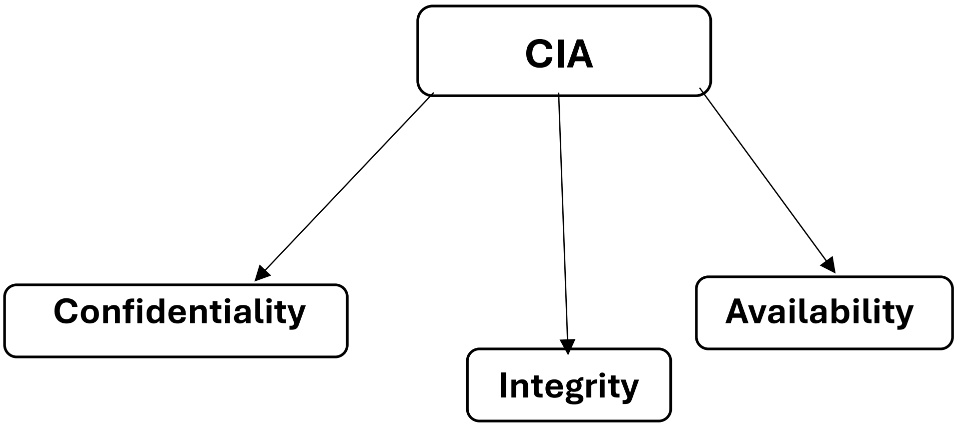
CYBERSECURITY BASICS

Cybersecurity:

Cybersecurity is the practice of protecting digital systems, networks, and data from unauthorized access, misuse, damage, or disruption. It mainly focuses on protecting data, systems, and services from cyber threats.
In the modern technology era, cybersecurity has become essential for running online services, hosting websites, storing data, and handling confidential information. Today, most people use smartphones, laptops, or computers to share data, transfer money, and store personal details.
Cybersecurity teams are responsible for securing these digital assets and ensuring that users' information remains safe. Without proper cybersecurity measures, attackers can easily steal, modify, or misuse sensitive data. Therefore, cybersecurity plays a critical role in today's technology-driven world.

CIA TRIAD:



Confidentiality:

Confidentiality means" Who can see data?". It ensures only authorized person can access sensitive data.
Attackers use methods like Phishing, Brute force to break confidentiality. Once it breaks Passwords get stolen, Personal data leaks may be possible. To protect confidentiality we need use Passwords, Multi-factor authentication, Encryption.

Integrity:

Integrity means" Is the data correct and unchanged?". It ensures that data is accurate and has not to be altered by unauthorized users.
Attackers use methods like SQL Injection, Man-in-the-middle attacks to break integrity. Once it breaks Altering records, Fake transaction may be possible. To protect integrity, we need to use Hashing, Digital signatures, Access controls.

Availability:

Availability means" Can users access the system when needed?". It ensures that systems and services remain accessible to authorized users.
Attackers use methods like DDoS Attacks, Server overload, Ransomware to break availability. Once it breaks Website may be crashed, Server disruption, Business loss also possible. To protect availability we need to use Backups, Redundancy, Load balancing, Monitoring.

Types of Attackers:

In cybersecurity, attackers are called thread actors. Different attacker have different skills, motivation, and targets.

1. Script Kiddies:
   They are beginners with little or no technical knowledge. They use pre-built tools and scripts. They don't know how to create their own exploits. They do this for fun or curiosity. They can do Website defacement, Simple DDoS, Password brute force using tools.
2. Insight Attackers:
   They are Employees, Ex-Employees, or trusted users of an organization. They already have authorized access. They do this for Revenge or financial gain. They ca do Data Theft, Privilege Abuse and Information leakage.
3. Hacktivists:
   They are Attackers driven by political or social causes. They targets organizations or governments. They do this for their Ideology, Protest, and Public awareness. They do Website defacement, Data leaks, DDoS attacks.
4. Cybercriminals:
   They are professional attackers, organized crime groups. They do this for Financial profit. They can do Ransomware, Banking fraud, Phishing campaigns.
5. Nation-State Attackers:
   They are government-sponsored hacking groups. They are highly skilled and well-funded. They do this for National security, Cyber warfare. They targets Military systems, Power grids, Banks, Government databases.

