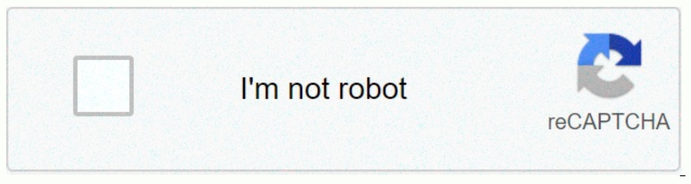

Continue

General psychology test questions and answers pdf

List of the most frequently asked security test interview questions with detailed answers: What are safety tests? Security testing is a process designed to reveal flaws in the security mechanisms of an information system that protect data and maintain functionality as intended. Safety tests are the most important type of test for any application. In this type of test, the tester plays an important role as an attacker and plays around the system to find security-related bugs. Here we have listed some top security test interview questions for your reference. Top 30 Security Test Interview Questions #1) What is security testing? Answer: Security tests can be considered the most important in all types of software testing. Its main objective is to find vulnerabilities in any software application (web or network) and to protect their data from possible attacks or intrusions. As many applications contain confidential data and must be protected from leaks. Software testing should be conducted periodically on these applications in order to identify threats and take immediate action on them. Q #2) What is vulnerability? Answer: Vulnerability can be defined as the weakness of any system by which intruders or bugs can attack the system. If security tests have not been rigorously conducted on the system, the risk of vulnerabilities increases. Patches or patches from time to time are needed to prevent a system from vulnerabilities. Q #3) What is intrusion detection? Answer: Intrusion detection is a system that helps identify and deal with possible attacks. Intrusion detection includes collecting information from many systems and sources, analyzing information, and finding possible ways to attack the system. Intrusion Detection verifies the following: Possible attacksAll abnormal activitiesAuditing system dataAnalysis of different data collected, etc. Q #4) What is SQL injection? Answer: SQL Injection is one of the common attack techniques used by hackers to obtain critical data. Hackers check for any flaws in the system through which they can pass SQL queries, bypass security controls, and return critical data. This is called 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 this type of attack. The security of the SQL database must be and the entry boxes and special characters must be handled correctly. Q #5) List the attributes of safety tests? Answer: There are seven attributes of security testing: AuthenticationAutorizationConfidentialityAvailabilityInteilgrityNon-repudiationResilienceQ #6) What is XSS or Cross-Site Scripting? Answer: XSS or cross-site scripting is a type of vulnerability that hackers used to attack web applications. It allows hackers to inject HTML or JAVASCRIPT code into a web page that can steal the confidential information of cookies and returns to the hackers. This is one of the most critical and common techniques that must be prevented. Q #7) What are SSL connections and an SSL session? Answer: The SSL or Secured Socket Layer connection is a transient peer-to-peer communication link where each connection is associated with an SSL Session.SSL session can be defined as an association between the client and the server typically created by the handshake protocol. There is a set of settings set and it can be shared by multiple SSL connections. Q #8) What is the penetration test? Answer: Penetration tests are conducted on security tests that help identify vulnerabilities in a system. A penetration test is an attempt to assess the security of a system by manual or automated techniques and if a vulnerability is found, testers use that 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 possible attack. The penetration tests can be done in two ways: the tests of the white box and the tests of the black box. In white box tests, all information is available with testers, while in black box tests, testers have no information and they test the system in real-world scenarios to uncover vulnerabilities. Q #9) Why is the penetration test important? Answer: Penetration tests are important because security vulnerabilities and system vulnerabilities can be very costly because the threat of attack is always possible and hackers can steal important data or even crash the system. It is impossible to protect all the information all the time. Hackers have always come up with new techniques to steal important data and it is necessary for testers as well to perform periodic tests to detect possible attacks. Penetration tests identify and protect a system through the above-mentioned attacks and help organizations ensure the security of their data. Q #10) Name the two common techniques used to protect a password file? Answer: Two common techniques for protecting a password file are hash passwords and a salt or password file access control. Q #11) List the full names of software security-related abbreviations? Answer: Software security abbreviations include: IPsec - Internet Protocol Security is a suite of protocols to secure InternetOSI - Open Systems InterconnectionISDN Integrated Services Digital NetworkGOSIP- Government Open Systems Interconnection ProfileFTP - File Transfer ProtocolDBA - Bandwidth Dynamic AllocationDDS 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 Answer: ISO/IEC 17799 is originally published in the UK and sets out best practices in information security management. It guidelines for all organizations large or small for information security. Q #13) List some of the factors that can cause vulnerabilities? Answer: Factors causing vulnerabilities are: Design defects: If there are flaws in the system that can allow hackers to attack the system easily. Passwords: If passwords are known to hackers, they can get the information very easily. The password policy must be strictly followed to minimize 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 the different methodologies in safety tests? Answer: Methodologies in security tests are: White Box- All information is provided to testers. Black Box - No information is provided to testers and they can test the system in a real-world scenario. Grey Box- Partial information is with testers and rest that they have to test for themselves. Q #15) List the seven main types of security tests according to the open source security testing methodology manual? Answer: The seven main types of security tests according to the open source security testing methodology manual are: Vulnerability Scanning: Automated Software scans a system against known vulnerabilities. Security scanning: A manual or automated technique to identify network and system weaknesses. Penetration test: The penetration test is on the security test that identifies vulnerabilities in a system. Risk assessment: This is an analysis of possible risks in the system. Risks are classified as low, medium and high security audits: a comprehensive inspection of systems and applications to detect vulnerabilities. Ethical hacking: Hacking is done on a system to detect defects in it rather than personal benefits. Posture Assessment: This combines security digitization, ethical hacking and risk assessments to demonstrate an organization's overall security posture. Q #16) What is SOAP and

