

**P.G. DIPLOMA IN INFORMATION SECURITY
(PGDIS)**

Term-End Examination

00084

December, 2014

**MSEI-025 : APPLICATION AND BUSINESS SECURITY
DEVELOPMENTS**

Time : 2 hours

Maximum Marks : 50

Note :

Section A – Answer all the objective type questions.

Section B – Answer all the very short answer type questions.

*Section C – Answer any **two** questions out of three short answer type questions.*

*Section D – Answer any **two** questions out of three long answer type questions.*

SECTION A

Answer all the objective type questions.

1. _____ is the recommended best practice for input validation. All input may only pass, if it is validated as known good input. 1

2. CSS stands for _____ . 1

3. MTA stands for _____ . 1
4. RFID stands for _____ . 1
5. _____ testing is also known as clear box testing. 1
6. _____ attacks are aimed at application components that take data as input and pass it to memory buffer for later use and manipulation. 1
7. ECB, CBC, CFB and OFB are four block cipher functions. 1
 - (a) True
 - (b) False
8. _____ security allows individual user or organisation to secure traffic for all applications without having to make any notifications to the applications. 1
9. To secure the channel from the application server to SQL server use _____ . 1
10. For _____, well documented coding standards will aid the creation of "Test Scripts". 1

SECTION B

Answer all the very short answer type questions.

11. How does web allocation work ? 2
12. Define buffer overflow attacks. 2
13. Write a short note on securing the server operating system. 2
14. How does time stamping work ? 2
15. Write a note on automated source code analysis. 2

SECTION C

Answer any 2 questions out of the 3 short answer type questions.

16. What is OCTAVE ? What are the limitations of using OCTAVE ? 5
17. What necessary steps should be taken for securing the Web server ? 5
18. Write pros and cons for both the testing techniques. 5

SECTION D

Answer any 2 questions out of 3 long answer type questions.

- 19.** Define the following : *2×5=10*
- (a) File-level security
 - (b) Application security
 - (c) Physical security
 - (d) Disk encryption
 - (e) Taking backup
- 20.** What are the major types of Web application attacks ? *10*
- 21.** Explain the methods of Encrypting data. *10*