IERG4210 WEB PROGRAMMING AND SECURITY (2024 SPRING)
ASSIGNMENT MARKING GUIDELINES

REVISION HISTORY

v1.0 Modified on 24/03/2024

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 6 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 → $0.9 \times S$, 25 hrs late →$0.81 \times S$, 49 hrs late →$0.729 \times S$, 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.

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 plagiarised. 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

PHASE 5: SECURE CHECKOUT FLOW (DEADLINE: APR 7 2023) (SUBTOTAL: 20')

This is a tough phase, yet the most critical one, to escalate your website (building skill) to the next (professional) level. (You'll likely be offered a job if you can demonstrate such a level of web programming skills.) The implementation has already been outlined as below. Be prepared to spend a substantial amount of time debugging.

Paypal Sandbox Accounts

1. Sign up at https://developer.paypal.com/dashboard/ : _____ / 1'
    a. Create two sandbox accounts – a merchant account and a buyer account:
        i. A merchant account – Email and Password
        ii. A buyer account – Email and Password
    b. Create a sandbox application linked to the merchant account:
        i. an application – Client ID

Paypal Integration - Front End

2. Create a checkout button via PayPal standard checkout APIs: _____ / 1'
    a. Include the PayPal JavaScript SDK
    b. Set up a container element for the button
    c. Render the button by *paypal.Buttons().render()*
3. When the checkout button is clicked, *createOrder()* is called: _____ / 3'
    a. It passes the *name* and *quantity* of every individual product (or any other data) to server.
    b. It waits for server to generate a JSON string named *orderDetails*.
    c. It submits the order now to PayPal using the *actions.order.create()* function.
4. After the buyer has completed the payment, *onApprove()* is called: _____ / 2'
    a. It passes the orderDetails to server.
    b. It clears the shopping cart.
5. If the buyer cancels the payments, *onCancel()* is called: _____ / 1'
    a. It passes necessary information to server.

Paypal Integration - Back End

6. Server follows the following steps to generate the *orderDetails*: _____ / 5'
    a. server generates a digest that is the hash from a string composed of at least:
        i. the *name* and *quantity* of each selected product,
        ii. The price of each selected product gathered from DB,
        iii. The total price of all selected products,
        iv. Currency code,
        v. Merchant's email address, and
        vi. A random salt
    b. server puts the generated digest in the *custom_id* of an order.
    c. server generates an UUID, and puts it in the *invoice_id of an order*.
    d. server generates other necessary fields of an order, including at least:
        i. amount - the total price and currency code
        ii. items - the *name*, *quantity*, *price* of each selected item

7. Server follows the following steps to insert and update the DB *orders* table: _____ / 3'

a. When *createOrder()* is called, it inserts a new entry:
    i. UUID - TEXT (Primary Key)
    ii. username - TEXT
    iii. digest - TEXT
    iv. salt - TEXT
b. When *onApprove()* is called, it updates the corresponding entry:
    i. orderDetails - TEXT
c. When *onCancel()* is called, it deletes the corresponding entry.

Miscellaneous Changes

8. Display the DB *orders* table in the admin panel: product list, payment status…etc. _____ / 2'
9. Let members check the most recent five orders in the member portal . _____ / 2'

References:
https://developer.paypal.com/docs/checkout/standard/integrate/
https://developer.paypal.com/sdk/js/reference/