Research Week 05

Chaz Davis

February 8, 2020

1 What is a relational database and what are its principal ingredients?

Relational database is a set of multiple data organized by tables, records, and columns and it creates the relationship between the database tables.

- the principal ingredients for a relational database
  - the main ingredient is a table
  - the table contains the set of data that consists of rows and columns
  - Rows are reffered as the tuples of records
  - columns are reffered to as attributes
  - the primary key is used for unique identification of a row in a table

2 How many primary keys and how many foreign keys may a table have in a relational database?

In a relational database. a primary key is a key that is used for identifying and defining the characteristics uniquely for each row. A primary key may have a single attribute or multiple attributes. a foreign key attribute of one table is a foreign key for another table. In a logical way, the foreign key is used to establish a link between two tables.

3 Explain the nature of the inference threat to an RDBMS.

An inference threat is the process of doing the authorized queries and collect the unauthorized data from the legal response received. it is related to database security. The problem of inference arises from when the grouping of the number of data items is more sensitive than the data item of individual or grouping the data items can be used to deduce the higher sensitivity of data.

4 What are the disadvantages of database encryption?

There are two difficulties for database encryption:
Key management - only authorized users are allowed to access the decryption key for data. Because, database is typically accessed by a large number of users and applications. So, database encryption is a complex task to provide the security keys to those selected portion of database to authorized users and applications.
Inflexibility - database encryption is more complex to search the records in database when the part of the database or entire database is encrypted.

5 What is an SQLi? How does one attack using this method?

There are several types of SQL injection attacks: in-band SQLi (using database errors or UNION commands), blind SQLi, and out-of-band SQLi.

6 Define Defensive coding.

Defensive Coding is developing a system that behaves in a predictable manner despite unexpected conditions or inputs. Defensive coding can generally be broken down into three main areas. Clean Code. Testable Code. Validation.

7 What is an attribute in a database. Give an example.

An attribute is a characteristic. It is a database component, such as a table. It may be a database field or instances in the row of a database.

8 Explain cascading authorizations. Is there a "downside " to this method of security?

Cascading Authorization is a grant option that allows the access rights to cascade through the multiple users. When the user has an access rights of the grant option to another user. Therefore, passing the access rights of the grant option of certain tables to multiple users in a cascade manner, known as cascading authorization.

9 What is an in-band attack? Is there such a thing as an out-of-band attack?

In-band SQLi is the most common and easy-to-exploit of th SQL injection attacks. In-band injection occurs when an attacker is able to use the same communication channel to both launch the attack and gather results. There is such a thing as Out-of-band injection. Its not very common, mostly because it depends on features being enabled on the database server being used by the web application. Out-of-band injection occurs when an attacker is unable to use the same channel to launch the attack and gather results.

10 What is "blind" SQL injection?

Blind SQLi is also called boolean based injection. It is an inferential injection technique that relies on sending a SQL query to the database which forces the application to return a different result depending on whether the query returns a TRUE or FALSE result. Depending on the result, the content within the HTTP response will change, or remain the same. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow since an attacker would need to enumerate a database, character by character.