OWASP threat dragon

DEFINITION:

OWASP Threat Dragon is a free, open-source threat modeling tool developed by the OWASP Foundation that helps software teams identify and mitigate security threats early in the development lifecycle. It provides an intuitive interface for creating data flow diagrams (DFDs), automatically applies the STRIDE threat classification model, and enables users to document, track, and manage security risks and mitigations in their application architecture. Available as both a desktop and web-based application, Threat Dragon promotes security by design and integrates seamlessly into DevSecOps workflows.

SYSTEM MODE:

- draw the architecture
- diagram should be as depth as possible
- the scope of the diagram should be identified

USES:

- Create data flow diagrams (DFDs)
- Identify threats using the **STRIDE** model
- Assign mitigations and track progress
- Export models for documentation and compliance

Creating the model

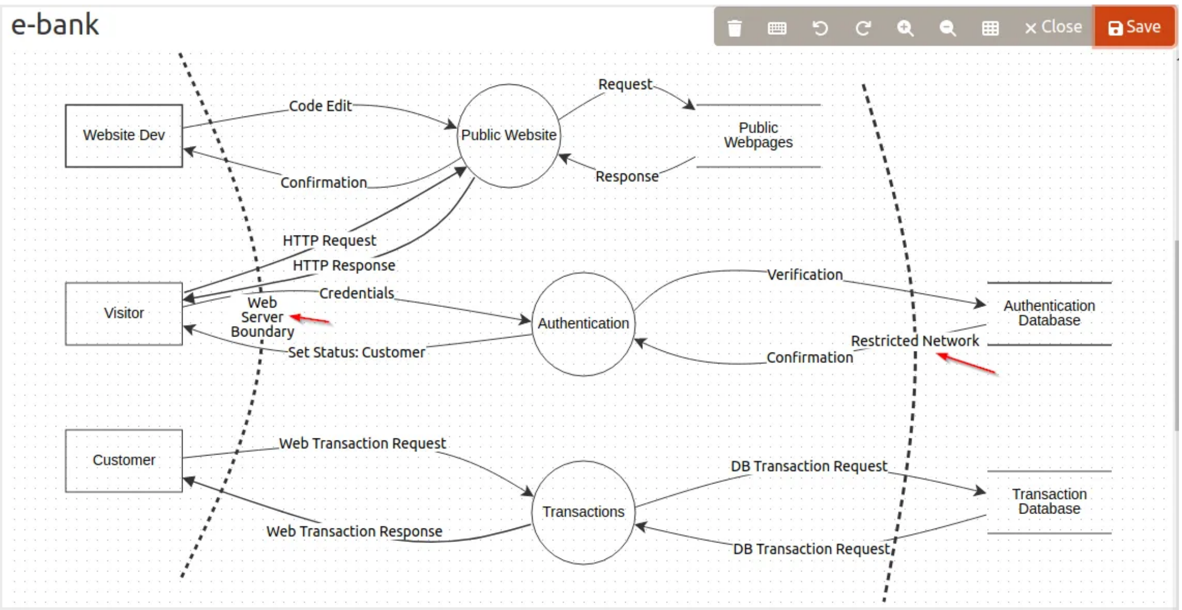
system model —> find threats —> address threats —> validate model

Workflow in Threat Dragon:

1. **Create a Model**
   - Define system name, description, and purpose.
2. **Draw a Data Flow Diagram**
   - Add elements like processes, data stores, external entities, and data flows.
3. **Identify Threats**
   - Threat Dragon auto-generates threats based on STRIDE for each element.
4. **Review & Mitigate**
   - Review each threat and define mitigations.
5. **Validate Model**

    - Use validation checks to find missing mitigations or other design flaws.
6. **Export or Save**
    - Save models locally (desktop) or to GitHub (web app).
    - Export threat reports for audits or documentation.

EXAMPLE:



EXTRAS:

explain me about the OWASP threat dragon?

OWASP Threat Dragon is a free and open-source threat modeling tool developed by the OWASP Foundation. It's designed to help teams identify and mitigate potential security threats during the design phase of software development.
It supports both desktop and web applications. The desktop app is built with Electron and stores models locally, while the web app integrates with GitHub for version-controlled model storage.

One of its key features is its use of the STRIDE methodology — which stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege — to automatically generate threat scenarios based on the elements in a data flow diagram (DFD).
The tool lets you visually design your system using components like processes, data stores, and external entities, and then helps you identify threats, validate the model, and suggest mitigations. It also supports exporting models and reports for documentation and compliance.
Overall, it promotes "security by design" and is especially useful for integrating threat modeling into DevSecOps pipelines or agile workflows. It's a great choice

for teams looking to adopt structured and collaborative threat modeling without licensing costs.