TORRENS UNIVERSITY AUSTRALIA

ASSESSMENT 3 BRIEF	
Subject Code and Title	SBD403 Security by Design
Assessment	Case Study Project
Individual/Group	Individual
Length	1,500 Words +/- 10% plus 4-6 minutes presentation with a poster
Learning Outcomes	The Subject Learning Outcomes demonstrated by successful completion of the task below include: a) Apply security by Design industry standard principles in systems development. b) Explain Secure Development Lifecycle models and identify an appropriate model for a given situation. c) Administer implementation of security controls, security risk mitigation approaches, and secure design architecture principles. d) Identify maturity models of secure systems development in the IT work environment. e) Demonstrate capabilities to incorporate security requirements in system specifications, design, development and testing phases of system development.
Submission	12-Week Duration: by 11:55pm AEST/AEDT, Wednesday of week 12 6-Week Duration: by 11:55pm AEST/AEDT, Wednesday of week 6
Weighting	40%
Total Marks	100 marks

Assessment Task

Write a design guide for a web based data retrieval application. This includes rights management, user credential management and secure design pattern

Please refer to the **Instructions** for details on how to complete this task.

Context

Cyber Security relies on well designed and implemented systems and applications. It is a crucial task to create a design document that addresses not only the desired technical features but all security related constraints and design systems. If such a design document lacks clarity and completeness, the resulting implementation is very likely flawed and creates a security risk.

Instructions

You are tasked to create a security design guide for a web based data retrieval application. This design guide must include all required security measures, their references to applicable standards (i.e. OWASP, ISO 27001) and the specification of technical methods, such as encryption algorithms or encrypted data transport. It is not necessary to include technical details on how the system should be coded or how the GUI design should look like. The guide must concentrate on the security aspects of the application.

The application is divided into three parts; Request, Retrieve and Review.

Part 1: Request

Scenario:

Consider a web interface where a user can log into and then request data from a database. The web interface incorporates a login page accessible by a login-button. After a successful login the web interface for the data retrieval is accessible and the interface displays a search field(s) that directly create(s) a SQL query to the database with the information stored (your instructor may demonstrate such an example, as required). The returned information is then displayed as a result to the user.

The data fields on the web interface may include:

- Name
- Address (separate field for unit, street, postal code, state, suburb)
- Phone number

Wildcard searches are often permitted for ‘Name’ and ‘Phone number’ for user convenience.

Task

You must create a security design specification (not a GUI layout or coding) that specifies how the individual fields of the web interface shall be sized and evaluated. It is also required to specify the method of transporting the data from

the web interface to the backend (web and database systems) and how the user authentication shall be performed. It must be specified where the login credentials are stored, how they are stored and what happens if a user tries to login with the wrong credentials. References to relevant standards or reasoning why a specific standard is not being followed is required.

Part 2: Retrieve

Scenario:

Consider an SQL-based database as a case example (note you are not expected to produce SQL codes and a sample database may be demonstrated by your instructor, if required). This database contains all retrievable data and shall only be accessible when a user is successfully logged in. The data stored in the database consists of:

- Name (last name is sufficient)
- Address (separate entries for unit, street, postal code, state, suburb)
- Phone number
- Medical status with one of the following possible entries:
  - Sick
  - Healthy
  - Cancer
  - Deceased
  - Flu
  - Covid
- Credit card data (credit card number and expiry stored as separate fields)

For simplicity, all fields can be formatted as strings.

Task:

In the design document it is mandatory that the appropriate field length is chosen with a detailed explanation of why this length is chosen. It is also mandatory that database security related issues are addressed such as SQL-escaping. Special knowledge of SQL-Databases is not required, you must describe your design choices in plain English. References to relevant standards or reasoning why a specific standard is not being followed is required.

Part 3: Review

A user rights model should exist that permits which user (group) is allowed to see what kind of data. Generally three groups of users must exist:

1. Normal user that only shall see name and address and phone number from the database,

2. Accounting users that can see name, address, phone number and credit card data from the database and
3. Privileged users that can see all data

Task:

The design paper has to address how to identify those users and how to create the individual access rights into the database. Again, it is not requested that you know the actual database programming. Description of the required user roles and general system design is adequate.

