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.geekcert.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

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:

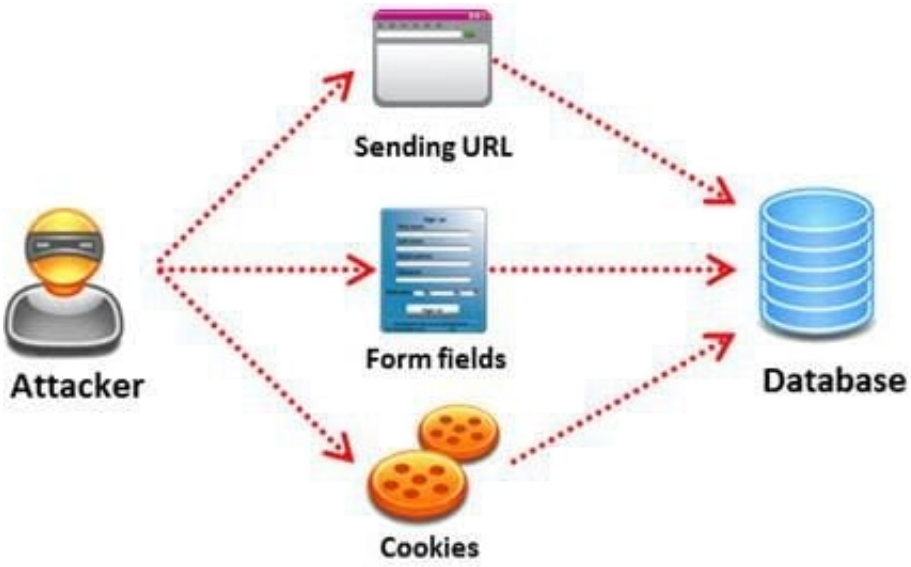
i)Read sensitive data from the database

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 2

Which among the following information is not furnished by the Rules of Engagement (ROE) document?

A. Techniques for data collection from systems upon termination of the test

B. Techniques for data exclusion from systems upon termination of the test

C. Details on how data should be transmitted during and after the test

D. Details on how organizational data is treated throughout and after the test

Correct Answer: D

QUESTION 3

Which one of the following is a supporting tool for 802.11 (wireless) packet injections, it spoofs 802.11 packets to verify whether the access point is valid or not?

A. Airsnort

B. Aircrack

C. Airpwn

D. WEPCrack

Correct Answer: C

QUESTION 4

You work as an IT security auditor hired by a law firm in Boston. You have been assigned the responsibility to audit the client for security risks. When assessing the risk to the clients network, what step should you take first?

A. Analyzing, categorizing and prioritizing resources

B. Evaluating the existing perimeter and internal security

C. Checking for a written security policy

D. Analyzing the use of existing management and control architecture

Correct Answer: C

QUESTION 5

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

A. Web Services Footprinting Attack

B. Service Level Configuration Attacks

C. URL Tampering Attacks

D. Inside Attacks

Correct Answer: A

412-79V8 VCE Dumps 412-79V8 Study Guide 412-79V8 Braindumps