WSDL? Answer: SOAP or Simple Object Access Protocol is an XML-based protocol whereby applications exchange information on HTTP. XML requests are sent via 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 with the requested service. The Web Service Description Language (WSDL) is an XML formatted language used by UDDI. Web Services Description Language describes web services and how to access them. Q #17) List the parameters an SSL session connection? Answer: The parameters that define an SSL session connection are: Random Server and clientServer write MACsecretClient write MACsecretServer write keyClient write keyInitialization vectorsSequence numbersQ #18) What is the file listing? Answer: This type of attack uses energetic navigation with URL manipulation attack. Hackers can manipulate the URL chain settings and which is generally not open to the public, such as the data obtained, the old version or the data being developed. Q #19) List the benefits that can be provided by an intrusion detection system? Answer: There are three advantages to an intrusion detection system. NIDS or Network Intrusion DetectionNNIDS or Network Node Intrusion Detection SystemHIDS or Host Intrusion Detection SystemQ #20) What is HIDS? Answer: The 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. It verifies whether critical files have been changed or deleted, and then an alert is generated and sent to the administrator. Q #21) List the main categories of SET participants? Answer: Here are the participants:CardholderMerchantIssuerAcquirerPayment gatewayCertification authorityQ #22) Explain URL manipulation? Answer: URL manipulation is a type of attack in which hackers manipulate the website URL to get critical information. The information is transmitted through the query chain settings via the HTTP GET method between the client and the server. Hackers can change the information between these settings and get authentication on the servers and steal critical data. In order to avoid this type of attack security test URL manipulation must be done. Testers themselves can try to manipulate the URL and check for possible attacks and if they are found, they can prevent such attacks. Q #23) What are the three categories of intruders? Answer: The three classes of intruders are: Masquerader: It can be defined as a person who is not allowed on the computer, but hacks the system's access control and get access to the user's accounts authenticated. Misfeasor: In this case, the user is authenticated to use the system's resources, but he abuses his access to the system. An underground user, it can be defined as an individual who hacks into the system's control system and bypasses the system's security system. Q #24) List the component used in SSL? Answer: Secure Sockets Layer or SSL is used to establish secure connections between customers and computers. Here is the component used in SSL:SSL Registered ProtocolHandshake protocolChange Cipher SpecEncryption algorithmsQ #25) What is port scanning? Answer: Ports are the point where information enters and exits any system. The scanning of ports to find flaws in the system is known as port scanning. There may be some weaknesses in the system at which hackers can attack and obtain critical information. These points must be identified and prevented from being misused. Here are the types port: Strobe: Digitization of known services. UDP: Digitalization of open UDP portsVanilla: In this scan, the scanner tries to connect to all 65,535 ports. Swipe: The scanner connects to the same port on more than one machine. Fragmented packages: The scanner sends fragments of packages that pass through simple packet filters into a firewallStealth scan: The scanner blocks the recording of the port's scanning activities. REBOUND FTP: The scanner goes through an FTP server to hide the source of the scan. Q #26) What is a cookie? Answer: A cookie is an item of information received from a web server and stored in a web browser that can be read anytime later. A cookie can contain password information, auto-filling information and if hackers get these details, it can be dangerous. Find out here how to test website cookies. Q #27) What are the types of cookies? Answer: The types of cookies are: Session Cookies - These cookies are temporary and last of this session only. Persistent Cookies - These cookies are stored on the hard drive and last until it expires or is removed manually. Q #28) What is a jar of honey? Answer: Honeypot is a fake computer system that behaves like a real system and attracts hackers to attack it. Honeypot is used to find flaws in the system and to provide a solution to these kinds of attacks. Q #29) List the settings that define an SSL session state? Answer: The parameters that define an SSL session state are: Session identifyPeer certificateCompression methodCipher specMaster secretIs resumableQ #30) Describe the network intrusion detection system? Answer: The network intrusion detection system is commonly known as NIDS. It is used to analyze passing traffic across the entire sub-network and to match known attacks. If a fault is identified, the administrator receives an alert. Conclusion I hope that these questions and answers to the security tests will be useful to you in preparing for the interview. These answers also help you understand the concept of the security test subject. Read also - Ethical Hacking CoursesSEeee article if you find it useful! Useful!