

**Group Members**

**1. Ahmad Rashid(2022677)**

**2. Aizaz ur Rehman(2022078)**

**3. Muhammad Aurangzaib Bhatti(2022355)**

**Week 2:** **Threat Modeling & Risk Assessment (Week 2)**

**1. Introduction**

Threat Modeling and Risk Estimation are fundamental steps in the secure software design process. The paper identifies potential attacks and assesses potential risks related to it and provides the mitigation plan to ensure the security of the Warehouse Management System (WMS).

**2. Threat Modeling**

**Potential Attack Vectors:**

Below are the primary threats to the WMS:

* **Unauthorized Access:** Attackers seeking to break into sensitive inventory and user data through credentials or privilege escalation.
* **SQL Injection:** Users with malicious intent can use insufficiently validated input fields to modify database queries.
* **Cross-Site Scripting (XSS)** is multiple of the Injection is in 2nd slide- Injection of untrusted data into a web page. This data can be used
* **Man-in-the-Middle (MITM) Attacks:** These are cyber-attacks where the attacker intercepts data messages between the front end and the back
* **Insider Threats:** There is the possibility that employees with a higher level of privileged access can accidentally or intentionally attack.
* **Denial of Service (DoS)** Attacks Overloading the system to disrupt availability and slow down business operations.
* **Data Breaches:** Unauthorized access to stored data due to weak encryption or misconfigurations
* **Session Hijacking:** It's process of gaining control over a user account through exploitation of an inadequately secure session-management

**3. Risk Assessment**

Each attack vector is evaluated based on likelihood and impact.

| **Threat** | **Likelihood** | **Impact** | **Risk Level** |
| --- | --- | --- | --- |
| Unauthorized Access | High | High | Critical |
| SQL Injection | Medium | High | High |
| Cross-Site Scripting (XSS) | Medium | Medium | Moderate |
| Man-in-the-Middle (MITM) | High | High | Critical |
| Insider Threats | Medium | High | High |
| Denial-of-Service (DoS) | Low | High | Moderate |
| Data Breaches | High | High | Critical |
| Session Hijacking | Medium | High | High |

**4. Security Mitigation Strategies**

To ameliorate the risks posed by the threats above we will use the following countermeasures:

* **Multi-Factor Authentication (MFA)** is used to enforce MFA for all user accounts, especially for admins.
* **Preventing SQL Injections:** Employ prepared statements and parameterized queries for validating database inputs.
* **Input validation** is critical in regards to web security. Misuse of unvalidated inputs can result in XSS and command injection attacks. To prevent these risks, all inputs should be strictly validated.
* **Secure Communication:** Utilize HTTPS for protection of data transmissions and prevention of MITM attacks.
* **Role-Based Access Control (RBAC).** The principle is to minimize insider threats by limiting users' access to the system according to their roles.
* **DDoS Protection and Rate Limiting:** This includes the ability to enforce rate-limiting and to utilize monitoring tools to detect and mitigate DoS attacks.
* **Data Encryption:** Sensitive data is encrypted both in rest and transit with AES-256 and TLS 1.2+.
* **Secure Session Management.** Enforce session expiration, regenerate session IDs on login, and use secure cookies.
* **Audit Logging.** Keeping the user's actions detailed log, to detect suspicious activities and potential breaches.
* **Performing Regular Security Audits & Penetration** Testing is a must-have. Regular security assessments should be performed to identify and mitigate new vulnerabilities.

**5. Conclusion**

Threat model and risk assessment help secure Warehouse Management System (WMS) in a structured way. Our goal is to decrease risks, protect the sensitive data and make the system more secure.