

Top 100 Cybersecurity

INTERVIEW

Questions for:

- ✓ Beginners
- ✓ Intermediate Level
- ✓ Advanced Level



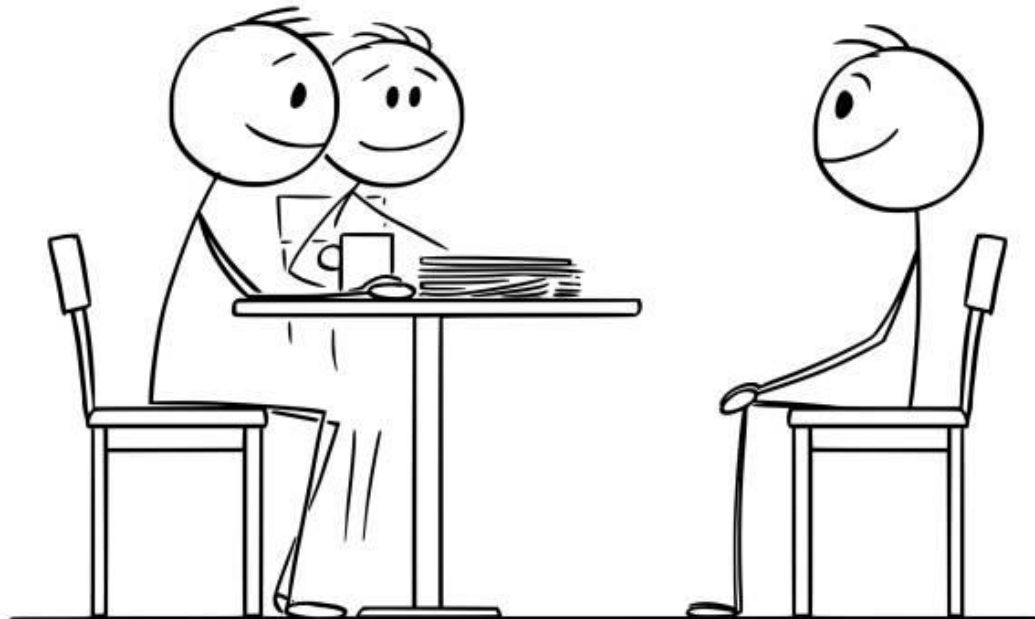
Mohammed Almunajam

Welcome to Your Cybersecurity Interview!



Hello there!

Welcome to your interview for a cybersecurity position. We're on the lookout for talented individuals passionate about **safeguarding our systems** from **the growing digital threats**.



Mohammed Almunajam

1. What is cybersecurity, and why is it important?

Cybersecurity: protects computer systems, networks, and data from theft, damage, or unauthorized access. It's **important** to safeguard sensitive information, maintain privacy, prevent financial losses, and protect critical infrastructure from cyber threats.

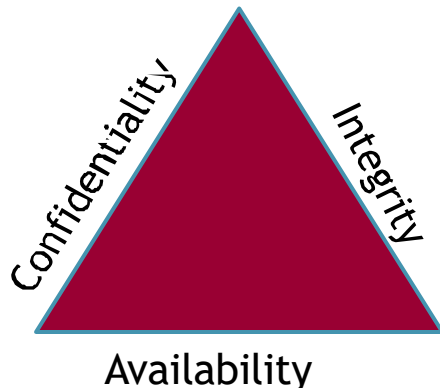
2. Define the terms Virus, Worm, Malware, and Ransomware

- Virus**: A program that replicates itself and spreads to other files or systems, often causing harm.
- Worm**: A computer worm is a type of malware that spreads to networks copies of itself .
- Malware**: A broader term encompassing any malicious software that disrupts or gains unauthorized access to computer systems.
- Ransomware**: A malicious software encrypting files or computer systems and requesting a ransom for their decryption.

3. What is Cryptography?

Cryptography is the practice and study of techniques for **securing information** and **communication** mainly to protect the data from third parties that the data is not intended for.

4.Explain CIA triad.



Confidentiality - restrict access to authorized individuals

Integrity - data has not been altered in an unauthorized manner

Availability - information can be accessed and modified by authorized individuals in an appropriate timeframe

5. Explain the difference between a Threat, Vulnerability, and Risk in cybersecurity.



6. What are some of the common Cyberattacks?



7. What is Phishing? Provide an example.

• **Phishing**: A cyberattack in which malicious actors employ deceptive emails or messages to deceive individuals into disclosing sensitive information.

