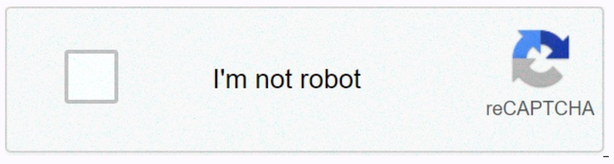

Continue

Amdocs sql online test questions and answers

List of Most Frequently Asked Security Testing Interview Questions with Detailed Answers: What is Security Testing? Security testing is a process designed to detect deficiencies in the security mechanisms of an information system that protects data and maintains functionality as planned. Security testing is the most important type of testing for each application. In this type of testing, the tester plays an important role as an attacker and play around the system to find security-related vass. Here we have listed some top security testing interview issues for your link. Top 30 Security Testing Interview QuestionsQ #1) What is Security Testing? A: Security testing can be considered the most important in all types of software testing. Its main goal is to find vulnerabilities in any software (web or network) application and protect their data from possible attacks or intruders. Because many apps contain confidential data and must be protected from leakage. Software testing must be carried out regularly on such applications in order to identify threats and take immediate action. Q #2) What is Vulnerability? A: A vulnerability can be defined as the weakness of any system through which intruders or bugs can attack the system. If security testing has not been done consistently on the system then the chances of vulnerabilities get increased. From time to time patches or fixes are required to prevent the system from vulnerabilities. Q #3) What is intrusion detection? A: Intrusion detection is a system that helps identify and deal with possible attacks. Intrusion detection involves gathering information from many systems and sources, analyzing information and finding possible ways to attack the system. Intrusion detection checks the following:Possible attacksAs any abnormal activityAudit system dataAnalysis of various data collected, etc. Q #4) What is SQL Injection? A: SQL Injection is one of the common offensive techniques used by hackers to obtain critical data. Hackers scan any loophole in the system through which SQL queries can pass, bypass security checks, and undo critical data. This is known as SQL injections. This can allow hackers to steal critical data or even crash the system. SQL injections are very critical and should be avoided. Regular security tests can prevent this kind of attack. SQL Database security needs to be defined correctly, and input fields and special characters should be handled correctly. Q #5) List of security testing attributes? A: There are seven attributes of security testing: AuthenticationAuthorizationConfidentialityAfidentialityAilabilityIntegrityNon-repudiationResilienceQ #6) What is XSS or Cross-Site Scripting? A: XSS or cross-site scripting is the type of vulnerability that hackers use to attack web applications. This allows hackers to apply or JAVASCRIPT code to a website that can steal confidential information from cookies and returns to hackers. It is one of the most critical and common techniques to avoid. Q #7) What are SSL and SSL sessions? A: An SSL or secure socket layer connection is a transient peer-to-peer communication connection where each connection is mapped to a single Session.SSL session can be defined as a connection between the client and the server's generally generated handshake protocol. There is a set of parameters defined and can be shared by multiple SSL connections. Question #8) What is Penetration Testing? A: Penetration testing is for security testing that helps identify vulnerabilities in the system. A penetration test is an attempt to evaluate system security by manual or automated techniques, and if any vulnerability error is detected, testers use this vulnerability to gain deeper access to the system and find other vulnerabilities. The main purpose of this testing is to prevent the system from any possible attacks. Penetration testing can be done in two ways–White Box Testing and Black Box Testing. In white-box testing, all information is available with testers, while in black box testing, testers have no information and test the system in real-world scenarios to detect vulnerabilities. Question #9) Why is Penetration testing important? Answer: Penetration testing is important because-Security breaches and gaps in systems can be very costly because threat of an attack is always possible and hackers can steal important data or even crash the system. It is not possible to protect all information at all times. Hackers always come up with new techniques to steal important data and it is necessary that testers also conduct periodic testing to detect possible attacks. Penetration testing identifies and protects the system with these attacks and helps organizations keep their data safe. Q #10) The name of two common techniques used to protect a password file? A: Two common techniques for protecting a password file are hash-passwords and salt value or password file access control. Q #11) List of full software security shortcut names? A: Shortcuts for software security include: IPsec - Internet Protocol Security is a set of protocols for InternetOSI security - Open Systems InterconnectionISDN Integrated Services Digital NetworkGOSIP- Government Open Systems ProfileFTP Link - File Transfer ProtocolDBA - Dynamic Bandwidth AllocationDDS - Digital Data SystemDES - Data -Encryption StandardCHAP – Challenge Handshake Authentication ProtocolBONDING – Bandwidth On Demand Interoperability GroupSSH – The Secure ShellCOPS Common Open Policy ServiceISAKMP – Internet Security Association and Key Management ProtocolUSM – User-based Security ModelTLS – The Transport Layer SecurityQ #12) What is ISO 17799? A: ISO/IEC 17799 is originally published in the United Kingdom and defines best practices for the management of guidelines for all organizations small or large to secure information. Q #13) List down some factors that may cause vulnerabilities? Answer: The factors causing the vulnerability are: Design flaws: If there are gaps in the system that can allow hackers to attack the system easily. Passwords: If passwords are known to hackers, they can get information very easily. Password policy should be strictly followed to minimize the risk of password theft.Complexity: Complex software can open the door to vulnerabilities. Human error: Human error is a significant source of security vulnerability. Message: Poor data management can lead to vulnerabilities in the system. Q #14) A list of different methodologies in security testing? A: The methodologies in the security testing are: White Box- All information is provided by the tester. Black Box-No information is provided