CSC 439/539: Advanced Information Security, Spring 2013
Instructor: Dr. Natarajan Meghanathan
Sample Questions on Module 6 Web Security

Web Security

1) Briefly explain the motivation to use web cookies? What are the two types of web cookies? How are they used?
2) Explain the two significant security features in web cookies.
3) What is the impact of DNS cache poisoning on web security? Explain with an example.
4) What are the characteristics of the two types of active code models for execution at the client side? Which one do you recommend and why? Explain.
5) What are the two types of XSS attacks? Explain their basic principle as well as the difference between the two attacks.
6) Briefly explain using an example [you need not explain with the actual code for php; however use the java script code as and when needed to explain the idea], how can the following attacks be conducted:
    a. Persistent XSS attack
    b. Non-persistent XSS attack
    c. Standalone XSRF attack
    d. XSRF attack in coordination with a persistent XSS attack
7) What could be the strategy of an attacker to make his scripting code look less obvious while launching an XSS attack?
8) What is the primary difference between XSS and XSRF attacks?
9) What is the implicit advantage in using the POST method, rather than the GET method, of data retrieval in web pages?
10) Explain the three potential solutions that were discussed in class to combat XSRF attacks.
11) Briefly explain the idea behind using the CAPTCHA kind of challenge-response authentication in websites. What is its use?
12) What are the different strategies one can adopt to protect against XSRF attacks: (i) as a user, (ii) as a developer.

SQL Injection attacks

13) Consider the SQL query statement below. What values could be passed for the username and password fields to successfully execute the query even without knowing either the username or the password?

    Statement = "SELECT * FROM 'CustomerDB' WHERE 'name' = ' "+ userName + " '
    AND 'password' = ' " + passwd + " ' ; "

14) Consider the SQL query statement below. How would use only the username field (and not the password field) along with the comment (--) operator and trigger a SQL code injection attack? You need to write an appropriate query statement that could be used to launch the attack.

    Statement = "SELECT * FROM 'CustomerDB' WHERE 'name' = ' "+ userName + " '
    AND 'password' = ' " + passwd + " ' ; "

15) Consider the following query. Show, using multiple SQL statements per execution, how you can exploit the lack of strong type checking and launch an injection attack leading to deletion of a table (say 'USERS' table) in the DBMS.

    Statement = "SELECT * FROM 'CustomerDB' WHERE 'id' = " + userID +";"