**Notes from 3/19 Meeting**

* Website updates were given and viewed; some vulnerabilities were tested.
* Hints were added to CSRF vulnerability along with a funny comic.
* Angela wrote an explanation on the CSRF vulnerability, (needs definition added).
* More fields need to be **added** in the feedback page (more input fields, more vulnerabilities).
* The feedback submitted **needs** to be stored in a separate file/dummy DB, make only a few employees have access to DB, and a script to delete data every day.
* Should **not** be able to change the login password (need default/customer accounts).
* The admin account **needs** the most privileges, employee accounts do **not** get the feedback option.
* Insecure file upload **needs** a temporary directory/to be stored in DB.
* **Add** page for Loans for sensitive data exposure vulnerability.
* User input fields **need** to be added in the contact area or within a new contact page, add the following fields: name, email, description, submit button for reflected/stored XSS.
* **Add** an application page for jobs upload such as resume, terms conditions, etc… mimic an actual banking sites page.
* Make the website look fuller by **adding** data similar to a real banking site, make it look busy.
* **Add** money transfer page with account transfers and online statements.
* **Add** name, account, and welcome banner to home page when user logs in.
* **Add** edit user page, allow edits to some accounts.
* **Add** SSL protocol vulnerability, mimic zero webappsecurity website.
* Complete website with all pages, then focus on adding vulnerabilities, the more input fields, the more vulnerabilities that can be implemented.
* Tentatively, the next meeting is **MON (24th)** unless otherwise communicated with Professor Tugali.
* These tasks should be completed by the end of the month.