



412-79V10^{Q&As}

EC-Council Certified Security Analyst (ECSA) V10

Pass EC-COUNCIL 412-79V10 Exam with 100% Guarantee

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

<https://www.passapply.com/412-79v10.html>

100% Passing Guarantee
100% Money Back Assurance

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

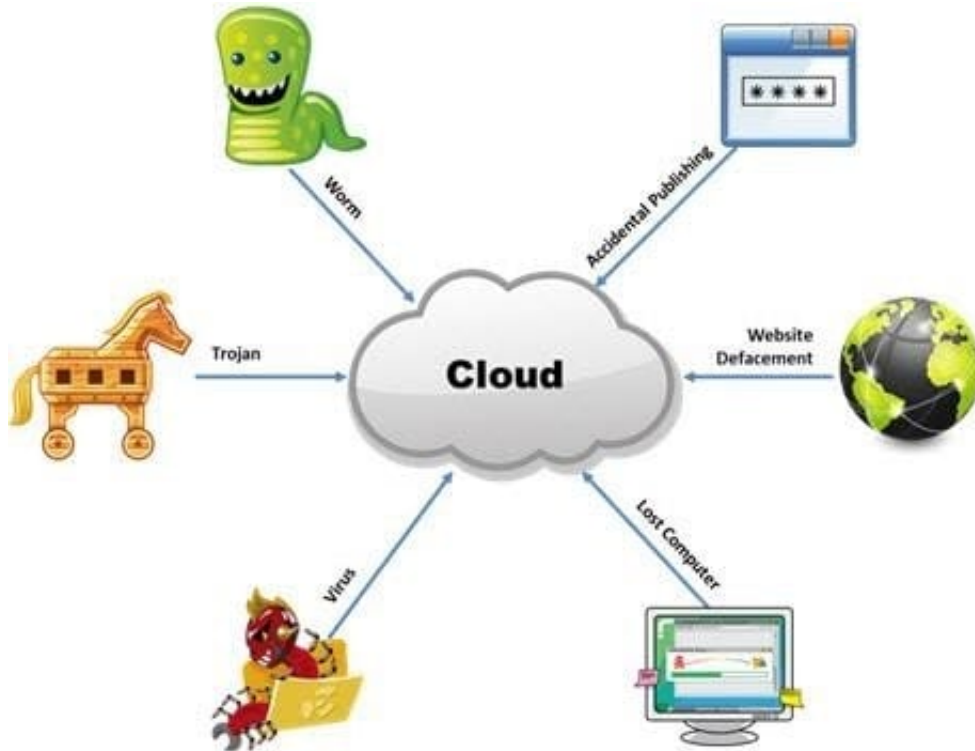
- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

The Internet is a giant database where people store some of their most private information on the cloud, trusting that the service provider can keep it all safe. Trojans, Viruses, DoS attacks, website defacement, lost computers, accidental publishing, and more have all been sources of major leaks over the last 15 years.



What is the biggest source of data leaks in organizations today?

- A. Weak passwords and lack of identity management
- B. Insufficient IT security budget
- C. Rogue employees and insider attacks
- D. Vulnerabilities, risks, and threats facing Web sites

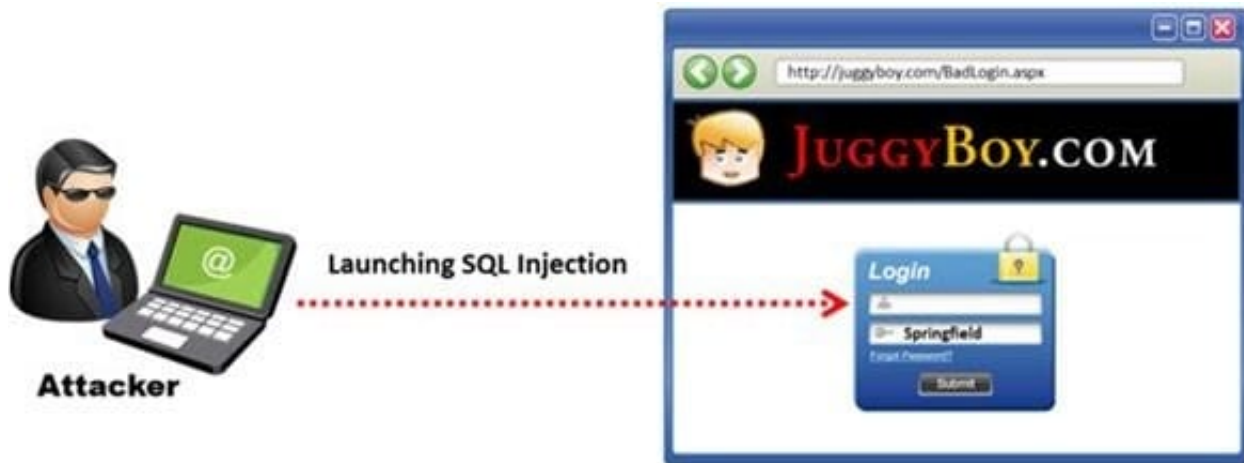
Correct Answer: C

QUESTION 2

SQL injection attacks are becoming significantly more popular amongst hackers and there has been an estimated 69 percent increase of this attack type.

