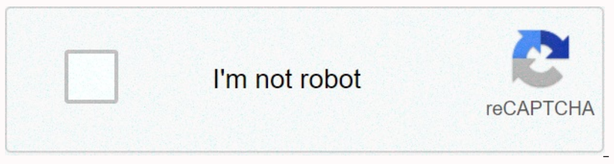

Continue

College board test 1 answers

You will inevitably end up juggling college applications and considering your funding options at the same time. The three main costs of college are tuition, room and boarding. Understanding all three will help you plan for college and prepare to ask for the financial help you need to get you through. Tuition is at the heart of the Higher Education Act. This is a fee associated with each course and is often calculated for credit. For example, a college can charge $300 for a loan for undergraduate courses, which means a three-loan undergraduate history course will cost $900. The average general education course is three or four credits. Undergraduates usually take three to five classes per semester. Some universities and universities provide a flat rate for teaching that covers the minimum and maximum number of units per semester. This may work well for a student who is committed to a full class schedule each semester. For example, a college can charge $300 per loan, but they also offer a flat rate of $4,500 per period for at least 12, but no more than 18 credits. A student with only 12 credits pays $375 per unit, while a full-load student pays $250 per unit. If a student is not commuting to college from home, the cost of living should be considered. For undergraduates, these costs are referred to as a room. Many colleges require students to live in campus dormitories within the first year or two. In their junior and senior years, they may be able to live off-campus. This depends entirely on the college in question. In some schools, it is common for students to spend all four years living on campus, while some students at other schools may never live in student housing. Living on campus is usually not the cheapest option, but it offers the convenience of one predictable price. There is also the convenience of living near your classroom and among your peers. Life off-campus can be filled with unwelcome surprises such as security deposits, rental costs during the summer holidays, scaly roommates, traffic-filled commutes to school, or neighbors who aren't interested in living next door to college students. On-campus room fees, if arranged through a college or university, are usually cited on a quarterly or semester basis. This is a reliable amount that you can plan for expenses. If you are providing for off-campus housing, you should set aside some money for unexpected costs, in addition to the monthly rent amount. You may think that a plate is another way to tell a food budget. Even if you live on campus, the cost of food should be considered a separate budget item. Most schools offer a variety of meals for their on-campus dining room. These can range from an unlimited meal plan to a set number of prepaid meals. as room plans. It will generally cost more for a student to eat on campus, but it's a predictable amount and a comfortable experience. If you are planning for off-campus board costs, it may be helpful to monitor food expenses for a few months before going to college. This will give you a better idea of how much money for food is needed. You should also look for grocery stores near where you will live. Is it close enough to go to the store? Will you have a car to drive? Is public transport a workable option? Most college websites provide a breakdown of estimated expenses. This information can usually be found in the university's financial assistance tab. If you are considering an off-campus living arrangement, and you can't find an estimate, call the university and ask for information. If you are not one of the lucky few who can ignore the price tags, you will need financial help. Your first step in the financial assistance process is filling out a free student assistance request (FAFSA) from the federal government. The FAFSA is a key document needed to receive federal financial assistance in the form of a grant, work degree program, student loan, or scholarship. Many universities and state governments use the same documentation to determine your eligibility for additional assistance. List of most frequently asked questions about security testing with detailed answers: What is security testing? Security testing is a process designed to identify flaws in information system security mechanisms that protect data and maintain functionality as intended. Security testing is the most important type of testing for all applications. In this type of testing, the tester plays an important role as an attacker and plays around the system to find security-related vulnerabilities. Here are some questions from the best security tests for your link. Top 30 Security Testing Interview Questions Q #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 applications contain confidential data and need to be protected from leakage. Software testing must be performed regularly in these applications in order to identify threats and take immediate action on them. Q #2) What is a vulnerability? A: Vulnerability can be defined as a weakness of any system through which intruders or bugs can attack the system. If security testing has not been rigorously performed on the system, the chances of a security threat increase. From time to time repair or repair is required to prevent the system from vulnerabilities. Q #3) What is intrusion detection? A: Intrusion detection is a system that helps in identifying and dealing with possible attacks. Intrusion detection involves collecting information from many resources, analysis of information and finding possible ways to attack the system. Intrusion Detection checks for the following: Possible attacks Any abnormal activity Auditing system data Analysis of various data collected, etc. Q #4) What is SQL Injection? A: SQL Injection is one of the common attack techniques used by hackers to obtain important data. Hackers check any gaps in the system that they can use to pass SQL queries, bypass security checks, and undo important data. This is known as SQL injection. This can allow hackers to steal critical data or even crash the system. SQL injections are very important and should be avoided. Regular security testing can prevent this kind of attack. Sql database security must be defined correctly, and input fields and special characters should be handled correctly. Q #5) List of security testing attributes? A: There are the following seven security testing attributes: Availability Integrity of Q #6 Authentication Authentication Availability) What is XSS scripting or cross-site scripting? A: XSS scripting or cross-site scripting is the type of vulnerability that hackers used to attack Web applications. This allows hackers to inject HTML or JAVASCRIPT code into a website that can steal confidential information from cookies and return to hackers. It is one of the most critical and common techniques that need to be prevented. Q #7) What are SSL connections and SSL sessions? A: An SSL or Secure Socket Layer connection is a two-party transient communication connection where each connection is associated with a single SSL session. An SSL session can be defined as an association between a client and a server generally created by a handshake protocol. There is a set of parameters defined and can be shared by multiple SSL connections. Q #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 a vulnerability has been found, testers use the vulnerability to gain deeper access to the system and find other vulnerabilities. The main purpose of this testing is to prevent the system from 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 whereas in black box testing, testers have no information and test the system in real-world scenarios to detect vulnerabilities. Q #9) Why is penetration testing important? A: Penetration testing