1. SQL injection is an attack in which _____ code is inserted into strings that are later passed to an instance of SQL Server.
*a) malicious
b) redundant
c) clean
d) non malicious

2. Point out the wrong statement.
a) SQL injection vulnerabilities occur whenever input is used in the construction of an SQL query without being adequately constrained or sanitized
b) SQL injection allows an attacker to access the SQL servers and execute SQL code under the privileges of the user used to connect to the database
*c) The use of PL-SQL opens the door to these vulnerabilities
d) None of the mentioned

3. Any user-controlled parameter that gets processed by the application includes vulnerabilities like _____
a) Host-related information
b) Browser-related information
c) Application parameters included as part of the body of a POST request
*d) All of the mentioned

4. Point out the correct statement.
a) Parameterized data cannot be manipulated by a skilled and determined attacker
*b) Procedure that constructs SQL statements should be reviewed for injection vulnerabilities
c) The primary form of SQL injection consists of indirect insertion of code
d) None of the mentioned

5. Which one is NOT a valid comment sign in case of MySQL?
a) #
b) --
*c) //
d) /*

6. Which option of sqlmap is required to test an application which expects the input with POST method?
a) --get
b) --post
*c) --data
d) --send

7. Which one can be used to bypass a basic login screen in case of MySQL?
a) 'OR 1=1//
b) 'OR 1=1
c) 'OR '1'=1
*d) 'OR 1=1-- -

8. Which of the following script is example of SQL injection attack?

```
*a)
var Shipcity;
ShipCity = Request.form ("ShipCity");
var SQL = "select * from OrdersTable where ShipCity = '" + ShipCity +
"'";

b)
var Shipcity;
ShipCity = Request.form ("ShipCity");

c)
var Shipcity;
var SQL = "select * from OrdersTable where ShipCity = '" + ShipCity +
"'";

d) All of the mentioned
```