CSC 440

Mark Frye

Alex Krebiehl

Khalid Alsuwaiyel

**Security Requirements Document**

This is the security requirements document for the Cincy Crime Stoppers. Below is a table that describes the various security requirements and what we have done to meet those requirements within our website. This document will focus on the handling of

|  |  |
| --- | --- |
| Security Requirements | Description of security measures taken |
| User Stored Passwords | Passwords are hashed before stored in the database by OpenBSD bcrypt() password hashing algorithm |
| Cryptographic keys and passwords for auto start of the application automatically generated by the startup process or stored in an encrypted key vault? | All passwords are store as an environment constant where values are assigned in a hidden files which prevent this file from being get pushed into our source control |
| Authentication attempts use TLS encrypted connections? | The connection uses TLS 1.2. It’s encrypted and authenticated using AES\_128\_GCM and uses RSA as the key exchange mechanism. |
| Does application use predefined queries to avoid SQL injection | All queries are performed through Active Record. |
| Does the application disallow all HTML input or encode all HTML output to prevent cross-site scripting attacks? | Beside authentication and date filter, no input is allowed at all. |