1. **# Threat Modeling as Code (T14)**

This project demonstrates \*\*Threat Modeling as Code\*\* using:

- ThreatSpec for threat annotations

- PlantUML/Mermaid for diagrams

- GitHub Actions CI/CD pipeline for automation

Steps Followed:

1. ThreatSpec :- A tool with which we can write annotations in our code itself which helps us to find error more efficiently.
2. Wrote a python code with annotations in it. (@threatens,@mitigates,@accepts,@exposes,@connects,@uses)
3. Downloaded all the tools and dependencies. (ThreatSpec, Mermaid, PlantUML)
4. Wrote a pipeline which runs the threat spec.(ThreatSpec run)

(ThreatSpec reports)

1. It generates the artifacts of threatspec reports and diagrams and upload it to artifacts.
2. Then the pipeline push the artifact to our github repo.
3. Created a baseline file, which is used at base to recognise the already known threats, and if any new threat is found we can block the pipeline.

**Screenshots :-**

