312-50V10 Q&As

Certified Ethical Hacker Exam (C|EH v10)

Pass EC-COUNCIL 312-50V10 Exam with 100% Guarantee

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

https://www.passapply.com/312-50v10.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications?

A. Validate and escape all information sent to a server

B. Use security policies and procedures to define and implement proper security settings

C. Verify access right before allowing access to protected information and UI controls

D. Use digital certificates to authenticate a server prior to sending data

Correct Answer: A

Contextual output encoding/escaping could be used as the primary defense mechanism to stop Cross-site Scripting (XSS) attacks.

References: https://en.wikipedia.org/wiki/Crosssite_scripting#Contextual_output_encoding.2Fescaping_of_string_input

QUESTION 2

What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?

A. Copy the system files from a known good system

B. Perform a trap and trace

C. Delete the files and try to determine the source

D. Reload from a previous backup

E. Reload from known good media

Correct Answer: E

QUESTION 3

What hacking attack is challenge/response authentication used to prevent?

A. Replay attacks

B. Scanning attacks

C. Session hijacking attacks

D. Password cracking attacks

Correct Answer: A

QUESTION 4

Which security control role does encryption meet?

A. Preventative

B. Detective

C. Offensive

D. Defensive

Correct Answer: A

QUESTION 5

Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, smallsized packets to the target computer, making it very difficult for an IDS to detect the attack signatures.

Which tool can be used to perform session splicing attacks?

A. Whisker

B. tcpsplice

C. Burp

D. Hydra

Correct Answer: A

One basic technique is to split the attack payload into multiple small packets, so that the IDS must reassemble the packet stream to detect the attack. A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. The \\'whisker\\' evasion tool calls crafting packets with small payloads \\'session splicing\\'.

References: https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques#Fragmentation_and_small_packets