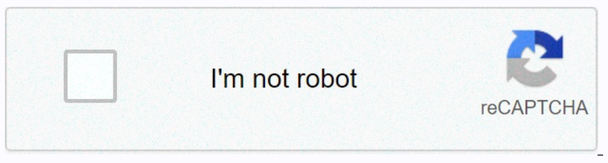

Continue

Us citizenship test pdf without answers

List of most frequently answered interview questions for safety testing with detailed answers: What is safety testing? Security testing is a process that is intended to expose flaws in the security mechanisms of an information system that protects data and maintains functionality as intended. Safety testing is the most important type of testing for all applications. In this type of testing, tests play an important role that attacks and plays around the system to find security-related errors. Here we have listed some top security test interview questions for your reference. Top 30 Security Testing Interview Q #1) What is Security Testing? Answer: Security testing can be considered the most important in all types of software testing. The main goal is to find vulnerabilities in any software (web or network) based application and protect their data from possible attacks or intruders. So many applications contain confidential data and must be protected from being leaked. Software testing must be done periodically on such applications to identify threats and to take immediate action on them. Q #2) What is the Vulnerability? Answer: Vulnerability can be defined as the weakness of any system where intruders or bugs can attack the system. If security testing is not performed thoroughly on the system, the chances of vulnerabilities are increased. Time-to-time updates or fixes are required to prevent a system from the vulnerabilities. Q #3) What is Intrusion Detection? Answer: Intrusion detection is a system that helps determine possible attacks and deal with it. Intrusion detection includes collecting information from many systems and sources, analyzing the information and finding possible ways to attack the system. Intrusion Detection controls the following: Possible attacks Any abnormal activity Revision of system data Analysis of various collected data, etc. Q #4) What is SQL Injection? A: SQL Injection is one of the common attack techniques used by hackers to get critical data. Hackers look for any loopholes in the system where they can send SQL queries, bypass the security checks, and return the critical data. This is called SQL injection. It could allow hackers to steal critical data or even crash a system. SQL injections are highly critical and must be avoided. Periodic security testing can prevent this type of attack. SQL database security must be set up correctly, and input boxes and special characters should be handled correctly. Q #5) List the attributes for security testing? A: There are the following seven attributes for security testing: Authentication Confidentiality Availability Integrity Non-Rejection Resilience Q #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 information from the cookies and returns to the hackers. It is one of the most critical and common techniques that must be prevented. Q #7) What are SSL connections and an SSL session? A: SSL or Secured Socket Layer connection is a temporary peer-to-peer communication link where each connection is associated with one SSL session. The SSL session can be defined as an association between client and server that is typically created by the handshake protocol. A set of parameters is defined, and it can be shared by multiple SSL connections. Q #8) What is Penetration Testing? A: Penetration testing is on security testing that helps identify vulnerabilities in a system. A penetration test is an attempt to evaluate the security of a system using manual or automated techniques, and if a vulnerability exists, testers use this vulnerability to gain deeper access to the system and find more vulnerabilities. The main purpose of this testing is to prevent a system from becoming possible. 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 do not have any information, and they test the system in real-world scenarios to find out vulnerabilities. Q #9) Why Penetration Testing Is Important? Answer: Penetration testing is important because- Security breaches and loopholes in the systems can be very costly as 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 necessary for testers also to perform periodic testing to detect possible attacks. Penetration testing identifies and protects a system in the event of the above 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 to protect a password file are-hashed passwords and a salt value or password file access control. Q #11) List of the full names of software security abbreviations? Answer: Software security abbreviations include: IPsec - Internet Protocol Security is a suite of protocols to secure Internet OSI - Open Systems Interconnection ISDN Integrated Services Digital Network GOSIP- Government Open Systems Interconnection Profile FTP - File Transfer Protocol DBA - Dynamic Bandwidth Allocation DDS - Digital Data System DES – Data -Encryption Standard CHAP - Challenge Handshake Authentication Protocol BONDING - Bandwidth on demand Interoperability Group SSH - Secure Shell COPS Common Open Policy Service ISAKMP - Internet Security Association and Key Management Protocol USM - User-based Security Model TLS - Transport Layer Security Q #12) What is ISO 17799? Answer: ISO/IEC 17799 is originally published in the UK and information security management practices. It has guidelines for all organizations small or large for information security. Q #13) List any factors that could cause vulnerabilities? Answer: Factors that cause vulnerabilities are: Design flaws: If there are loopholes in the system that can allow hackers to attack the system easily. Password: If passwords are known to hackers, they can get the information very easily. Password policy should be closely monitored to minimize the risk of password stealing. Complexity: Complex software can open doors about vulnerabilities. Human error: Human error is a significant source of security issues. Administration: Poor management of the data could lead to system vulnerabilities. Q #14) List the different methods in safety testing? Answer: Methods in safety testing are: White Box- All information is given to the testers. Black Box- No information is given to the testers, and they can test the system in a real scenario. Grey Box- Partial information is with testers and rest they must test on their own. Q #15) List down the