TASK -1

Introduction to Cyber Security:

Cybersecurity is the practice of protecting digital devices, networks, and sensitive data from threats like hacking, malware, and phishing.

- Protects systems, networks, and personal information
- Uses security tools, policies, and safe online practices
- Prevents data theft, system damage, and unauthorized access

Cyber Security involves using security technologies, rules, and skilled people to prevent threats, detect attacks, and recover from incidents.

Cyber security helps individuals and organisations reduce the risk and impact of cyber attacks.

CIA Traid:

The CIA Traid stands for **Confidentiality,Integrity,Availability.**

It is the foundation of strong security systems, protecting sensitive data from unauthorized access, changes, and disruptions.

Confidentiality:

- Keeping data private and secret, preventing unauthorized access or disclosure.

Example:

1. Online banking protects account details using passwords, PINs, and OTPs.
2. Social media uses privacy settings to restrict access to personal messages and data.

Integrity:

- Ensuring data is accurate, consistent, and hasn't been tampered with.

Example:

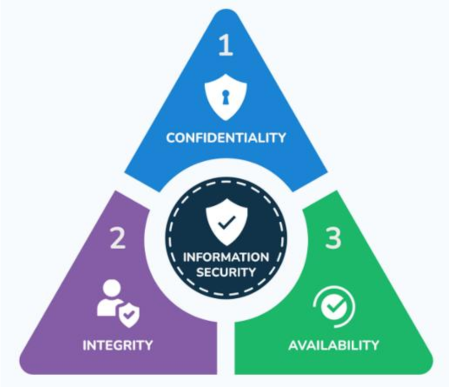
1. Banking systems ensure transaction data is not altered during transfers.
2. Social media platforms protect posts and profiles from unauthorized modification.

Availability:

- Making sure authorized users can access data and systems when required.

Example:

1. ATMs and mobile banking services remain accessible at all times.
2. Social media platforms allow users to log in and communicate without service interruptions.



Types of cyber attacks:

1.Script Kiddies:

Individuals with limited skills who use ready-made hacking tools. They are motivated by fun or recognition and typically launch simple attacks like website defacement or basic DDoS.

2.Insiders:

Authorized users who misuse their access, either intentionally or by mistake. They are dangerous because they have internal system knowledge and direct access to sensitive data.

3.Hacktivists:

Attackers who use hacking to support political or social causes, aiming to spread messages or expose organizations using methods like defacement, DDoS, or data leaks.

4. Nation-State Actors:

Government-backed groups that carry out advanced cyber attacks for national interests, using highly sophisticated tools and long-term campaigns like APTs.

Attack surface:

An attack surface is the total number of entry points through which an attacker can try to access or exploit a system.

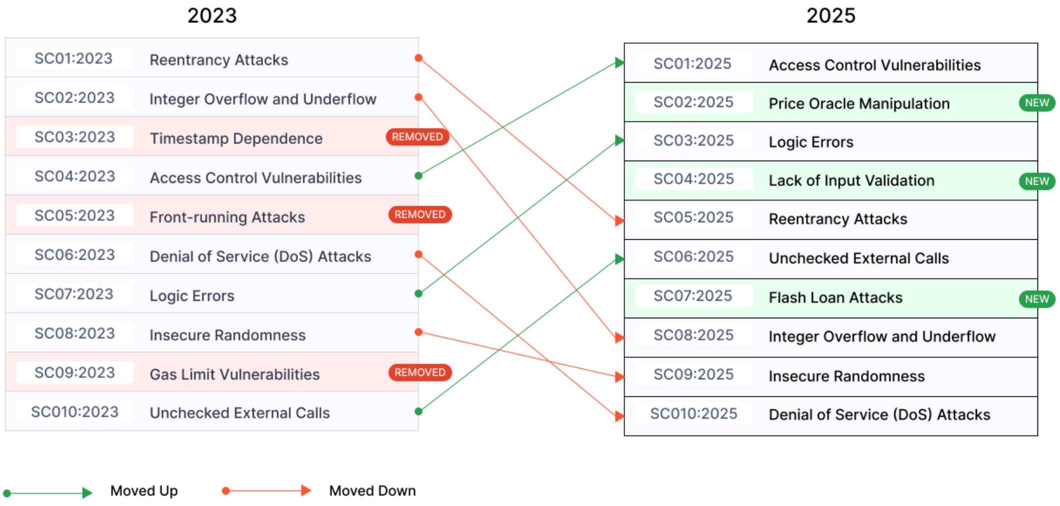
Common attack surfaces:

- **Web Applications:** SQLi, XSS
- **Mobile Apps:** Insecure storage
- **APIs:** Broken authentication
- **Networks:** Unauthorized access
- **Cloud Infrastructure:** Misconfiguration

OWASP TOP 10:

OWASP, or the Open Web Application Security Project, is a non-profit foundation that promotes secure software development by providing free, open-source resources, tools, and best practices for improving application security, with its well-known OWASP Top 10 list highlighting critical web application risks.

- Broken Access Control – Users gain unauthorized access.
- Cryptographic Failures – Weak or missing data encryption.
- Injection – Malicious input (e.g., SQL injection).
- Insecure Design – Flawed application architecture.
- Security Misconfiguration – Improper security settings.
- Vulnerable Components – Outdated or insecure libraries.
- Identification & Authentication Failures – Weak login mechanisms.
- Software & Data Integrity Failures – Untrusted updates or code.
- Security Logging & Monitoring Failures – Attacks go undetected.
- Server-Side Request Forgery (SSRF) – Server fetches malicious URLs.



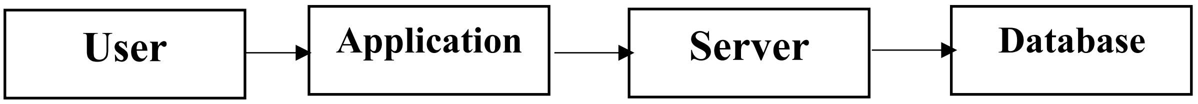
2023

SC01:2023	Reentrancy Attacks	
SC02:2023	Integer Overflow and Underflow	
SC03:2023	Timestamp Dependence	REMOVED
SC04:2023	Access Control Vulnerabilities	
SC05:2023	Front-running Attacks	REMOVED
SC06:2023	Denial of Service (DoS) Attacks	
SC07:2023	Logic Errors	
SC08:2023	Insecure Randomness	
SC09:2023	Gas Limit Vulnerabilities	REMOVED
SC010:2023	Unchecked External Calls	

2025

SC01:2025	Access Control Vulnerabilities	
SC02:2025	Price Oracle Manipulation	NEW
SC03:2025	Logic Errors	
SC04:2025	Lack of Input Validation	NEW
SC05:2025	Reentrancy Attacks	
SC06:2025	Unchecked External Calls	
SC07:2025	Flash Loan Attacks	NEW
SC08:2025	Integer Overflow and Underflow	
SC09:2025	Insecure Randomness	
SC010:2025	Denial of Service (DoS) Attacks	

DATA FLOW:



- **User → Application:** User enters data through a web or mobile application.

- **Application → Server:** Application sends data to the server for processing.
- **Server → Database:** Server validates and stores or retrieves data from the database.

Possible attack in Data Flow:

1. **User → Application:** Phishing, keylogging, malicious input.
2. **Application → Server:** Man-in-the-middle (MITM), data interception.
3. **Server → Database:** SQL injection, unauthorized database access.

Mapping Daily-Use Applications to Attack Surfaces:

Email:

- Phishing links
- Malicious attachments
- Email spoofing

WhatsApp:

- Malicious links
- Fake messages
- Account takeover

Banking Apps:

- Weak authentication
- Insecure APIs
- Man-in-the-middle attacks