This exploit is used to great effect by the hacking community since it is the primary way to steal sensitive data from web applications. It takes advantage of non-validated input vulnerabilities to pass SQL commands through a web application for execution by a back-end database.

The below diagram shows how attackers launched SQL injection attacks on web applications.



Which of the following can the attacker use to launch an SQL injection attack?

- A. Blah\\' "2=2 ?
- B. Blah\\' and 2=2 -
- C. Blah\\' and 1=1 -
- D. Blah\\' or 1=1 -

Correct Answer: D

QUESTION 3

Which one of the following 802.11 types uses either FHSS or DSSS for modulation?

- A. 802.11b
- B. 802.11a
- C. 802.11n
- D. 802.11-Legacy

Correct Answer: D

QUESTION 4

Which one of the following acts makes reputational risk of poor security a reality because it requires public disclosure of any security breach that involves personal information if it is unencrypted or if it is reasonably believed that the information has been acquired by an unauthorized person?

- A. California SB 1386
- B. Sarbanes-Oxley 2002
- C. Gramm-Leach-Bliley Act (GLBA)

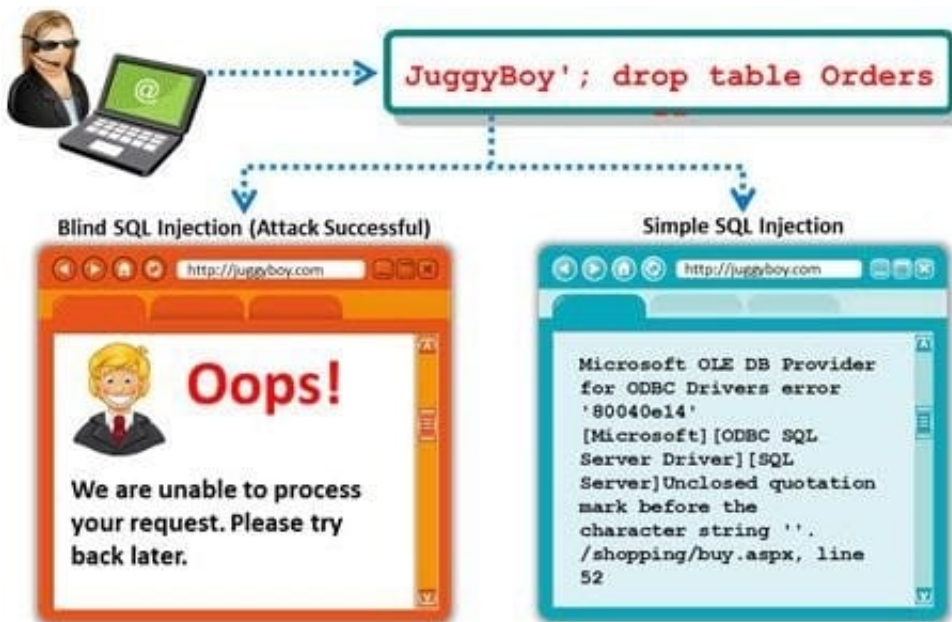


D. USA Patriot Act 2001

Correct Answer: A

QUESTION 5

A Blind SQL injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the application response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.



It is performed when an error message is not received from application while trying to exploit SQL vulnerabilities. The developer's specific message is displayed instead of an error message. So it is quite difficult to find SQL vulnerability in such cases.

A pen tester is trying to extract the database name by using a blind SQL injection. He tests the database using the below query and finally finds the database name.

```
http://juggyboy.com/page.aspx?id=1; IF (LEN(DB_NAME())=4) WAITFOR DELAY '\\00:00:10\\'
```

```
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),1,1)))=97) WAITFOR DELAY '\\00:00:10\\'
```

```
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),2,1)))=98) WAITFOR DELAY '\\00:00:10\\'
```

```
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),3,1)))=99) WAITFOR DELAY '\\00:00:10\\'
```

```
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),4,1)))=100) WAITFOR DELAY '\\00:00:10\\'
```

What is the database name?

A. WXYZ



B. PQRS

C. EFGH

D. ABCD

Correct Answer: D

Reference: <http://www.scribd.com/doc/184891028/CEHv8-Module-14-SQL-Injection-pdf> (see module 14, page 2049 to 2051)

[412-79V10 Practice Test](#)

[412-79V10 Study Guide](#)

[412-79V10 Exam Questions](#)