32445

|_ MySQL 5.0.18 - Query Logging Bypass URL: https://www.exploit-db.com/exploits/27326

|_ MySQL 5.0.20 - COM_TABLE_DUMP Memory Leak/Remote Buffer Overflow URL: https://www.exploit-db.com/exploits/1741

|_ MySQL 5.0.45 - 'Alter' Denial of Service URL: https://www.exploit-db.com/exploits/4615

|_ MySQL 5.0.45 - (Authenticated) COM_CREATE_DB Format String (PoC) URL: https://www.exploit-db.com/exploits/9085

|_ MySQL 5.0.75 - 'sql_parse.cc' Multiple Format String Vulnerabilities URL: https://www.exploit-db.com/exploits/33077

|_ MySQL 5.0.x - IF Query Handling Remote Denial of Service CVE_ID: CVE-2007-2583

|___|_ URL: https://www.exploit-db.com/exploits/30020

|_ MySQL 5.0.x - Single Row SubSelect Remote Denial of Service URL: https://www.exploit-db.com/exploits/29724

|_ MySQL 5.1.13 - INFORMATION_SCHEMA Remote Denial of Service URL: https://www.exploit-db.com/exploits/31444

|_ MySQL 5.1.23 - Server InnoDB CONVERT_SEARCH_MODE_TO_INNOBASE Function Denial of Service URL: https://www.exploit-db.com/exploits/30744

|_ MySQL 5.1.48 - 'EXPLAIN' Denial of Service URL: https://www.exploit-db.com/exploits/34506

|_ MySQL 5.1.48 - 'Temporary InnoDB' Tables Denial of Service URL: https://www.exploit-db.com/exploits/34505

|_ MySQL 5.1/5.5 (Windows) - 'MySQLJackpot' Remote Command Execution URL: https://www.exploit-db.com/exploits/23073

|_ MySQL 5.5.45 (x64) - Local Credentials Disclosure URL: https://www.exploit-db.com/exploits/40337

|_ MySQL 5.5.45 - procedure analyse Function Denial of Service CVE_ID: CVE-2015-4870

|___|_ URL: https://www.exploit-db.com/exploits/39867

|_ MySQL 5.5.8 - Remote Denial of Service CVE_ID: CVE-2011-5049

|___|_ URL: https://www.exploit-db.com/exploits/18269

|_ MySQL 6.0 yaSSL 1.7.5 - Hello Message Buffer Overflow (Metasploit) URL: https://www.exploit-db.com/exploits/9953

|_ MySQL 6.0.4 - Empty Binary String Literal Remote Denial of Service URL: https://www.exploit-db.com/exploits/32348

|_ MySQL 6.0.9 - 'GeomFromWKB()' Function First Argument Geometry Value Handling Denial of Service URL: https://www.exploit-db.com/exploits/33398

|_ MySQL 6.0.9 - SELECT Statement WHERE Clause Sub-query Denial of Service URL: https://www.exploit-db.com/exploits/33397

|_ MySQL 6.0.9 - XPath Expression Remote Denial of Service URL: https://www.exploit-db.com/exploits/32838

|_ MySQL < 5.6.35 / < 5.7.17 - Integer Overflow CVE_ID: CVE-2017-3599

|___|_ URL: https://www.exploit-db.com/exploits/41954

|_ MySQL AB Eventum 1.x - 'get_jsrs_data.php?F' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/26058

|_ MySQL AB Eventum 1.x - 'list.php?release' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/26057

|_ MySQL AB Eventum 1.x - 'view.php?id' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/26056

|_ MySQL AB ODBC Driver 3.51 - Plain Text Password URL: https://www.exploit-db.com/exploits/22946

|_ MySQL Blob Uploader 1.7 - 'download.php' SQL Injection / Cross-Site Scripting URL: https://www.exploit-db.com/exploits/44709

|_ MySQL Blob Uploader 1.7 - 'home-file-edit.php' SQL Injection / Cross-Site Scripting URL: https://www.exploit-db.com/exploits/44710

|_ MySQL Blob Uploader 1.7 - 'home-filet-edit.php' SQL Injection / Cross-Site Scripting URL: https://www.exploit-db.com/exploits/44711

|_ MySQL Blob Uploader 1.7 - 'home-filet-edit.php' SQL Injection URL: https://www.exploit-db.com/exploits/44712

|_ MySQL Commander 2.7 - 'home' Remote File Inclusion CVE_ID: CVE-2007-1439

|___|_ URL: https://www.exploit-db.com/exploits/3468

|_ MySQL Edit Table 1.0 - 'id' SQL Injection URL: https://www.exploit-db.com/exploits/45639

|_ MySQL Eventum 1.5.5 - 'login.php' SQL Injection URL: https://www.exploit-db.com/exploits/1134

