

K P Uday Krishna

CB.SC.P2CYS23012

SSE Assignment

Assignment 1

Case study: Corporate HRMS System

Define the Scope and Objectives

Scope:

- A corporate HRMS System where employees can log in, view account details, Change the database, Apply Leave.

Objectives:

- Identify potential threats.
- Assess the impact and likelihood of threats.
- Develop mitigation strategies.

Entities:

- Employee (External Entity)
- Web Server (Process)
- Database Server (Data Store)
- Authorization Server (Internal Entity)

➤ Click On Create A Model

The screenshot shows the Microsoft Threat Modeling Tool 2016 main interface. At the top, it says "MICROSOFT THREAT MODELING TOOL 2016". Below this, there's a "Threat Model:" section with three main options: "Create A Model", "Open A Model", and "Getting Started Guide". Each option has a brief description. Under "Create A Model", there's a "Template For New Models" section with a dropdown menu showing "SDL TM Knowledge Base (Core)(4.1.0.9)" and a "Browse..." button. To the right of this is a "Recently Opened Models" section with a link to "Sample Threat Model.tmx". Further right is a "Threat Modeling Workflow" section with a 4-step process: 1. Select your template, 2. Create your data flow diagram model, 3. Analyze the model for potential threats, 4. Determine mitigations. Below the "Threat Model:" section is a "Template:" section with two main options: "Create New Template" and "Open Template", each with a brief description. To the right of this is a "Template Workflow" section with a 5-step process: 1. Define stencils, 2. Define categories, 3. Define threat properties, 4. Define threat, 5. Share your template.

Threat Model:

- Create A Model**
Model your system by drawing diagram (s). Make sure you capture important details.
- Open A Model**
Open an existing model and analyze threats against your system; do not worry, the tool will help you identify them.
- Getting Started Guide**
A step-by-step guide to help you get up and running now.

Template For New Models
SDL TM Knowledge Base (Core)(4.1.0.9) [Browse...](#)

Recently Opened Models
[Sample Threat Model.tmx](#)

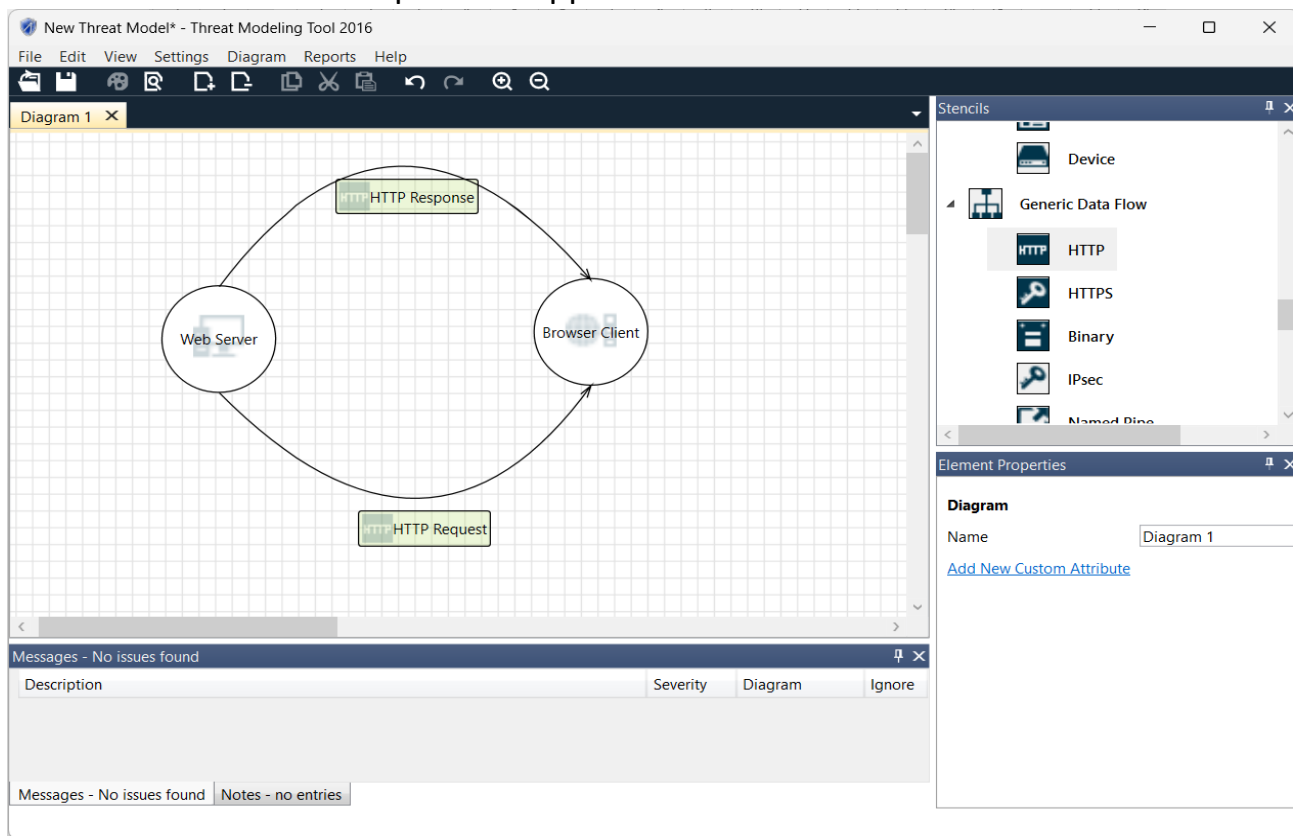
Threat Modeling Workflow
1. Select your template.
2. Create your data flow diagram model.
3. Analyze the model for potential threats.
4. Determine mitigations.