• **Example**: An email claiming to be from a bank, requesting the recipient to provide their login credentials by clicking a link that leads to a fake website.

Mohammed Almunajam

8. What is a Brute Force Attack? How can you prevent it?

Brute Force is a way of finding out the right credentials by repetitively trying all the permutations and combinations of possible credentials.

Prevent Brute Force attacks (Password Length - Password Complexity - Limiting Login Attempts)

9. What is a DDoS attack and how does it work?

A Distributed Denial of Service (DDoS) attack inundates a target server or network with excessive traffic originating from numerous sources, making it inaccessible to genuine users

10. What is Port Scanning?

Port Scanning is the technique used to identify open ports and service available on a host. **Hackers** use port scanning to find information that can be helpful to exploit vulnerabilities.

11. What are cookies in a web browser?

Cookies are stored by websites on a user's device. They are used to track user preferences, session information, and provide a personalized browsing experience.

12. How can you prevent a Man-In-The-Middle attack?

a type of attack where the hacker places himself in between the communication of two parties and steal the information

Use **secure** communication protocols, verify digital certificates, and **avoid public Wi-Fi** for sensitive transactions. Implementing strong encryption also helps

Mohammed Almunajam

13. .What is XSS?

XSS(Cross-Site Scripting) is a cyberattack that enables hackers to inject malicious client-side scripts into web pages. XSS can be used to hijack sessions and steal cookies,

14. What is an ARP ?

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.

ARP poisoning is sending fake addresses to the switch so that it can associate the fake addresses with the IP address of a genuine computer on a network and hijack the traffic.

15. What is a Botnet?

A Botnet is a number of devices connected to the internet where each device has one or more bots running on it. The bots on the devices and malicious scripts used to hack a victim.

16. What is social engineering? Give an example.

• **Social engineering** manipulates individuals to disclose confidential information or perform actions for malicious purposes.

• **Example:** Pretending to be a trusted colleague and asking for login credentials over the phone.

17. What is the difference between IDS and IPS?

• **IDS (Intrusion Detection System):** Monitors network traffic and generates alerts when suspicious activity is detected.

• **IPS (Intrusion Prevention System):** Not only detects but also actively blocks or prevents suspicious network activity.

Mohammed Almunajam

18. What is SSL encryption?

SSL (Secure Sockets Layer) encryption is a protocol that ensures secure data transmission between a user's web browser and a website server, protecting data during transit.

19. Define the terms Encryption and Decryption.

- **Encryption:** Converting plaintext data into a coded format to protect it from unauthorized access.

- **Decryption:** Converting encrypted data back into its original, readable form.

20. What is two-factor authentication, and why is it important?

- Two-factor authentication enhances security by necessitating users to furnish two distinct forms of verification, typically a password and a temporary code, thereby bolstering protection.

- **It's important** because even if a password is compromised, unauthorized access is prevented without the second factor.

21. What is a VPN and why is it used?

- **A Virtual Private Network** encrypts and secures internet connections, ensuring privacy and anonymity.

- **It protects** data from **eavesdropping**, accesses restricted content, and enhances public Wi-Fi security.

22. What is SQL injection.

SQL Injection exploits vulnerabilities in SQL queries to manipulate a database.

Mohammed Almunajam

23. What is Cryptography?

Cryptography is the practice and study of techniques for securing information and communication mainly to protect the data from third parties that the data is not intended for.

24. What is a Firewall?

It is a security system designed for the network. A firewall is set on the boundaries of any system or network which monitors and controls **network traffic**.

25. What do you mean by data leakage?

Data leakage is an unauthorized transfer of data to the outside world. Data leakage occurs via email, optical media, laptops, and USB keys.

26. Explain the difference between asymmetric and symmetric encryption.

Symmetric encryption requires the same key for encryption and decryption. On the other hand, **asymmetric encryption** needs different keys for encryption and decryption.

27. Explain WAF

WAF stands for Web Application Firewall. WAF is used to protect the application by filtering and monitoring incoming and outgoing traffic between web application and the internet.

