# Free Questions for ECSAv10 by certsinside

## Shared by Parsons on 07-06-2022

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

**Question Type:** MultipleChoice

One needs to run "Scan Server Configuration" tool to allow a remote connection to Nessus from the remote Nessus clients. This tool allows the port and bound interface of the Nessus daemon to be configured.

By default, the Nessus daemon listens to connections on which one of the following?

## Options:

**A)** Localhost (127.0.0.1) and port 1241

**B)** Localhost (127.0.0.1) and port 1240

**C)** Localhost (127.0.0.1) and port 1246

**D)** Localhost (127.0.0.0) and port 1243

## Answer:

A

# Question 2

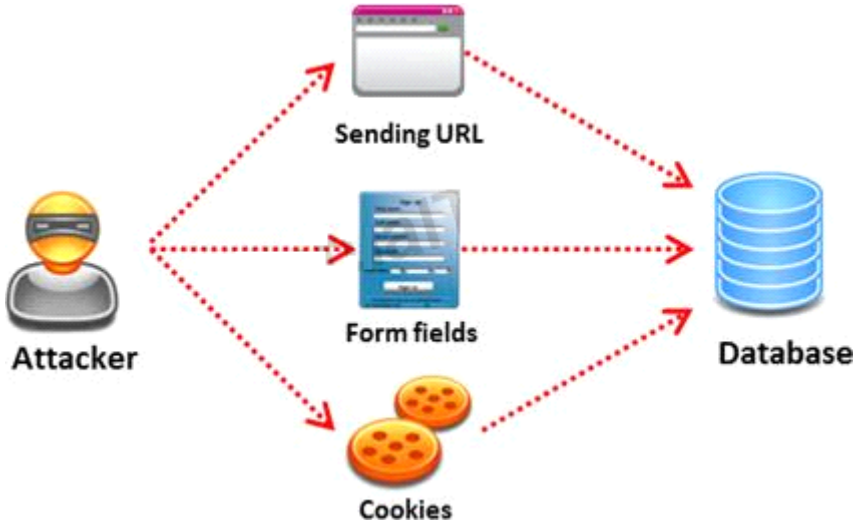
**Question Type:** **MultipleChoice**

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?

### Options:

**A)** Automated Testing

**B)** Function Testing

**C)** Dynamic Testing

**D)** Static Testing

### Answer:

D

## Question 3

**Question Type:** **MultipleChoice**

What is kept in the following directory? HKLM\SECURITY\Policy\Secrets

### Options:

**A)** Service account passwords in plain text

**B)** Cached password hashes for the past 20 users

**C)** IAS account names and passwords

**D)** Local store PKI Kerberos certificates

### Answer:

A

## Question 4

**Question Type:** MultipleChoice

What is a good security method to prevent unauthorized users from "tailgating"?

### Options:

**A)** Electronic key systems

**B)** Man trap

**C)** Pick-resistant locks

**D)** Electronic combination locks

### Answer:

B

# Question 5

**Question Type:** **MultipleChoice**

Security auditors determine the use of WAPs on their networks with Nessus vulnerability scanner which identifies the commonly used WAPs.

One of the plug-ins that the Nessus Vulnerability Scanner uses is ID #11026 and is named "Access Point Detection". This plug-in uses four techniques to identify the presence of a WAP.

Which one of the following techniques is mostly used for uploading new firmware images while upgrading the WAP device?

### Options:

**A)** NMAP TCP/IP fingerprinting

**B)** HTTP fingerprinting

**C)** FTP fingerprinting

**D)** SNMP fingerprinting

### Answer:

C

# Question 6

**Question Type:** MultipleChoice

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

### Options:

**A)** 222

**B)** 224 or more

**C)** 240 or less

**D)** 225 or more

### Answer:

D

# Question 7

**Question Type:** MultipleChoice

One needs to run "Scan Server Configuration" tool to allow a remote connection to Nessus from the remote Nessus clients. This tool allows the port and bound interface of the Nessus daemon to be configured.

By default, the Nessus daemon listens to connections on which one of the following?

### Options:

**A)** Localhost (127.0.0.1) and port 1241

**B)** Localhost (127.0.0.1) and port 1240

**C)** Localhost (127.0.0.1) and port 1246

**D)** Localhost (127.0.0.0) and port 1243

**Answer:**

A

# Question 8

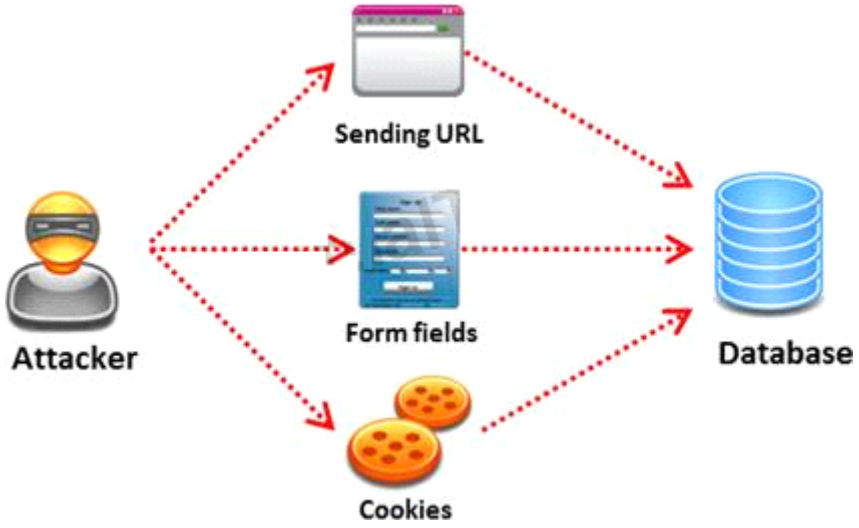
**Question Type:** **MultipleChoice**

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?

## Options:

**A)** Automated Testing

**B)** Function Testing

**C)** Dynamic Testing

**D)** Static Testing

## Answer:

D