|  |  |
| --- | --- |
| SFIT, Department of Information Technology | **2025** |

**St. Francis Institute of Technology**   
**(An Autonomous Institution)**   
AICTE Approved | Affiliated to University of Mumbai

A+ Grade by NAAC: CMPN, EXTC, INFT NBA Accredited: ISO 9001:2015 Certified

**Department of Information Technology**

A.Y. 2025-2026   
Class: BE-IT A/B, Semester: VII   
Subject: Secure Application Development Lab

Student Name: Student Roll No:

**Experiment – 3: Study and exercise on Threat Modeling**

**Aim:** To study and excise on Threat Modeling

|  |  |
| --- | --- |
| **Objective:** After performing the experiment, the students will be able to – | |
| ▪ | To generate Threat model using Microsoft Threat modeling tool |
| ▪ | To get familiar with the features provided by the tool |
| ▪ | To Learn about generated threat categories |
| ▪ | To find mitigations for the generated threats |

**Lab objective mapped: To understand the methodologies and standards for developing secure code**

**Prerequisite:**Basic knowledge Information Security, software engineering

**Requirements:** Personal Computer, Windows operating system browser, Internet Connection etc.

**Pre-Experiment Theory:**

**What is threat modeling?**

Threat modeling is a structured process with these objectives: identify security requirements, pinpoint security threats and potential vulnerabilities, quantify threat and vulnerability criticality, and prioritize remediation methods.

Threat modeling methods create these artifacts:

 An abstraction of the system

 Profiles of potential attackers, including their goals and methods

 A catalog of threats that could arise

Threat modeling works by identifying the types of threat agents that cause harm to an application or computer system. It adopts the perspective of malicious hackers to see how much damage they could do. When conducting threat modeling, organizations perform a thorough analysis of the software architecture, business context, and other artifacts (e.g.,

Secure Application Development Lab



|  |  |
| --- | --- |
| SFIT, Department of Information Technology | **2025** |

functional specifications, user documentation). This process enables a deeper understanding and discovery of important aspects of the system. Typically, organizations conduct threat modeling during the design stage (but it can occur at other stages) of a new application to help developers find vulnerabilities and become aware of the security implications of their design, code, and configuration decisions. Generally, developers perform threat modeling in four steps:

|  |  |
| --- | --- |
|     | **Diagram.** What are we building?  **Identify threats.** What could go wrong?  **Mitigate.** What are we doing to defend against threats? **Validate.** Have we acted on each of the previous steps? |

**Discuss various threat categories and mitigations mentioned by Microsoft threat modeling tool**

Microsoft uses the STRIDE model categorizes different types of threats and simplifies the overall security conversations.

|  |  |
| --- | --- |
| **Category** | **Description** |
| **Spoofing** | Involves illegally accessing and then using another user's authentication information, such as username and password |
| **Tampering** | Involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet |
| **Repudiation** | Associated with users who deny performing an action without other parties having any way to prove otherwise—for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations.  Non-Repudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package |
| **Information Disclosure** | Involves the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers |
| **Denial of Service** | Denial of service (DoS) attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability |
| **Elevation of Privilege** | An unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively  penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed |

**Mitigation categories**

Secure Application Development Lab