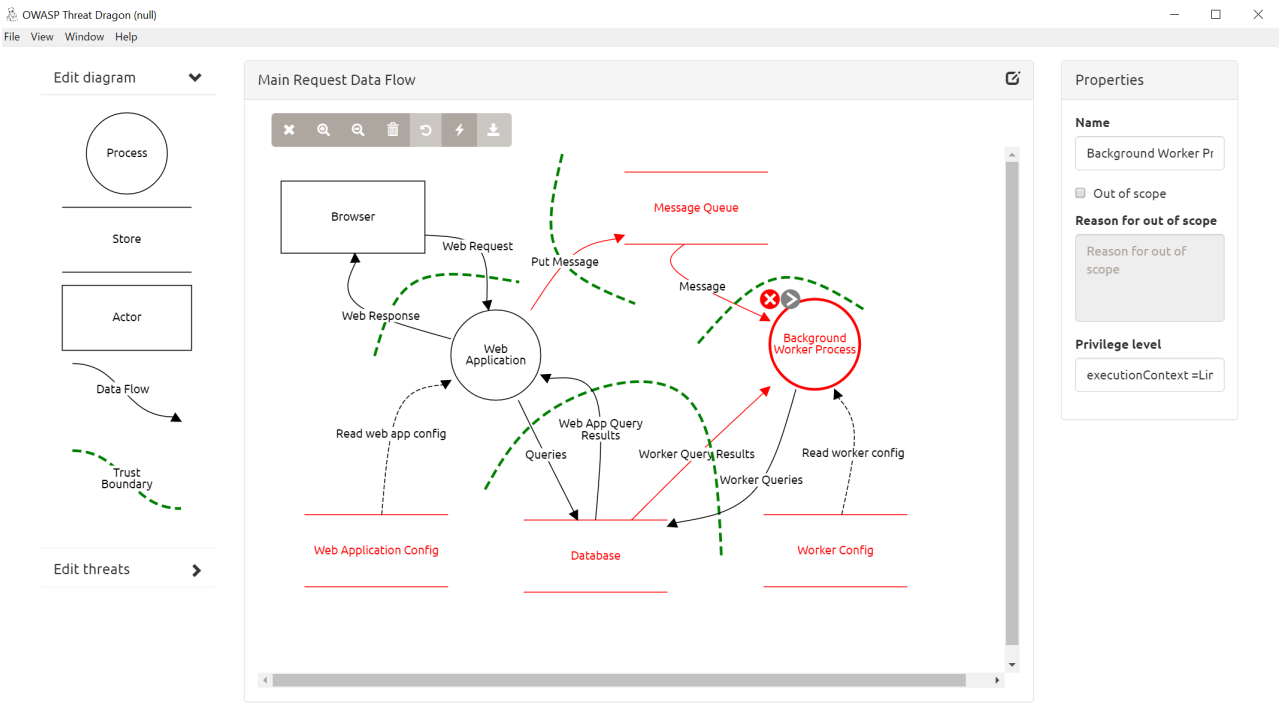
Introduction to OWASP Threat dragon

Overview



In this lab, you are going to learn how to use OWASP Threat Dragon to draw Threat Model Diagram.

Threat Dragon is a free, open-source, cross-platform threat modeling application including system diagramming and a rule engine to auto-generate threats/mitigations. It is an OWASP Incubator Project. The focus of the project is on great UX, a powerful rule engine and integration with other development lifecycle tools.

Outcomes

Upon completion of this session, you should be able to

- Use OWASP Threat Dragon to draw threat model diagram
- Determining and ranking threats
- Entry of mitigations and counter measures
- Apply the threat model diagram in the project

1: Installation

The application comes in two variants:

1. A web application
2. A desktop application

For Web application, You can refer to https://github.com/owasp/threat-dragon, pull the code and follow the steps to execute.

For standalone application, you can download the files via https://github.com/OWASP/threat-dragon-desktop/releases/tag/v1.3

2: Create a model

Loading a demo model

If you are wondering how to start, you can load a sample threat model. On the welcome page, to download the sample, click or tap 

This should give you some ideas on how to get started with your own model.

3: Generate threats

Processes, data stores and actors

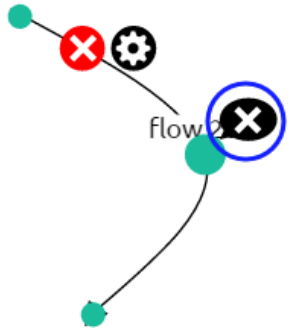
Add model elements to your diagram by clicking or tapping the relevant shape in the stencil on the left side of the diagram editor. Once added they can be selected by clicking them to see their properties and threats and dragged around the diagram. to delete an element, first select it and then click on the red icon it the elements top left corner...

