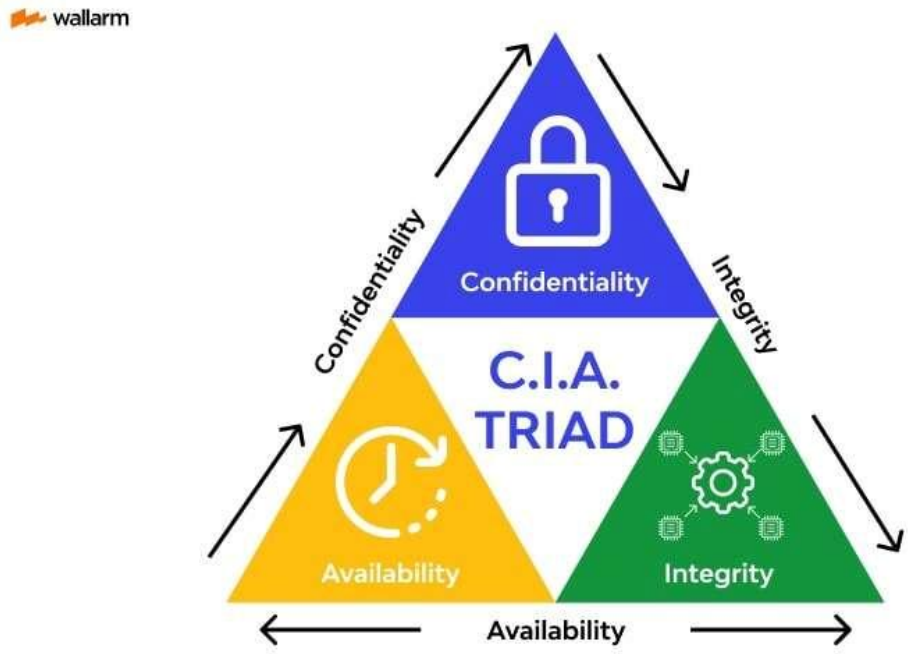
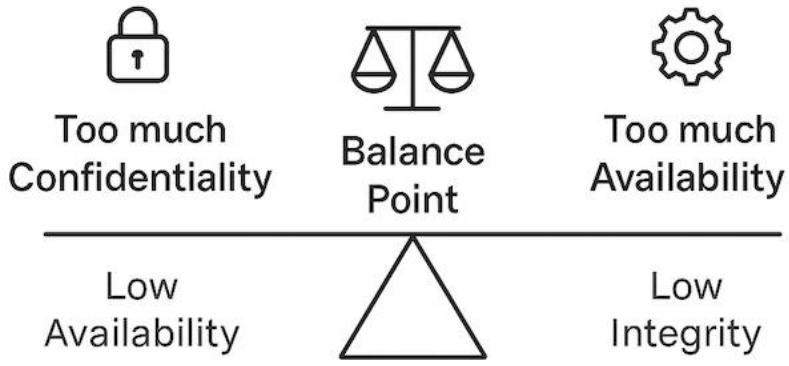
ELEVATE LABS (CYBER SECURITY INTERNSHIP)

Task 1: Understanding Cyber Security Basics & Attack Surface

1. Understanding What Cybersecurity Is (CIA Triad)

Cybersecurity means protecting computers, applications, networks, and data from unauthorized access, misuse, or damage. The foundation of cybersecurity is based on three main principles called the **CIA Triad**.





Confidentiality

Confidentiality ensures that information is accessible only to authorized users.
For example, in a banking application, only the account holder should be able to see account details. In WhatsApp, messages are protected using end-to-end encryption so that no third party can read them. If confidentiality fails, sensitive data may leak.

Integrity

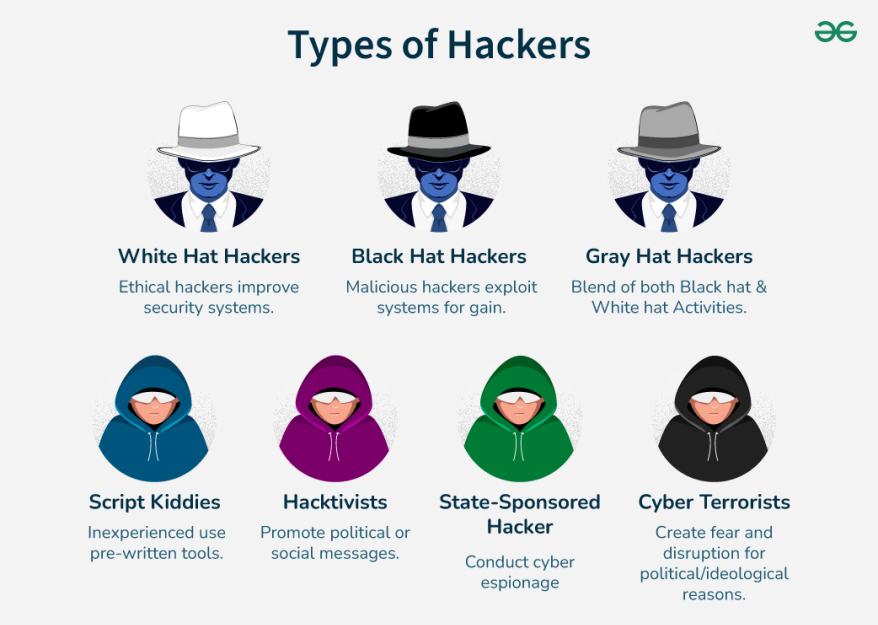
Integrity ensures that data remains accurate and unchanged unless modified by authorized users.
For example, bank transaction amounts should not be altered, and exam results should not be modified by attackers. If integrity is compromised, it can lead to fraud or misinformation.

