**INFORMATION SYSTEM**

**QUESTIONS**

1. Discuss hacking database server
2. Describe how to use oracle worm
3. Describe steps for performing SQL injection techniques
4. Describe SQL injection techniques
5. Describe SQL injection oracle
6. Describe SQL injection in my SQL

**ACRONYMS**

SQL -Structured Query Language

SQLi -Structured Query Language injection

WORM -write-once-read-many

PL/SQL - Procedural Language/ Structured Query Language

HTML- Hypertext Markup Language

BSQL-Block Structured Query Language

1. **Discuss hacking database server**

Hacking is an act of compromising digital devices and networks by identifying the weakness, so as to gain unauthorized access to their data. Database hacking therefore can be define as the act of identifying and exploiting the weakness of a computer or server of a company so as to gain unauthorized access to the database of an organization and obtain the information of interest. When database server is hacked, then the database security is compromised and hence this is referred to as hacking of the database server.

Different developers have come up with different software that can be used to hack different database systems depending on the type of database. These software are used to skillfully have a random (get in and out) access to the database without the knowledge of the organization. Such software includes the following: brute forcing, SQL(Structured Query Language) injection, packet sniffing etc.

It is therefore important to put in to place the appropriate arrays of tools, controls and procedure to ensure that the confidentiality, integrity and accessibility of the database is enhanced.

1. **Describe how to use oracle worm**

The write-once-read-many (WORM) technology is one common application used in many organization for data integrity **(**[***Http://doc/oracle.com***](http://doc/oracle.com)***)*.** There are different types of worm files that can be created; but the most common types include the following; crypto worms, Email worms, Internet worms applications. Our main focus here is oracle worm and how it works. ***Oracle is software used to make database management systems which are used to create and manage systems*** In his article “Oracle warm may become a threat”, Don Burleson explained that the Oracle at times referred to as “voyager” worm is a primitive worm that is not a dangerous worm that can be enhanced to become self-propagating. This makes it clear that the worm can be manipulated to allow the hacker to gain access to the username and password of an individual and hence it is a malicious threat to the database security.

Quoting the DBA village, Burleson explained that the worm is written in PL/SQL (Procedural Language/ Structured Query Language) where the Oracle worm accesses the details. He further outlines that the accounts that use default password have high chances of being invaded by this worm. It is important to understand how this worm works.

1. The worm uses the utl\_indaddr procedure to obtain the IP address of the server where the database information.
2. The worm then scans all the addresses in the same range of network and checks on the active listerner on other server.
3. Each active listener responds with the $ORACLE\_SID and Voyager hence obtains three things (protocol, IP Address, ORACLE\_SID) needed for it to access the database through TNS
4. Voyager then issues a series of log-on attempts using the oracle installer default user/ID combination (prior to 10g).This includes the “system/manager” and sys/change\_on\_install”.
5. **Describe steps for performing SQL injection techniques**

SQL injection is one of the most common hacking techniques where a malicious code is introduced in a SQL statement via webpage input. SQL injection occurs when one is require giving username or userid but instead, giving an SQL statement that when run on the database, it introduces the code to the webpage.

The following are the procedure /steps of SQL injections

1. The attacker looks for the webpage that can allow one to submit data by login page, search page, etc. or a page that will displays the HTML commands such as GET by checking the source code of the site.
2. For one to check the source code of a website, Right click on the webpage then click on “**view source**”.

The source code will be displayed in the notepad of the HTML, then looks for “FORM” tag in the HTML code. The codes between the <FORM> and </FORM> hare said to have potential parameters that if manipulated can be used to find the vulnerability of the webpage.

1. When a single quote is put under the text box provided on the webpage, it will accept the user username and password. This will checks if the user input variable is protected or interpreted by the server

When an error message such as use “a”= “a” is displayed, then the website is said to be at risk of an SQL Injection attack.

1. Finally the attacker will use SQL command such as SELECT statement command to obtain data from the database or INSERT statement to add information to database
2. **Describe SQL injection techniques**

SQL injection techniques used to inject or introduce the malicious code into the webpage.it can be divided into three main categories. The categories include the following:

1. **In-band SQLi**- this is where the attacker uses the same channel of communication to channel their attack due to the simplicity of the SQL injection. There are two types of In-band SQLi namely: error **based SQLi and union based SQLi.**
	* 1. ***The error based SQLi***- the attacker causes the database to cause error and uses the information obtained from the error to get access to the database.
		2. ***Union based SQLi***- on the other hand the attacker uses the union operator to combine the benign SQL statement with a malicious statement
2. **Inferential (Blind) SQLi**- this is where the attacker is able to construct the database by sending payload, and then observe the response from the web application and the resulting behavior of the database server.it is called blind SQLi since the attacker does not see the information from the database transferred to their system. Inferential SQLi is categorized into two i.e.
	* 1. ***Boolean***- the attacker sends an SQL code to the database which is supposed to return a true or false statement. The feedback that the attacker gets from then database can be unchanged or modified. The attacker then works with the true or false statement that comes as a result.
		2. ***Time-based***- as the name suggests, the attacker sends an SQL code to the database which takes time before sending a true or false results. During this wait time the attacker can see if the feedback will be true or false and the message can be generated instantly or after some wait time. The attacker then manipulates the results accordingly.
3. **Out-of-band SQLi** – for the attacker to use this technique, some features of the database must be enabled on the web page otherwise the attacker may not modify it to its advantage. This technique depends on the capacity of the server to create an HTTP request to send information to the attacker.
4. **Describe SQL injection oracle**

This is a hacking technique used by the attacker, whereby they inject unexpected text in dynamically-constructed SQL statement, which compromise the security of the database

The code injected tries to minimize the calls of the database and hence maximize the chances of the activities of the attacker. The most common tool used by the attacker is an open source tool called BSQL hacker, used to discover weak point of the database. BSQL uses data from finger prints database, user details and permission, then change the attackers permission to database admin which allows them to obtain available data from the database.

This can be prevented using different techniques which include; validation of the input, statement of the statics, minimum permission, encryption of confidential data etc.

1. **Describe SQL injection in my SQL**

SQL injection as said earlier is the introduction of a malicious code into the database via a webpage.

There are different techniques used by the attacker to obtain the details of the database. These techniques as discussed in question (4) above includes: in-band SQLi, which is categorized into error-based SQLi and union based SQLi. inferential (Blind) SQLi which is divided into Boolean SQLi and Time-based SQLi and lastly Out-of-band SQLi.

There is much similarity between the SQLi in my SQL and Oracle. The main difference is in the techniques used by the attacker to obtain details in from the database.

**REFERENCE**

Burleson, Donald K. *Oracle High-Performance SQL Tuning*. McGraw-Hill Education, 17 Aug. 2001.

Burleson, Donald K. *Oracle9i High-Performance Tuning with STATSPACK*. McGraw-Hill Education, 12 Apr. 2002.

Arup Nanda, and Steven Feuerstein. (2006) *Oracle PL/SQL for DBAs*. Beijing O’reilly 9780596005870

<https://www.w3schools.com/sql.com>.

[***Http://doc/oracle.com***](http://doc/oracle.com)