Cyber Security Internship – Task 1

Understanding Cyber Security Basics & Attack Surface

1. Introduction to Cyber Security

Cyber security is the practice of protecting systems, networks, applications, and data from digital attacks. These attacks are usually intended to access, modify, or destroy sensitive information, disrupt services, or cause financial and reputational damage. Cyber security ensures safe and reliable use of digital technology in areas such as banking, communication, healthcare, and government systems.

2. CIA Triad (Confidentiality, Integrity, Availability)

The CIA Triad represents the three core principles of cyber security.

- **Confidentiality**

Confidentiality ensures that sensitive information is accessible only to authorized users. It prevents unauthorized access to data.

Example:
Encryption used in banking applications ensures that only the intended user can view transaction details.

- **Integrity**

Integrity ensures that data remains accurate, complete, and unaltered during storage or transmission.

Example:
Hashing mechanisms ensure that files or transactions are not modified without authorization.

- **Availability**

Availability ensures that systems, services, and data are accessible to users whenever required.

Example:
DDoS attacks impact availability by making websites or services unavailable to legitimate users.

3. Types of Cyber Attackers

Different attackers have different motivations and skill levels.

- **Script Kiddies**

Inexperienced attackers who use pre-built tools and scripts to exploit known vulnerabilities.

- **Insider Threats**

Employees or trusted individuals who misuse their authorized access intentionally or unintentionally.

- **Hacktivists**

Attackers motivated by political, social, or ideological reasons.

- **Cyber Criminals**

Attackers focused on financial gain through phishing, ransomware, or fraud.

- **Nation-State Actors**

Highly skilled attackers sponsored by governments for espionage or cyber warfare.

4. Attack Surface

An attack surface refers to all possible points where an attacker can attempt to gain unauthorized access to a system or data.

Common Attack Surfaces

- Web applications (login pages, forms)
- Mobile applications
- APIs
- Network ports and services
- Cloud infrastructure
- Email systems

A larger attack surface increases the chances of successful attacks.

5. OWASP Top 10 Overview

The OWASP Top 10 is a globally recognized list of the most critical web application security risks.

Importance of OWASP Top 10

- Helps organizations identify common vulnerabilities
- Improves secure coding practices
- Reduces risk of application-level attacks

Common OWASP Vulnerabilities

- Injection attacks (SQL Injection)
- Broken Authentication
- Broken Access Control
- Security Misconfiguration
- Sensitive Data Exposure
- Cross-Site Scripting (XSS)

These vulnerabilities are dangerous because they can lead to data breaches and system compromise.

OWASP Top 10: 2025

The OWASP Top 10:2025 represents the most critical security risks affecting modern web applications. These vulnerabilities are dangerous because they are widely exploited in real-world attacks and often lead to data breaches, system compromise, and major business disruption.

A01:2025 – Broken Access Control
What it is:
Improper enforcement of user permissions and access rules.

Why it is dangerous:
Attackers can access unauthorized data, escalate privileges, and perform sensitive actions without proper authorization.

A02:2025 – Security Misconfiguration
What it is:
Insecure default settings, exposed services, or incorrect system configurations.

Why it is dangerous:
Creates easy entry points for attackers and can lead to full system compromise with minimal effort.

A03:2025 – Software Supply Chain Failures
What it is:
Compromise of third-party libraries, dependencies, or CI/CD pipelines.

Why it is dangerous:
Allows attackers to inject malicious code into trusted software, impacting multiple systems at once.

A04:2025 – Cryptographic Failures
What it is:
Weak, outdated, or improperly implemented encryption mechanisms.

Why it is dangerous:
Exposes sensitive information such as passwords, personal data, and financial records.

A05:2025 – Injection
What it is:
Execution of untrusted input as commands or database queries.

Why it is dangerous:
Enables attackers to manipulate databases, bypass authentication, and gain control over backend systems.

A06:2025 – Insecure Design
What it is:
Architectural flaws caused by lack of secure design principles and threat modeling.

Why it is dangerous:
These weaknesses are difficult to fix and create long-term security risks across the application.

A07:2025 – Authentication Failures
What it is:
Weak authentication controls, poor session management, or credential misuse.

Why it is dangerous:
Leads to account takeover, identity theft, and unauthorized system access.

A08:2025 – Software or Data Integrity Failures
What it is:
Failure to verify the integrity of software updates, plugins, or critical data.

Why it is dangerous:
Attackers can inject malicious code or manipulate trusted data sources.

A09:2025 – Security Logging & Alerting Failures
What it is:
Insufficient logging, monitoring, or alerting mechanisms.

Why it is dangerous:
Attacks remain undetected for long periods, increasing damage and recovery time.

A10:2025 – Mishandling of Exceptional Conditions
What it is:
Improper handling of application errors and exceptions.

Why it is dangerous:
Exposes internal system details and sensitive information that assist attackers.

Key Takeaway:
The OWASP Top 10:2025 highlights vulnerabilities that directly impact confidentiality, integrity, and availability. Understanding and mitigating these risks is essential for building secure applications, improving SOC detection, and reducing overall cyber risk.

6. Real-World Application Attack Surface Mapping

Email Applications

Attack Surfaces:

- Login pages
- Email attachments
- Embedded links

Possible Attacks:

- Phishing
- Malware delivery
- Credential theft

Banking Applications

Attack Surfaces:

- Mobile applications
- Backend APIs

Possible Attacks:

- Man-in-the-Middle attacks
- Credential stuffing
- Unauthorized transactions

Messaging Applications (e.g., WhatsApp)

Attack Surfaces:

- Media sharing
- Account authentication

Possible Attacks:

- Malware through files
- Account takeover

7. Data Flow in Applications

A typical data flow in an application is:

User → Application → Server → Database → Response to User

Possible Attack Points

- User input (SQL Injection, XSS)
- Network communication (MITM attacks)
- Authentication mechanisms
- Database access controls

Understanding data flow helps in identifying where security controls are required.

8. Difference Between Threat, Vulnerability, and Risk

- **Threat:** A potential cause of harm (e.g., hacker, malware)
- **Vulnerability:** A weakness that can be exploited (e.g., unpatched software)
- **Risk:** The likelihood and impact of a threat exploiting a vulnerability

9. Importance of Attack Surface Awareness

Understanding attack surfaces helps organizations:

- Reduce exposure to attacks
- Implement better security controls
- Improve incident response and prevention strategies

10. Conclusion

This task provided a strong foundation in cyber security fundamentals by covering the CIA triad, types of attackers, attack surfaces, OWASP Top 10 vulnerabilities, and real-world application risks. Understanding these concepts is essential for identifying threats, reducing risks, and building secure systems in modern digital environments.

Author

Parijat Das

B.Tech in Computer Science | Aspiring Cyber Security Professional