

412-79V8^{Q&As}

EC-Council Certified Security Analyst (ECSA)

Pass EC-COUNCIL 412-79V8 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/412-79v8.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

A pen tester has extracted a database name by using a blind SQL injection. Now he begins to test the table inside the database using the below query and finds the table: `http://juggyboy.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype='U')=3) WAITFOR DELAY '00:00:10'-'http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),1,1)))=101) WAITFOR DELAY '00:00:10'-- http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),2,1)))=109) WAITFOR DELAY '00:00:10'-- http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),3,1)))=112) WAITFOR DELAY '00:00:10'--`

What is the table name?

- A. CTS
- B. QRT
- C. EMP
- D. ABC

Correct Answer: C

QUESTION 2

Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not have the buffering capacity to forward a datagram. Each ICMP message contains three fields: type, code, and checksum. Different types of Internet Control Message Protocols (ICMPs) are identified by a type and code field.



Which of the following ICMP messages will be generated if the destination port is not reachable?

- A. ICMP Type 11 code 1
- B. ICMP Type 5 code 3
- C. ICMP Type 3 code 2
- D. ICMP Type 3 code 3

Correct Answer: D

QUESTION 3

Rules of Engagement (ROE) document provides certain rights and restriction to the test team for performing the test and helps testers to overcome legal, federal, and policy-related restrictions to use different penetration testing tools and techniques.

Rules of Engagement Template

DATE: *[Date]*

TO: *[Name and Address of NASA Official]*

FROM: *[Name and Address of Third Party performing the Penetration Testing]*

CC: *[Name and Address of Interested NASA Officials]*

RE: Rules of Engagement to Perform a Limited Penetration Test in Support of
[required activity]

[Name of third party] has been contracted by the National Aeronautics and Space Administration (NASA), [Name of requesting organization] to perform an audit of NASA's [Name of risk assessment target]. The corresponding task-order requires the performance of penetration test procedures to assess external and internal vulnerabilities. The purpose of having the "Rules of Engagement" is to clearly establish the scope of work and the procedures that will and will not be performed, by defining targets, time frames, test rules, and points of contact.

What is the last step in preparing a Rules of Engagement (ROE) document?

- A. Conduct a brainstorming session with top management and technical teams
- B. Decide the desired depth for penetration testing
- C. Conduct a brainstorming session with top management and technical teams
- D. Have pre-contract discussions with different pen-testers

Correct Answer: B

QUESTION 4

Many security and compliance projects begin with a simple idea: assess the organization's risk, vulnerabilities, and breaches. Implementing an IT security risk assessment is critical to the overall security posture of any organization.

An effective security risk assessment can prevent breaches and reduce the impact of realized breaches.



What is the formula to calculate risk?

- A. Risk = Budget x Time
- B. Risk = Goodwill x Reputation
- C. Risk = Loss x Exposure factor
- D. Risk = Threats x Attacks

Correct Answer: C

QUESTION 5

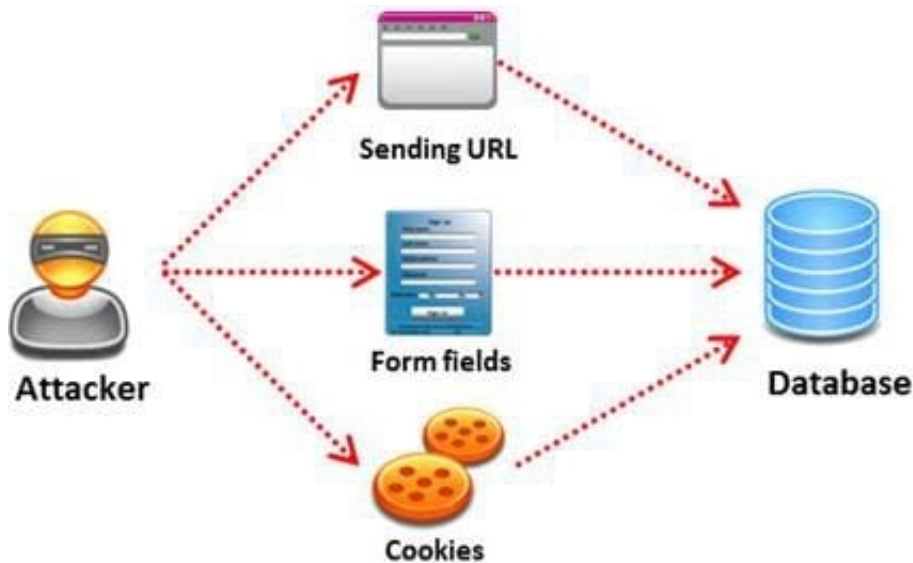
SQL injection attack consists of insertion or "injection" of either a partial or complete SQL query via the data input or transmitted from the client (browser) to the web application.

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

[412-79V8 Practice Test](#)

[412-79V8 Exam Questions](#)

[412-79V8 Brindumps](#)