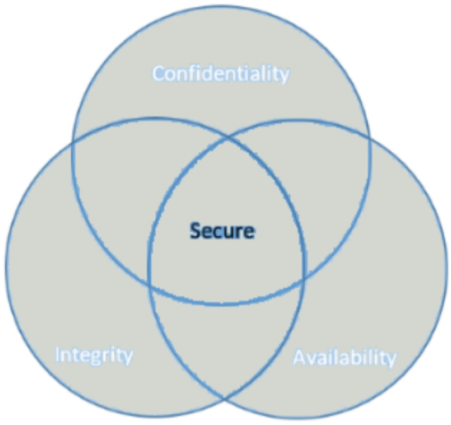
Powerofinformation

TOP 80 Application Security and Information Security Job Interview Questions & Answer

1. What is the CIA triangle?

CIA provides a standard for evaluating and implementing information security – irrespective of the system and/or organization in question.



Confidentiality: Data is accessible only to its concerned audience
Integrity: Ensuring that data is kept intact without meddling in the middle
Availability: Data and computers are available to authorized parties, as needed

2. What do you understand by Risk, Vulnerability & Threat?

Threat: Someone or something has potential to harm a system or an organization
Vulnerability: Weakness in a system that can be exploited by a potential hacker
Risk: Potential for loss or damage when threat exploits a vulnerability

3. What is Cognitive Cyber security?

Cognitive Cyber security is an application of AI technologies patterned on human thought processes to detect threats and protect physical and digital systems.

4. What is difference between IPS and IDS system?

IDS: Intrusion Detection System
IPS: Intrusion Prevention System

IDS just detect the intrusion and leave the rest to the administrator for assessment and evaluation. IPS detects the intrusion and takes necessary action to further prevent intrusion.

Also, there is a difference in the positioning of these devices in the network. Although they work on the same concept, the placement is different.

5. What are the steps to set up a firewall?

Following are the steps to set up a firewall

1. *Username/password:* modify the default password for a firewall device
2. *Remote administration:* Disable the feature of the remote administration
3. *Port forwarding:* Configure appropriate port forwarding for certain applications to work properly, such as web server or FTP server
4. *DHCP server:* Installing a firewall on a network with an existing DHCP server will cause conflict unless the firewall's DHCP is disabled
5. *Logging:* To troubleshoot firewall issues or potential attacks, ensure that logging is enabled and understand how to view logs
6. *Policies:* You should have solid security policies in place and make sure that the firewall is configured to enforce those policies.

6. Explain SSL and TLS?

SSL (Secure Sockets Layer) certificates create a foundation of trust by establishing a secure connection. SSL certificates have a key pair: a public and a private key. These keys work together to establish an encrypted connection.

TLS (Transport Layer Security)) is also an identification tool just like SSL, but it offers better security features. It provides additional protection to the data and hence SSL and TLS are often used together for better protection.

7. How can you prevent man in the middle (M.I.T.M) attack?

Now to answer that question, allow me to first tell you *what is MITM attack?*

A **MITM** attack happens when a communication between two parties (systems) is intruded or intercepted by an outside entity. This can happen in any form of online communication such as email, social media web surfing etc. They are trying to eavesdrop on your private conversations,

then they can also target all the information inside your devices and the outcome could be catastrophic.

Now here are some methods to prevent such attack,

The first method to prevent this attack would be an encryption (preferably public key encryption) between both the parties. This way, they both will have an idea with whom they are talking because of the digital verification.

The second method is to avoid open Wi-Fi networks and if it is necessary then use plugins like HTTPS, Forced TLS etc.

8. What is Vulnerability Assessment & Penetration testing?

A vulnerability assessment is the process of finding and measuring the severity of vulnerabilities in a system. Vulnerability assessments yield lists of vulnerabilities, often prioritized by severity and/or business criticality.

Vulnerability assessments typically involve the use of automated testing tools such as web and network security scanners, whose results are typically assessed, and escalated to development and operations teams. In other words, vulnerability assessments involve in-depth evaluation of a security posture designed to uncover weaknesses and recommending appropriate remediation or mitigation to remove or reduce risk.

In contrast, penetration testing is typically a **goal-oriented** exercise. A penetration testing has less to do with uncovering vulnerabilities, and is rather more focused on simulating a real-life attack, testing defenses and mapping-out paths a real attacker could take to fulfill a real-world goal. In other words, a penetration test is **usually about how an attacker is able to breach defenses and less about specific vulnerabilities**

9. Difference between Vulnerability Assessment & Penetration testing?

	Vulnerability scan	**Penetration test**
Frequency	At least quarterly, especially after new equipment is loaded or the network undergoes significant changes	Once or twice a year, as well as anytime the Internet-facing equipment undergoes significant changes

Reports	Provide a comprehensive baseline of what vulnerabilities exist and what changed since the last report	Concisely identify what data was compromised
Performed by	Typically conducted by in-house staff using authenticated credentials; does not require a high skill level	Best to use an independent outside service and alternate between two or three; requires a great deal of skill
Value	Detects when equipment could be compromised	Identifies and reduces weaknesses

10. What's the difference between Symmetric and Asymmetric encryption?

Symmetric encryption uses the same key to encrypt and decrypt, while Asymmetric uses different keys for encryption and decryption. Therefore many times an Asymmetric connection will be established first, then send creates the Symmetric connection.

