

[Contact Us](#)[My Account](#)[Home](#)[Training ▼](#)[Resources ▼](#)[Store](#)

\$0.00 0 items

[Cart](#)[Discounts](#)[About](#)[Home](#) > [CEHv10 – Module 16 – Quiz](#)

# CEHv10 – Module 16 – Quiz

## CEHv10 – Module 16 – Quiz

### Results

4 of 5 questions answered correctly

Your time: 00:00:26

**Course**  
**Progress**

**You have reached 4 of 5 point(s), (80%)**

[Click Here to Continue](#)

**RESTART QUIZ**

**VIEW QUESTIONS**

1. Question

Roy is a senior penetration tester working in a Gensolutions Inc, a US based company. The company uses the Oracle database to store all its data. It also uses Oracle DataBase Vault in order to restrict user from accessing the confidential data from their database. One day Roy was asked to find all the possible vulnerabilities of the company's Oracle Database Vault. Roy tried different kinds of attacks to penetrate into the company's Oracle DB Vault and succeeded. Which of the following attack helped Roy to bypass Gensolutions Oracle DB Vault? Select one:

- ☐ a. Denial of service attack
- ☒ **b. SQL Injection**
- ☐ c. Session Hijacking
- ☐ d. Sniffing

**Correct**

2. Question

In the SQL Injection Characters, which of the following character represents the global variable?

## Course Navigation

n

- [!\[\]\(098e47036f78288d477e334896a43770\_img.jpg\) Meet Your Instructor](#)
- [!\[\]\(4eae4ca9e3bdd839cea72df3843a6754\_img.jpg\) Module 01:  
Introduction to Ethical Hacking](#)
- [!\[\]\(85c10fe0ae97c3e2f0e940987ab0a900\_img.jpg\) Module 02:  
Footprinting and Reconnaissance](#)
- [!\[\]\(886bb00f68a0102765319f7e3e73d979\_img.jpg\) Module 03: Scanning Networks](#)
- [!\[\]\(0fbfb77cc5f54acd9a6cc5e2e99729c4\_img.jpg\) Module 04:  
Enumeration](#)
- [!\[\]\(bcfed6d10b13d512440f89f52a81eafd\_img.jpg\) Module 05:  
Vulnerability Analysis](#)
- [!\[\]\(7c161aecd27f28132b5df13a9dbd5b32\_img.jpg\) Module 06: System Hacking](#)
- [!\[\]\(373b3207d9e62a918403ab5e91b2855d\_img.jpg\) Module 07: Malware Threats](#)
- [!\[\]\(2e9585cd44ce64ade7ac985d8a30af53\_img.jpg\) Module 08: Sniffing](#)
- [!\[\]\(146c45a3634224f0483e8b640b8cc13b\_img.jpg\) Module 09: Social Engineering](#)
- [!\[\]\(dcaf00e56c3a4ccf6a305b7f606c9996\_img.jpg\) Module 10: Denial-of-Service](#)
- [!\[\]\(0de8d9b9ba8e30a7f37ff54102575809\_img.jpg\) Module 11: Session Hijacking](#)

- ☐ a. %
- ☐ b. @@variable
- ☐ c. ||
- ☒ d. @variable

**Incorrect**

3. Question

Attacker uses the '%00' character prior to a string in order to bypass detection mechanism. Identify the type of evasion technique used by the attacker.

- ☐ a. Case Variation
- ☐ b. URL Encoding
- ☒ c. Null Byte
- ☐ d. Obfuscated Codes

**Correct**

4. Question

Identify the following technique, in which the attacker use drones to detect open wireless networks

➔ [Module 12: Evading IDS, Firewalls, and Honeypots](#)

➔ [Module 13: Hacking Web Servers](#)

➔ [Module 14: Hacking Web Applications](#)

➔ [Module 15: SQL Injection](#)

⬇ [Module 16: Hacking Wireless Networks](#)

- ✓ Understanding Wireless Concepts
- ✓ Understanding Different Wireless Encryption Algorithms
- ✓ Understanding Wireless Threats
- ✓ Understanding Wireless Hacking Methodology
- ✓ Wireless Hacking Tools
- ✓ Understanding Bluetooth Hacking Techniques
- ✓ Wireless Hacking Countermeasures
- ✓ Wireless Security Tools

- ☐ a. WarChalking
- ☒ **b. WarFlying**
- ☐ c. WarWalking
- ☐ d. WarDriving

**Correct**

5. Question

The testing that is also called black box testing, which require no knowledge of the inner design of the code is called.

- ☐ a. Fuzzing Test
- ☒ **b. Function Test**
- ☐ c. Static Test
- ☐ d. Dynamic Test

**Correct**

✓ Overview of  
Wireless  
Penetration  
Testing

✓ Module 16 Lab 01

✓ Module 16 Lab 02

✓ Module 16 Lab 03

✓ Module 16 - Full

➔ [Module 17: Hacking  
Mobile Platforms](#)

➔ [Module 18: IoT Hackin](#)

➔ [Module 19: Cloud  
Computing](#)





➔ [Module 20:  
Cryptography](#)

---


Return to [Certified  
Ethical Hacker  
\(CEH\)v10](#)

1-888-330-HACK  
Mon - Fri / 8:00AM -  
5:00PM





Featured  
Courses

-  CEH
-  C|CISO
-  CHFI
-  ECSA

Featured  
White Paper

-  Ethical  
Hacking:  
Choosing the  
Right Pathway

Browse

-  Our Courses
-  Learning  
Options
-  iClass Specials
-  Cart