Name: Kaushal Kotkar Department: Cyber Security

Div: BE-15 Roll No: 54

Subject: DSO

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Experiment No. – 8** | | | | |
| **Date of Performance:** | 02/09/2024 | | | |
| **Date of Submission:** | 09/09/2024 | | | |
| Program Execution/ formation/ correction/  ethical practices (06) | Timely Submission  (01) | Viva (03) | Experiment Total (10) | Sign with Date |
|  |  |  |  |  |

**Experiment No. 8**

**Aim:** To implement threat models to identify threats in the system using Threat Dragon.

**Lab Outcome:** Use Sonarqube and snyk to perform code quality checks and Threat Dragon to create threat models to identify threats in the system

**Theory:**

**Threat Dragon:** Threat Dragon is an open-source threat modeling tool used to identify and mitigate security threats in software systems. Threat modeling is a systematic approach to identifying potential security risks and vulnerabilities in a software system during the design phase. Threat Dragon helps teams visualize and analyze these threats, allowing for better risk management and security enhancement.

**Why Use Threat Dragon:**

* **Security Analysis:** Threat Dragon allows you to systematically identify and assess security threats and vulnerabilities.
* **Collaboration:** It facilitates collaboration among team members by providing a central platform for threat modeling.
* **Visual Representation:** Threat models are often represented as diagrams, making it easier to understand and communicate security risks.

**Steps to Implement Threat Models Using Threat Dragon:**

1. **Access Threat Dragon:**

Go to the Threat Dragon website or install the Threat Dragon application locally if available.

1. **Create a New Project:**

Start by creating a new project, giving it a meaningful name like "Demo Threat Model."

Fill in project details such as title, owner, system description, contributors, and reviewers.

1. **Create Diagram:**

Using Threat Dragon's diagramming tools, create a flowchart or diagram that represents the system's architecture and data flows.

1. **Identify Threats:**

Collaborate with your team to identify potential threats and vulnerabilities within the system based on the diagram and system description.

1. **Rate and Prioritize Threats:**

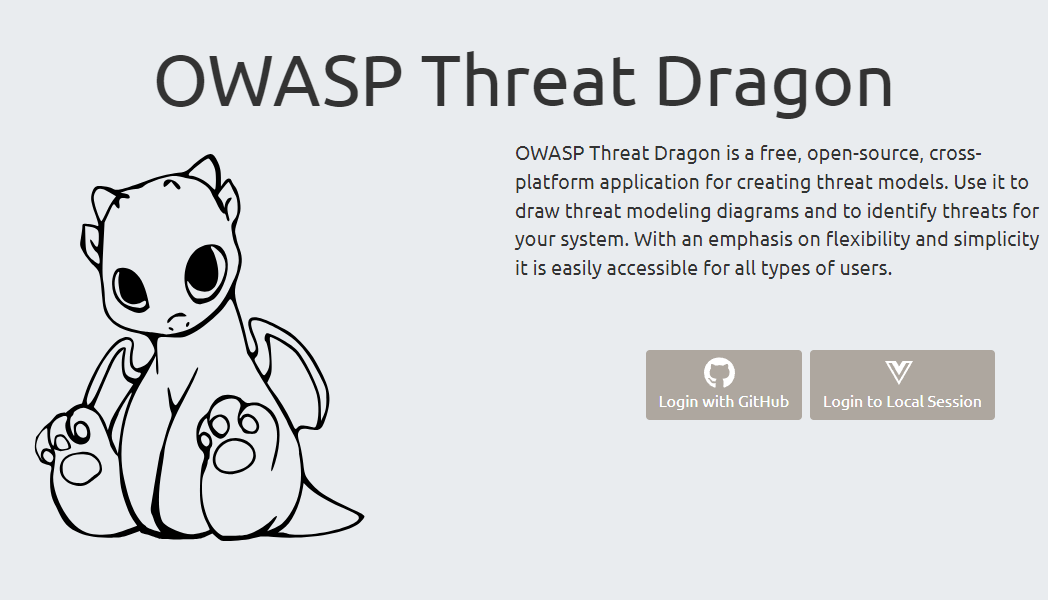
Rate the identified threats based on severity and impact.

