SECURE SYSTEMS ENGINEERING

Assignment- 1

V NANDITHA
CB.SC.P2CYS23018
(2nd Year / 3rd Sem- MTech, CYBERSECURITY)

Case Study: Online Retail System

Scope:

An online retail system where customers can browse products, add items to their cart, make purchases, and track orders. The system also allows administrators to manage inventory, process orders, and analyze sales data.

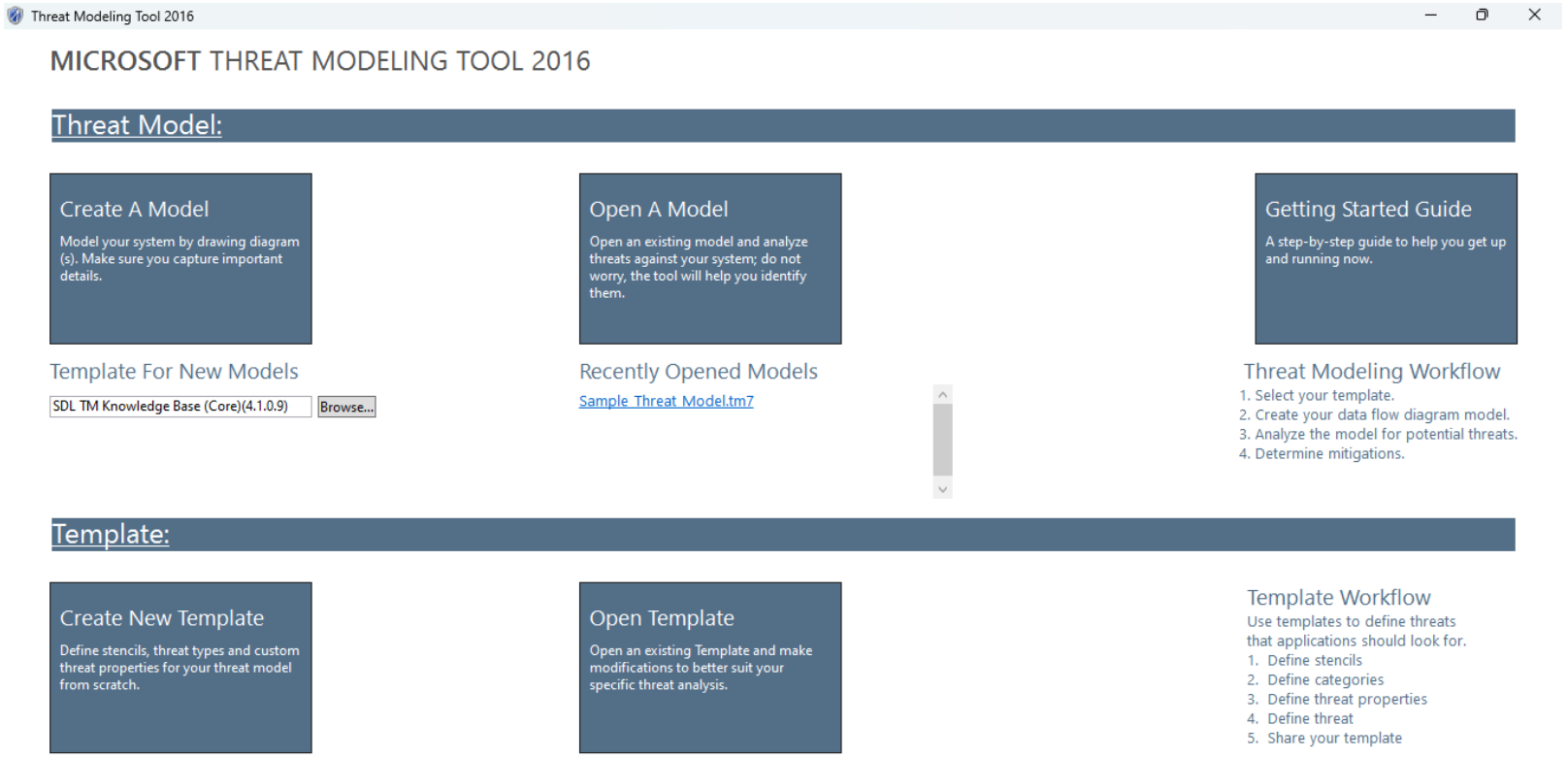
Objectives:

- Identify potential security threats.
- Assess the impact and likelihood of these threats.
- Develop strategies to mitigate these threats.