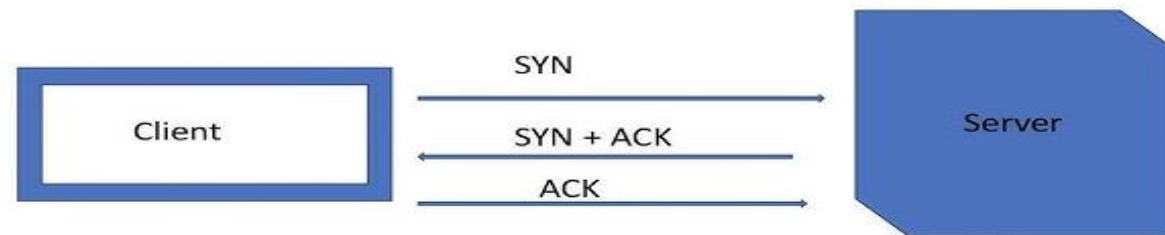
28. What is network sniffing?

Network sniffing is a tool used for analyzing data packets sent over a network.

Mohammed Almunajam

29. What is a three-way handshake?

A three-way handshake is a method used in a TCP/IP network to create a connection between a host and a client.



30. What is SSH?

SSH stands for Secure Switch Shell or Secure Shell. It is a utility set that provides system administrators with a secure way to access data on the network **remotely**.

31. What is a zero-day vulnerability?

It refers to a security vulnerability present in software or hardware that is undisclosed to **the vendor and lacks an existing solution**. This loophole can be leveraged by malicious actors before a remedy is created.

32. How does a rootkit work and how would you detect it?

A rootkit is **malicious** software that gives attackers unauthorized access to a computer or network. Detection involves using specialized anti-rootkit tools and **monitoring** for suspicious system behavior.

33. What is black box testing and white box testing?

Black box testing: It is a software testing method in which the internal structure or program code is hidden.

White box testing: A software testing method in which internal structure or program is known by tester.

Mohammed Almunajam

34. Define the term residual risk. What are three ways to deal with risk?

It is a threat that balances risk exposure after finding and eliminating threats.

Three ways to deal with risk are:

Reduce it

Avoid it

Accept it.

35. Define Exfiltration.

Data exfiltration refers to the unauthorized transfer of data from a computer system. This transmission may be manual and carried out by anyone having physical access to a computer.

36. What is the difference between HIDS and NIDS?

HIDS(Host IDS) and NIDS(Network IDS) are both Intrusion Detection System and work for the same purpose i.e., to detect the intrusions.

The only difference is that the HIDS is

set up on a particular host/device. It monitors the traffic of a particular device and

suspicious system activities. On the other hand, NIDS is set up on a network. It monitors

traffic of all device of the network.

37. How to make the user authentication process more secure?

In order to authenticate users, they have to provide their identity.

The ID and Key can be used to confirm the user's identity. This is an ideal way how the system should authorize the user.

Mohammed Almunajam

38. Discuss the ISO 27001/27002 standards.

It is a framework for information security management systems (ISMS), while ISO 27002 provides guidelines for implementing security controls and practices within an organization.

39. What is a remote desktop protocol?

Remote Desktop Protocol (RDP) is developed by Microsoft, which provides GUI to connect two devices over a network.

40. Give some examples of a symmetric encryption algorithm.

Following are some examples of symmetric encryption algorithm.

RCx

Blowfish

Rijndael (AES)

DES

41. What is incident response, and how is it managed?

Incident response encompasses a methodical strategy for handling and diminishing security incidents, encompassing key phases such as preparation, detection, containment, eradication, recovery, and Lesson.

42. Discuss the importance of disaster recovery planning in cybersecurity.

Disaster recovery planning encompasses the proactive preparation and responsive actions required to safeguard against data loss or system failures, ultimately ensuring the uninterrupted operation of a business.

43. Explain steps to secure web server.

Follow the following steps to secure your web server:

- ✓ Update ownership of file.
- ✓ Keep your webserver updated.
- ✓ Disable extra modules in the webserver.
- ✓ Delete default scripts.

