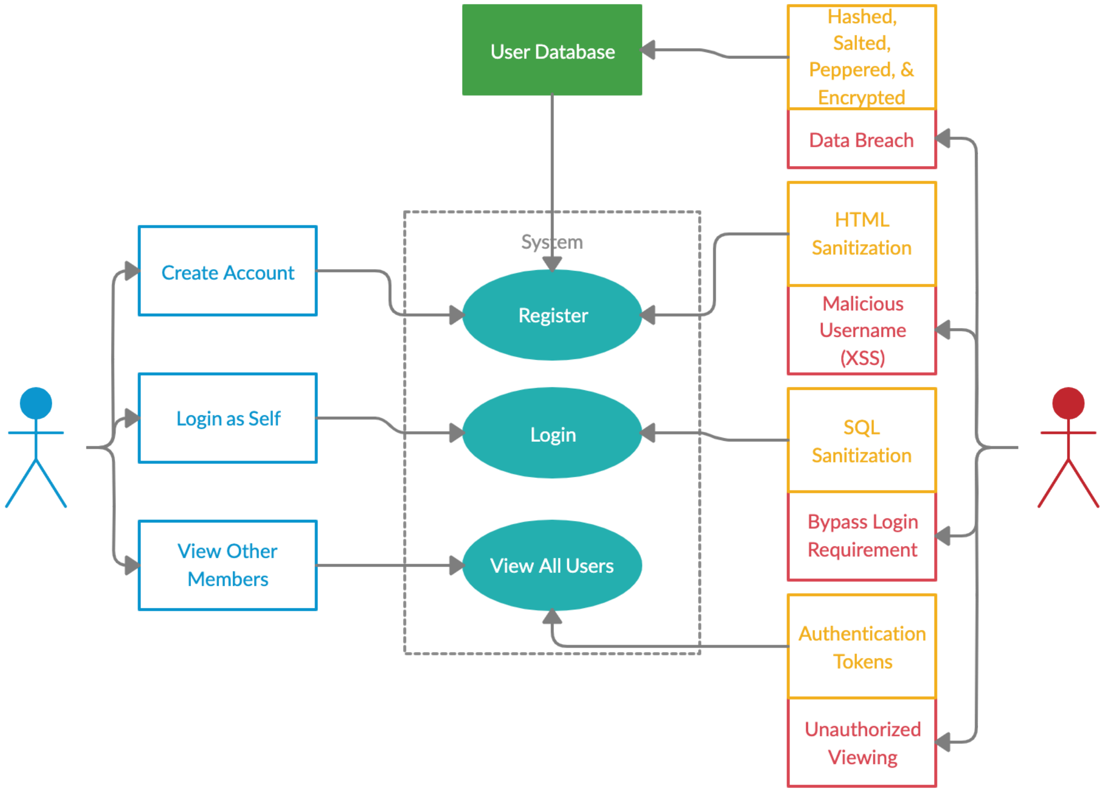
Safety Scouts - Durden, Johson, Trinity, Casella

Mini-Project 1 Use / Abuse Case Diagram



Security Policy

A normal user would have to be able to register with their information, login to their account, and, once logged in, see a list of all the current users. The main security policy is that only users can have access to their account and that the full list of users must be both safe for and exclusive to users.

Risks

Login attempts are made using SQL so a single insecure query could expose the database to the attacker. This would allow the attacker to access user information, insert false entries, and deny service by thrashing the database.

Username's are used to identify users in the Users page. A malformed username using HTML script tags could expose users to XSS attacks if not properly sanitized. This could compromise the users browser and even system.

URLs are descriptive and could be reasonably guessed. This could be used to gain access directly to areas that should be secured through login if not secured by some other means. This would result in unauthorized access to strictly exclusive information.

Cookies could be stolen, copied, or CSRF'd resulting in unauthorized access or actiona from the user's accounts and release of exclusive information.

The user database contains login information for all users. Should this be compromised either internally or externally, all stored information would be made entirely public.