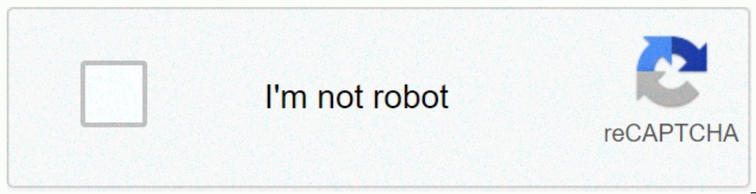

Continue

Software testing interview questions and answers guru99

List of the most frequently asked security test interview questions with detailed answers: What is a security check? Security screening is a process designed to expose faults in the security mechanisms of an information system that protect data and maintain functionality as intended. Security checking is the most important type of test for any application. In this type of test, the controller plays an important role as an attacker and plays around the system to detect security-related errors. Here we have listed some top security test interview questions for your report. Top 30 Safety Tests Interview Q #1) What are Safety Tests? Answer: Security tests can be considered the most important in all types of software testing. Its main goal is to find vulnerabilities in any software (web or networking) based on the application and protect their data from possible attacks or intruders. Since many applications contain confidential data and must be protected from leakage. Software testing should be done periodically in such applications to detect threats and take immediate action on them. Q #2) What is vulnerability? Answer: Vulnerability can be defined as the weakness of any system through which intruders or errors can attack the system. If the security check has not been rigorously performed on the system, then the chances of vulnerability increase. It takes time so far to prevent a system from vulnerabilities. Q #3) What is intrusion detection? Answer: Intrusion detection is a system that helps identify and counter potential attacks. Intrusion detection includes collecting information from multiple systems and sources, analyzing information, and finding possible ways to attack the system. Detection of intrusions controls the following: Possible attacks Any abnormal activity Control of system data Analysis of various data collected, etc. Q #4) What is SQL injection? Answer: SQL Injection is one of the common attack techniques used by hackers to get critical data. Hackers check for any gap in the system through which SQL queries can pass, bypass security checks, and return critical data. This is known as SQL injection. It can allow hackers to steal critical data or even crash a system. SQL injections are very critical and should be avoided. Periodic security tests can prevent such attacks. SQL database security must be set correctly, and input boxes and special characters must be treated correctly. Q #5) List of test characteristics Answer: There are the following seven features of security control: Authentication authorization confidentiality integrity non-disclaimer Durability Q #6) What is XSS or cross-site script? Answer: XSS or cross-site script is a type of vulnerability that hackers used to attack web applications. Allows hackers to enter HTML or JAVASCRIPT code into a web page that can steal the information from cookies and returns to hackers. It is one of the most critical and common techniques to be prevented. Q #7) What are SSL connections and an SSL session? Answer: The SSL or Secured Socket Layer connection is a transitional peer-to-peer connection where each connection is associated with an SSL session. The SSL session can be defined as an association between the client and the server that is generally created by the handshake protocol. There is a configuration set that is defined and can be shared by multiple SSL connections. Q #8) What is the Penetration Test? Answer: Penetration control is in security tests that help identify vulnerabilities in a system. An penetration test is an attempt to assess the security of a system with manual or automated techniques, and if a vulnerability is found, testers use this vulnerability to gain deeper access to the system and find more vulnerabilities. The main purpose of this test is to prevent a system from any potential attacks. The penetration test can be done in two ways -White Box tests and black box tests. In white box testing, all information is available with testers while in black box tests, testers do not have any information and test the system in real scenarios to discover vulnerabilities. Q #9) Why Penetration Test Is Important? Answer: Penetration tests are important because- Security breaches and loopholes in systems can be very costly since the threat of attack is always possible and hackers can steal important data or even crash the system. It is impossible to protect all information all the time. Hackers always come up with new techniques to steal important data, and it is also necessary for testers to perform periodic tests to detect potential attacks. Penetration control identifies and protects a system from the above-mentioned attacks and helps organizations keep their data safe. Q #10) Name the two common techniques used to protect a password file? Answer: Two common techniques for protecting a password file are hashed passwords and a salt value or password file access control. Q #11) List of full names of abbreviations related to software security? Answer: Shortcuts related to software security include: IPsec - Internet Protocol Security is a suite of protocols for securing the Internet OSI - Open Systems Interconnection ISDN Integrated Services Digital Network GOSSIP- Government Open Systems Interconnection Ftp Profile - Protocol DBA files - Dynamic DDS bandwidth distribution - Digital DES data system - Data -Encryption Standard CHAP - Authentication handshake challenge welding protocol - bandwidth on-demand interoperability group SSH - The secure shell COPS Common Open Policy Service ISAKMP - Internet Security Association and Key Management Protocol USM - User-based Security Model TLS - Security Transfer Layer Q #12) What is ISO 17799? Answer: ISO/IEC 17799 is originally published in the United Kingdom and practices for Information Security Management. It has guidelines for all organisations large or small for information security. Q #13) List down certain factors that can cause vulnerabilities? Answer: Factors that cause vulnerabilities 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 minimise the risk of password theft. Complexity: Complex software can open doors to vulnerabilities. Human error: Human error is an important source of security vulnerabilities. Management: Poor data management can lead to system vulnerabilities. Q #14) List of different methodologies in safety tests? Answer: The methodologies in the safety tests are: White box- All information is provided to the testers. Black Box- No information is provided to testers and they can test the system in a real scenario. Grey Box- Some information is with the testers and rest that they have to try on their own. Q #15) List below the seven main types of safety tests according to the open source safety test methodology manual? Answer: The seven main types of security tests according to the open source security screening methodology manual are: Vulnerability Analysis Scan: Automated software scans a system against known vulnerabilities. Security scan: Manual or automated technique to detect network and system failures. Penetration tests: The penetration test is in safety tests that help identify vulnerabilities in a system. Risk assessment: Includes analysis of potential risks in the system. Risks are classified as low, medium and high. Security check: Full control of systems and applications to detect vulnerabilities. Ethical hacking: Hacking is done on a system to detect flaws in it rather than personal benefits. Stop rating: This combines security scanning, ethical piracy and risk assessments to show an overall security posture of an organization. Q #16) What is SOAP and WSDL? Answer: SOAP or the 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, and then a SOAP client sends a SOAP message to the server. The server responds again with a SOAP message along with the requested service. The Web Services Description Language (WSDL) is a formatted XML language that is used UDDI. The Web Services description language describes Web services

