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

Revision History

v1.0 Published on 12/03/2024

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 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 4: Securing the Website (Deadline: Mar 24 2024) (Subtotal: 30')

In this phase, you will protect your website against many popular web application security threats.

1. No XSS Injection and Parameter Tampering Vulnerabilities in the whole website
   - [UI Enhancement Only] Proper and vigorous client-side input restrictions for all forms _____ / 1'
   - Proper and vigorous server-side input sanitizations and validations for all forms _____ / 2'
   - Proper and vigorous context-dependent output sanitizations _____ / 2'
2. Mitigate SQL Injection Vulnerabilities in the whole website _____ / 2'
   - Apply parameterized SQL statements
3. Mitigate CSRF Vulnerabilities in the whole website _____ / 2'
   - Apply and validate secret nonces for every form
   - ALL forms must defend against Traditional and Login CSRF
4. Authentication for Admin Panel
   - Create a user table (or a separate DB with only one user table) _____ / 1'
     - Required columns: ***userid (primary key), email, password***
     - Data: *at least 2 users of your choice, 1 admin and 1 normal user (using admin flag)*
     - Security: Passwords must be properly salted and hashed before storage
   - Build a *login page* that requests for *email* and *password* _____ / 3'
     - Upon validated and authenticated, redirect the user to the *admin panel* or main page
     - Indicate user name (or "guest" if not logged in) in your website
     - Otherwise, prompt for errors (i.e. either email or password is incorrect)
     - A separated normal user login page is not compulsory
   - Maintain an authentication token using `Cookies` (with `httpOnly`)
     - Cookie name: `auth`; value: a hashed token; property: `httpOnly` _____ / 2'
     - Cookies persist after browser restart (i.e. 0 < expires < 3 days) _____ / 1'
     - No Session Fixation Vulnerabilities (rotate session id upon successful login) _____ / 1'
     - Configure all authentication cookies to use the Secure and HttpOnly flags _____ / 1'
   - Validate the authentication token before revealing and executing admin features _____ / 3'
     - If successful, let admin users access the admin panel and execute admin features
     - Otherwise (e.g. empty or tampered token), redirect back to the *login page* or main page
     - Security: *admin panel* must validate the auth. token
   - Provide a logout feature that clears the authentication token _____ / 1'
   - Supporting Change of Password _____ / 2'
     - Must validate the current password first
     - New password can not be the same as the current password.
     - Logout user after the password is changed
5. All generated session IDs and nonces are not guessable throughout the whole assign. _____ / 1'
   - e.g., the login token must not reveal the original password in plaintext
   - e.g., the CSRF nonce when applied in a hidden field must be random
6. Apply SSL certificate for `secure.s[1-80].ierg4210.ie.cuhk.edu.hk`
   - Certificate Application _____ / 2'
     - When generating a CSR, use `CUHK` as Organization Name
     - Apply for a 90-day free certificate at https://www.ssl.com/certificates/free/buy/ or https://letsencrypt.org/ (or others)
     - Reminder: the application process can take more than a day, so apply early!!
   - Certificate Installation
     - Install the issued certificate and apply security configurations in Nginx _____ / 1'

        - Apply strong algorithms and secure cipher suites
    - Host admin panel at https://secure.s[1-80].ierg4210.ie.cuhk.edu.hk/admin _____ / 2'
        - redirect users to **https** website if come from `http://[secure...]` or `http://[...]/admin`

References

https://en.wikipedia.org/wiki/Cross-site_request_forgery