APJ Abdul Kalam Technological University
First Semester M.Tech Degree Examination January 2016
Ernakulam II Cluster

COMPUTER SCIENCE AND ENGINEERING
Specialization: COMPUTER SCIENCE AND ENGINEERING

05CS 6011 – WEB SECURITY

Time: 3 hrs.   Max. Marks: 60

I.
   a) Describe the common encoding schemes used in Web Applications.   (5 Marks)

   b) How can you gather login information from a web application using brute force attacks?
                                                                                        (7 Marks)

II.

a) You are trying to exploit a SQL injection flaw by performing a UNION attack to retrieve data. You do not know how many columns the original query returns. How can you find this out?   (6 Marks)

b) You have submitted a single quotation mark at numerous location through-out the application. From the resulting error messages you have diagnosed several potential SQL injection flaws. Which one of the following would be the safest location to test whether more crafted input has an effect on the application's processing?

     (i) Registering a new user

     (ii) Updating your personal details

     (iii) Unsubscribing from the service

                                                                                        (5 Marks)

c) You have found a SQL injection vulnerability in a login function, and you try to use the input ' or 1=1-- to bypass the login. Your attack fails, and the resulting error message indicates that the -- characters are being stripped by the application's input filters. How could you circumvent this problem?   (1 Mark)

III.

 a) If someone is able to exploit a hole in a web application to execute files with the privileges of the Apache server program then the attacker will not be able to access the rest of the file system. Explain how can we restrict this type of access?   (12 Marks)

b) Write the methods to block spam phrases?   (6 Marks)

<div align="center">OR</div>

IV. How does Cross site scripting work and also how to protect a server from Cross site scripting?

                                                                               (18Marks)

V.

   a) Data is stored in the cloud .Do we still need Cloud penetration testing?   (9 Marks)

   b) Why is foot printing necessary? Specify the steps that a hacker must follow to make a foot print of an organization   (9 Marks)

<div align="center">OR</div>

VI.

   a) Security is important in cloud Environment. Specify few design principles for securing the cloud?   (10 Marks)

   b) If you are a victim of Denial of Service (Dos) then what you do?   (8 Marks)