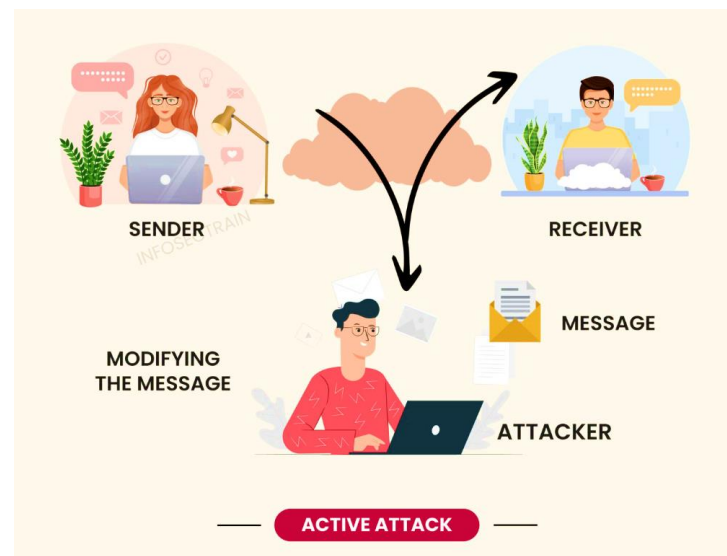
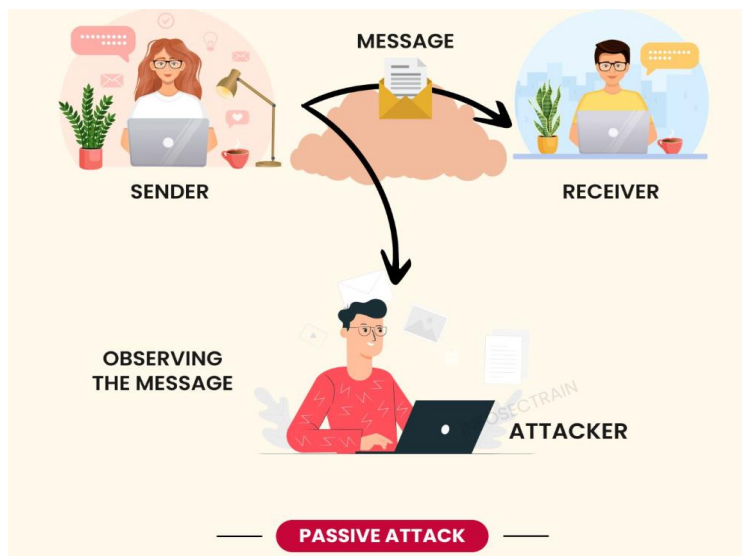
44. What is a Security Information and Event Management (SIEM) System?

SIEM systems gather, correlate, and scrutinize security-relevant data from diverse origins to identify and react to security events.

45. What is Microsoft **Baseline** Security Analyzer?

Microsoft Baseline Security Analyzer or **MBSA** is a graphical and command-line interface that provides a method to find missing security updates and misconfigurations.

46. What is the difference between active and passive cyber attacks?



47. Explain the concept of endpoint security.

Endpoint security focuses on securing individual devices (endpoints) like computers and mobile devices by using antivirus, anti-malware, and intrusion detection systems.

48. Discuss the role of artificial intelligence in cybersecurity.

AI is used for threat detection, pattern recognition, and anomaly detection to improve cybersecurity defenses and automate incident response.

49. What are the challenges in cloud security?

Challenges include data breaches, compliance, data loss prevention, and securing shared responsibility models in cloud environments.

50. What is a Security Operations Center (SOC)?

SOC is a centralized team responsible for real-time monitoring, detecting, and responding to security incidents.

51. Discuss the importance of compliance in cybersecurity.

Compliance ensures that an organization follows relevant laws and regulations, helping protect data and avoid legal consequences.

52. Name some tools used for packet sniffing.

Following are some tools used for packet sniffing.

- Tcpdump
- Wireshark
- NetworkMiner
- Dsniff

53. What are Hacking Tools?

Hacking Tools are computer **programs** and **scripts** that help you find and exploit weaknesses in computer systems, web applications, servers, and networks.

54. What do you mean by Shoulder Surfing?

A shoulder surfing attack describes a situation in which an attacker can physically look at a device's screen or keyboard and enter passwords to obtain personal information.

55. Explain honeypot and its Types.

Honeypot is a decoy computer system which **records** all the transactions, interactions, and actions with users.

Honeypot is classified into two categories:

- 1) **Production honeypot**
- 2) **Research honeypot.**

56. What is Public Key Infrastructure?

A Public Key Infrastructure, or PKI, is the governing authority behind the issuance of digital certificates. Protect sensitive data and give users and systems unique identities.

