Hue Manatees

Security Document

Password Security: The password is sent across the network to the Amazon Web Server, amazon web server advertises that it has a certificate to have the data in a secure state in transmission. To secure the password during the storage state we implemented a password hashing class that implements SHA3 to hash it and uses a cryptographic random number generator to provide the salt to defend against rainbow table attacks. Unfortunately during the processing state the password will be clear in memory until removed by garbage collection….

Personal Information: Once again Amazon Web Server’s certificate defends during transmission. The main thing of interest is that this site is modeled in a way similar to Facebook. That means that by design people will be placing personal details on the site with the intent of sharing them. Currently the only defense to information planned is to not share what you want to keep private. I would propose in a future hypothetical iteration that there be limitation controls over who can access personal details such as requiring both parties be friends or permissions for what is allowed to be displayed.

Database: There exist a few defenses to defend against attacks such as SQL injection. First off, all queries are sent as prepared statements, in owasp documentation it can be found that this is not an ‘end all be all’ of sql security. To defend against unintended modification of the database user queries are handled by a ‘user’ that does not have insert/modification privileges.

XSS: Before a post is stored it is stripped of potential tags. This limits what the user can display and as such it may be wise to select some kind of markup language that allows variety of writing but forbids java script.