by testers and can test the system in a real-world scenario. Grey Box-Partial information is with testers and rest to be tested on their own. Q #15) List out the seven main types of security tests according to the Open Source Security Testing Methodology Manual? Answer: The seven main types of security testing according to the open source security testing methodology manual are: Vulnerability Scanning: Automated software scans the system against known vulnerabilities. Security scan: Manual or automated technique to identify network and system weaknesses. Penetration testing: Penetration testing is for security testing that helps identify vulnerabilities in the system. Risk assessment: Includes an analysis of possible risks in the system. Risks are classified as low, medium and high.security audit: Complete scan of systems and applications to detect vulnerabilities. Ethical hacking: Hacking is done on the system to detect flaws in it rather than personal benefits. Guest posturs: This combines security scanning, ethical hacking and risk assessment to show the overall security posture of an organization. Q #16) What is SOAP and WSDL? A: SOAP or Simple Object Access Protocol is an XML-based protocol through which applications exchange information over HTTP. XML requests are sent by Web services in SOAP format then the SOAP client sends a soap message to the server. The server responds again with a SOAP message along with the requested service. Web Services Description Language (WSDL) is an xml formatted language that uses UDDI. The web services description language describes web services and how to access them. Q #17) List of parameters that define the SSL session connection? A: The parameters that define the SSL session connection are:Server and client randomServer write MACsecretClient write MACsecretServer write keyClient write keyInnitialization vectorsSevent numbersQ #18) What is file enumeration? Answer: This kind of attack uses strong browsing with URL manipulation of the attack. Hackers can manipulate parameters in the URL string and can get critical which are generally not open to the public, such as the data obtained, the old version or the data that are under development. Q #19) List of advantages that can be provided by the intrusion detection system? A: There are three advantages of an intrusion detection system. NIDS or Network Intrusion DetectionNNIDS or Network Node Intrusion Detection SystemHIDS or Host Intrusion Detection SystemQ #20) What is HIDS? A: Hids or Host Intrusion Detection system is a system in which a snapshot of an existing system is taken and compared to the previous snapshot. Checks whether critical files have been modified or deleted then a warning is generated and sent to the administrator. Q #21) List of main categories of SET participants? A: These are the participants: CardholderMerchantIssuerAcquirerPayment gatewayCertification authorityQ #22) Explain the URL manipulation? A: URL manipulation is a type of attack in which hackers manipulate the url of a website to obtain critical information. The information is passed to parameters in the query string by using the HTTP GET method between the client and the server. Hackers can change information between these parameters and get authentication on servers and steal critical data. To prevent this kind of attack security testing URL manipulation should be done. Testers themselves can try to manipulate urls and check for possible attacks, and if found they can prevent these kinds of attacks. Question #23) What are the three classes of intruders? Answer: Three classes of intruders are: Fancy dress: It can be defined as an individual who is not authorized on a computer, but hacks the access control system and gain access to verified user accounts. Misfeasor: In this case, the user is verified to use system resources, but he abuses his access to the system. A secret user, it can be defined as an individual who hacks the system control system and bypasses the system security system. Q #24) List of components used in SSL? A: The Secure Sockets Layer protocol or SSL is used to secure connections between clients and computers. Below are the folders used in SSL: SSL Uploaded ProtocolHandshake ProtocolChain Cipher SpecEncryption AlgorithmsQ #25) What is port scanning? A: Ports are where information goes to and from any system. Scanning ports to detect any gaps in the system is known as Port Scanning. There may be several vulneras in the system that hackers can attack and get critical information. These points should be identified and prevented from any abuse. There are types of port checks:Strobe: Scan known services. UDP: Scan open UDPVanilla ports: With this scan, the scanner tries to connect to all 65,535 ports. Sweep: The scanner connects to the same port on more than one computer. Fragmented packets: Scanner sends packet fragments that get through simple packet filters in firewallStealth scan: scanner blocks computer from recording port control activities. FTP bounce: The scanner passes through the FTP server in order to disguise the source of the scan. Q #26) What is a cookie? A: A cookie is information received from a web server and stored in a web browser that you can read at any time later. A cookie may contain password information, some autofill information, and if hackers receive this information, it can be dangerous. Learn how to test website cookies here. Question #27) What are the types of cookies? A: Cookie types are:Session cookies – these cookies are temporary and last only in this session. Persistent cookies – These cookies are stored on your hard disk and last until they expire or are deleted manually. Question #28) What is honeypot? Answer: Honeypot is a fake computer system that beears as a real system and attracts hackers to attack. Honeypot is used to find gaps in the system and provide solutions for these kinds of attacks. Q #29) List of parameters that define the status of an SSL session? A: The parameters that define the status of the SSL session are:Session identifierPeer certificateCompression methodCipher specMaster secretIs resumableQ #30) Describe the network intrusion detection system? A: The network intrusion detection system is commonly known as NIDS. It is used to analyze transmission across the subnet and to align with known attacks. If a space is identified, the administrator receives a notification. Conclusion I hope these security testing interview questions and answers are useful for you to prepare for the interview. These answers will also help you understand the concept of a security testing topic. Read also = > Ethical Hacking CoursesShare this article if you find it useful! Useful!