IDERA® | SQL Security Whitepaper

# SOLUTIONS TO THE MOST COMMON METHODS OF SQL SERVER INTRUSION

# SQL INJECTION

SQL injection, a known attack vector for websites or any applications using SQL database, is a code injection technique, used to attack data-driven applications, in which specifically constructed SQL statements with criminal intent are executed. SQL injection exploits a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed.

SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

To help protect against SQL injection, IDERA SQL Secure provides Idera Level-3 Strong Template which ensures that the following security checks listed below are in place. Additionally, IDERA SQL Compliance Manager provides real-time auditing of activity to SQL Server and helps identify and alert on abnormal activity.

| Category | Security Check Descriptions |
|---|---|
| Access | Dangerous Extended Stored Procedures (XSPs) (xp_cmdshell, xp_login, xp_startmail, xp_makewebtask) |
| Access | Stored Procedures Encrypted |
| Access | User Defined Extended Stored procedures exist |
| Auditing | C2 Audit Trace enabled - records successful and unsuccessful attempts to access objects and statements |
| Auditing | Login Audit Level - Checks for failed and successful logins |
| Configuration | SQL Server Version - ensures that the right version of SQL Server is installed |
| Configuration | xp_cmdshell enabled - Determine whether the xp_cmdshell extended stored procedure is enabled |

# DATABASE PERMISSIONS

Limiting the permissions on the database login used by the web application to only what is needed may help reduce the effectiveness of any SQL injection attacks that exploit any weakness that may exist on your SQL Server instance.

IDERA SQL Secure can help you to identify the SQL Server permissions that are currently in place so that you can verify that users have only the access that they need.

| Category | Security Check Descriptions |
|---|---|
| Access | Database roles and members - Shows information about database roles and their members |

# DEFAULT LOGIN IDS AND LOGINS WITH "BLANK" PASSWORDS

Even though with more recent SQL Server versions it's less likely to configure Logins with "blank" passwords, this vulnerability may still exist. DBAs may fail to change the passwords that are installed with a "blank" default password when they are setting up the server or may be misconfigured by less experienced DBAs. As more servers are brought online, this security check can be missed and propagated throughout the enterprise.

Hackers typically follow the path of least resistance. If the DBA doesn't rename the default login ids like "sa", the hacker can use sophisticated algorithms to figure out the passwords and hack into the SQL Server.

IDERA SQL Secure will help you to establish consistent baselines across your SQL Server environment to ensure that login ids like "sa" are disabled, blank passwords are not allowed, and the login audit level for failed/successful logins are enabled. IDERA SQL Secure templates Idera Level-2 Balanced or Idera Level-3 Strong are recommended. Furthermore IDERA SQL Compliance Manager has the ability to audit and alert on failed/successful logins.

| Category | Security Check Descriptions |
|---|---|
| Configuration | "sa" account not disabled - Determine whether the SQL Server "sa" account has been disabled |
| Login | Blank Passwords - Determine whether any SQL Logins have blank passwords |
| Login | "sa" account has blank password - Determine whether the SQL Server "sa" account has a blank password |
| Auditing | C2 Audit Trace enabled - records successful and unsuccessful attempts to access objects and statements |
| Auditing | Login Audit Level - Checks for failed and successful logins |

# PRIVILEGED USER ACCESS

The “Privileged User” may access sensitive information such as payroll information about co-workers or in some cases acquire information to sell customer information, such as social security number, name, address, or date of birth, to an outside entity for identity theft which is a multibillion dollar industry. In other cases the “Privileged User” may want to acquire information for financial gain.

With IDERA SQL Compliance Manager you can explicitly specify privileged users and roles to be audited specifically: logins, failed logins, security changes, administrative actions, DDL, DML, and SELECT operations. In addition, IDERA SQL Compliance Manager leverages policy-based algorithms to track changes to your SQL Server objects and data. IDERA SQL Compliance Manager gives you detailed visibility to determine who did “what”, “when”, “where”, and “how”. IDERA SQL Compliance Manager helps you to ensure compliance with regulatory and data security requirements such as Sarbanes-Oxley, HIPAA, PCI DSS, and CIS. IDERA SQL Compliance Manager goes beyond traditional auditing approaches by providing real-time monitoring and auditing of all data access, updates, schema modifications, and permission changes.