Data flows and trust boundaries

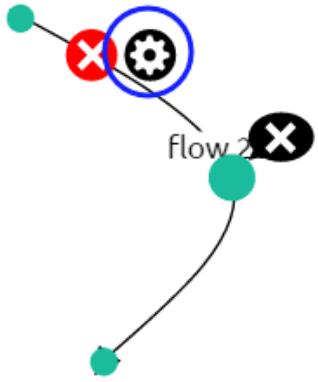
Data flows and trust boundaries can be added to the diagram by clicking their shape in the stencil on the left side of the diagram editor. Once added, their ends can be dragged around the diagram. To connect the end of a data flow to a process, data store or actor, you can drag one of its ends onto the element.

An easier way to draw data flows between elements is to select your first element, then click the grey link tool, next to the red remove tool near the top right of the selected element. This turns the link tool green. Then, when you click another element, a new data flow will be created, linking the first element to the second.

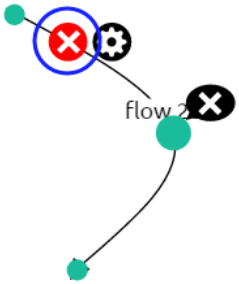
Extra vertices can be added by clicking at some point on the line. These new vertices can also be dragged to position the data flow or trust boundary. Vertices can be removed by clicking the remove tool that appears when you mouse near to the vertex.



A data flow can be selected by clicking the **Link options** tool that appears when you mouse near to the link. Once selected you can edit its properties or add threats to it. Trust boundaries cannot be selected.

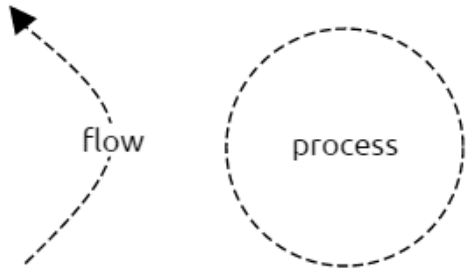


Data flows and trust boundaries can be deleted by clicking the red remove tool that appear when you mouse near to them.



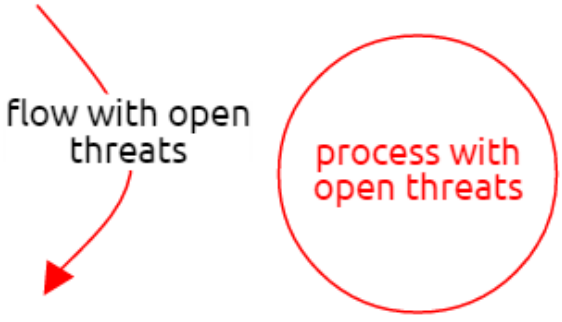
Out of scope elements

Processes, data stores, actors and data flows can be marked as out of scope. You can use this for elements that are needed to help a diagram make sense, but for which you are not interested in creating threats. To help reviewers (and as a reminder for future-you) you can specify a reason why elements have been marked out of scope. Threat generation is disabled for these elements. Out of scope elements are indicated in diagrams with dashed lines:



Elements with open threats

Processes, data stores, actors and data flows that have open (unmitigated) threats are highlighted in red so that you know where to focus your attention:



Threat model report

From the Threat Model details view you can see a summary report of your model listing the diagrams, elements and threats. Towards the bottom right of the page click “Report”

You can customize the report to show or hide

- Out of scope model elements
- Mitigated threats
- Threat model diagrams

4: More about passwordless design

Passwordless design becomes more popular in recent years, you can understand a little bit more about Microsoft, Apple and Google’s implementation of passwordless design:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-phone

https://developer.apple.com/documentation/authenticationservices

https://blog.google/technology/safety-security/a-simpler-and-safer-future-without-passwords/

You can try to remove your password if you have a Microsoft account:

https://techcommunity.microsoft.com/t5/azure-active-directory-identity/introducing-password-removal-for-microsoft-accounts/ba-p/2747280

5: Reference

https://github.com/OWASP/threat-dragon-desktop

https://hub.docker.com/r/appsecco/owasp-threat-dragon/

https://docs.threatdragon.org/#threat-generation

https://docs.threatdragon.org/#threat-model-diagrams

https://dzone.com/articles/threat-modelling-tools-analysis-101-owasp-threat-d

END OF DOCUMENT