UNB | Canadian Institute for Cybersecurity

Instructor: Saqib Hakak
Course: CS 4417/CS6417

**Final report submission date: April 01, 2024**
**Project is to be done individually.**
**Total points = 25**

**PLEASE NOTE, IT IS VERY UNLIKELY ATTACK TREE AND SURFACE CAN BE SIMILAR. IN CASE, I FOUND EVIDENCE OF CHEATING/COPYING DESIGN TREE, ALL THE PARTIES INVOLVED WILL BE AWARDED ZERO IN WHOLE PROJECT. PLEASE USE YOUR OWN INTITUTION AND KNOWLEDGE.**

## Detailed Guidelines

Each graduate student will develop a client-server-based application of their choice using any preferable programming language. The application developed must have the following functionality:

1. Login page ((i) must be able to log in/out, (ii) change password, (iii) be able to add new users/customers with least privileges) 3 points
2. Input field (such as feedback forum, contact page) 2 points
3. Buy or sell products 3 points
4. Database to store data 2 points

From the security perspective, you will start your project using the following steps:

1. Read about Agile and DevOps. Choose either of these.
   This will be the first part in your project report. You must justify why did you choose a particular one.
2. The second component of your project will be to think like an attacker. Before you start development process, design the attack surface for your whole application and attack tree for the login page and input field. Explore diverse attack scenarios from the literature/standards (e.g, NIST, ISO).
3. Follow the remaining steps outlined in the selected SDLC to complete your project.
4. Due to time constraint, focus on testing your application for:
   (i) Authentication: Verify the strength of authentication mechanism. Test for weak or easily guessable passwords.
   (ii) Check for proper input validation to prevent injection attacks such as SQL injection, cross-site scripting (XSS), and command injection. Ensure that user inputs are sanitized and validated before processing.
   (iii) You can use automated testing tools. You can also explore fuzzing (if interested).

## Undergraduate:

For UG, all the above conditions are applicable except they don’t need the functionality of buying or selling products. Also, they need to design the attack tree only for login page (no need for the input page).

Instructor: Saqib Hakak
Course: CS 4417/CS6417

1. Login page ((i) must be able to log in/out, (ii) change password, (iii) be able to add new users/customers with least privileges) 5 points
2. Input field (such as feedback forum, contact page) 3 points
3. Database to store data 2 points

From the security perspective, you will start your project using the following steps:

5. Read about Agile and DevOps. Choose either of these.
   This will be the first part in your project report. You must justify why did you choose a particular one.
6. The second component of your project will be to think like an attacker. Before you start development process, design the attack surface for your whole application and attack tree for the login page only. Explore diverse attack scenarios from the literature/standards (e.g, NIST, ISO).
7. Follow the remaining steps outlined in the selected SDLC to complete your project.
8. Due to time constraint, focus on testing your application for:
   - (iv) Authentication: Verify the strength of authentication mechanism. Test for weak or easily guessable passwords.
   - (v) Check for proper input validation to prevent injection attacks such as SQL injection, cross-site scripting (XSS), and command injection. Ensure that user inputs are sanitized and validated before processing.
   - (vi) You can use automated testing tools. You can also explore fuzzing (if interested).

## Final Report (10 points):

The final report should consist of:

1. **Abstract** – *max 300 words*
2. **Introduction:** [Which SDLC you selected and why – *Max 2 single column pages (font size 12)]*
3. **Attack tree and surface:** Show the attack tree and surface. Provide overview of different attacks. Highlight what standard did you consult to design attack tree and surface. 5 points
4. **Technical controls:** Explain what technical controls you implemented to address the attack concerns.
5. **Testing:** What testing tools did you choose.
6. **Discussion:** In this section, mention what did you learn from this project. 1 point
7. **Appendix** – Put all your code sample

The remaining 4 points will be on organisation of your report, grammatical mistakes etc.

Instructor: Saqib Hakak
Course: CS 4417/CS6417

## Presentation (5 points):

Include following information:

1. One slide on Overview of your project (what is project about)
2. Demo of showing functionalities for all the above 4 components by providing required input.

   **You will be asked to test your application using some undesired input during demo.**

## GUIDELINES:

- DO NOT COPY/PASTE project from the internet. Any project copied from internet will be awarded zero points. In case of any similar projects between students with same source-code etc., zero points will be awarded.
- You can reuse some part of code for your project from internet for basic functionalities. But provide and cite appropriate references wherever applicable.