Basis of Comparison	Symmetric Encryption	Asymmetric Encryption
Encryption key	Same key for encryption & decryption	Different keys for encryption & decryption
Performance	Encryption is fast but more vulnerable	Encryption is slow due to high computation
Purpose	Used for bulk data transmission	Often used for securely exchanging secret keys

11. What are some examples of symmetric encryption algorithms?

Blowfish, AES, RC4, DES, RC5, and RC6 are examples of symmetric encryption. The most widely used symmetric algorithm is AES-128, AES-192, and AES-256.

12. What are some examples of asymmetric encryption algorithms?

Popular asymmetric key encryption algorithm includes Diffie Hellman, EC, DSAC, EIGamal, RSA, DSA, and Elliptic curve techniques, PKCS.

13. What is an IV (Initialization vector)?

An initialization vector (IV) is an arbitrary number that can be used along with a secret key for data encryption. This number, also called a nonce, is employed only one time in any session.

The use of an IV prevents repetition in data encryption, making it more difficult for a hacker using a dictionary attack to find patterns and break a cipher. For example, a sequence might appear twice or more within the body of a message. If there are repeated sequences in encrypted data, an attacker could assume that the corresponding sequences in the message were also identical. The IV prevents the appearance of corresponding duplicate character sequences in the cipher text.

14. What are block cipher modes?

Block cipher is an encryption algorithm which takes fixed size of input say b bits and produces a cipher text of b bits again. If input is larger than b bits it can be divided further. For different applications and uses, there are several modes of operations for a block cipher.

15. What are some common block cipher modes?

ECB and CBC.

16. What's the main difference in security between ECB and CBC?

ECB just does a one-to-one lookup for encryption, without using an IV, which makes it fairly easy to attack using a chosen-plaintext attack. CBC uses an IV for the first block and then propagates the XOR of the previous block onto subsequent ones. The difference in results can be remarkable.

17. Can you describe Rainbow table?

A rainbow table is a listing of all possible plaintext permutations of encrypted passwords specific to a given hash algorithm.

Rainbow tables are often used by password cracking software for network security attacks. All computer systems that require password-based authentication store databases of passwords associated with user accounts, typically encrypted rather than plaintext as a security measure.

18. What is a Social Engineer?

Social Engineer is an art. Someone that will talk people into revealing passwords or sensitive information that will be used hacked application, systems.

19. Why is backing up data files important?

In information technology, a backup, or data backup, or the process of backing up, refers to the copying into an archive file of computer data that is already in secondary storage

- Backups ensure that the information can be reached whenever want.
- If the information is damaged it can be recovered
- The business continues to operate

20. What can you do if you fall victim to identity theft?

- Contact the fraud department of each three credit bureaus and request a fraud alert be put on your file
- File a report with your local police or the police in the community where the theft took place

21. What is residual risk?

Residual risk is the threat that remains after all efforts to identify and eliminate risk have been made.

There are four basic ways of dealing with risk: reduce it, avoid it, accept it or transfer it. Since residual risk is unknown, many organizations choose to either accept residual risk or transfer it

22. What is Zero Day Exploit?

A zero day exploit is a cyber-attack that occurs on the same day a weakness is discovered in software. At that point, it's exploited before a fix becomes available from its creator.

23. What is network sniffing?

System sniffing includes utilizing sniffer tools that empower real- time monitoring and analysis of data streaming over PC systems. Sniffers can be utilized for various purposes, regardless of whether it's to steal data or manage systems.

Network sniffing is utilized for ethical and unethical purposes. System administrators utilize these as system monitoring and analysis tool to analyze and avoid network related issues, for example, traffic bottlenecks

Cyber criminals utilize these devices for untrustworthy purposes, for example, character usurpation, email, delicate information hijacking etc.

24. What do you mean by DOS (Denial of administration) assault? Explain. What are the regular types of DOS assault?

Denial of Service is a malicious attack on network that is executed by flooding the system with useless traffic. Despite the fact that DOS does not cause any data breach or security breach, it can cost the site proprietor a lot of cash and time.

- Buffer Overflow Attacks
- SYN Attack
- Teardrop Attack
- Smurf Attack
- Viruses

25. What is Pharming and Defacement?

Pharming is a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent. Pharming has been called "phishing without a lure."

Defacement: The attacker replaces the firm's site with an alternate page. It contains the hacker's name, images and may even incorporate messages and background music.

26. What is an ARP and how does it work?

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.

When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address.

The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine.

If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it.

Self-learning security systems use data mining, pattern recognition, and natural language processing to simulate the human brain, albeit in a high-powered computer model.

27. What is ARP Spoofing?

ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. Once the attacker's MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address. ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol.

