

B4.5-R4: INTERNET TECHNOLOGY AND WEB SERVICES

NOTE:

1. Answer question 1 and any FOUR from questions 2 to 7.
2. Parts of the same question should be answered together and in the same sequence.

Time: 3 Hours

Total Marks: 100

1.
 - a) Explain IPV6 packet header format with an example.
 - b) Explain in brief on the 3-Tier Web Architecture.
 - c) Explain the 'Request object' and 'Response object' in ASP with one example each.
 - d) Explain in brief on structure of Perl programming language.
 - e) Explain in brief on Web Service Protocol Stack.
 - f) Write different procedures to connect MySQL database connectivity with PHP scripting as front-end in a Web-based development environment. Explain with an example.
 - g) Explain 'SQL Injection Attack' with an example

(7x4)

2.
 - a) Explain TCP/IP Protocol Stack and mapping with layers of OSI reference model.
 - b) How HTTPS protocol works to ensure secure communication? Compare the same with HTTP communication.

(9+9)

3.
 - a) What is the role of a Web Server Gateway Interface?
 - b) Differentiate between IIS and Apache Web servers?
 - c) What is XML? Explain in details on XML Schemas along with validation.

(3+6+9)

4.
 - a) Explain on Client-side scripting and Server-side scripting with request to a small Web-application.
 - b) What is ActiveX control and how it works? Explain with an example.

(9+9)

5.
 - a) Write and explain the Objects of Web Services Description Language (WSDL).
 - b) What is Voice over IP? Explain how quality of service ensured?

(9+9)

6.
 - a) Explain in details on Virtual reality.
 - b) What do you understand about LAMP and WAMP Technologies that are being used in a Web application development? Write merits and limitations of both Technologies.

(9+9)

7. Explain the following vulnerabilities that occur in a Web-based Application Development. Explain the same on how to gate such vulnerabilities?
 - a) Un-validated Input
 - b) Broken Account and Session Management
 - c) Cross-Site Scripting (XSS) Flaws
 - d) Buffer Overflows
 - e) Injection Flaws
 - f) Denial of service

(18)