is important because- Security breaches and system gaps can be very costly because the threat of an 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 and it is essential that testers also carry out regular testing to identify possible attacks. Penetration testing identifies and protects the system with the above attacks and helps organizations keep their data safe. Q #10) Name two common techniques used to protect a password file? A: Two common password file protection techniques are - hashed passwords and salt value or password file access control. Q #11) Provide full names of software security-related shortcuts? A: Software security-related shortcuts include: IPsec - Internet Protocol Security is a set of Protocols for Internet Security 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 - The Secure Shell COPS Common Open Policy Service ISAKMP - Internet Security Association and Key Management Protocol USM - User-Based Security Model TLS - The Transport Layer Security Q #12) What iso 17799? Answer: ISO/IEC 17799 is originally published in the UK and defines best practices for managing information security. It has guidelines for all organizations small or large for information security. Q #13) A list of some factors that can cause vulnerabilities? Answer: The factors causing the vulnerability are: Design errors: If there are gaps in the system that can allow hackers to easily attack the system. Passwords: If passwords are known to hackers, they can get information very easily. Password policies 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 an important source of security vulnerabilities. Management: Poor data management can lead to system vulnerabilities. Q #14) Indicate different methodologies in security testing? A: The methodologies in security testing are: White Box-All information is provided to testers. Black Box- Testers are not provided with any information and can test the system in a real-world scenario. Grey Box- Partial information is with testers and rest, which they must test themselves. Q #15) A list of 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 guide are: Vulnerability Checker: Automated software scans the system against known vulnerabilities. Security scanning: A manual or automated technique to identify network and system vulnerabilities. Penetration testing: Penetration testing is for security testing that helps identify vulnerabilities in the system. Risk assessment: Includes analysis of potential risks System. Risks are classified as low, medium and high. Security auditing: Complete inspection of vulnerability detection systems and applications. Ethical hacking: Hacking is done on the system to reveal flaws in it rather than personal benefits. Posture rating: It combines security scanning, ethical hacking and risk assessment to show the overall security attitude of the 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 SOAP Web services, and the 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 an XML language used by UDDI. The web service description language describes web services and how to access them. Q #17) Specify the parameters that define the SSL session connection? Answer: The parameters that define the SSL session connection are: Server and client random server write MACsecret Client write MACsecret Server write key Client write key Inventive vectors Sequence q #18) What is file enumeration? A: This kind of attack uses an emphatic url manipulation attack. Hackers can manipulate parameters in the URL string and can obtain critical data that is generally not open to the public, such as the data reached, the old version, or the data that is in development. Q #19) List of benefits that can be provided by the intrusion detection system? A: There are three advantages of an intrusion detection system. NIDS or NNIDS intrusion detection system or HIDS network node intrusion detection system or Q #20) What is HIDS? A: Hids or guest intrusion detection system is the system in which an image of an existing system is taken and compared to the previous snapshot. Checks whether important files have been modified or deleted, then an alert is generated and sent to the administrator. Q #21) List the main categories of SET participants? Answer: Below are the participants: Cardholder Merchant Acquirer Payment Gateway Certification Authority Q #22) Explain the URL manipulation? A: URL manipulation is a type of attack in which hackers manipulate the URL of a site to obtain important information. The information is passed in the parameters in the query string through the HTTP GET method between the client and the server. Hackers can change the information between these parameters and get authentication on servers and steal important data. To prevent this kind of attack, url manipulation security testing should be performed. Testers themselves can try to manipulate the URL and check for possible attacks, and if they find that they can prevent these kinds of attacks. Q #23) What are the three classes of intruders? Answer: Three classes of intruders are: Masquerade: It can be defined as which is not authorized on the computer, but hacks system access control and gains access to authenticated user accounts. Misfeasor: In this case, the user is authenticated to use system resources, but abused their 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) Indicate the component used in SSL? A: SSL or SSL is used to establish secure connections between clients and computers. Below are the components used in SSL: SSL Recorded protocol Handshake protocol Change Cipher Spec Encryption Algorithms Q #25) What is port scanning? A: Ports are where information goes in and out of any system. Scanning ports to detect any gaps in the system is called Port Scanning. There may be vulnerabilities in the system that hackers can attack and get important information. These points should be identified and prevented from any abuse. Below are the following types of port scanning: Strobe: Scan known services. UDP: Scan open Vanilla UDP ports: With this scan, the scanner attempts to connect to all 65,535 ports. Dragging: The scanner connects to the same port on more than one computer. Fragmented packets: The scanner sends packet fragments that can be accessed through simple packet filters in the Stealth scan firewall: The scanner blocks the scanned computer from recording port scanning activities. FTP bounce: The scanner passes through the FTP server to mask 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 can be read at any time later. A cookie may contain password information, some autofill information, and if hackers obtain this information, it can be dangerous. Learn how to test website cookies here. Q #27) What are the types of cookies? A: Cookie types are: Relational cookies – These cookies are temporary and last only in this session. Persistent cookies - These cookies stored on your hard drive and last until it expires or is manually deleted. Q #28) What is honeypot? Answer: Honeypot is a fake computer system that acts like 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) Specify the parameters that define the state of the SSL session? A: The parameters that define the ssl session state are: Peer Certificate Compression method Cipher spec Master secret Is resumable Q #30) Describe network intrusion detection system? A: The network intrusion detection system is commonly known as NIDS. It is used to analyze traffic forwarding across the subsite to match known attacks. If a gap is detected, the administrator receives an alert. Conclusion I hope that these questions and answers to safety testing are prepare for the interview. These answers also help you understand the concept of security testing. Read also => Ethical Hacking Courses Share this article if you find it useful! Useful!