**Security and privacy**

Senior Project Website uses codeIgniter *‘open source web application framework, PHP’* to prevents.

No changes to any of the following occurs going from SPWv.3 to SPWv.4. The following information is entirely from SPWv.3 design document.

SQL Injection

System takes care of avoiding SQL injection attacks by using the Active Record class from the Code Igniter framework for all interaction with SPW Website, which produces safer queries since the values are escaped automatically by the system.

URI Security

Malicious data can be passed to the application via the URI strings. This is prevented in our system by the use of the Code Igniter framework which is fairly restrictive regarding which characters it allows in the URI strings.

Cross-site scripting (XSS)

Cross scripting is also prevented by the use of the Code Igniter Cross Site Scripting Hack prevention filter which has been configured to run automatically to filter all POST and COOKIE data that is encountered.

Cross-site request forgery (CSRF)

Cross site forgery has been also addressed by enabling the CSRF protection on Code Igniter, which turns on a complicated algorithm that allow SPW website to know if the data it receives actually comes from a form on this website, avoiding with it this type of attacks.

Session Encryption

SPW uses the Code Igniter Session class to manage user session information, which is stored as serialized and encrypted in a cookie.

One-Way password encryption

SHA-1 function is used to encrypt users’ passwords in database, which allow website to keep secured user’s password for the website and therefore all their profile information in the website.

The SHA-1 algorithm has two important properties that make of it the more secure algorithm website could use to secure user’s information. The first one is that is a one-way hashing algorithm, which makes impossible to revert back an encrypted output to the initial, plain-text input, and that any given input always maps to the same encrypted value. This ensures that the passwords stored on the server cannot be deciphered by anyone. This way, even if an attacker gains reading permission to the user table, it will do him no good.

It is important to add that no unnecessary information is stored for a user and email addresses are only displayed to registered users.