Availability

Availability ensures that systems and services are accessible when needed.
For example, banking servers, ATMs, and communication apps like WhatsApp must be available 24/7. Attacks like DDoS can affect availability by making systems unreachable.

2. Types of Attackers

Different attackers have different skills, motives, and targets.



4

Script Kiddies are beginners who use ready-made hacking tools without deep technical knowledge. They usually attack for fun or attention.

Insiders are employees or trusted users who misuse their access, either intentionally or accidentally. Insider attacks are dangerous because insiders already have system access.

Hacktivists attack organizations or governments for political or social reasons. They often aim to deface websites or leak sensitive information.

Nation-State Actors are government-sponsored hackers with advanced skills and resources. They target critical infrastructure, defense systems, and national data.

3. Common Attack Surfaces

An attack surface refers to any point where an attacker can try to gain access to a system.

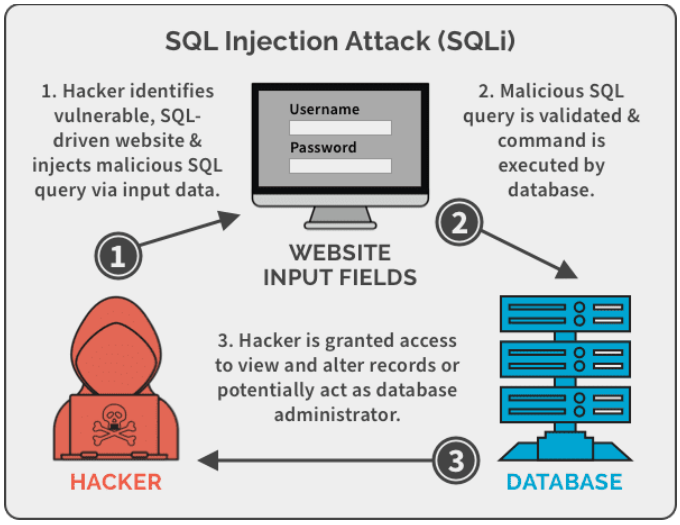
4

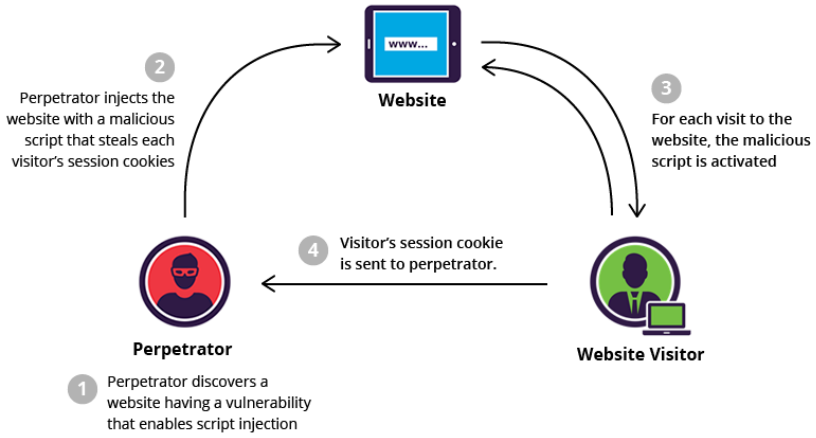
Common attack surfaces include:

- Web applications (login pages, forms)
- Mobile applications (insecure storage, permissions)
- APIs (broken authentication)
- Networks (open ports, weak firewalls)
- Cloud infrastructure (misconfigured storage and access control)

4. OWASP Top 10 Vulnerabilities

The **OWASP Top 10** lists the most critical security risks in web applications.





These vulnerabilities are dangerous because:

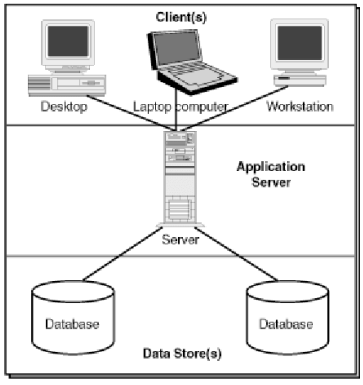
- **SQL Injection** can allow attackers to steal or modify database data
- **Broken Authentication** can lead to account takeover
- **Cross-Site Scripting (XSS)** can steal user sessions
- **Security Misconfiguration** can expose entire servers

Understanding OWASP Top 10 helps identify common developer mistakes that attackers exploit.

5. Mapping Daily Applications to Attack Surfaces

- **Email** → phishing attacks, weak passwords
- **WhatsApp** → account takeover, malicious links
- **Banking apps** → fake apps, man-in-the-middle attacks
- **Social media** → credential stuffing, XSS
- **Cloud storage** → misconfigured permission

6. Data Flow in an Application



A typical data flow works as follows:

1. User enters data in an application
2. Application sends the request to the server
3. Server processes the request
4. Database stores or retrieves the data
5. Response is sent back to the user

7. Points Where Attacks Can Occur

- **User level** → phishing, malware
- **Application level** → XSS, broken authentication
- **Network level** → man-in-the-middle attacks
- **Server level** → remote code execution
- **Database level** → SQL injection, data theft

Attackers usually target the weakest point in this flow.

8. Final Summary

Cybersecurity focuses on protecting data and systems using confidentiality, integrity, and availability. Different attackers such as script kiddies, insiders, hacktivists, and nation-state actors target systems for different reasons. Applications expose multiple attack surfaces including web apps, mobile apps, APIs, networks, and cloud infrastructure. The OWASP Top 10 highlights common vulnerabilities that can lead to serious security breaches. By understanding how data flows from users to servers and databases, it becomes easier to identify where attacks may occur and how to prevent them.