IDERA SQL Secure will help you to establish consistent baselines across your SQL Server environment to ensure help limit access to sensitive data. Below are a few security checks you can add to SQL Secure policies and apply to your environment.

| Category | Security Check Descriptions |
|---|---|
| Access | Database roles and members - Shows information about database roles and their members |
| Access | Dynamic Data Masking - Determine whether dynamic data masking is configured for specified columns on SQL Server 2016 or later |
| Access | Remote Access - Determine whether Remote Access is enabled on the SQL Server |
| Access | Row-Level Security - Determine whether row-level security is configured for specified tables on SQL Server 2016 or later |
| Access | Sysadmins Own Trustworthy Databases - Determine whether any trustworthy databases are owned by system administrators on SQL Server 2005 or later |
| Access | Unacceptable Database Ownership - Determine whether if a database is found with an unacceptable owner |

# SUMMARY

Understanding how SQL Server can be infiltrated is the key to understanding how to prevent intrusions. The consequences for inadequate permissions are tremendous. Businesses could incur:

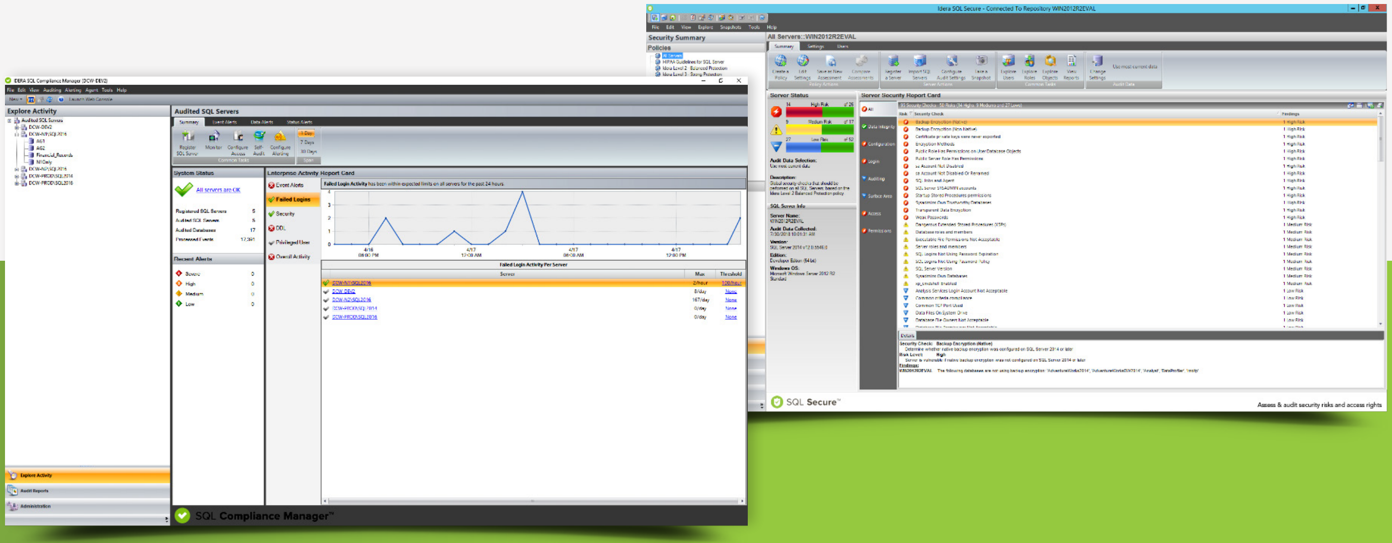
1. Data breaches
2. Fines
3. Loss of customers
4. Decrease in customer confidence
5. Loss of revenue

Don't let your SQL Server environment become an infiltration story. Proactive management of your SQL Server permissions is the best way to prevent catastrophic activities. IDERA SQL Secure helps you to establish the right security checks to your entire SQL Server environment.

Beyond that, DBAs need to monitor and audit the activity on their SQL Server environment. IDERA SQL Compliance Manager makes it possible to track the actions of privileged users, alert DBAs for any suspicious issues, and generate reports to demonstrate regulatory compliance.

Let's face it: DBAs have a wide range of responsibilities. On average, 5% of a DBA's time is spent on security planning and implementation. DBAs must have the right tools to enable them to work smarter, manage the environment more efficiently, and comply with regulations like SOX, PCI DSS, and frameworks like COBIT. IDERA SQL Compliance Manager and IDERA SQL Secure give you the coverage and functionality you need to protect your SQL Server environment from intrusion.

Start for FREE


Idera SQL Secure - Connected To Repository WIN2012R2EVAL
Security Summary
All Servers : WIN2012R2EVAL
Server Security Report Card
Server Status
SQL Secure
Assess & audit security risks and access rights
IDERA SQL Compliance Manager
Explore Activity
Audited SQL Servers
System Status
All servers are OK
Enterprise Activity Report Card
Failed Logins
Failed Login Activity Per Server
Recent Alerts
Explore Activity
Audit Reports
Administration
SQL Compliance Manager