|_ MySQL File Uploader 1.0 - 'id' SQL Injection URL: https://www.exploit-db.com/exploits/41267

|_ MySQL MaxDB 7.5 - WAHTTP Server Remote Denial of Service URL: https://www.exploit-db.com/exploits/24805

|_ MySQL MaxDB Webtool 7.5.00.23 - Remote Stack Overflow URL: https://www.exploit-db.com/exploits/960

|_ MySQL Quick Admin 1.5.5 - 'cookie' Local File Inclusion CVE_ID: CVE-2008-4455

|___|_ URL: https://www.exploit-db.com/exploits/6641

|_ MySQL Quick Admin 1.5.5 - Local File Inclusion URL: https://www.exploit-db.com/exploits/7020

|_ MySQL Server 4/5 - Str_To_Date Remote Denial of Service URL: https://www.exploit-db.com/exploits/28026

|_ MySQL Smart Reports 1.0 - 'id' SQL Injection / Cross-Site Scripting URL: https://www.exploit-db.com/exploits/44708

|_ MySQL Squid Access Report 2.1.4 - HTML Injection URL: https://www.exploit-db.com/exploits/20055

|_ MySQL Squid Access Report 2.1.4 - SQL Injection / Cross-Site Scripting URL: https://www.exploit-db.com/exploits/44483

|_ MySQL User-Defined (Linux) (x86) - 'sys_exec' Local Privilege Escalation URL: https://www.exploit-db.com/exploits/46249

|_ MySQL yaSSL (Linux) - SSL Hello Message Buffer Overflow (Metasploit) URL: https://www.exploit-db.com/exploits/16849

|_ MySQL yaSSL (Windows) - SSL Hello Message Buffer Overflow (Metasploit) URL: https://www.exploit-db.com/exploits/16701

|_ MySQLDriverCS 4.0.1 - SQL Injection URL: https://www.exploit-db.com/exploits/35892

|_ MySQLDumper 1.21 - 'sql.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/28783

|_ MySQLDumper 1.24.4 - 'filemanagement.php?f' Traversal Arbitrary File Access URL: https://www.exploit-db.com/exploits/37129

|_ MySQLDumper 1.24.4 - 'index.php?page' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/37133

|_ MySQLDumper 1.24.4 - 'install.php' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/37127

|_ MySQLDumper 1.24.4 - 'install.php?language' Traversal Arbitrary File Access URL: https://www.exploit-db.com/exploits/37126

|_ MySQLDumper 1.24.4 - 'main.php' Multiple Cross-Site Request Forgery Vulnerabilities URL: https://www.exploit-db.com/exploits/37131

|_ MySQLDumper 1.24.4 - 'menu.php' PHP Remote Code Execution URL: https://www.exploit-db.com/exploits/37134

|_ MySQLDumper 1.24.4 - 'restore.php?Filename' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/37125

|_ MySQLDumper 1.24.4 - 'sql.php' Multiple Cross-Site Scripting Vulnerabilities URL: https://www.exploit-db.com/exploits/37128

|_ MySQLDumper 1.24.4 - Multiple Script Direct Request Information Disclosures URL: https://www.exploit-db.com/exploits/37130

|_ MySQLNewsEngine - 'Affichearticles.php3' Remote File Inclusion URL: https://www.exploit-db.com/exploits/29569

|_ Online Doctor Appointment Booking System PHP and Mysql 1.0 - 'q' SQL Injection URL: https://www.exploit-db.com/exploits/49059

|_ Oracle MySQL (Windows) - FILE Privilege Abuse (Metasploit) URL: https://www.exploit-db.com/exploits/35777

|_ Oracle MySQL (Windows) - MOF Execution (Metasploit) URL: https://www.exploit-db.com/exploits/23179

|_ Oracle MySQL - 'ALTER DATABASE' Remote Denial of Service URL: https://www.exploit-db.com/exploits/14537

|_ Oracle MySQL / MariaDB - Insecure Salt Generation Security Bypass URL: https://www.exploit-db.com/exploits/38109

|_ Oracle MySQL 5.1.48 - 'HANDLER' Interface Denial of Service URL: https://www.exploit-db.com/exploits/34520

|_ Oracle MySQL < 5.1.49 - 'DDL' Statements Denial of Service URL: https://www.exploit-db.com/exploits/34522

|_ Oracle MySQL < 5.1.49 - 'WITH ROLLUP' Denial of Service URL: https://www.exploit-db.com/exploits/15467

|_ Oracle MySQL < 5.1.49 - Malformed 'BINLOG' Arguments Denial of Service URL: https://www.exploit-db.com/exploits/34521

|_ Oracle MySQL < 5.1.50 - Privilege Escalation URL: https://www.exploit-db.com/exploits/34796

