Notes from 3/3 meeting

-Josephine Poulin

> *The meeting began with a recap of the last week of work, the three vulnerabilities added, and new implementation suggestions.*

Vulnerabilities added:

- File upload vulnerability
- User enumeration vulnerability
- SQL injection vulnerability

Suggestions are as follows:

- Limit the file upload vulnerability so the server does not crash in the future
- Create a Denial of Service (DOS) attack by having no filter and adding a flag to congratulate the student
- Populate the error message from SQL injection into a pop up instead of the bottom of the screen
- Generate 50-60 users for session hijacking/user enumeration
- CSRF token with session ID's, make them vulnerable
- CyberSec Team explain how to implement CSRF onto the website
- Research the use of Microsoft products to employ for the website, since they partner with WVNCC: user logs, inputs, gaant chart etc...
- Input fake data into website through "news websites" for future DOM based attacks

To Do by Monday 3/10

- Five (5) different vulnerabilities implemented within the website, preferably: Stored cross-site scripting (XSS), Cross-site request forgery (CSRF), Click-jacking, Session Hijacking, + one more
- Better changes to website appearance (UI)
- Remove the placeholder text within website, create actual text filler related to site