Assignment 2

Developing a Secure Web Application

Assessors: **Ryan Attard**
Assessment Type: **Home assignment**

Assignment Guidelines

Read the following instructions carefully before you start the assignment. If you do not understand any of them, ask your invigilator.

- This assignment is a HOME assignment.
- Fill in and print the assignment sheet and produce a properly structured, neat documentation.
- Copying is Strictly Prohibited and will be penalised according to disciplinary procedures.
- This assignment has a total of 63 marks.
- Deadline is 10/12/2018

Your task is to develop a very simple Music Sharing application. This website will be used by amateur musicians to promote themselves by posting short clips (mp3) online of any composed music. This is a brief listing of the features your client wants to have:

- Users should be able to register and log into their accounts
- User is able to create/ upload a music files
- User is able to share a music clip that should bear a description/title with other members of the website, on which they can leave comments.
- The website should be administered by people who if the see that any music clip shall be blocked/deleted, they can do so.

Please follow the following tasks to guide you building your web application and its documentation.

Task 1 (AA1) – Threat Modelling [7 marks]

Do the Threat Modelling on the scenario of this application. In this process you have to outline clearly the:

a) Assets [1]
b) Trust Levels [1]
c) Entry Points [1]
d) Threats (with STRIDE classification) [2]
e) Mitigation for Threats [2]

Marking scheme	Score
Failure to mention <u>important</u> Assets, Trust Levels, Entry Points, Threats (which 5 are required), proper mitigations for the threats mentioned and Security Requirements will result in loss of the attributed mark. Notation is also important.	

Task 2 (AA2) – DFD [7 marks]

Design a DFD Level 1 of your web application using proper notation

Marking scheme	Score
• Proper notation has to be used • Showing all type of users • Showing all processes	

• Showing all data that is to be input in the system The above have all to be present and properly designed	

Task 3 (SE2)- Development [10 marks]

The following list of countermeasures should be implemented:

- Validation of file types (only mp3 or wav files should be accepted) [1]
- Validation for file size (less than 8mb should be accepted) [1]
- Proper error handling using try-catch and custom errors attribute setting [1]
- Strong Authentication system [1]
- Strong Authorization when you have privileged rights for admin users [1]
- Files uploaded cannot be navigated or downloaded unless the user forging the request has got the required access rights [2]

Develop any other 3 counter measures from the ones listed here: [3]

- Captcha;
- A logging / audit system which saves (error) logs in a structured way;
- A forgot password feature;
- A blocking user feature after 3 failed attempts;
- Code obfuscation of any client-side code;
- Make use of Database Transactions to promote integrity in your features (especially when a user is registering or when allocating permissions to multiple users or when deleting a music clip);

Marking scheme	Score
Marks have already been attributed to every task. If any of the task is not working properly you will lose the associated mark.	

Task 4 (AA5)- Simple Cryptography [7 marks]

One of the requirements is to (symmetrically) encrypt any *querystring* values [3], hash passwords [2] and (show that you know how to) encrypt the connection string inside the *web.config* [2].

Marking scheme	Score
Marks have already been attributed to every task. If any of the task is not working properly or not implemented, you will lose the associated mark.	

Task 5 (SE3)- Advanced Cryptography [10 marks]

Files uploaded should be encrypted using hybrid encryption [6]. When the file is uploaded it should be digitally signed with the user's private key (the user who uploaded the file) and when it is opened/downloaded it should be digitally verified with the signature [4].

Marking scheme	Score
Marks have already been attributed to every task. If any of the task is not working properly you will lose the associated mark.	

Task 6 (KU5) – Identify tools used [5 marks]

You need to identify any tools that need to be set up in order to further protect the database from calls made by low-privileged users in the database context. This means that the user if he manages to discover the username and the password of the connection string and connects directly in the database, cannot for example delete any entries!

Marking scheme	Score
Proper authorization should be implemented for the above feature	

Task 7 (AA3) – Testing [7 marks]

For this task you should develop 2 snippets of code that will individually test 2 functionalities of your friend's core application.

The following are examples of what you can come up with:

- Example 1: You may develop a testing method that will test thoroughly the login functionality of your friend. This method shall try (randomly or systematically) to combine a number of inputs that will be input as username and password and see whether at some point it will return true meaning you have guessed a user account. In other words its like developing an application that will perform a brute force attack on the login method of your friend.

- Example 2: You may develop an application which passes clear data to your friend's encryption method and then the same code should pass the encrypted data to the decryption method and see whether you obtain the original data. Needless to say, you may randomize multiple inputs to check that it works always properly.

The above are just examples given to guide you. You may implement different testing applications such as:

- To test that digital signing really works;
- To test any input fields and their validations in the methods using various combinations;
- To test for any querystrings encryption and decryption;
- Trying to pass a number of different filetypes and check whether they were accepted or not;

Always seek advice from your tutor if you have doubts about implementing something else.

Marking scheme	Score
Your methods contain 3.5 marks each. They should show a meaningful technical implementation that is testing a functionality from the website.	

Task 8 (SE1) – Review [10 marks]

The outcomes from the above methods (in Task 7) should be discussed in a report. Report what you found; positive and negative technical comments should accompany your answer.

Marking scheme	Score

5 marks for each review with flawless arguments and detailed explanation of what you did, why and what was the outcome depending on the code you implemented in Task 7	

Task1 –

AA1	0 marks	1 marks	2 marks	Score
Assets	Missing important assets	All important assets are identified	n.a.	
Trust Levels – 1 mark	Missing important trust levels	All important trust levels are identified	n.a.	
Entry Points -1 mark	Missing important entry points	All important entry points are identified	n.a.	
Threats (with STRIDE classification) – 2 mark	Missing threats (5 should be mentioned) or missing Stride classification	3 valid threats should be mentioned with the majority having proper STRIDE classification	5 valid threats should be mentioned with the majority having proper STRIDE classification	
Mitigation for Threats - 2 marks	Missing or Incorrect Mitigations for the majority of mentioned threats	Half of the mitigations require refinement or correction	All threats have correct mitigations	

Task 2

AA2	0 marks	2 marks	5 marks	Score
DFD – 7 marks	DFD Makes no sense or left out	Proper notation	Showing all entry points and processes	

Task 3

SE2	Score
No Of Functionalities Implemented Correctly:	

Task 4

AA5	0 marks	1 marks	2 marks	3 marks	Score
Encryption of QueryString	Left out	n.a	n.a	Properly done (at least once)	
Encryption of connection string			Properly done	n.a	
Hashing of Passwords			Properly done	n.a	

Task 5

SE3	0 marks	4 marks	6 marks	Score
Hybrid Encryption of files	Left out	n.a	Properly done	
Digital Signing of files	Left out	Properly done	n.a.	

Task 6

KU5	0 marks	2 marks	5 marks	Score
Attend Interview &	Student does not answer to any of the questions asked OR does not attend to interview	Answer half of the questions asked	Answer correctly to all the questions asked	

Task7

AA3	0 marks	3.5 marks	7 marks	Score
Testing Method	Left out or no demonstration that tests were run successfully	Only 1 testing method implemented in such a way that it tests thoroughly a functionality	2 testing methods implemented in such a way that it tests thoroughly a functionality	

Task 8

SE1	0 marks	5 mark	10 marks	Score
Reviews	Left out or not valid	1 review is technical illustrating clearly what have been done in Task 7, why certain methods were applied and what was the student trying to achieve and outcome discussed.	2 reviews are technical illustrating clearly what have been done in Task 7, why certain methods were applied and what was the student trying to achieve and outcome discussed.	