28. How can you avoid ARP poisoning?

Static ARP entries

This solution involves a lot of administrative overhead and is only recommended for smaller networks. It involves adding an ARP entry for every machine on a network into each individual computer.

Mapping the machines with sets of static IP and MAC addresses helps to prevent spoofing attacks, because the machines can ignore ARP replies. Unfortunately, this solution can only protect you from simpler attacks.

Encryption

Protocols such as HTTPS and SSH can also help to reduce the chances of a successful ARP poisoning attack. When traffic is encrypted, the attacker would have to go to the additional step of tricking the target's browser into accepting an illegitimate certificate. However, any data transmitted outside of these protocols will still be vulnerable.

VPNs

A VPN can be a reasonable defense for individuals, but they are generally not suitable for larger organizations. If it is just a single person making a potentially dangerous connection, such as using public Wi-Fi at an airport, then a VPN will encrypt all of the data that travels between the client and the exit server. This helps to keep them safe, because an attacker will only be able to see the cipher text.

Packet filters

These filters analyze each packet that gets sent across a network. They can filter out and block malicious packets, as well as those whose IP addresses are suspicious. Packet filters can also tell if a packet claims to come from an internal network when it actually originates externally, helping to reduce the chances of an attack being successful.

29. What is port blocking within LAN?

Restricting the users from accessing a set of services within the local area network is called port blocking.

Stopping the source to not to access the destination node via ports. As the application works on the ports, so ports are blocked to restricts the access filling up the security holes in the network infrastructure.

30. What is a VLAN?

VLAN is a set of hosts that communicate with each other as if they were connected to the same switch (as if they were in the same domain), even if they are not. VLANs avoid the requirement of computers to be in the same physical location to be in the same broadcast domain, which allows to group hosts logically rather than their physical location. There are two types of VLANs called Static VLANs and Dynamic VLANs. Static VLANs are VLANs that are manually configured by providing a name, VLAN ID (VID) and port assignments. Storing the hardware addresses of host devices in a database so that the switch can assign the VLAN dynamically at any time when a host is plugged in to a switch creates dynamic VLANs.

31. What is a VPN?

VPN provides a secure method for connecting to a private network through a public network that is not secure such as the Internet. Data that is sent through the unsecure public network are encrypted to maintain the security. VPNs allow only authorized users to access it and this is done through authentication. VPNs use passwords, biometrics, etc for authenticating its users. VPNs are widely used by organizations to share their data and other network resources with workers located in remote locations. Use of VPNs would reduce the network cost of an organization, since it removes the requirement of having leased lines to connect organization's network with offices located in remote locations. VPNs can vary depending on factors like the protocol it uses to send traffic, security provisions, whether the VPN provides site-to-site or remote access, etc.

32. What protocols fall under TCP/IP internet layer?

OSI Ref. Layer No.	OSI Layer Equivalent	TCP/IP Layer	TCP/IP Protocol Examples

5,6,7	Application, Session, Presentation	Application	NFS, NIS+, DNS, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP, and others
4	Transport	Transport	TCP, UDP
3	Network	Internet	IP, ARP, ICMP
2	Data Link	Data Link	PPP, IEEE 802.2
1	Physical	Physical Network	Ethernet (IEEE 802.3) Token Ring, RS-232, others

33. What is incident management?

Incident management (IM) is the practice of restoring services as quickly as possible after an incident. IT incident management helps keep an organization prepared for unexpected hardware, software and security failings, and it reduces the duration and severity of disruption from these events. It can follow an established ITSM framework, such as IT infrastructure library (ITIL) or COBIT, or be based on a combination of guidelines and best practices established over time.

34. What Are Black, Gray, and White Box Testing?

Black-Box Testing

In a black-box testing assignment, the penetration tester is placed in the role of the average hacker, with no internal knowledge of the target system. Testers are not provided with any architecture diagrams or source code that is not publicly available. A black-box penetration test determines the vulnerabilities in systems that are exploitable from outside the network.

Gray-Box Testing

Gray-box pen testers typically have some knowledge of a network's internals, potentially

including design and architecture documentation and an account internal to the network.

The purpose of gray-box penetration testing is to provide a more focused and efficient assessment of a network's security than a black-box assessment.

White-Box Testing

White-box testing goes by several different names, including clear-box, open-box, auxiliary and logic-driven testing. It falls on the opposite end of the spectrum from black-box testing and penetration testers are given full access to source code, architecture documentation and so forth. The main challenge with white-box testing is sifting through the massive amount of data available to identify potential points of weakness, making it the most time-consuming type of penetration testing.

35. What is the difference between Red, Blue, and Purple Teams?

Red Teams are external entities brought in to test the effectiveness of a security program. This is accomplished by emulating the behaviors and techniques of likely attackers in the most realistic way possible. The practice is similar, but not identical to, penetration testing, and involves the pursuit of one or more objectives.

Blue Teams refer to the internal security team that defends against both real attackers and Red Teams. Blue Teams should be distinguished from standard security teams in most organizations.

Purple teams are ideally superfluous groups that exist to ensure and maximize the effectiveness of the Red and Blue teams.