Template:

- Create New Template**
Define stencils, threat types and custom threat properties for your threat model from scratch.
- Open Template**
Open an existing Template and make modifications to better suit your specific threat analysis.

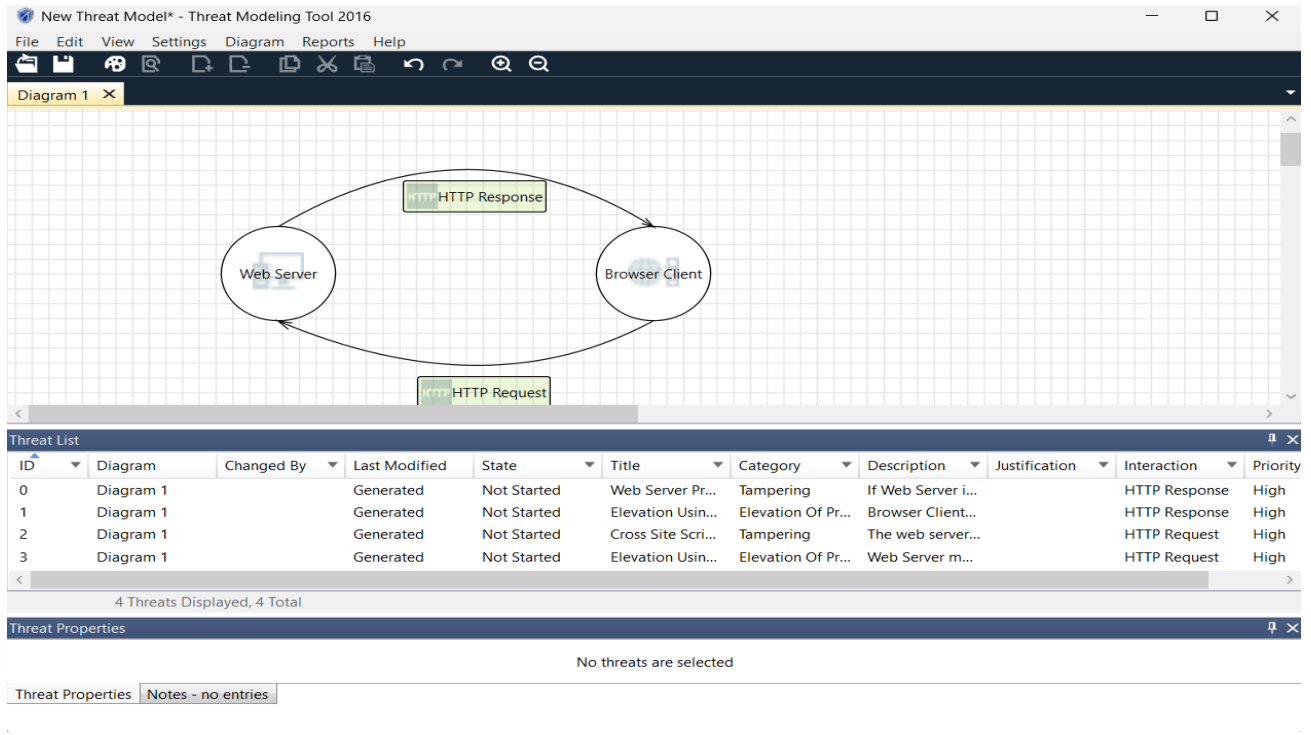
Template Workflow
Use templates to define threats that applications should look for.
1. Define stencils
2. Define categories
3. Define threat properties
4. Define threat
5. Share your template

- Now the resultant canvas will be:
- Demo of Simple Web Application



➤ Identify and Analyse Threats:

Navigate to '**View**' then click '**analysis view**'



The Data flow sequence will be.

Employee -> Web Application (Submit credentials)

- **Data Flow Type:** HTTP
- **Description:** Employee submits login credentials to the web application.

