CSC 438 Systems and Software Security, Spring 2014
Instructor: Dr. Natarajan Meghanathan
Question Bank for Module 9: SQL Injection Attacks and Multi-level Database Security

1) What is referred to as an "Inference Attack" on a database? Which kind of SQL queries are often misused to cause this attack?

2) What are the three solutions that we discussed to counter Inference Attacks? Explain their operating principle and the associated tradeoffs (advantages and disadvantages), if any.

3) Consider the table below. Show how using innocuous SQL queries (explain the sequence of queries and what they are expected to return) that individually return non-sensitive data, one can reveal sensitive information such as the salary of user Sheila Smith?

Name	Sex	Title	City	State	Salary
Bob Kelly	M	DBA	Atlanta	GA	$75,000
Sheila Smith	F	Receptionist	Chicago	IL	$30,000
Alex Ryder	M	Salesman	Dallas	TX	$45,000
Yousuf Khan	M	Programmer	Houston	TX	$70,000
Laura Richards	F	Consultant	Detroit	MI	$65,000
Michelle Donald	F	Director	Los Angeles	CA	$85,000

4) Consider the table shown below. Show how using innocuous SQL queries (explain the sequence of queries and what they are expected to return) that individually return non-sensitive data, one can reveal sensitive information such as (i) financial aid received by student 'Adams' and (ii) Race of student 'Adams'?

Name	Sex	Race	Aid	Fines	Drugs	Dorm
Adams	M	C	5000	45.	1	Holmes
Bailey	M	B	0	0.	0	Grey
Chin	F	A	3000	20.	0	West
Dewitt	M	B	1000	35.	3	Grey
Earhart	F	C	2000	95.	1	Holmes
Fein	F	C	1000	15.	0	West
Groff	M	C	4000	0.	3	West
Hill	F	B	5000	10.	2	Holmes
Koch	F	C	0	0.	1	West
Liu	F	A	0	10.	2	Grey
Majors	M	C	2000	0.	2	Grey

5) What is a SQL View? How different it is from a table? What is the use of SQL Views to avoid Inference Attacks? Discuss any potential tradeoff.

6) What is a "Virtual Private Database"? How is it different from "SQL Views"?

7) Explain the functioning of a row-wise VPD vis-à-vis a column-wise VPD. What is the advantage associated with the latter?

8) Explain the principle behind Multi-Level Secure (MLS) databases and how it could lead to polyinstantiation? You can choose an appropriate simple example to put forth your explanation.

9) What is meant by polyinstantiation in the context of a MLS database? Explain the advantage(s) and disadvantage(s) that it brings with.

10) What is the difference between visible and invisible polyinstantiation?

11) Assume a database has 4 records (rows), each represented at a unique security clearance level. Consider the four security clearance levels to be: Top Secret, Secret, Confidential and Unclassified. If invisible polyinstantiation is allowed, then what would be the maximum number of records in the database?

12) 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 + " ' ; "

13) 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 + " ' ; "

14) 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 +";"

15) What vulnerabilities cannot be exploited in MySQL with regards to injection attacks?

16) Explain the use of Parameterized Statements to prevent SQL injection attacks.

17) Briefly describe the two solutions (other than the use of Parameterized Statements) discussed in class to prevent SQL injection attacks.

18) Consider a database system that uses server-side column-wise VPD to control inference attacks. Let the following table *Employee* be part of this system. Assume that the *Salary* column is the only column that is categorized to be sensitive (the rest of the columns are not sensitive).

Name	Age	Salary	Sex	State
John Peters	30	$4,500	M	MI
Michael Roberts	23	$2,300	M	AL
Edward Perkins	28	$5,000	M	NY

Let user Michael Roberts launch the following two queries. What would be the output of each of these queries? Explain how these queries would be executed at the server side.
(a) Select Average(Salary) from Employee where Sex = 'M';
(b) Select Average(Age) from Employee where Sex = 'M';