Task 1: Understanding Cyber Security Basics & Attack Surface

What is Cyber Security?

Cyber Security is the practice of **protecting computers, servers, mobile devices, networks, and data** from digital attacks.

It is based on the **CIA TRIAD**.

Confidentiality: Protect sensitive data like banking passwords and WhatsApp messages.
Integrity: Prevent unauthorized modifications, e.g., changing bank transactions.
Availability: Ensure services are always online, like UPI apps or social media.

Term	Meaning	Banking Example	Social Media Example
Confidentiality	Only authorized people access data	Your ATM PIN is hidden	Only you can read your DMs
Integrity	Data must not be altered	No one can change ₹5000 to ₹50	Profile data not modified
Availability	System always accessible	Bank app works 24/7	WhatsApp server always online

Types of Cyber Attackers

Type	Description	Example
Script Kiddies	Beginners using pre-made hacking tools	Using SQL injection tool
Insiders	Employees misusing access	Staff stealing customer data
Hacktivists	Hackers with political/social motives	Website defacement

Type	Description	Example
Nation-State Actors	Government-sponsored hackers	Cyber espionage

Attack Surfaces

Layer	Example Attack Surface
Web Applications	Login forms, file uploads, user input fields
Mobile Apps	Weak API authentication, insecure storage
APIs	Token leakage, broken access control
Networks	Open ports, weak firewall, unencrypted traffic
Cloud Infrastructure	Misconfigured storage buckets, public S3 storage

OWASP Top 10 Vulnerabilities

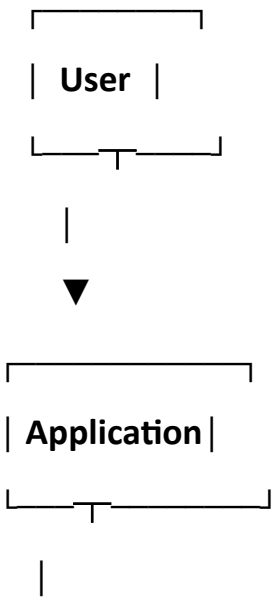
#	Vulnerability	Why Dangerous
1	Broken Access Control	Unauthorized users access restricted areas
2	Injection	SQL Injection, NoSQL Injection compromises DB
3	Security Misconfiguration	Admin panel exposed or default configs
4	Authentication Failures	Weak passwords allow account takeover
5	Sensitive Data Exposure	Plaintext storage of passwords or sensitive info
6	Cross-Site Scripting (XSS)	Attackers inject scripts into webpages
7	Using Vulnerable Components	Exploiting outdated libraries

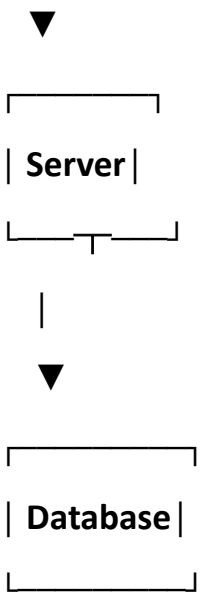
#	Vulnerability	Why Dangerous
8	Insufficient Logging & Monitoring	Attacks go undetected
9	Server-Side Request Forgery (SSRF)	Internal server access by attackers
10	Insecure Design	Poor system logic leads to vulnerabilities

Daily Apps & Attack Surfaces

App	Attack Surface	Example Attack
Email	Email client + Server	Phishing, spam links
WhatsApp	Mobile App + API	Fake APK, message spoofing
Banking App	App + Server + Database	SQL Injection, Man-in-the-Middle (MITM)
Social Media	Web & Mobile	Brute force, account takeover

Data Flow Diagram





Attack Points in Flow

- **User: Phishing, Social Engineering**
- **Application: XSS, CSRF**
- **Server: Malware, DoS**
- **Database: SQL Injection, Data Breach**

Sample Vulnerable Code (SQL Injection)

$query = "SELECT * FROM users WHERE username = '$user' AND password='$pass'";

Attack Input:

Username: admin' OR '1'='1

Impact: Attacker logs in without credentials.

Summary

Cyber security is critical for protecting digital systems and sensitive data.
Understanding the CIA triad, types of attackers, attack surfaces, OWASP Top 10, and data flow attack points helps prevent cyber-attacks. Awareness of vulnerabilities in daily-used apps like banking, email, and WhatsApp is key for safety.