Generally, this design paper shall be created with the security concept in mind and not with the technical details. The paper must include the following topics:

- Handling of data input with an explanation for why this form or method is being used
- Prevention of malicious data input
- Prevention of login trials with incorrect credentials by a robot
- The secure storing and retrieving of account credentials
- The rights model and prevention of gaining unwanted rights
- General security designs
- General risk assessment of applications of that type

If encryption algorithms or any other method for ensuring security is required, a detailed specification of that is mandatory. Detailed specification includes possible algorithms and minimum keylength.

If a requirement from one part is needed in another part this must be reflected in the description of the other part, i.e. if the web page requires a secured field in the database this must be described in the database part.

The student shall present their solution(s) with a one-page poster and a 4-6 minutes presentation about the solution.

As preparation, please review all material provided and discussed during the modules 1 – 8. Additional individual research in the library and on the internet is recommended.

Hint: It is a good idea to research the topic of “SQL code injection”.

Hint: If access to the database is defined to require database credentials (username and password), the handling of these credentials in the database itself is not a required part of the assignment.

Applicable standards

The report must include references to applicable standards or industry good practises where appropriate. It is mandatory that the chosen design is compared to the relevant standards and, where it is divergent, to be explained why the standard is not followed.

Referencing

Referencing is essential for this assessment. A minimum of one reference for each topic is required for this, including at least 8 academic sources.

(An academic source is one that has been peer-reviewed).

Your references will be evaluated for their relevance to the case study. Remember you must ensure that your arguments and justifications are based on sound reasoning and clear relevance.

Ensure that you reference according to the appropriate APA style, for citing and referencing information, as well as all appropriate research sources.

Please see more information on referencing here: http://library.laureate.net.au/research_skills/referencing

Submission Instructions

Submit your **Assessment 3 Report** via the **Assessment** link in the main navigation menu in SBD403 Secure By Design. Please name your file in the following format: Lastname_First initial_course code_assessment number, e.g., Smith_A_SBD403_A3. The Learning Facilitator will provide feedback via the Grade Centre in the LMS portal. Feedback can be viewed in My Grades.

NOTE: The poster has to be submitted one week prior to the presentation date via the **Assessment** link in the main navigation menu in SBD403 Secure By Design. Please name your file in the following format: Lastname_First initial_course code_poster_assessment number, e.g., Smith_A_SBD403_poster_A3.

The presentation is online with a date set forth by the assessor. All three group members have to be present and present their individual part of the paper and poster.

Academic Integrity

All students are responsible for ensuring that all work submitted is their own and is appropriately referenced and academically written according to the Academic Writing Guide. Students also need to have read and be aware of Torrens University Australia Academic Integrity Policy and Procedure and subsequent penalties for academic misconduct. These are viewable online.

Students also must keep a copy of all submitted material and any assessment drafts.

Special Consideration

To apply for special consideration for a modification to an assessment or exam due to unexpected or extenuating circumstances, please consult the Assessment Policy for Higher Education Coursework and ELICOS and, if applicable to your circumstance, submit a completed Application for Assessment Special Consideration Form to your Learning Facilitator

TORRENS UNIVERSITY AUSTRALIA

Assessment Rubric

Assessment Attributes	Fail (Yet to achieve minimum standard) 0-49%	Pass (Functional) 50-64%	Credit (Proficient) 65-74%	Distinction (Advanced) 75-84%	High Distinction (Exceptional) 85-100%
Knowledge and understanding of secure storing of user credentials and user rights model Keywords are: • Encrypted passwords • Explicit user database • Secure encryption mechanism	Demonstrates a partially-developed understanding of secure storage of data by: • Not using encryption • No separation of user credentials database and actual data database • No rights model for	Demonstrates a functional knowledge of secure storage of data by: • Using encryption but with unspecified or weak algorithm • A basic rights model is described	Demonstrates proficient knowledge of secure storage of data by: • Using encryption and specifying an adequate algorithm • The rights management is basic but a model for ensuring that users belong to a (rights) group	Demonstrates advanced knowledge of secure storage of data by: • Encryption is used for user credentials with a strong algorithm • User and group rights model is present with detailed description of chosen design	Demonstrates exceptional knowledge of secure storage of data by: • Encryption with strong algorithms is used for all kind of data, user credentials and actual data • User and group rights are well defined and