Web Application -> Authorization Server (Verify credentials)

- **Data Flow Type:** HTTPS
- **Description:** The web application sends the credentials to the authorization server for verification.

Authorization Server -> Web Application (Send account details)

- **Data Flow Type:** HTTPS

- Description: The authorization server sends the account details back to the web application.

Web Application -> Employee (Display account details)

- **Data Flow Type:** HTTP
- Description: The web application displays the account details to the customer.

Employee -> Web Application (Request Applying Leave)

- **Data Flow Type:** HTTPS
- Description: The employee requests a applying leave through the web application.

Web Server -> Authorization Server (Update Leave Account)

- **Data Flow Type:** HTTPS
- Description: The web server sends the leave request to the authorization server to update the leaves.

Web Server -> SQL Database Server(Initiate request for Update)

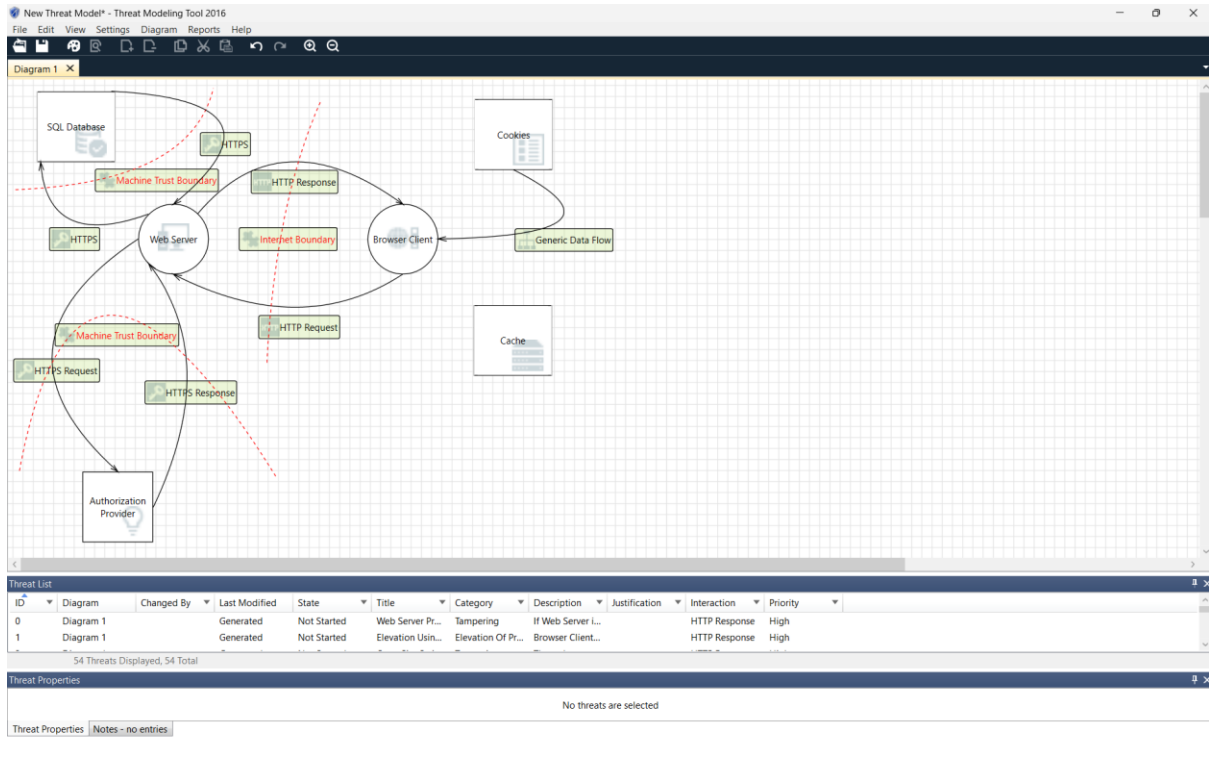
- **Data Flow Type:** HTTPS
- Description: The web server initiates the request with the database server

SQL Database Server -> Web Server (Confirm Update)

- **Data Flow Type:** HTTPS
- Description: The SQL Database Server confirms the update and sends the confirmation back to the web server.

