CY321 Semester Project

WEEK-02

Submitted to: Dr. Zubair Ahmad

TA: Ma’am Jazia

Submission Date: March 14, 2025

Threat Modeling & Risk Assessment Report

1. Introduction

This report outlines the threat modeling and risk assessment for the secure ride-hailing website. The goal is to identify potential threats, assess their risks, and define mitigation strategies to ensure a secure platform for users and drivers.

2. Identified Assets

The following critical assets require protection:

- **User Data:** Names, emails, phone numbers, passwords
- **Driver Data:** License details, ride history
- **Ride Details:** Pickup/drop-off locations, timestamps
- **Authentication Mechanisms:** JWT tokens, hashed passwords
- **Communication Data:** Chat messages between drivers and riders

3. Threat Actors

The possible threat actors and their motivations include:

- **Malicious Hackers:** Attempting to steal or manipulate data
- **Insider Threats (Disgruntled Employees):** Misuse of system privileges
- **Competitors:** Engaging in data scraping or disruption
- **Unintentional Threats:** Users making security mistakes (e.g., weak passwords)

4. Attack Vectors

Potential attack vectors that could be exploited:

- **SQL Injection (SQLi):** Injecting malicious SQL queries via input fields
- **Cross-Site Scripting (XSS):** Injecting scripts to steal session tokens or manipulate the UI
- **Broken Authentication:** Exploiting weak password policies or exposed API keys
- **Session Hijacking:** Taking over user sessions via stolen JWTs

- **Man-in-the-Middle (MITM) Attacks:** Intercepting unencrypted communication

5. Risk Assessment

The likelihood and impact of each attack vector are assessed as follows:

Threat	Likelihood	Impact	Overall Risk
SQL Injection (SQLi)	High	High	**Critical**
Cross-Site Scripting (XSS)	Medium	High	**High**
Broken Authentication	High	High	**Critical**
Session Hijacking	Medium	High	**High**
MITM Attacks	Medium	Medium	**Medium**

6. Security Mitigation Strategies

For each identified risk, the following mitigation strategies will be implemented:

Threat	Mitigation Strategy
SQL Injection	Use **prepared statements & ORM** (e.g., Django ORM, SQLAlchemy)
XSS	Sanitize user inputs, use **Content Security Policy (CSP)**
Broken Authentication	Implement **strong password hashing (bcrypt)** and **multi-factor authentication (MFA)**
Session Hijacking	Use **secure cookies**, **short-lived JWTs**, and enforce **HTTPS**
MITM Attacks	Enforce **SSL/TLS (HTTPS)** for secure communication

7. Conclusion

This threat modeling and risk assessment provide a foundational security approach for the ride-hailing website. By implementing these mitigation strategies, we aim to minimize

security risks and ensure a secure user experience. The next phase will focus on designing the system architecture and implementing security controls accordingly.