Attack Surface:

Attack surface is the total number of points where an attacker can try to enter, attack, or interact with a system.

Attack Surface	Includes	Possible Attacks	Examples
Web Application	Login pages, Forms, Search boxes, Payment pages	SQL Injection, XSS, Broken authentication	1. Online banking website 2. E-commerce website
Mobile Application	Android / iOS apps, APIs used by mobile apps, Local storage on device	Insecure APIs, Hardcoded credentials, Reverse engineering	1. Banking app 2. WhatsApp
API	REST APIs, Backend services	Broken authentication, Excessive data exposure, Rate limiting issues	Mobile app communicating with server
Cloud	Cloud servers, Storage buckets, IAM roles	Misconfigured storage, Exposed credentials, Privilege escalation	1. AWS S3 bucket 2. Azure VM
Network	Wi-Fi networks, Routers, Firewalls, Open ports	Man-in-the-middle, Port scanning, Unauthorized access	1. Public WiFi 2. Office network

Attack Surface in Daily Life:

In Email service, the attack surfaces are Login page, Mobile app, Email server, Network connection, APIs.

In Banking app, the attack surfaces are Mobile app, Backend server, Database, Internet connection, Cloud infrastructure.

OWASP:

OWASP stands for Open Web Application Security Project. It is a non-profit organization that focuses on improving the security of web applications.

OWASP Top 10 is a list of the 10 most critical web application security risks. If a web app is vulnerable to OWASP Top 10 issues, it is considered insecure.

Issues	Meaning	Example	Impact
Broken Access Control	Users can access things they should NOT be allowed to.	Normal user accessing admin page, Viewing someone else's data	• Data leaks • Privilege abuse
Cryptographic Failures	Sensitive data is not properly encrypted.	Passwords stored in plain text, Data sent without encryption	• Data exposure • Privacy violations
Injection (SQL Injection, Command Injection)	Attacker sends malicious input that the system executes.	SQL Injection reading database data	• Data theft • Data modification • Full system compromise
Insecure Design	Application logic itself is insecure.	No limit on login attempts	Easy exploitation
Security Misconfiguration	Wrong or default security settings.	Default passwords, Open admin panels	Unauthorized access
Vulnerable and Outdated Components	Using old or vulnerable software libraries.	Old frameworks with known bugs	Easy exploitation
Identification and Authentication Failures	Weak login or authentication mechanisms.	Weak passwords, No MFA	Account takeover
Software and Data Integrity Failures	Untrusted updates or code execution.	Malicious software updates	Malware injection
Security Logging and Monitoring Failures	Attacks are not logged or detected.	No alert on failed login attempts	Attacks go unnoticed
Server-Side Request Forgery (SSRF)	Server is tricked into making requests it should not.	Accessing internal systems	Internal network exposure

Data Flow in an Application:

Data Flow describes how information moves inside a system. Data travels through multiple layers.

User → Application → Server → Database → Server → Application → User

1. User:
   User enters data like username, password, message, or payment. User uses browser or mobile app for enter his data.
   Example:
   Logging into bank app
   Sending WhatsApp message
2. Application:
   Application must be a Mobile app or website. It collects user input and sends requests to server.
   Example:
   Login page
   Message Box
3. Server:
   Server do its work in backend. It processes requests and communicates with database.
   Example:
   Verifying login credentials
   Processing transactions
4. Database:
   It stores data like user details, messages, transactions.
   Example:
   Account balance
   Chat history

Attacks in Data Flow:

Attacks can happen at every stage of the data flow.
User ----> Phishing, Malware, Weak passwords.
Application----> XSS, Broken authentication. Input manipulation.
Server------>Security misconfiguration, Privilege escalation.
Database----> SQL Injection, Unauthorized access.

Summary:

This task helped me to understand the fundamentals of cybersecurity, including the CIA triad, different types of attackers, attack surfaces, and common web vulnerabilities defined by OWASP. By understanding how data flows through an application, I learned where an attacker can steal data or corrupt data. This knowledge provides me a strong foundation for understanding real-world cyber threats and security practices.