Introduction to Computer Security – G6077

**Weighting:** 50% of marks for the module

**Version Information:** Version 1, 21st Oct 2022

**Lovejoy’s Antique Evaluation Web Application**

In this coursework, you will develop a secure web application for a local antique dealer named Lovejoy. Lovejoy wants a minimum viable product allowing customers to register and then request evaluations of potential antique objects. Lovejoy has many rivals in the antique business who may sometimes resort to underhand tactics and so is very concerned about the security of the application.

Your secure web application will need to have these features for the minimum viable product (MVP) release: user registration and login, a password policy, “request evaluation” page and then an extension of the “request evaluation” page file upload to allow upload of photos. Finally, Lovejoy needs a request listing page.

You should build Lovejoy’s MVP focusing on the following features in each task. As well as the code, you should submit a report as described in the appendix below, where you will provide a self-reflection on the security and for each feature. Mark allocation for each task are as described below and in the security analysis grid. You should reflect upon your work and provide estimates of how much you’ve achieved by filling out the grid, which if completed will be allocated 5 marks. There are thus 35 marks for completing the application reasonably, 60 marks for the security features identified and implemented, and 5 marks for self-reflection.

You have a choice of technologies from which to build the application:

* PHP (host it for free on 000webhost)
* Java,
* Python

No other approach is allowed

|  |  |
| --- | --- |
| Task 1 - Develop a secure web form that allows customers to register in the application. They must register an email address, password, name and contact telephone number. The users’ details should be stored in a database. | Code Quality 5 marks |
| Database Design 5 marks |
| Task 2 - Develop a secure login feature. | Code Quality 5 marks |
| Task 3 – Extend the password management feature to provide password strength recommendations and password recovery. | Code Quality 5 marks |
| Task 4 - Implement a “Request Evaluation” web page only accessible to logged in users. This web page should have a comment box to type in the details of the object and their request, and a dropdown box for preferred method of contact between phone or email. | Code Quality 5 marks |
| Task 5 – Extend the “Request Evaluation” page to allow for file upload of a photo of the object | Code Quality 5 marks |
| Task 6 – Implement a page that displays a list of evaluation requests. This page should only be visible to an administrator role | Code Quality 5 marks |

## Submission guidance

You are only submitting the report to the Canvas. The report template is provided below. The template

**Report** - Use the template provided in the Canvas for the report. Provide screenshots of all

the marking criteria elements and annotate where necessary. Use bullet points to

give any explanation. Don’t write paragraphs.

**Report will have**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Excellent (10-9 marks)**  **Student must have gone beyond** | **Good (8-6 marks)** | **Average (5-3 marks)** | **Poor (2-0 marks)** | **Criteria** |
| Policy has no flaw, and its implementation is excellent. Various mechanisms implemented to ensure password policy is secure. | Policy has no flaws, but implementation of policy is simple. | Password policy has very few flaws. However, different sections of policy are implemented and working. | Policy has many flaws for example password is not encrypted, and no salt applied. Password forgot policy has security flaws. | **Password policy 10marks**  Password entropy, encrypted storage, security questions and recovery of password |
| Several countermeasures are implemented, and the quality of countermeasures are excellent. | Countermeasures are implemented in all the pages however quality of implementation is simple. | Implemented countermeasures only in some parts of the application. | Very little effort to implement countermeasures to avoid these vulnerabilities. | **Vulnerabilities 10 marks**  SQL injection, XSS, CSRF, File Upload and any other obvious vulnerability. |
| All the requirements are implemented to authenticate users. Implementation quality is excellent. | All requirements are implemented to authenticate the user. However, quality of implementation is simple. | Only some obvious requirements are not implemented. | Lots of obvious authentication’s requirements are not implemented. | **Authentication 10 marks**  User identity management (registration and login etc), Email verification for registration, 2 factor authentications (PIN and or email), |
| Excellent implementation of countermeasures against these attacks. | No flaws in countermeasures however quality of implementation is simple. | Some flaws in countermeasures | Very little effort against these attacks. | **Obfuscation/Common attacks 10 marks**  Brute force attack – Number of attempts  Botnet attack – Captcha  --------  Dictionary attack/Rainbow table attack |
| Implementation of other security features has no flaws. No obvious security feature is ignored. | Several security features implemented. Implementation has flaws. | Other security features are implemented but obvious ones are ignored. | Very little effort to implement some obvious other security features like storage of confidential information. | **Other security features like confidentiality of important information 10 marks**  For example, identify information that needs to be stored as encrypted. |
| Claimed features are complex. Quality of achievement is excellent. | Claimed features are complex however quality of achievement/implementation could have been better. | Claimed features are somewhat complex and implementation could have been better. | Claimed features are not complex and challenging. | **Deeper understanding, two extra web security 10 marks**  Carry out your investigation and implement two more security features. These need to be complex and challenging one. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **5 marks** | **5 marks** | **5 marks** | **5 marks** | **5 marks** | **10 marks** |  |
| List evaluation-Task6 | Request evaluation – task 5 | Request evaluation – task 4 | Forgot password-Task3 | Login-Task2 | User registration/Database-Task1 | **Features of webs application** |
|  |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **Up to 5 marks** | **0 marks** |  |
| Fully completed | Marking not completed | **Self-reflection** |

# Report

You will be submitting this report to the Canvas.

1) Application URL: URL to your web-application, this can be hosted anywhere. You will need to ensure that it is available till end of Jan.

2) Code file Location. Upload your code to OneDrive and provide a link here. Set up correct permission so that anyone with a link can view it.

3) Test users’ detail: If you don’t provide this, we will not be able to test your work fully.

## Task 0 – Self-reflection

Marking grid filled up by you.

## Task 1 – User registration

Registration feature code screenshots

Database Table

Why do you think it is secure? Use bullet points to provide your reasons and back it up with code snippet from your application.

-

-

-

## Task 2 - Develop a secure login feature.

Login feature code screenshots

Why do you think it is secure? Use bullet points to provide your reasons and back it up code snippet from your application.

## Task 3 - Implement password strength and password recovery

List each password policy element that you implemented and back it up with code snippets from your application

## Task 4 - Implement a “Evaluation Request” web page.

Request Evaluation feature screenshot

Why do you think it is secure?

## Task 5 - Develop a feature that will allow customers to submit photographs

Code of the feature

Why do you think it is secure?

## Task 6 – Request Listing Page

Code of the feature

Why do you think it is secure?