Web Server -> Employee (Display HRMS System)

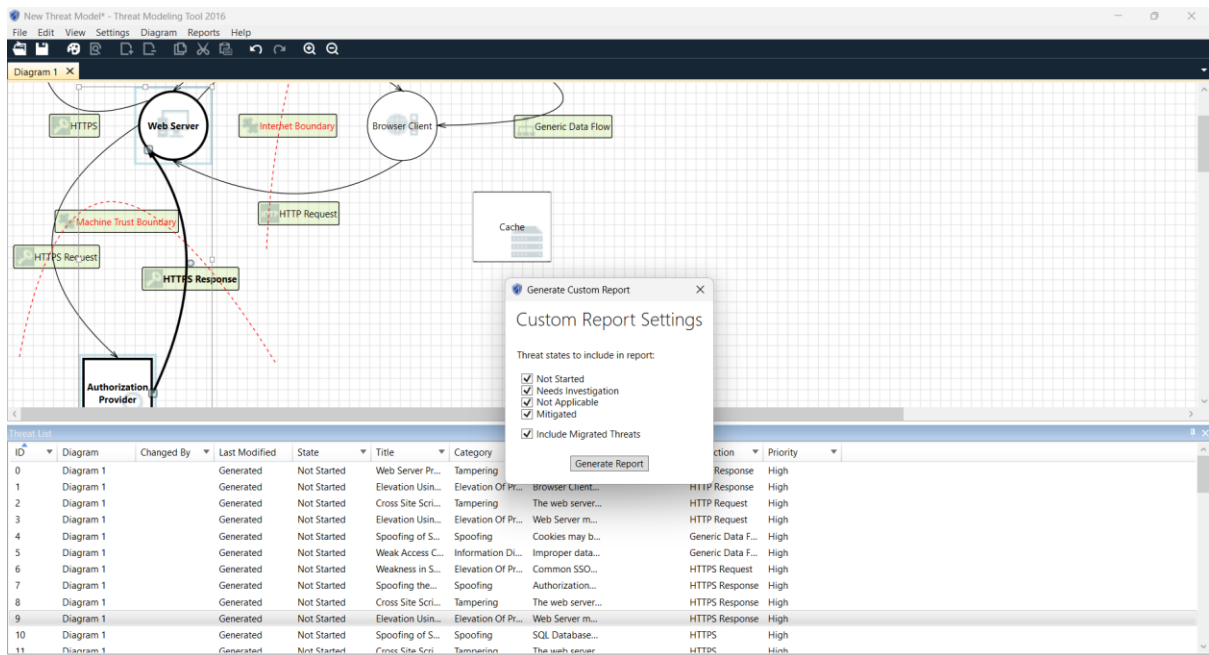
- **Data Flow Type:** HTTPS
- **Description:** The web server displays the leave status to the employee in HRMS System



➤ Analysis View

Threat List										
ID	Diagram	Changed By	Last Modified	State	Title	Category	Description	Justification	Interaction	Priority
0	Diagram 1		Generated	Not Started	Web Server Pr...	Tampering	If Web Server i...		HTTP Response	High
1	Diagram 1		Generated	Not Started	Elevation Usin...	Elevation Of Pr...	Browser Client...		HTTP Response	High
2	Diagram 1		Generated	Not Started	Cross Site Scri...	Tampering	The web server...		HTTP Request	High
3	Diagram 1		Generated	Not Started	Elevation Usin...	Elevation Of Pr...	Web Server m...		HTTP Request	High
4	Diagram 1		Generated	Not Started	Spoofing of S...	Spoofing	Cookies may b...		Generic Data F...	High
5	Diagram 1		Generated	Not Started	Weak Access C...	Information Di...	Improper data...		Generic Data F...	High
6	Diagram 1		Generated	Not Started	Weakness in S...	Elevation Of Pr...	Common SSO...		HTTPS Request	High
7	Diagram 1		Generated	Not Started	Spoofing the...	Spoofing	Authorization...		HTTPS Response	High
8	Diagram 1		Generated	Not Started	Cross Site Scri...	Tampering	The web server...		HTTPS Response	High
9	Diagram 1		Generated	Not Started	Elevation Usin...	Elevation Of Pr...	Web Server m...		HTTPS Response	High
10	Diagram 1		Generated	Not Started	Spoofing of S...	Spoofing	SQL Database...		HTTPS	High
11	Diagram 1		Generated	Not Started	Cross Site Scri...	Tampering	The web server...		HTTPS	High
12	Diagram 1		Generated	Not Started	Persistent Cros...	Tampering	The web server...		HTTPS	High
13	Diagram 1		Generated	Not Started	Weak Access C...	Information Di...	Improper data...		HTTPS	High
14	Diagram 1		Generated	Not Started	Spoofing of D...	Spoofing	SQL Database...		HTTPS	High
15	Diagram 1		Generated	Not Started	Potential SQL I...	Tampering	SQL injection i...		HTTPS	High
16	Diagram 1		Generated	Not Started	Potential Exces...	Denial Of Servi...	Does Web Ser...		HTTPS	High
17	Diagram 1		Generated	Not Started	Potential Data...	Repudiation	Web Server cla...		HTTPS	High

➤ We can choose a specific threat and check its properties



- A report is generated which lists all the threats in our model

Threat Modeling Report

Created on 24-05-2024 21:48:03

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	54
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	54
Total Migrated	0