Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2015/2016

COURSE NAME	:	SYSTEM SECURITY
COURSE CODE	:	BIS 33503
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JUNE / JULY 2016
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **FOUR (4)** PAGES

SECTION A

Q1 Match these OWASP best practices checklist (on the left) to its correct checklist header (on the right).

Item	OWASP best practices checklist
1	Remove unnecessary default vendor content (e.g., sample schemas)
2	Disable any default accounts that are not required to support business requirements
3	The application should connect to the database with different credentials for every trust distinction (e.g., user, read-only user, guest, administrators)
4	Restrict access to logs to only authorized individuals
5	Utilize a master routine for all logging operations
6	Do not store sensitive information in logs, including unnecessary system details, session identifiers or passwords
7	Conduct all encoding on a trusted system (e.g., The server)
8	Utilize a standard, tested routine for each type of outbound encoding
9	All cryptographic functions used to protect secrets from the application user must be implemented on a trusted system (e.g., The server)
10	Protect master secrets from unauthorized access

Item	OWASP checklist header (group)
A	Database Security
B	Error Handling and Logging
C	Output Encoding
D	Cryptographic Practices

(20 marks)

Q2 Explain the following techniques used for database security and give **ONE (1)** example for implementing each of this techniques.

(a) Authorization

(b) Audit Trail

(c) Backup

(d) Access Control

(e) View

(20 marks)

Q3 Discuss any **FIVE (5)** Information Communication Technology (ICT) related risks to be treated using Risk Treatment Plan in **Table Q(3)** below. Example of one of the risk treatmet is given below.

Table Q(3)

RISK IDENTIFICATION	RISK TREATMENT			
Event	**Action**	**Plan**	**Risk Owner**	**Resolved by**
Rogue (illegal) wifi AP is put in UTHM	Reduce	Buy 5 % of AP with anti-rouge AP management from total number of wifi AP in UTHM to jam the signal from rogue wifi AP signal within UTHM (in main campus and at hostels). Only allowed UTHM legal wifi AP to operate.	IT Department	31 Dec. 2016

(20 marks)

Q4 Currently, your organization have over 50 systems consisting of mostly online applications and client-servers systems which use Oracle database. There is a new tender exercise for reevaluating existing database. Three databases are proposed namely Oracle, Tibero and Cassandra in this tender exercise. As an IT Officer for this organization, you are required to **EVALUATE** the best database for the organization. Justify your answers by giving **FOUR (4)** strong points to support your evaluation.

(20 marks)

Q5 You are responsible for implementing secure coding best practices in your company. Outline **FIVE (5)** best practices checklist focusing on **data protection** for the secure coding implementation in your company.

(20 marks)

- END OF QUESTION –