36. What are 7 OSI layers?

Layer Name	Key Responsibilities	Data Type Handled	Scope	Common Protocols and Technologies
Physical	Encoding and Signaling; Physical Data Transmission; Hardware	Bits	Electrical or light signals	(Physical layers of most of the

	Specifications; Topology and Design		sent between local devices	technologies listed for the data link layer)
Data Link	Logical Link Control; Media Access Control; Data Framing; Addressing; Error Detection and Handling; Defining Requirements of Physical Layer	Frames	Low-level data messages between local devices	IEEE 802.2 LLC, Ethernet Family; Token Ring; FDDI and CDDI; IEEE 802.11 (WLAN, Wi-Fi); HomePNA; HomeRF; ATM; SLIP and PPP
Network	Logical Addressing; Routing; Datagram Encapsulation; Fragmentation and Reassembly; Error Handling and Diagnostics	Datagrams / Packets	Messages between local or remote devices	IP; IPv6; IP NAT; IPsec; Mobile IP; ICMP; IPX; DLC; PLP; Routing protocols such as RIP and BGP
Transport	Process-Level Addressing; Multiplexing/	Datagrams /	Communication between	TCP and UDP; SPX;

	Demultiplexing; Connections; Segmentation and Reassembly; Acknowledgments and Retransmissions; Flow Control	Segments	software processes	NetBEUI/ NBF
Session	Session Establishment, Management and Termination	Sessions	Sessions between local or remote devices	NetBIOS, Sockets, Named Pipes, RPC
Presentation	Data Translation; Compression and Encryption	Encoded User Data	Application data representations	SSL; Shells and Redirectors; MIME
Application	User Application Services	User Data	Application data	DNS; NFS; BOOTP; DHCP; SNMP; RMON; FTP; TFTP; SMTP; POP3; IMAP; NNTP; HTTP; Telnet

37. What is Forward Secrecy?

Forward Secrecy is a system that uses ephemeral session keys to do the actual encryption of TLS data so that even if the server's private key were to be compromised, an attacker could not use it to decrypt captured data that had been sent to that server in the past.

38. What are salted hashes?

Salt is a random data. When a properly protected password system receives a new password, it creates a hash value of that password, a random salt value, and then the combined value is stored in its database. This helps to defend against dictionary attacks and known hash attacks.

39. What are the three ways to authenticate a person?

Something they know (password), something they have (token), and something they are (biometrics). Two-factor authentication often times uses a password and token setup, although in some cases this can be a PIN and thumbprint.

40. What steps will you take to secure a server?

Secure servers use the Secure Sockets Layer (SSL) protocol for data encryption and decryption to protect data from unauthorized interception.

Here are four simple ways to secure server:

Step 1: Make sure you have a secure password for your root and administrator users

Step 2: The next thing you need to do is a make new user on your system. These will be the users you use to manage the system

Step 3: Remove remote access from the default root/administrator accounts

Step 4: The next step is to configure your firewall rules for remote access

41. Why do you need DNS monitoring?

The DNS allows your website under a certain domain that is easily recognizable and also keeps the information about other domain names. It works like a directory for everything on the Internet. Thus, DNS monitoring is very important since you can easily visit a website without actually having to memorize their IP address.

42. Can you explain what application security is? Why Web Application Security is Important?

Application security is the use of software, hardware, and procedural methods to protect applications from external and internal threats.

Because attackers are exploiting web application security vulnerabilities to gain access to private data, organizations must go to even greater lengths to protect websites and apps than they do to protect their computers and other network-connected devices.

Applications have an increasingly crucial role in our lives, yet they are also a real security threat, with hackers always finding new ways to bypass security defenses.

43. List out the techniques used to prevent web server attacks?

- Patch Management
- Secure installation and configuration of the O.S
- Safe installation and configuration of the web server software
- Scanning system vulnerability
- Anti-virus and firewalls
- Remote administration disabling
- Removing of unused and default account
- Changing of default ports and settings to customs port and settings

44. Why is API security important?

Applications use APIs to connect services and to transfer data. Unsecure APIs are behind major data breaches. Medical, financial, and personal data are sensitive data. Not all data is the same nor should be protected in the same way. How you approach API security will depend on what kind of data is being transferred.

45. What is REST Security Design Principles?

1. **Least Privilege:** An entity should only have the required set of permissions to perform the actions for which they are authorized, and no more. Permissions can be added as needed and should be revoked when no longer in use.

2. **Fail-Safe Defaults:** A user's default access level to any resource in the system should be "denied" unless they've been granted a "permit" explicitly.

3. **Economy of Mechanism:** The design should be as simple as possible. All the component interfaces and the interactions between them should be simple enough to understand.

4. **Complete Mediation:** A system should validate access rights to all its resources to ensure that they're allowed and should not rely on cached permission matrix. If the access level to a given resource is being revoked, but that isn't reflected in the permission matrix, it would violate the security.

5. **Open Design:** This principle highlights the importance of building a system in an open manner—with no secret, confidential algorithms.