57. What is Spoofing?

Spoofing is a type of attack on computing devices in which an attacker attempts to steal the identity of a legitimate user and pretend to be someone else

58. Explain Advanced Persistent Threats (APT).

APTs are long-term, targeted cyberattacks by skilled adversaries. They use stealth, persistence, and sophisticated techniques to breach systems

59. Discuss the role of blockchain in cybersecurity.

Blockchain can enhance security through decentralized consensus, data integrity, and immutable records. It's used in secure transactions and identity management.

60. What is Backdoor?

It is a malware type in which security mechanism is **bypassed** to access a system.

61. What is Trojan virus?

Trojan is a **malware** employed by hackers and cyber-thieves to gain access to any computer. Here attackers use social engineering techniques to execute the trojan on the system.

62. How do you approach securing a large, distributed network?

Employ **segmentation**, strong access controls, regular audits, and network monitoring to protect against threats across a vast network.

63. What are the risks associated with public Wi-Fi?

- **Malware, Viruses, and Worms.**
- **Rogue Networks.**
- **Unencrypted Connections**
- **Network Snooping.**
- **Session Hijacking, Log-in Credential Vulnerability.** *Mohammed Almunajam*

64. What is IP blocklisting?

IP blocklisting is a method used to block unauthorized or malicious IP addresses from accessing your network.

65. What is a traceroute?

Traceroute is a widely used command line tool available on almost all operating systems. A complete route to the destination address is displayed. It also shows the time (or delay) between intermediate routers.

66. What is the difference between VA (Vulnerability Assessment) and PT (Penetration Testing)?

Penetration testing: This is performed to find vulnerabilities, malicious content, bugs, and risks. Used to set up an organization's security system to protect its IT infrastructure.

Vulnerability assessment: It is the technique of finding and measuring (scanning) security vulnerabilities in a particular environment.

67. What is Nmap?

Nmap is a tool which is used for finding networks and in security auditing.

68. What is the importance of forensics in cybersecurity?

Forensics helps investigate incidents, gather evidence, and understand attack vectors, aiding in incident response and legal actions

69. How do you manage security in a DevOps environment?

Implement security into the development pipeline with automation, continuous monitoring, and collaboration between development and security teams.

70. Explain the concept of a digital signature.

A digital signature employs cryptographic methods to confirm the genuineness and unaltered state of a digital document or message, assuring both the sender's authenticity and the content's integrity.

71. Discuss the challenges and solutions in endpoint detection and response (EDR).

EDR solutions monitor and respond to endpoint threats in real-time, providing visibility and incident response capabilities.

72. what is the difference between hashing and encryption?

encryption is a two-way function that includes encryption and decryption whilst hashing is a one-way function that changes a plain text to a unique digest that is irreversible.

73. Explain the concept of container security.

Secure containerized applications with image scanning, access controls, and runtime protection to prevent vulnerabilities.

74. How do you measure the effectiveness of a cybersecurity program?

Use metrics like risk assessments, incident response times, and security posture evaluations to measure program effectiveness

75. Discuss the challenges in securing wireless networks.
Challenges include **rogue access points** and **eavesdropping**. Solutions include **strong encryption**, **network monitoring**, and **user education**.
76. What is the role of machine learning in detecting cyber threats?
ML algorithms **analyze** large datasets to detect anomalies and patterns associated with cyber threats, enabling proactive security measures.
77. Explain the concept of federated identity management.
Federated identity allows users to access multiple systems with a single set of credentials, enhancing convenience and security.
78. What are the latest developments in cybersecurity threats?
Threats evolve with new attack vectors, **such as** supply chain attacks, ransomware, and AI-driven attacks.
79. How do you manage security in a hybrid cloud environment?
Secure hybrid cloud environments with consistent security policies, identity management, and data protection across on-premises and cloud resources.
80. What strategies would you implement for securing mobile applications?
Secure mobile apps with encryption, code reviews, secure APIs, and regular updates to protect against vulnerabilities and data breaches.

81. Explain the concept of threat hunting.

Threat hunting involves proactively searching for **indicators** of compromise within an organization's network to detect and mitigate threats before they cause harm.

82. What is a DMZ, and why is it used?

A DMZ (Demilitarized Zone) is a network segment that acts as a buffer zone between the internet and an organization's internal network, providing an additional layer of security

83. How does DNSSEC enhance security?

DNSSEC (Domain Name System Security Extensions) adds an additional layer of security by **digitally signing** DNS records, ensuring data integrity and authenticity.

