# IERG4210 Web Programming and Security (2024 Spring)
## Assignment Marking Guidelines

## Revision history

v1.0 Published on 05/02/2024

## General Guidelines

The assignment is designed to let students practice what they have learned in the course. Students must be aware of web application security throughout web development. The whole assignment is split into 5 phases, leading all the way to a creative and functional shopping cart upon completion. Students should take a real-world website, parknshop.com, as a reference. In the assignment, students are expected to understand and apply proper security design principles and programming skills, regardless of which programming languages and libraries the students desire to use. The marking checklist included in the next page therefore outlines only the general requirements with a result-oriented basis in order to encourage students' creativity. For detailed guidance, students should refer to both lecture and tutorial notes.

## Submission Policy

Students are required to package all of their source code, a README file, and any external resources (e.g. database, images, css and js files) into a zip file and submit it to the Blackboard. Each phase is associated with a firm submission deadline.

- Late Submission Penalty -- Late submission will lead to your mark reduction by the formula $0.9^n$, where $n$ is the round-up number of days delayed (e.g., assume your score is $S$ and your submission is 9 hrs late $\rightarrow 0.9 \times S$, 25 hrs late $\rightarrow 0.81 \times S$, 49 hrs late $\rightarrow 0.729 \times S$, and so forth).
- *Final Demonstration* – Students will sign up for a timeslot to demonstrate their websites to a marker, who will then grade it according to the checklist. The marker will then evaluate the student's understanding with questions.
- *Early Submission Incentive* – For every 48-hour advanced submission in one phase, the deadline for Phase 4 or 5 can be extended by 24-hour, and no part thereof is accepted. For instance, submitting 100 hours earlier in phase 1 will gain an extension of 48 hours for the Phase 4 or 5 deadline.
- Grading - If there is any inconsistency, TA will grade your assignments based on the file and timestamp that you submitted to Blackboard.

## Honesty in Academic Work

CUHK places very high importance on honesty in academic work submitted by students, and adopts a policy of *zero tolerance* on cheating in examinations and plagiarism. Students are NOT allowed to submit anything that is plagiarized. Therefore, we treat every assignment our students submit as original except for source material explicitly acknowledged. We trust that students acknowledge and are aware of University policy and regulations on honesty in academic work, and of the disciplinary guidelines and procedures applicable to breaches of such policy and regulations, as contained in the website http://www.cuhk.edu.hk/policy/academichonesty/.

# IERG4210 Web Programming and Security (2024 Spring)

## Assignment Marking Checklist v1

### Phase 2A: Secure Server Setup (Deadline Feb.17, 2024) (Subtotal: 5')

In this phase, you are required to set up a secure server for later development. Some guidance will be given in the tutorial.

1. Instantiate a free Virtual Cloud Machine (**Amazon EC2** recommended or other free VPS) _____ / 1'
   - Details of the Free Usage Tier: http://aws.amazon.com/free
   - You can apply for the education coupon on AWS
   - With a Linux distribution, install only Ngnix, NodeJS and SQLite (or MySQL)
     - To minimize the attack surfaces, always install only what you need
2. Apply necessary security configurations _____ / 2'
   - Apply proper firewall settings to your VM: block all ports except 22, 80 and 443 only
   - Apply proper updates for the server software packages in a regular manner
   - Hide the versions of OS, Ngnix, and NodeJS in HTTP response headers
3. Configure the VM so that your website is accessible at http://sxx.ierg4210.ie.cuhk.edu.hk _____ / 2'
   - Apply for an elastic public IP, and ALWAYS associate it with the instantiated VM
   - Submit your elastic IP through the provided Google Form link[1] before 5pm, Feb 17, 2024
   - TAs will then assign you a domain name and configure the DNS mapping for you
   - Upload all your pages to the server. They should then be accessible through:
     - http://[your-own-public-IP], or
     - http://sxx.ierg4210.ie.cuhk.edu.hk

### Phase 2B: Data Presentation & Management (Deadline Feb. 25, 2024) (Subtotal: 20')

In this phase, you will implement the core functions of the website mainly with NodeJS and SQL.

1. SQL: Create a database with the following structures (to be covered in the tutorial) _____ / 1'
   - A table for *categories*
     - Required columns: *cid (primary key), name*
     - Data: at least 3 categories of your choice
   - A table for *products*
     - Required columns: *pid (primary key), cid, name, price, description*
     - Data: at least 3 products for each category
2. HTML, NodeJS & SQL: Create an *admin panel*
   - Design several HTML forms to manage[2] *products* in DB _____ / 5'
     - Dropdown menu to select *cid* according to its *name*
     - Input fields for inputting *name*, *price*
     - Textarea for inputting *description*
     - File field for uploading an image (format: jpg/gif/png, size: <=5MB)
       - For the file uploaded, store it with its name based on the unique lastInsertId()[3] (or other reasonable ways) _____ / 1'
   - Design several HTML forms to manage *categories* in DB _____ / 2'
3. HTML, NodeJS, SQL: Update the *main page* created in Phase 1
   - Populate the *category list* from DB _____ / 1'
   - Based on the category selected by the user, populate the corresponding *product list* from DB _____ / 3'

---

[1] https://forms.gle/bxthQcxDx4d9vrm48

[2] 'Mange' means that you can insert, update and delete information in the Database through the admin panel.

[3] https://www.php.net/manual/en/pdo.lastinsertid.php

        - The *cid=[x]* is reflected as a query string in the URL
4. HTML, NodeJS & SQL: Update the *product details page* created in Phase 1 _____ / 2'
    - Display the details of a product based on its DB record
    - Display the inventory of a product based on its DB record
5. Support of automatic image resizing for product images _____ / 3'
    - When a large image is uploaded, the server will resize it and show a thumbnail image in the panel
    - On the main page, display thumbnails. On the product description page, display the larger image
6. Supporting HTML5 Drag-and-drop file selection in the admin panel _____ / 2'
    - Create a dropping area that takes an image
    - Display a thumbnail (i.e. smaller width and height) if the dropped file is an image; reject it otherwise