6. **Separation of Privilege:** Granting permissions to an entity should not be purely based on a single condition; a combination of conditions based on the type of resource is a better idea.

7. **Least Common Mechanism:** It concerns the risk of sharing state among different components. If one can corrupt the shared state, it can then corrupt all the other components that depend on it.

8. **Psychological Acceptability:** It states that security mechanisms should not make the resource more difficult to access than if the security mechanisms were not present. In short, security should not make worse the user experience.

46. What are some of the most common API security best practices?

Here are some of the most common ways you can strengthen your API security:

- **Use tokens**. Establish trusted identities and then control access to services and resources by using tokens assigned to those identities.

- **Use encryption and signatures**. Encrypt your data using a method like TLS (see above). Require signatures to ensure that the right users are decrypting and modifying your data, and no one else.

- **Identify vulnerabilities**. Keep up with your operating system, network, drivers, and API components. Know how everything works together and identify weak spots that could be used to break into your APIs. Use sniffers to detect security issues and track data leaks.

- **Use quotas and throttling**. Place quotas on how often your API can be called and track its use over history. More calls on an API may indicate that it is being abused. It could also be a programming mistake such as calling the API in an endless loop. Make rules for throttling to protect your APIs from spikes and Denial-of-Service attacks.

- **Use an API gateway**. API gateways act as the major point of enforcement for API traffic. A good gateway will allow you to authenticate traffic as well as control and analyze how your APIs are used.

- **Input validation** Input validation vulnerability is characterized by the ability to decide at each step of the execution whether or not the program is in a safe state**. Input validation**, also known as data validation, is the proper testing of any input supplied by a user or application. Input validation refers to how your application filters, scrubs, or rejects input before additional processing. While input validation can be either whitelisted or blacklisted, it is preferable to whitelist data. Whitelisting only passes expected data. In contrast, blacklisting relies on programmers predicting all unexpected data

- **Error handling** Improper handling of errors can introduce a variety of security problems for a web site. The most common problem is when detailed internal error messages such as stack traces, database dumps, and error codes are displayed to the user (hacker).

47. What is web API security?

Web API security is concerned with the transfer of data through APIs that are connected to the Internet. Web API is an extensible framework for building HTTP based services that can be accessed in different applications on different platforms such as web, windows, mobile etc.

48. What are REST API and SOAP API?

REST APIs use HTTP and support Transport Layer Security (TLS) encryption. TLS is a standard that keeps an Internet connection private and checks that the data sent between two systems (a server and a server, or a server and a client) is encrypted and unmodified. REST APIs also use JavaScript Object Notation (JSON), which is a file format that makes it easier to transfer data over web browsers. By using HTTP and JSON, REST APIs don't need to store or repackage data, making them much faster than SOAP APIs.

SOAP APIs use built-in protocols known as Web Services Security (WS Security). These protocols define a rules set that is guided by confidentiality and authentication. SOAP APIs support standards set by the two major international standards bodies, the Organization for the Advancement of Structured Information Standards (OASIS) and the World Wide Web Consortium (W3C). They use a combination of XML encryption, XML signatures, and SAML tokens to verify authentication and authorization. In general, SOAP APIs are praised for having more comprehensive security measures, but they also need more management. For these reasons, SOAP APIs are recommended for organizations handling sensitive data.

49. What is Cloud Security?

Cloud security, also known as cloud computing security, consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data and infrastructure. These security measures are configured to protect data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices. From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business. And because these rules can be configured and managed in one place, administration overheads are reduced and IT teams empowered to focus on other areas of the business.

50. How can we improve cloud security?

1. Implement Strong Authentication Protocol
2. User Access Management Solutions.
3. Monitor, Log, and Analyze User Activities.
4. Provide Employee Training.

5. Implement a Data Backup and Recovery Policy.
6. Take Advantage of Cloud Computing Without the Security Risks.
7. Deploy Two-Factor Authentication
8. Monitor, Log, and Analyze User Activities

51. What is XSS?

Cross-Site Scripting (or XSS) refers to client-side code injection attack wherein an attacker can execute malicious into a legitimate website or web application. JavaScript can run on the client side. It has 3 types. These are reflected, stored and DOM XSS. Input validation, encoded user inputs are ways to protest against XSS.

52. How does one defend against XSS?

1. Escaping

The first method you can and should use to prevent XSS vulnerabilities from appearing in your applications is by escaping user input. Escaping data means taking the data an application has received and ensuring it's secure before rendering it for the end user. By escaping user input, key characters in the data received by a web page will be prevented from being interpreted in any malicious way. In essence, you're censoring the data your web page receives in a way that will disallow the characters – especially < and > characters – from being rendered, which otherwise could cause harm to the application and/or users.

2. Validating Input

Validating input is the process of ensuring an application is rendering the correct data and preventing malicious data from doing harm to the site, database, and users. While whitelisting and input validation are more commonly associated with SQL injection, they can also be used as an additional method of prevention for XSS. Whereas blacklisting, or disallowing certain, predetermined characters in user input, disallows only known bad characters, whitelisting only allows known good characters and is a better method for preventing XSS attacks as well as others.