for password (i.e. sha2-256) • User rights • Group model **Percentage for this criterion = 30%**	user groups • No definition of user and user groups		is described	• Some reasoning for the security design is present	implemented • Extensive reasoning for the security design is presented
Secure set up of the database and database retrieval Keywords • Maximum field length for database fields • Mechanisms for preventing field	Demonstrates a partially-developed understanding of secure databases by: • No use of encryption • No checks for database field overflows • Insufficient database field length and no explanation of	Demonstrates a functional knowledge of secure databases by: • Use of encryption with weak or unspecified algorithm • No checks for database field overflows • Sufficient database field	Demonstrates proficient knowledge of secure databases by: • Use of encryption with adequate algorithm • Not all fields are encrypted • Checks for database field	Demonstrates advanced knowledge of secure databases by: • Use of encryption with adequate algorithm • Not all fields are encrypted, just the sensitive ones • Checks for	Demonstrates exceptional knowledge of secure databases by: • Use of encryption with adequate algorithm • All fields are encrypted or whole database storage is

overflows • SQL query system which prevent code injection • Encryption of all data fields **Percentage for this criterion = 25%**	chosen length • No checks for SQL code injection	length but no explanation given • No SQL code injection prevention	overflows • Sufficient database field length but insufficient/no explanation • SQL code injection for some fields but not all	database field overflows • SQL code injection prevention throughout • Sufficient database field length with reasonable explanation	encrypted • Checks for database field overflows • SQL code injection prevention throughout • Sufficient database field length with reasonable explanation

Web page operation Keywords • Maximum allowed number of login failures and result of that • Storage and use of database credentials • Search field limits • Secure wild card handling **Percentage for**	Demonstrates a partially-developed understanding of secure databases by: • No checks for maximum login retries at all • Database credentials are stored in code unencrypted • Search field boundaries are not defined nor checked • Wild card handling is not defined	Demonstrates a functional knowledge of secure databases by: • Checks for maximum login retries but no explanation what should be the result of that • Database credentials are stored in code in clear text • Search field boundaries are defined but not checked • Wild card handling is not defined	Demonstrates proficient knowledge of secure databases by: • Checks for maximum login retries with explanation what should be the result of that • Database credentials are stored in code but encrypted • Search field boundaries are defined and checked • Wild card handling is defined	Demonstrates advanced knowledge of secure databases by: • Checks for maximum login retries with explanation what should be the result of that • Database credentials are not stored in code no mentioning of encryption • Search field boundaries are defined and checked • Wild card handling is defined	Demonstrates exceptional knowledge of secure databases by: • Checks for maximum login retries with explanation what should be the result of that • Database credentials are not stored in code and are encrypted with the database encryption algorithm (specified) • Search field boundaries are defined and checked, error handling is described

this criterion = 30%					• Wild card handling is defined and executed
Effective Communication (Written) **Percentage for this criterion = 5%**	Presents information. No detailed explanation is presented. Specialised language and terminology is rarely or inaccurately employed. Meaning is repeatedly obscured by errors in the communication of ideas, including errors in structure, sequence, spelling, grammar, punctuation and/or the acknowledgement of sources.	Communicates in a readable manner that largely adheres to the given format. Detailed explanation is rarely given but present. Generally employs specialised language and terminology with accuracy. Meaning is sometimes difficult to follow. Information, arguments and evidence are structured and sequenced in a way that is not always clear and logical. Some errors are evident in spelling, grammar and/or punctuation.	Communicates in a coherent and readable manner that adheres to the given format. Accurately employs specialised language and terminology. Meaning is easy to follow. Information, arguments and evidence are structured and sequenced in a way that is clear and logical. Occasional minor errors present in spelling, grammar and/or punctuation.	Communicates coherently and concisely in a manner that adheres to the given format. Accurately employs a wide range of specialised language and terminology. Engages audience interest. Information, arguments and evidence are structured and sequenced in a way that is, clear and persuasive. Spelling, grammar and punctuation are free from errors.	Communicates eloquently. Expresses meaning coherently, concisely and creatively within the given format. Discerningly selects and precisely employs a wide range of specialised language and terminology. Engages and sustains audience's interest. Information, arguments and evidence are insightful, persuasive and expertly presented. Spelling, grammar and punctuation are

