جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY
كلية علوم الحاسب وتقنية المعلومات
College of Computer Science and Information Technology

CYS 538: Web Technology and Security

Academic Year 2022-2023 / Third semester

Project - Teamwork

Due Date: 1 June 2022

This assignment is meant to give you the opportunity to create your first website to increase your understanding of the course in terms of developing websites, connecting to a database, and performing security testing against known web vulnerabilities. This project aims to apply computer security concepts to secure web applications against the discovered vulnerabilities.

The requirements of this project are as follows:

1. Each team must create a website based on their own choice (for example, Online shopping, University website like PeopleSoft, or Bank Website).
2. Use HTML, JavaScript, PHP, and MySQL for the database.
3. Your website must contain the following (Note: work on your code in any editor you like):
    - Login page (maintain the session for the logged user)
    - Pages that contain data viewed from a database
    - Pages that send data to the database
    - Secure Data Storage (storing password securely)
    - Handling the user input: Perform Input validation/sanitization on user inputs
        - **Use of prepared statement**
        - **Input Validation/Sanitization**
            - at the client-side (with HTML or JavaScript).
            - at server-side (with PHP).

4. **Test your website against a chosen attack/vulnerability:** Each team select one attack from the below list (First Come First Serve):
    1. RFI/LFI
    2. CSRF
    3. SQLi
    4. XSS
    5. Path Traversal Attack
    6. Weak Session IDs

    In this section, you will:
    - Explain the attack and what vulnerabilities could lead to this attack.
    - Implement the attack: it depends on your implementation that attack could be either failed or successful.

    - **Failed** due to security countermeasure in place.
    - **Successful** due to that lack of security countermeasures or improper security countermeasures in place.

5. **Countermeasures**: in this section you need to:
    1. **identify and explain what are the countermeasures** to defend against the chosen attack (in general).
    2. **Practically implement** the appropriate countermeasures to secure this input or the component in which that vulnerability was found.

6. Each team must submit a technical report illustrating their work.

General Notes:

- Configure Ubuntu as web server (Apache2), and prepare the LAMP stack on your web server on a virtual machine.
- If you would like to use your favorite editor on your host (computer), you can do this. After the webpages are ready, then move your code to Ubuntu after configuring it as web server apache2.

Submission Instructions:

- Follow standard report format.
- Due date (final submission): 1 June 2023 @ 11:59 PM
- Include all references with details and cite references in the text or diagrams, even if re-use source code from others (code snippet).
- Submit **pdf** file and include the **github repository** link in the appendices.
- Avoid plagiarism, do not extract line-by-line from any sources in your report.
- Late submission will be penalized with 20% deduction per day.

Grading:

Requirements		**Marks**
Coding	Login page (maintain the session for the logged user)	1
	Pages that contain data viewed from a database	1
	Pages that send data to the database	1
	Handling the user input: perform Input validation/sanitization	1.75
	Secure Data Storage (storing password securely)	0.75
Test your website against a chosen attack.		2
Countermeasures	Identify and explain what are the countermeasures to defend against the chosen attack.	1.5
	Practically implement countermeasures	1
Presentation	Present your work in the class.	3
Report Structure	Clear structure following the formal report.	1.5
		15