|_ Oracle MySQL for Microsoft Windows - Payload Execution (Metasploit) URL: https://www.exploit-db.com/exploits/16957

|_ OraclMySQL 5.1.48 - 'LOAD DATA INFILE' Denial of Service URL: https://www.exploit-db.com/exploits/34510

|_ paBugs 2.0 Beta 3 - 'class.mysql.php' Remote File Inclusion CVE_ID: CVE-2006-5079

|___|_ URL: https://www.exploit-db.com/exploits/2437

|_ PHP 4.4.0 - 'mysql_connect function' Local Buffer Overflow URL: https://www.exploit-db.com/exploits/1406

|_ PHP 4.4.7/5.2.3 - MySQL/MySQLi 'Safe_Mode' Bypass CVE_ID: CVE-2007-3997

|___|_ URL: https://www.exploit-db.com/exploits/4392

|_ PHP 4.x/5.x MySQL Library - 'Safe_mode' Filesystem Circumvention (1) URL: https://www.exploit-db.com/exploits/21264

|_ PHP 4.x/5.x MySQL Library - 'Safe_mode' Filesystem Circumvention (2) URL: https://www.exploit-db.com/exploits/21265

|_ PHP 4.x/5.x MySQL Library - 'Safe_mode' Filesystem Circumvention (3) URL: https://www.exploit-db.com/exploits/21266

|_ PHP-MySQL-Quiz - SQL Injection URL: https://www.exploit-db.com/exploits/10876

|_ PHP-Nuke 8.0 Final - 'INSERT' Blind SQL Injection (MySQL) URL: https://www.exploit-db.com/exploits/3344

|_ PHP-Nuke Module Eve-Nuke 0.1 - 'mysql.php' Remote File Inclusion CVE_ID: CVE-2007-1778

|___|_ URL: https://www.exploit-db.com/exploits/3591

|_ PHP/Mysql Site Builder 0.0.2 - 'htm2PHP.php' File Disclosure URL: https://www.exploit-db.com/exploits/2969

|_ PHPwebnews 0.2 MySQL Edition - 'det' SQL Injection CVE_ID: CVE-2008-6812

|___|_ URL: https://www.exploit-db.com/exploits/5999

|_ PHPwebnews 0.2 MySQL Edition - 'id_kat' SQL Injection CVE_ID: CVE-2008-6813

|___|_ URL: https://www.exploit-db.com/exploits/5998

|_ PHPwebnews 0.2 MySQL Edition - 'SQL' Insecure Cookie Handling URL: https://www.exploit-db.com/exploits/6136

|_ Plixer Scrutinizer NetFlow and sFlow Analyzer 9 - Default MySQL Credential (Metasploit) URL: https://www.exploit-db.com/exploits/20355

|_ Point of Sales (POS) in VB.Net MySQL Database 1.0 - SQL Injection CVE_ID: CVE-2018-18805

|___|_ URL: https://www.exploit-db.com/exploits/45721

|_ ProFTPd - 'mod_mysql' Authentication Bypass CVE_ID: CVE-2009-0542

|___|_ URL: https://www.exploit-db.com/exploits/8037

|_ PromoteWeb MySQL - 'id' SQL Injection CVE_ID: CVE-2008-5069

|___|_ URL: https://www.exploit-db.com/exploits/6577

|_ Robert Zimmerman PHP / MySQL Scripts - Authentication Bypass URL: https://www.exploit-db.com/exploits/10260

|_ Symantec Web Gateway 5.0.3.18 - Blind SQL Injection Backdoor via MySQL Triggers URL: https://www.exploit-db.com/exploits/20044

|_ waldronmatt FullCalendar-BS4-PHP-MySQL-JSON 1.21 - 'description' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/47548

|_ waldronmatt FullCalendar-BS4-PHP-MySQL-JSON 1.21 - 'start' SQL Injection URL: https://www.exploit-db.com/exploits/47546

|_ Woltlab Burning Board 2.3.4 - 'Class_DB_MySQL.php' Cross-Site Scripting URL: https://www.exploit-db.com/exploits/27444

|_ WordPress Plugin Google Document Embedder 2.5.16 - 'mysql_real_escpae_string' Bypass SQL Injection URL: https://www.exploit-db.com/exploits/35447

|_ Zabbix Agent 3.0.1 - 'mysql.size' Shell Command Injection CVE_ID: CVE-2016-4338

|___|_ URL: https://www.exploit-db.com/exploits/39769

|_ Zend Framework 1.11.4 - 'PDO_MySql' Security Bypass URL: https://www.exploit-db.com/exploits/35784

|_ ZoomStats 1.0.2 - 'mysql.php' Remote File Inclusion CVE_ID: CVE-2006-5065

|___|_ URL: https://www.exploit-db.com/exploits/2420

enumeration, 192:168:0:102