and how to access them. Q #17) List of parameters that define an SSL session connection? Answer: The parameters that determine an SSL session connection are: Server and client random Server write MCSecret Client record MACsecret Server write key Client write key Sequence vectors Sequence numbers Q #18) What is file enumeration? Answer: This type of attack uses strong browsing with URL URL Attack. Hackers can manipulate parameters in the URL string and can get critical data that generally doesn't open for the public such as the achieved data, the old version or the data that is under development. Q #19) List of benefits that can be provided by an intrusion detection system? Answer: There are three benefits of an intrusion detection system. NIDS or NNIDS Intrusion Detection Network or Network Node HIDS Intrusion Detection System or Host Intrusion Detection System Q #20) What is HIDS? Answer: HIDS or Host Intrusion Detection System is a system in which a snapshot of the existing system is taken and compared to the previous snapshot. Checks whether the critical files were modified or deleted, then an alert is created and sent to the administrator. Q #21) List under the main categories of SET participants? Answer: Below are the participants: Cardholder Merchant Publisher Buyer Portal Payment Authority Q #22) Explain URL Manipulation? Answer: URL handling is a type of attack in which hackers manipulate the URL of the website to obtain critical information. The information is passed to the query string parameters through the HTTP GET method between client and server. Hackers can change the information between these parameters and authenticate the servers and steal critical data. In order to avoid this type of attack security tests of URL manipulation should be done. The testers themselves can try to manipulate the URL and check for possible attacks, and if found they can prevent such attacks. Q #23) What are the three categories of intruders? Answer: The three categories of intruders are: Masquerader: It can be defined as a person who is not authorized on the computer, but hacks system access control and access the user's accounts with authentication. Misfeasor: In this case, the user is validated to use the system resources, but misuses his access to the system. Secret user, It can be defined as a person who hacks the system control system and bypasses the system security system. Q #24) List of the item used in SSL? Answer: Secure Sockets Layer or SSL is used to make secure connections between clients and computers. Below is the item used in SSL: SSL Registered Protocol Handshake Protocol Change Cipher Spec Encryption Algorithms Q #25) What is port scanning? Answer: Ports are the point where information goes in and out of any system. Scan the ports to find out any gaps in the system known as port scanning. There may be some weak points in the system in which hackers can attack and get critical information. These points should be identified and prevented from any abuse. Here are the types of port scans: Strobe: Scan known services. UDP: UDP Vanilla Open Door Scan: In this scan, the scanner attempts to connect to all 65,535 ports. Scan: The scanner connects to the same port on more than one device. Fragmented packages: packages: Scanner sends packet fragments that get through simple packet filters to a Stealth firewall scan: The scanner prevents the scanned computer from recording port scanning activities. FTP bounce: The scanner passes through an FTP server in order to disguise the source of the scan. Q #26) What is a cookie? Answer: A cookie is a piece of information obtained from a web server and stored in a web browser that can be read at any time later. A cookie can contain password information, some autocomplete information, and if hackers get those details it can be dangerous. Learn here how to test the cookies of the website. Q #27) What are the types of Cookies? Answer: The types of cookies are: Session Cookies – These cookies are temporary and last only in this session. Persistent cookies – These cookies are stored on the hard drive and last until they expire or are manually removed. Q #28) What is a pot? Answer: Honeypot is a fake computer system that behaves like a real system and attracts hackers to attack it. Honeypot is used to discover gaps in the system and provide a solution for these kinds of attacks. Q #29) List of parameters that define an SSL session state? Answer: The parameters that determine an SSL session state are: Session ID Peer Certificate Cipher Compression Method Master Secret Can #30) Describe the Network Intrusion Detection System? Answer: The network intrusion detection system is generally known as NIDS. It is used to analyze transit traffic across the subnet and to match known attacks. If a gap is found, the administrator receives a notification. Conclusion I hope these security test interview questions and answers are useful to prepare for the interview. These answers also help you understand the meaning of the security audit issue. Also Read = > Ethical Hacking Lessons Share this article if you find it useful! Useful!