					free from errors.
Effective Communication (Presentation/Oral) **Percentage for this criterion = 5%**	Difficult to understand for audience, no logical/clear structure, poor flow of ideas, argument lacks supporting evidence. Specialised language and terminology is rarely or inaccurately employed. Stilted, awkward and/or oversimplified delivery. Limited use of engaging presentation techniques. (e.g. posture; eye contact; gestures; volume,	Presentation is sometimes difficult to follow. Information, arguments and evidence are presented in a way that is not always clear and logical. Employs some specialised language and terminology with accuracy. Correct, but often stilted or awkward delivery. Sometimes uses engaging presentation techniques (e.g. posture; eye contact; gestures; volume, pitch	Presentation is easy to follow. Information, arguments and evidence are well presented, mostly clear flow of ideas and arguments. Accurately employs specialised language and terminology. Correct, but occasionally stilted or awkward delivery. Uses engaging presentation techniques (e.g. posture; eye contact; gestures; volume, pitch and pace of	Engages audience interest. Information, arguments and evidence are very well presented; the presentation is logical, clear and well-supported by evidence. Accurately employs a wide range of specialised language and terminology. Clear and confident delivery. Confidently and consistently uses a range of engaging presentation	Engages and sustains audience interest. Expertly presented; the presentation is logical, persuasive, and well- supported by evidence, demonstrating a clear flow of ideas and arguments. Discerningly selects and precisely employs a wide range of specialised language and terminology. Clear, confident and persuasive delivery. Dynamic, integrated and professional use of a wide range of

	pitch and pace of voice) Presentation aids are not employed or developed as directed.	and pace of voice) Employs basic, but generally accurate presentation aids as directed. A number of aspects require further refinement (e.g. amount of information, styling, editing, etc.).	voice) Employs clear and somewhat engaging presentation aids as directed. A few aspects require further refinement (e.g. amount of information, styling, editing, etc.).	techniques (e.g. posture; eye contact, expression; gestures; volume, pitch and pace of voice; stance; movement) Employs succinct, styled and engaging presentation aids that incorporate a range of elements (graphics, multi-media, text, charts, etc.).	engaging presentation techniques (e.g. posture; eye contact, expression; gestures; volume, pitch and pace of voice; stance; movement) Employs succinct, creative and engaging presentation aids that effectively integrate a wide range of elements (graphics, multi-media, text, charts, etc.).
Correct citation of key resources and evidence **Percentage for this criterion = 5%**	Demonstrates inconsistent use of good quality, credible and relevant resources to support and develop ideas. Referencing is omitted or does not resemble APA.	Demonstrates use of credible and relevant resources to support and develop ideas, but these are not always explicit or well developed. Referencing resembles APA, with frequent or	Demonstrates use of credible resources to support and develop ideas. Referencing resembles APA, with occasional errors.	Demonstrates use of good quality, credible and relevant resources to support and develop arguments and statements. Show evidence of wide scope within the	Demonstrates use of high-quality, credible and relevant resources to support and develop arguments and position statements. Show evidence of wide scope within and

		repeated errors.		organisation for sourcing evidence. APA referencing is free from errors.	without the organisation for sourcing evidence. APA referencing is free from errors.

The following Subject Learning Outcomes are addressed in this assessment	
SLO a)	Apply security by Design industry standard principles in systems development.
SLO b)	Explain Secure Development Lifecycle models and identify an appropriate model for a given situation.
SLO c)	Administer implementation of security controls, security risk mitigation approaches, and secure design architecture principles.
SLO d)	Identify maturity models of secure systems development in the IT work environment.
SLO e)	Demonstrate capabilities to incorporate security requirements in system specifications, design, development and testing phases of system development.