NCAG
Network Claim Assessors Group

Database Credentials Policy

1. Overview

1.1. Database authentication credentials are a necessary part of authorizing application to connect to internal databases. However, incorrect use, storage and transmission of such credentials could lead to compromise of very sensitive assets and be a springboard to wider compromise within the organization.

2. Scope

2.1. This policy is directed at all system implementer and/or software engineers who may be coding applications that will access a production database server on the Company Network. This policy applies to all software programs, modules, libraries or API (Application Programming Interface) that will access a Company, multi-user production database. It is recommended that similar requirements be in place for non-production servers and lab environments since they don't always use sanitized information.

2.2. This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of the company's networks.

2.3. Software applications running on company network may require access to one of the many internal database servers. In order to access these databases, a program must be authenticated to use the database by presenting acceptable credentials. If the credentials are improperly stored, the credentials may be compromised leading to a compromise of the database.

3. Policy Statement

3.1. General Requirements

3.1.1. In order to maintain the security of the company's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

3.2. Specific Requirements

3.2.1. Storage of Data Base Usernames and Passwords:

3.2.1.1. Database usernames and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable or writeable.

3.2.1.2. Database credentials may reside on the database server. In this case, a hash function number identifying the credentials may be stored in the executing body of the program's code.

3.2.1.3. Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.

3.2.1.4. Database credentials may not reside in the documents tree of a web server.

3.2.1.5. Pass through authentication must not allow access to the database based solely upon a remote user's authentication on the remote host.

3.2.1.6. Passwords or pass phrases used to access a database must adhere to the relevant policy implemented, if applicable.

3.3. Retrieval of Database Usernames and Passwords

3.3.1. If stored in a file that is not source code, then database usernames and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the username and password must be released or cleared.

3.3.2. The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the username and password) and any functions, routines, or methods that will be used to access the credentials.\

3.3.3. For languages that execute from source code, the credentials' source file must not reside in the same browsable or executable file directory tree in which the executing body of code resides.

3.4. Access to Database usernames and passwords

3.4.1. Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.

3.4.2. Database passwords used by programs are system-level passwords as defined by the relevant policy, if applicable.

3.4.3. Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Password Policy.

3.4.4. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

4. Enforcement

4.1. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with the Network Claim Assessors Group.

5. Definitions

Terms	**Description**
LDAP server	Lightweight Directory Access Protocol, is an Internet protocol that email, and other programs use to look up information from a server

CEO name THYS BOTES CEO signature Thys Botes

MD (Network Claims Assessors)

Signed at PANORAMA on this 12 day of APRIL 20 22