* **Non- repudiation –** It is used as a reference to digital security, and it a way of assurance that the sender of a message cannot disagree with having sent the message and that the recipient cannot repudiate having received the message.
* End to End Encryption – If a user send a message like “Hi”, the message is encrypted, and in the network in its actual form, the decryption happens only hwne it reaches the recipient.
* **Example:** phonepe, Facebook messenger, slack, gmail.

Transaction – of money, messages, chat windows,

* It combines authentication and integrity: non-repudiation authenticates the identity of a user who performs a transaction, and ensures the integrity of that transaction.

# Types of security testing:

1. **Vulnerability Scanning:** Vulnerability scanning is performed with the help of automated software to scan a system to detect known vulnerability patterns.

**Tool name –** OWASP ZAP – Scanning, Burp Suite

1. **Security Scanning:** Security scanning is the identification of network and system weaknesses. Later on, it provides solutions for reducing these defects or risks. Security scanning can be carried out in both manual and automated ways.
2. **Penetration Testing:** Penetration testing is the simulation of the attack from a malicious hacker. It includes an analysis of a particular system to examine for potential vulnerabilities from a malicious hacker who attempts to hack the system.
3. **Risk Assessment:** In risk assessment testing security risks observed in the organization are analysed. Risks are classified into three categories i.e., low, medium, and high. This testing endorses controls and measures to minimise the risk.
4. **Security Auditing:** Security auditing is an internal inspection of applications and operating systems for security defects. An audit can also be carried out via line-by-line checking of code
5. **Ethical Hacking:** Ethical hacking is different from malicious hacking. The purpose of ethical hacking is to expose security flaws in the organization’s system
6. **Posture Assessment:** It combines security scanning, ethical hacking, and risk assessments to provide an overall security posture of an application.
7. **Network security testing:** Network security testing is a type fo testing that focuses on identifying vulnerabilities in the network infrastructure. It includes testing firewalls, routers, and other network devices to identify potential vulnerabilities.
8. **API security Testing:** Using Postman we can do security testing, by testing the authentication, authorization of the API’s.

API will also have tokens(passwords).

<https://students.masaischool.com/lectures/87293?tab=notes>

26:17