**Task Description**

Together with this task description, you received the following documents:

* **Document 1:** A correct functional specification (user stories) of a system to be developed and its security specifications that contain defects.
* **Document 2:** Security properties related with high-level security requirements.
* **Document 3:** Defects Reporting Form.

You are asked to inspect the security specifications (see document 1). The goal is to identify the following defects.

**DEFECTS TYPES**

**Omission:** Necessary information has been omitted in the security specification.

**Ambiguity:** The security specification has multiple interpretations.

**Inconsistency:** Two or more security specifications are in conflict with one another.

**Incorrect fact**: The security specification is not true under the conditions specified for the system.

Please follow the steps below.

1. When you start the review, please write down the time in the document 3.
2. Read and analyze the user stories and its security specifications (see document 1).
3. Consider the high-level security requirements (see document 2) as a model to verify the security specifications.
4. Record the defects identified in the Defect Report Form (see document 3).
5. When you finish the review, write down the time in the document 3.

**Thank you very much for your participation!**

**DOCUMENT 1**

**A correct functional specification with user stories and its security specifications.**

|  |  |
| --- | --- |
| **User Story 1** | **Security Specification** |
| As a admin, I want to DELETE the personal information of customers so I can keep depured my database. | **1.1** The system shall verify all SQL queries and thus not susceptible to SQL injection. |
| **1.2** The system shall identify the originator of any information before that information is used by the system. |
| **1.3** The system shall protect sensitive data from external attacks using controls such as a host-based firewall or OS patching. |
| **1.4** The system shall implement data validators such as whitelisting, greylisting or blacklisting). |
| **1.5** The system shall ensure that all users have admin permission (to read, write, delete). |

|  |  |
| --- | --- |
| **User Story 2** | **Security Specification** |
| As a user, I want to LOGIN so I can access to certain information. | **2.1** The system shall prevent that the password from being displayed in clear text. |
| **2.2** Failed login attempts shall record for audit trail and incident reporting purposes. |
| **2.3** The system shall encrypt the credentials stored in the database using TLS protocol. |
| **2.4** The system shall only accept complex passwords. |
| **2.5** The system shall restore the user's password for each failed attempt. |

**DOCUMENT 2**

**Security properties related with High-level Security requirements**

|  |  |
| --- | --- |
| **Security Property** | **High-level Security Requirements (HLSR)** |
| **Confidentiality (C)** | C1. Sensitive data shall be protected from unauthorized observation or disclosure both in transit and when stored. |
| C2. System sessions shall be unique to each individual and cannot be shared. |
| C3. System sessions are invalidated when no longer required and timed out during periods of inactivity. |
| C4. TLS protocol shall be used where sensitive data is transmitted. |
| C5. System shall use strong algorithms and ciphers at all times. |
| C6. Users are associated with a well-defined set of roles and privileges. |
| C7. The digital identity of the sender of a communication must be verified. |
| C8. Only those authorized are able to authenticate and credentials are transported and stored in a secure manner. |
| C9. Passwords treatment must include complex passphrases, options to recover and reset the password AND default passwords not allowed. |
| **Integrity (I)** | I1. Any unauthorized modification of data must yield an auditable security-related event. |
| I2. All input is validated to be correct and fit for the intended purpose. |
| I3. Data from an external entity or client shall never be trusted and shall be handled accordingly. |
| **Availability (A)** | A1 The application server shall be suitably hardened from a default configuration. |
| A2 HTTP responses contain a safe character set in the content type header. |
| A3. Backups must be implemented and recovery strategies must be considered. |

**DOCUMENT 3**

**Defects Reporting Form**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Inspection start time: \_\_\_\_\_\_\_\_\_

Inspection end time: \_\_\_\_\_\_\_\_\_

Please register the defects identified.

**Discrepancy List**

Omission ( O ) Ambiguity ( A ) Inconsistency ( IS ) Incorrect (IC)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Location** | |  |  |
| **ID** | **Security Specification** | **HLSR** | **Type** | **Description** |
| **1** |  |  |  |  |
| **2** |  |  |  |  |
| **3** |  |  |  |  |
| **4** |  |  |  |  |
| **5** |  |  |  |  |
| **6** |  |  |  |  |
| **7** |  |  |  |  |
| **8** |  |  |  |  |
| **9** |  |  |  |  |
| **10** |  |  |  |  |
| **11** |  |  |  |  |
| **12** |  |  |  |  |
| **13** |  |  |  |  |
| **14** |  |  |  |  |

**List of Seeded Defects**

|  |  |  |
| --- | --- | --- |
| **Security Specification (SS)** | **Defect Type** | **Description** |
| **1.1** | **Omission** | According to the HLSR I2, all input must be validated, not only SQL queries. Thus, this SS has a defect. |
| **1.2** | **------** | **OK** |
| **1.3** | **Ambiguity** | The SS reflects a weak statement, “such as” indicates an unclear definition of the control to be implemented. |
| **1.4** | **Ambiguity** | The SS reflects a weak statement, “such as” indicates an unclear definition of the control to be implemented. |
| **1.5** | **Incorrect** | All users cannot have admin permissions. |
| **4.1** | **------** | **OK** |
| **4.2** | **------** | **OK** |
| **4.3** | **Omission** | According to HLSR IA3, credentials are transported and stored in a secure manner. However, the SS states only encrypting credentials at rest. |
| **Incorrect** | TLS is not an algorithm. It is a protocol that defines the algorithm to be used. |
| **4.4** | **Omission** | According to HLSR IA4, passwords should not only consider complex password. There are others items to be consider. |
| **Ambiguous** | Complex passwords is ambiguous. Is it a password with capital letter only and special characters? Is it a password with 10 characters length?. |
| **4.5** | **Incorrect** | Restoring the user's password for each failed attempt would not be correct for the user, therefore, this is incorrect. |

|  |  |  |  |
| --- | --- | --- | --- |
| **HLSR** | **User Story** | **Defect Type** | **Description** |
| I1 | 1 | Omission | The high-level security requirement is not defined in the specification. |
| IA1/C6 | 4 | Omission | The high-level security requirement is not defined in the specification. |
| IA2/C7 | 4 | Omission | The high-level security requirement is not defined in the specification. |