seven main types of security testing according to the Open Source Security Testing methodology manual? A: The seven main types of security testing according to the open source security testing methodology manual are: Vulnerability Scanning: Automated software scans a system against known vulnerabilities. Security scan: Manual or automated technique to identify network and system weaknesses. Penetration testing: Penetration testing is on security testing that helps identify vulnerabilities in a system. Risk assessment: It involves analysis of possible risks in the system. Risk is classified as Low, Medium and High. Security Audit: Complete inspection of systems and applications to detect vulnerabilities. Ethical hacking: Hacking is done on a system to detect bugs in it rather than personal benefits. Attitude assessment: This combines security scanning, ethical hacking and risk assessments to show a general security position for an organization. Q #16) What is SOAP and WSDL? A: SOAP or Simple Object Access Protocol is an XML-based protocol in 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 back again with a SOAP message along with the requested service. Web Services Description Language (WSDL) is an XML-formatted language used by UDDI. Web Services Description Languages describe web services and how to access them. Q #17) List the parameters that define an SSL session connection? Answer: The parameters that define an SSL session connection are: Server and Client Random Server Write MACsecret Client Write MACsecret Server Key Client Key Initialization Vectors Sequence Numbers Q #18) What is file enumeration? A: This type of attack uses powerful browsing with the URL Attack. Hackers can manipulate the parameters of the URL string and can get the critical data that is not usually opened to the public, such as obtained data, old version, or data that is being developed. Q #19) List the benefits that can be provided by an intrusion detection system? Answer: There are three advantages of an intrusion detection system. NIDS or Network Intrusion Detection NNIDS or Network Node Intrusion Detection System HIDS or Host Intrusion Detection System Q #20) What is HIDS? Answer: HIDS or Host Intrusion Detection system is a system where a snapshot of the existing system is taken and compared to the previous snapshot. It checks whether critical files were modified or deleted, and then a notification is generated and sent to the administrator. Q #21) List down the main categories of SET participants? Answer: The following are participants: Cardholder Seller Issuer Acquirer Payment gateway CERTIFICATION AUTHORITY Q #22) Explain URL manipulation? A: URL manipulation is a type of attack in which hackers manipulate the url of the site to get the critical information. The information is passed in the parameters of the query string through the HTTP GET method between client and server. Hackers can change the information between these parameters and get authentication on the servers and steal the critical data. To avoid this type of attack security testing of URL manipulation should be done. Testers themselves can try to manipulate the URL and look for possible attacks, and if they find that they can prevent such attacks. Q #23) What are the three classes of invaders? Answer: The three classes of intruders are: Masquerader: It can be defined as a person not authorized on the computer, but hacks the system's access control and accesses authenticated user accounts. Misfeasor: In this case, the user is authenticated to use the system resources, but he abuses his access to the system. Secret user, it can be defined as a person who hacks the control system of the system and bypasses the system security system. Q #24) List component used in SSL? Answer: The Secure Sockets Layer protocol or SSL is used to secure connections between clients and computers. Below is the component used in SSL: SSL Recorded protocol Handshake protocol Change Cipher Spec Encryption algorithms Q #25) What is port scanning? Answer: Ports are the point at which information goes in and out of any system. Scanning the ports to determine any loopholes in the system is known as Port Scanning. There may be some weak points in the system that hackers can attack and get the critical information. These points should be identified and prevented from abuse. The following are the types of port scans: Strobe: Scanning of known services. UDP: Scanning open UDP ports Vanilla: In this scan, the scanner attempts to connect to all 65,535 ports. Sweep: The scanner connects to the same port on more than one machine. Fragmented packages: Scanner sends package fragments that come through simple package filters in a firewall Stealth scan: The scanner blocks the scanned computer from recording port scanning activities. FTP bounce: The scanner goes through an FTP server to hide the source of the scan. Q #26) What is a cookie? A: A cookie is a cookie received from a web server and stored in a web browser that can be read anytime later. A cookie can contain password information, some autofill information, and if any hackers get those details, it can be dangerous. Learn how to test cookies on the website. Q #27) What are the types of cookies? Answer: Types of cookies are: Session cookies – These cookies are temporary and last only in that session. Persistent cookies – These cookies stored on your hard drive and last until it expires or manual removal of it. Q #28) What is a honeypot? Answer: Honeypot is a fake computer system that behaves like a real system and attracts hackers to attack it. Honeypot is used to find out loopholes in the system and to provide a solution for such attacks. Q #29) List the parameters that define an SSL session state? Answer: The parameters that define an SSL session state are: Session identifier Peer certificate Compression method Cipher spec Master secret Is resumable Q #30) Describe the system for network detection detection? Answer: Network Intrusion Detection system in general is known as NIDS. It is used for analysing passing traffic across the subnet and to match with the known attacks. If an identified one 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 also help you understand the concept of the security testing topic. Read also => Ethical Hacking Courses Share this article if you find it helpful! Useful!