Overview

Web applications present a unique set of security issues for developers. Applications created with security in mind from the start will be the most secure and resistant to malicious attacks. The AKN Public Services Project has identified the biggest threats to user security and has mitigated these risks.

Risk Mitigation

|  |  |
| --- | --- |
| Access to Account Credentials | This application has Administrator login accounts that consist of a username and password. Passwords are stored in the database but they are stored using an MD5 Hash 128 bit algorithm. |
| SQL Injection | Two effective mitigation strategies for eliminating SQL injection are prepared queries and character whitelists.  Both the results from the drop down options and the typed user input all use whitelists. For the user record searches, only the minimum necessary characters are allowed as input. For the street number and street name input, A-Z, a-z, 0-9 and space are the only allowable characters. The street direction only allows N, S, E or W and all other drop down filters only allow 0-9 as these should only be returning an ID number. Any character that is not in the whitelist will be removed.  This effectively prevents SQL injection as no special characters can be used in the inputs. This also holds true if a malicious person attempts to use a developer console to edit drop down options or attempts to spoof the form submission. |
| Cross Site Scripting | Cross Site Scripting (XSS) can occur when using values passed through the URL. These variables are a string which could be changed to contain unwanted Javascript.  In this project, before these values are ever used, the same whitelist strategy is used to restrict the characters to only 0-9. In both instances where variables are passed through the URL, only numbers should be needed. |