3. Sanitizing

A third way to prevent cross-site scripting attacks is to sanitize user input. Sanitizing data is a strong defense, but should not be used alone to battle XSS attacks. It's totally possible you'll find the need to use all three methods of prevention in working towards a more secure application. Sanitizing user input is especially helpful on sites that allow HTML markup, to ensure data received can do no harm to users as well as your database by scrubbing the data clean of potentially harmful markup, changing unacceptable user input to an acceptable format.

53. What is Cross-Site Request Forgery?

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. CSRF attacks specifically target state-changing requests, not theft of data, since the attacker has no way to see the response to the forged request. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

54. What is difference between XSS and CSRF?

Two of the most common attacks against web sites and web application are XSS (Cross-site Scripting) and CSRF (Cross-Site Request Forgery). Both kind of attacks are exploited regularly on applications. *In case of XSS, the victim's trust for a web site is exploited, in case of CSRF, the web site's trust for a victim's browser is exploited.*

55. How does defend against CSRF?

The most common method to prevent Cross-Site Request Forgery (CSRF) attacks is to append CSRF tokens to each request and associate them with the user's session. Such tokens should at a minimum be unique per user session, but can also be unique per request. By including a challenge token with each request, the developer can ensure that the request is valid and not coming from a source other than the user.

56. Why input validation is important for applications?

Input validation is required to prevent web form abuse by malicious users. Improper validation of form data is one of the main causes of security vulnerabilities. It exposes your applications to attacks such as header injections, cross-site scripting, HTTP Verb

tampering and Parameter Pollution, LDAP injection, ORM injection, XML injection, Server-Side Includes (SSI) Injection, XPath injection, Code injection and SQL injections.

57. How can SQL injection be prevented?

Sanitize user input: User input should be never trusted it must be sanitized before it is used
Stored procedures: These can encapsulate the SQL statements and treat all input as parameters
Regular expressions: Detecting and dumping harmful code before executing SQL statements
Database connection user access rights: Only necessary and limited access right should be given to accounts used to connect to the database
Error messages: Error message should not be specific telling where exactly the error occurred it should be more generalized.

58. What is Brute Force Attack?

A Brute Force Attack is the simplest method to gain access to a site or server (or anything that is password protected). It tries various combinations of usernames and passwords again and again until it gets in. Attackers automate the process of creating numerous passwords to be tested against a target.

59. What are the various ways to handle account brute forcing?

1. Password Length.
2. Password Complexity.
3. Limit Login Attempts.
4. Modifying htaccess file.
5. Using Captcha.
6. Two Factor Authentications.
7. Create rule of Web Application Firewall (WAF)

60. If you had to both encrypt and compress data during transmission, which would you do first, and why?

Compress and then encrypt is better. Data compression removes redundant character strings in a file. So the compressed file has a more uniform distribution of characters. This also provides shorter plaintext and cipher text, which reduces the time spent encrypting, decrypting and transmitting the file.

61. What is the data leak?

Data leakage is when data gets out of the organization in an unauthorized way.

Data can get leaked through various ways – emails, prints, laptops getting lost, unauthorized upload of data to public portals, removable drives, photographs etc.

62. What are the factors that can cause data loss?

- Human error
- System misconfiguration
- A system breach from a hacker
- A home-grown application developed to interface to the public
- Inadequate security control for shared documents or drives
- Corrupt hard-drive
- Back up are stored in an insecure place

63. List out the steps to successful data loss prevention controls?

- Create an information risk profile
- Create an impact severity and response chart
- Based on severity and channel determine incident response
- Create an incident workflow diagram
- Assign roles and responsibilities to the technical administrator, incident analyst, auditor and forensic investigator
- Develop the technical framework
- Expand the coverage of DLP controls
- Append the DLP controls into the rest of the organization
- Monitor the results of risk reduction

64. What is DLP (Data Loss Prevention)?

DLP (Data Loss Prevention) is an acronym for data loss prevention, or data leak prevention, and refers to network security tools that can identify confidential information, track its movement through an enterprise, and prevent unauthorized exposure or disclosure of sensitive data by enforcing leak prevention policies. Sensitive information is:

- Corporate data, including strategic planning documents, financial documents, due diligence research and employee information.

- Intellectual property such as product design documents, internal price lists, source code and process documentation.
- Customer information, including credit card numbers, medical records, financial statements and Social Security numbers.

65. What is DLP (Data Loss Prevention)'s relationship to application security?

When building micro services, desktop programs, web applications and mobile apps, application security solutions can help development teams augment DLP (Data Loss Prevention) by eradicating software vulnerabilities that can lead to data leaks.

Application testing promotes enterprise data protection by identifying and eradicating software weaknesses that can lead to serious breaches. By testing to ensure that micro services, web, mobile, and desktop applications are free of flaws and vulnerabilities, developers and IT teams can help to achieve enterprise data protection more easily and successfully.

66. What is DevOps?

Combining "development" and "operations" formed the term.