84. What is the purpose of **GDPR**, and how does it impact cybersecurity practices?

GDPR (General Data Protection Regulation) aims to **protect** the personal data of individuals and imposes strict requirements on organizations regarding data protection and privacy, influencing cybersecurity practices.

85. How do you ensure compliance with regulatory requirements in your organization?

Ensuring compliance involves conducting regular audits, implementing security controls, and staying updated with relevant regulations and standards.

86. You discover a data breach in your organization. Outline the steps you would take to contain and mitigate the breach.

The first step would be to isolate affected systems, followed by identifying the source of the breach, notifying stakeholders, and implementing remediation measures to prevent future incidents.

87. How would you respond to a ransomware attack targeting critical systems?

Responding to a ransomware attack involves disconnecting affected systems from the network, notifying relevant authorities, restoring data from backups, and enhancing security measures to prevent future attacks.

88. How can you secure data in transit?

Securing data in transit involves encrypting data as it travels between devices or networks. Common protocols like SSL/TLS are used to encrypt data, ensuring that it remains confidential and protected from eavesdropping or interception.

89. What do you mean by Forward Secrecy ?

Forward secrecy is a feature of some key agreement protocols that guarantees that the session keys will remain secure even if the server's private key is compromised.

90. What Is Identity Theft?

Identity theft occurs when an attacker uses a target's private data to impersonate or steal from them.

91. Describe the role of 'security awareness training' in creating a security-conscious workforce.

Security awareness training educates employees about cybersecurity risks and best practices, fostering a security-conscious workforce. Its role includes:

- Reducing the likelihood of falling victim to social engineering attacks.
- Encouraging employees to report security incidents promptly.
- Promoting a culture of security where security is everyone's responsibility.
- Enhancing overall security posture by reducing human-related risks.

92. What is 'security incident escalation,' and when is it necessary during an incident response?

Security incident escalation is the process of elevating an incident to a higher level of authority or expertise when necessary. It is essential during an incident response when:

- The incident exceeds the capabilities or knowledge of the initial responders.
- Critical decisions or actions require approval from senior management.
- Specialized expertise is needed to investigate or mitigate the incident effectively.
- Escalation protocols ensure a timely and appropriate response.

93. What Are Spyware Attacks?

Spyware is a kind of malware that is covertly installed on a targeted device to collect private data.

94. Can You Reset a Password-Protected BIOS Configuration?

BIOS (**B**asic **I**nput or **O**utput **S**ystem) is a firmware located on a memory chip, often in a computer's motherboard or system board. A typical BIOS security feature is a user password that must be entered to boot up a device. If you wish to reset a password-protected BIOS configuration, you'll need to turn off your device, locate a password reset jumper on the system board, remove the jumper plug from the password jumper-pins,

95. Explain Active Reconnaissance?

Active reconnaissance is a type of **cyberattack** used to gather intelligence about a system's vulnerabilities. To conduct this kind of reconnaissance, attackers must interact with the target via automated scanning or manual testing with tools like **traceroute**.

96. What do you mean by a Null Session?

A null session occurs when a user is **not authorized** using either a username or a password. It can provide a security concern for apps because it implies that the person making the request is unknown.

97. What do you mean by System Hardening?



98. Differentiate between spear phishing and phishing?



Phishing



Spear Phishing

99. How do you assess and manage the security of third-party vendors you may use?

1. **Risk Assessment:** Identify potential risks.
 2. **Vendor Selection:** Choose vendors with strong security measures.
 3. **Security Requirements:** Clearly define expectations in contracts.
 4. **Security Controls:** Implement access restrictions and monitoring.
 5. **Monitoring:** Continuously oversee vendors' security practices.
 6. **Incident Response:** Prepare for and address security incidents.
 7. **Training:** Educate employees on security risks and protocols.
- Following these steps will enhance overall security and minimize vulnerabilities

100. What is Burp Suite?

Burp Suite is a penetration testing tool, consisting of various tools, such as proxy, spider, scanner, etc., that are used for web application security testing.

Mohammed Almunajam

The End

"Thank you for exploring the top 100 cybersecurity questions with us. Let's remember that in the realm of cybersecurity, knowledge is power. Stay curious, stay safe, and continue to learn and adapt to the ever-evolving digital landscape."

Best regards,
MOHAMMED ALMUNAJAM



<https://www.linkedin.com/in/mohammed-almunajam-676057142/>



almonjmm@gmail.com