**Activity 1**

1.) What is the URL of your Github project?

**Github –** <https://github.com/jwj3767/WebProjSkitter>

**Zenhub –** <https://app.zenhub.com/workspace/o/jwj3767/webprojskitter/milestones>

**Travis Ci –** <https://travis-ci.org/jwj3767/WebProjSkitter/branches>

2.) How did you breakup your projects and what are the security ramifications?

**We decided to map out what the minimum requirements were for each step and map out the required work. We also decided to not split up who would captain the other activities because we believed that it would be beneficial to both of us to learn as much as we can.**

**The security ramifications of our project that we found in our plans were seen in our SQL database and 2-step verification. The reason we thought that our SQL database would be in need of more security is because the passwords would be stored in plain text in our designing stages. The reason we also thought that 2-step verification would be a good idea is to ensure that the user and only the user is logging in. Additionally, whenever an user would like to change their username, password, or email we also felt that it would be a good idea for them to insert a verification token.**

3.) How did you choose to break down your milestones into various issues (tasks)?

**We choose to break down our milestones for our project in Travis CI, by setting milestones for each activity in our project. However, we also plan to go back and set more milestones for each activity.**

4.) How do you ensure that after each issue/milestone that security has been verified? How would you identify such issues in an ideal environment?

**In order to ensure that security has been verified after each issue or milestone, we felt that running tests on Travis CI would most likely be our best solution through creating scripts to test each issue or milestone. We could use it to attempt to breach the website, or we could try to mine passwords.**

**Activity 2**

1.) What Web Application Security mechanisms are involved in your topology? What security mechanisms would ideally be involved?

**In our topology, SAML is used to authenticate users. Ideally, the site would also have an SSL certificate to ensure privacy. Additionally, we would also set up 2-step verification to protect user accounts as well.**

2.) What testing framework did you choose and why?

**We have to use Travis CI as our testing framework because after doing more research on other testing frameworks, we came to the conclusion that Travis CI is the most smoothly working framework that would run tests on our project.**

**Activity 3**

* **Skitter can be run with the following command**
  + ***docker-compose up --scale phpnginx=2***

**Activity 5**

* **HTML and CSS files are all located in the WebProjSkitter/phpnginx/htmlfiles directory.**

**Activity 6**

* How do you prevent CSRF attacks changing the user’s settings?
  + **When users change their settings I only allow for a user change their profile picture. This decision was made because if a user had the ability to change their email or display name then there would be a possibility that someone could change their account and pose as someone else.**
* How do you sanitize user input to ensure there isn’t malicious content (sqli/xss)?
  + **User input is sanitized in registration and when logging in by requiring that users enter in a proper email. Making a “tweet” or “skit” has not been added yet, therefore there is no need to sanitize when people post on to their profile.**

**Activity 7**

**Activity 8 & 9**

* **Professor permitted to skip these last two parts**