312-50V8$^{Q\&As}$

Certified Ethical Hacker v8

Pass EC-COUNCIL 312-50V8 Exam with 100% Guarantee

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

https://www.geekcert.com/312-50v8.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A security analyst in an insurance company is assigned to test a new web application that will be used by clients to help them choose and apply for an insurance plan. The analyst discovers that the application is developed in ASP scripting language and it uses MSSQL as a database backend. The analyst locates the application\\'s search form and introduces the following code in the search input fielD. IMG SRC=vbscript:msgbox("Vulnerable");> originalAttribute="SRC" originalPath="vbscript:msgbox("Vulnerable");>"

When the analyst submits the form, the browser returns a pop-up window that says "Vulnerable".

Which web applications vulnerability did the analyst discover?

A. Cross-site request forgery

B. Command injection

C. Cross-site scripting

D. SQL injection

Correct Answer: C

QUESTION 2

RC4 is known to be a good stream generator. RC4 is used within the WEP standard on wireless LAN. WEP is known to be insecure even if we are using a stream cipher that is known to be secured.

What is the most likely cause behind this?

A. There are some flaws in the implementation.

B. There is no key management.

C. The IV range is too small.

D. All of the above.

E. None of the above.

Correct Answer: D

QUESTION 3

Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common?

A. They are written in Java.

B. They send alerts to security monitors.

C. They use the same packet analysis engine.

D. They use the same packet capture utility.

Correct Answer: D

QUESTION 4

Bill is attempting a series of SQL queries in order to map out the tables within the database that he is trying to exploit.

Choose the attack type from the choices given below.

A. Database Fingerprinting

B. Database Enumeration

C. SQL Fingerprinting

D. SQL Enumeration

Correct Answer: A

QUESTION 5

The FIN flag is set and sent from host A to host B when host A has no more data to transmit (Closing a TCP connection). This flag releases the connection resources.

However, host A can continue to receive data as long as the SYN sequence numbers of transmitted packets from host B are lower than the packet segment containing the set FIN flag.

A. false

B. true

Correct Answer: B