Explanation of Gartner:

"DevOps represents a change in IT culture, focusing on rapid IT service delivery through the adoption of agile, lean practices in the context of a system-oriented approach. DevOps emphasizes people (and culture), and seeks to improve collaboration between operations and development teams. DevOps implementations utilize technology— especially automation tools that can leverage an increasingly programmable and dynamic infrastructure from a life cycle perspective."

67. What is DevSecOps?

DevSecOps involves creating a 'Security as Code' culture with ongoing, flexible collaboration between release engineers and security teams. The DevSecOps movement, like DevOps itself, is focused on creating new solutions for complex software development processes within an agile framework.

68. What is security source code analysis for applications?

Source code analysis tools, also referred to as Static Application Security Testing (SAST) Tools, are designed to analyze source code and/or compiled versions of code to help find security flaws.

Some tools are starting to move into the IDE. For the types of problems that can be detected during the software development phase itself, this is a powerful phase within the development life cycle to employ such tools, as it provides immediate feedback to the developer on issues they might be introducing into the code during code development itself. This immediate feedback is very useful, especially when compared to finding vulnerabilities.

69. Could you give some information about Burp Suite tabs that are used when you make penetration testing?

Burp Intruder is a powerful tool for performing automated customized attacks against web applications. It is extremely flexible and configurable, and can be used to automate all kinds of tasks that arise when testing applications.

Note: Using Burp Intruder may result in unexpected effects in some applications. Until you are fully familiar with its functionality and settings, you should only use Burp Intruder against non-production systems.

Burp Spider is a tool for automatically crawling web applications. While it is generally preferable to map applications manually, you can use **Burp Spider** to partially automate this process for very large applications, or when you are short of time.

Scanner: Burp Scanner is a tool for automatically finding security vulnerabilities in web applications. It is designed to be used by security testers, and to fit in closely with your existing techniques and methodologies for performing manual and semi-automated penetration tests of web applications.

Note: Using Burp Scanner may result in unexpected effects in some applications. Until you are fully familiar with its functionality and settings, you should only use Burp Scanner against non-production systems.

Repeater: Burp Repeater is a simple tool for manually manipulating and reissuing individual HTTP and WebSocket messages, and analyzing the application's responses. You can use Repeater for all kinds of purposes, such as changing parameter values to test for input-based vulnerabilities, issuing requests in a specific sequence to test for logic flaws, and reissuing requests

The main Repeater UI lets you work on multiple different messages simultaneously, each in its own tab. When you send messages to Repeater, each one is opened in its own numbered tab. You can rename tabs by double-clicking the tab header.

Sequencer: Burp Sequencer is a tool for analyzing the quality of randomness in a sample of data items. It is used to test for an application's session tokens, anti-CSRF tokens, password, reset tokens, etc.

Decoder: Burp Decoder is a simple tool for transforming encoded data into its canonical form, or for transforming raw data into various encoded and hashed forms. It is capable of intelligently recognizing several encoding formats using heuristic techniques. Different transformations can be applied to different parts of the data. The following decode and encode operations are available:

- URL
- HTML
- Base64
- ASCII hex
- Hex
- Octal
- Binary
- GZIP

Burp Comparer is a simple tool for performing a comparison between any two items of data. Some common uses for Burp Comparer are as follows:

- When looking for username enumeration conditions, you can compare responses to failed logins using valid and invalid usernames, looking for subtle differences in the responses.
- When an Intruder attack has resulted in some very large responses with different lengths than the base response, you can compare these to quickly see where the differences lie.

- When comparing the site maps or Proxy history entries generated by different types of users, you can compare pairs of similar requests to see where the differences lie that give rise to different application behavior.
- When testing for blind SQL injection bugs using Boolean condition injection and other similar tests, you can compare two responses to see whether injecting different conditions has resulted in a relevant difference in responses.

Burp Extender lets you extend the functionality of Burp Suite in numerous ways. This page contains technical details to help you develop Burp extensions. The extensibility API is extremely rich and powerful, and lets extensions carry out numerous useful tasks (ref. https://portswigger.net/burp).

70. What is Anti-tamper software for mobile application security testing?

Anti-tamper software (or **tamper-resistant software**) is software that makes it harder for an attacker to modify it. The measures involved can be passive such as obfuscation to make reverse engineering difficult or active tamper-detection techniques that aim to make a program malfunction or not operate at all if modified. It is essentially tamper resistance implemented in the software domain. It shares certain aspects but also differs from related technologies like copy protection and trusted hardware, though it is often used in combination with them. Anti-tampering technology typically makes the software somewhat larger and also has a performance impact.

Tampering with your application has several benefits for the attackers: Authentication bypass, geo-location falsification, stealing sensitive data and many others. It can then be leveraged to get access to offline documents, location falsification, payment and medical related sensitive information.

71. What is insecure data storage? How can mobile application prevent insecure data storage?

Some sensitive data such as passwords, credit card numbers, account records, or any other type of information stored in mobile devices' without encrypted.

