JNAC

Andrew Azenabor

James Nguyen

Carson Siu

Nicholas Sylvestre

**Web Application Security**

**Passwords and Storage**

For this project the focus of security was placed in several key areas. On the front end, to ensure that the user is protected, there is group of regular expressions that examine the desired password entered during registration. Depending on the password complexity (based on length, upper/lowercase characters, and usage of symbols), the website then indicates to the user how strong their chosen password is. As the password length gets longer, the strength value increases due to the increase in password entropy.

A rating scale developed for this website looks at the various types of characters used in the password and gives the password one point for each category that is fulfilled. It is recommend that, at the very least, the password be of a “Good” rating in strength and requires that all passwords have a minimum length of 6 characters. The scale considers any password with a strength of less than 2 points to be weak, exactly 2 points is good and greater than 2 to be strong.

The passwords themselves are stored on the website’s database. They are encrypted using the SHA-256 hashing algorithm so that they are not in plain text for anyone, including the database administrator, to see. Because SHA-256 is a one-way hashing algorithm, there is no easy way to decrypt the hashed values and to brute force the values would be a long and tedious task. In the event that the database somehow becomes compromised, the data stolen should be relatively useless to the attacker since the values will be encrypted.

**Input Validation and Sanitization**

In regards to handling user input, whether it be signing up for the website or posting on the message board, the input is sanitized to ensure that there cannot be any form of cross site scripting or SQL injection attacks. This prevents the users from inputting their own code on to the website that could affect other users and also prevents them from manipulating the website’s databases. This is done by ensuring that all special characters have been properly escaped and set to their respective ASCII values rather than allowing the characters to become part of the code.

**Site Protection**

To ensure that the website’s users are protected from outside threats the website also does not allow users who are not registered to post on the forums. Only registered users may do so and helps prevent spammers and trolls from derailing topics of discussion or posting malicious links.

Additional security can be managed by administrative staff and moderators who can manually check the forums for any suspicious links and posts that could be of potential threat.