Chicken Farm Ethics

C2C Taylor Coffey

C2C Tia Kolakowski

C2C Peter Ye

CS364

Captain Josiah Lane

When it comes to the use of our web application to help maintain accessible records for our chicken farm, several privacy concerns exist. In order to properly ensure that the data is kept secure from malicious attackers, we should strive to do whatever is possible to protect from attacks such as SQL injections or cross site scripting. In the case of an SQL injection specifically, the two main steps we can take is to employ input validation and use prepared statements for inputs. Input validation specifically ensures that users cannot use malicious inputs to execute unwanted queries on the database, and instead are only able to enter text that is confirmed “safe”. By preventing users from using input forms to enter exploitative commands, we can take steps to mitigating the risks associated with having a large database of sensitive information.

As an agricultural firm, it is likely that we will in some part contract with the United States government or work with the FDA. Because of the status of being government contractors, we are required to comply with standards set forth in the Privacy Act of 1974. Since we use Social Security Numbers to identify individuals in the system, it is vital to defend our database from being exposed and risking the personal identifiers of the employees. Furthermore, in order to comply with the Privacy Act, we must also ensure that there are both administrative and physical security measures in place preventing any leaks of data or vulnerabilities. The servers must be safely and professionally maintained in a secure location, and not accessible to those without proper levels of authentication.

Once fully developed, our website must meet the security requirements that prevent malicious actors from gaining access to sensitive data. Accomplishing this requires the use of both back-end safety measures handling user input and adherence to policies from the Privacy Act.