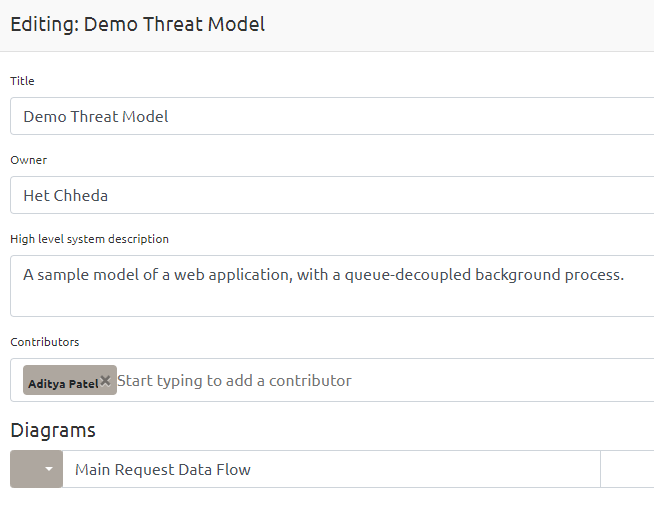
Prioritize them to address the most critical threats first.

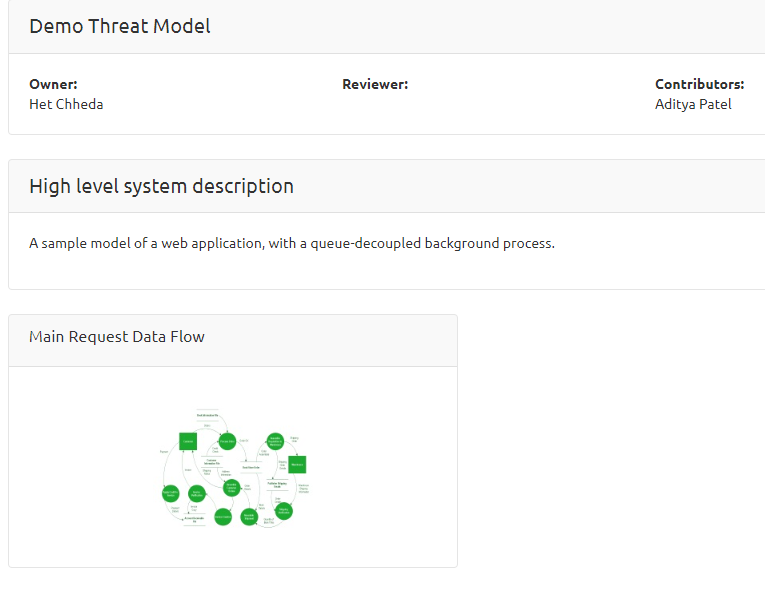
1. **Provide Mitigation Strategies:**

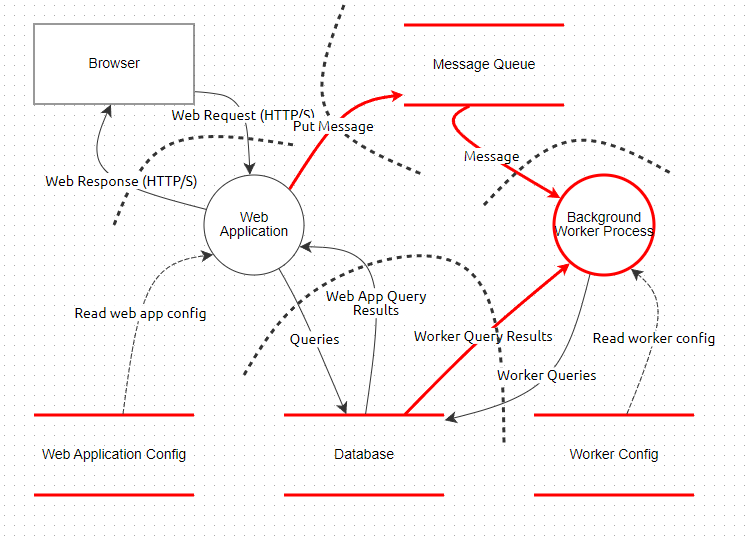
For each threat, define mitigation strategies or security controls that can be implemented to mitigate the risk.

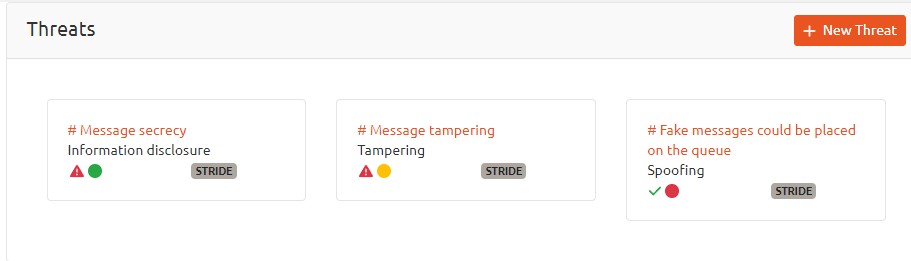
**Output:**











**Conclusion:**

Implementing threat models with Threat Dragon is a proactive approach to enhancing software security. It allows teams to visualize, identify, prioritize, and mitigate potential threats early in the development process, resulting in a more secure and robust software system.