A few examples of the errors that are commonly made when securing data storage include:

- Simply not encrypting critical data

- Insecurely storing keys, certificates, and passwords
- Weak choices of algorithm
- The attempt to create one's own encryption algorithm
- Not including the proper support for encryption key changes and other necessary maintenance precautions

If the sensitive data must indeed be stored, some general rules of thumb are:

- Do not store credentials on the phone file system. A standard login each time the application is opened and that the appropriate session timeouts are put into place.
- Be particular about the cryptography that is being implemented and use solutions that avoid the leakage of binary signature that are often used in encryption libraries.
- Avoid using hardcoded encryption or decryption keys.
- Add another layer of encryption beyond the default encryption methods provided by the operating system

72. What is AndroidManifest.xml file?

Every app project must have an `AndroidManifest.xml` file (with precisely that name) at the root of the project source set. The manifest file describes essential information about your app to the Android build tools, the Android operating system, and Google Play (ref. https://developer.android.com/guide/topics/manifest/manifest-intro).

Among many other things, the manifest file is required to declare the following:

- The app's package name, which usually matches your code's namespace. The Android build tools use this to determine the location of code entities when building your project. When packaging the app, the build tools replace this value with the application ID from the Gradle build files, which is used as the unique app identifier on the system and on Google Play
- The components of the app, which include all activities, services, broadcast receivers, and content providers. Each component must define basic properties such as the name of its Kotlin or Java class. It can also declare capabilities such as which device

configurations it can handle, and intent filters that describe how the component can be started.

- The permissions that the app needs in order to access protected parts of the system or other apps. It also declares any permission that other apps must have if they want to access content from this app.
- The hardware and software features the app requires, which affects which devices can install the app from Google

73. Could you give some examples for Application Security policies?

FISMA compliance, HIPAA compliance, The National Institute of Standards & Technology (NIST) compliance, The Open Web Application Security Project (OWASP), PCI, PCI DSS, The Sarbanes-Oxley Act (SarbOx), SOX compliance. OWASP Application Security Verification Standard (ASVS)

74. What is Poor Code Quality for mobile application?

It can pass untrusted inputs to method calls made within mobile code. These types of issues are not necessarily security issues in and of themselves but lead to security vulnerabilities. Poor code-quality issues are typically exploited via malware or phishing scams (ref.OWASP).

Code quality issues can be avoided by doing the following:

- Maintain consistent coding patterns that everyone in the organization agrees upon;
- Write code that is easy to read and well-documented;
- When using buffers, always validate that the lengths of any incoming buffer data will not exceed the length of the target buffer;
- Via automation, identify buffer overflows and memory leaks through the use of third-party static analysis tools; and
- Prioritize solving buffer overflows and memory leaks over other 'code quality' issues.

75. What are vulnerability classifiers and quantifiers for mobile application security?

Common Weakness Enumeration (CWE): CWE is a software weakness classification system

maintained by the MITRE Corporation

Common Vulnerabilities and Exposures (CVE): The CVE dictionary is a naming scheme for software vulnerabilities that also is hosted by MITRE

Common Vulnerability Scoring System (CVSS): The Common Vulnerability Scoring System Version (CVSS) is a vulnerability scoring system owned and maintained by the Forum of Incident Response and Security Teams (FIRST)

76. What is malware?

Malware is the collective name for a number of malicious software variants, including viruses, ransom ware and spyware. Malware typically consists of code developed by cyber attackers, designed to cause extensive damage to data and systems or to gain unauthorized access to a network. Malware is typically delivered in the form of a link or file over email and requires the user to click on the link or open the file to execute the malware.

77. What is adware?

Adware is the name given to programs that are designed to display advertisements on your computer, redirect your search requests to advertising websites and collect marketing-type data about you – for example, the types of websites that you visit – so that customized adverts can be displayed.

78. Your supervisor is very busy and asks you to log into the HR Server using her user-ID and password to retrieve some reports. What should you do?

Decline the request and remind your supervisor that it is against policy. User IDs and passwords must not be shared. If pressured further, report the situation to management

79. A friend sends an electronic gift card (e-card) to your work email. You need to click on the attachment to see the card. What should you do?

Delete the message.

This one has four big risks:

- Some attachments contain viruses or other malicious programs. It's risky to open unknown or unsolicited attachments.
- Also, in some cases just clicking on a malicious link can infect a computer. Unless you are sure a link is safe, don't click on it.
- Email addresses can be faked, so just because the email says it is from someone you

know, you can't be certain of this without checking with the person.

- Finally, some websites and links look legitimate, but they're really hoaxes designed to steal your information.

80. The mouse on your computer screen starts to move around on its own and clicks on things on your desktop. What do you do?

a) Call your co-workers over so they can see

b) Disconnect your computer from the network

c) Unplug your mouse

d) Tell your supervisor

e) Turn your computer off

f) Run anti-virus

g) All of the above

Since it seems possible that someone is controlling the computer remotely, it is best if you can disconnect the computer from the network (and turn off wireless if you have it) until help arrives. If possible, don't turn off the computer. This is definitely suspicious. Immediately report the problem to your supervisor