Testpassport問題集

更に上のクオリティ　更に上のサービス

一年で無料進級することに提供する

Http://www.testpassport.jp

Exam : **C2150-139**

Title : IBM Certified Specialist - IBM Rational AppScan, Standard Ed

Version : DEMO

1. In which three areas does AppScan test for vulnerabilities?

A. the network layer, the web application, the web server

B. the operating system, the web application platform, the database

C. the web application, the web server, the web application platform

D. the web application platform, the network layer, the web server

Answer: C

2. After 30 minutes your scan stops with an out-of-session error.

What is a possible cause of this error?

A. Redundant path limit was too low.

B. A parameter was not tracked.

C. Flash parsing was turned off.

D. Platform authentication was not configured.

Answer: B

3. How does an attacker exploit Web application vulnerabilities?

A. by hacking the firewall

B. by installing viruses on a users machine

C. by sending malicious HTTP requests

D. by sniffing the traffic between a user and the Web server

Answer: C

4. What does a Cross-site Scripting vulnerability allow an attacker to do?

A. execute a malicious script on the Web server

B. change the Web server configuration

C. steal a users session tokens

D. drop database tables

Answer: C

5. Which type of vulnerability allows an attacker to browse files that shouldnt be accessible (e.g. *.bak,

"Copy of", *.inc, etc.) or pages restricted for users with higher privileges?

A. Insecure Cryptographic Storage

B. Injection Flaw

C. Failure to Restrict URL Access

D. Insecure Communication

Answer: C

6. What is indicative of an Information Leakage vulnerability?

A. When the user logs in, Hello, username!?is displayed.

B. The exception call stack is displayed.

C. The message Incorrect username or password!?is displayed.

D. The message Script error: Please contact the Web sites administrator!?is displayed.

Answer: B

7. Why is it important to encrypt the HTTP traffic for an authenticated connection between a client and Web server?

A. to prevent SQL injection

B. to prevent sensitive information from being stolen

C. to prevent Cross-site Scripting

D. to prevent Web site defacement

Answer: B

8. What are the implications of Malicious File Execution vulnerabilities?

A. user impersonation and authentication bypass

B. authentication bypass and site defacement

C. site defacement and complete takeover of the application

D. complete takeover of the application and user impersonation

Answer: C

9. How can an attacker use the information gained by an SQL debug message?

A. steal sensitive information from other users

B. run scripts on other users' browsers

C. alter the communication protocol used by the site

D. can potentially understand the query's structure

Answer: D

10. Which statement is true about network firewalls preventing Web application attacks?

A. Network firewalls cannot prevent attacks because ports 80 and 443 must be open.

B. If configured properly, network firewalls can prevent attacks.

C. Network firewalls cannot prevent attacks because it is too complex to configure.

D. Network firewalls can prevent attacks because they can detect malicious HTTP traffic.

Answer: A