Adam Howard

Cincinnati Job Outlook Portal Security Document

Credential Management

Credentials for the application are managed and stored from the SQL database that manages all application information. The default ASP.NET membership model is used for the Cincinnati Job Outlook Portal. This means that user passwords are encrypted using the Crypto class built into the System.Web.Helpers namespace. The full source code can be viewed here: http://aspnetwebstack.codeplex.com/SourceControl/changeset/view/1962da8fcfe4#src/System.Web.Helpers/Crypto.cs.

To summarize, the Crypto class uses a combination of SHA256 for a hashing algorithm and PBKDF2 as a key derivation function to create a cryptographic key. More information on SHA256 can be found here: http://csrc.nist.gov/groups/STM/cavp/documents/shs/sha256-384-512.pdf and information about PBKDF2 can be found here: http://en.wikipedia.org/wiki/PBKDF2#Systems_that_use_PBKDF2.

Input Encoding

The Cincinnati Job Outlook Portal does not have many user input fields, but any input fields are protected against HTML injection attacks on the server, and a server error is thrown if any dangerous input is entered. Since debug mode is disabled for non-local execution, users will not see the stack trace but instead only see an error page.

SQL Queries

The majority of the SQL that is used by the Cincinnati Job Outlook Portal is generated by LINQ statements. LINQ parameterizes the requests that it sends to the database so there is no possibility of SQL injection. The few queries that are not generated by LINQ are used for deleting table data and are not affected by user input in any way and are only executable by code available to administrators.