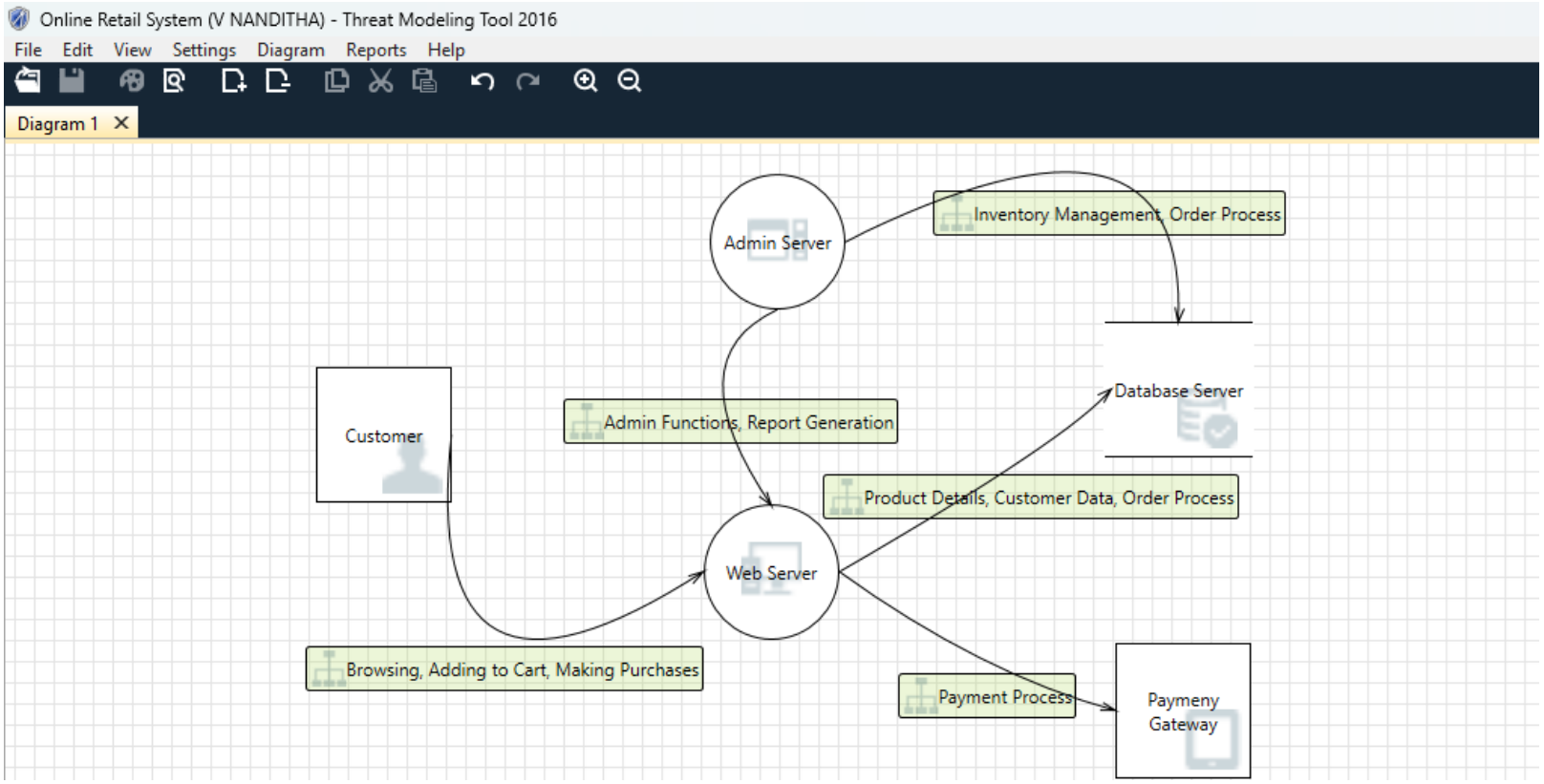
Entities:

- Customer (External Entity)
  - Can browse products, add items to cart, and make purchases.
  - Can view order history and track order status.
- Web Server (Process)
  - Serves the front-end interface to customers and administrators.
  - Handles HTTP requests and responses.
- Database Server (Data Store)
  - Stores product information, customer data, order details, and inventory records.
  - Ensures data integrity and availability.
- Payment Gateway (External Entity)
  - Processes customer payments securely.
  - Interfaces with banking systems for transaction approvals.
- Admin Server (Internal Entity)
  - Provides tools for administrators to manage products, inventory, and orders.
  - Generates reports and analytics for business insights.

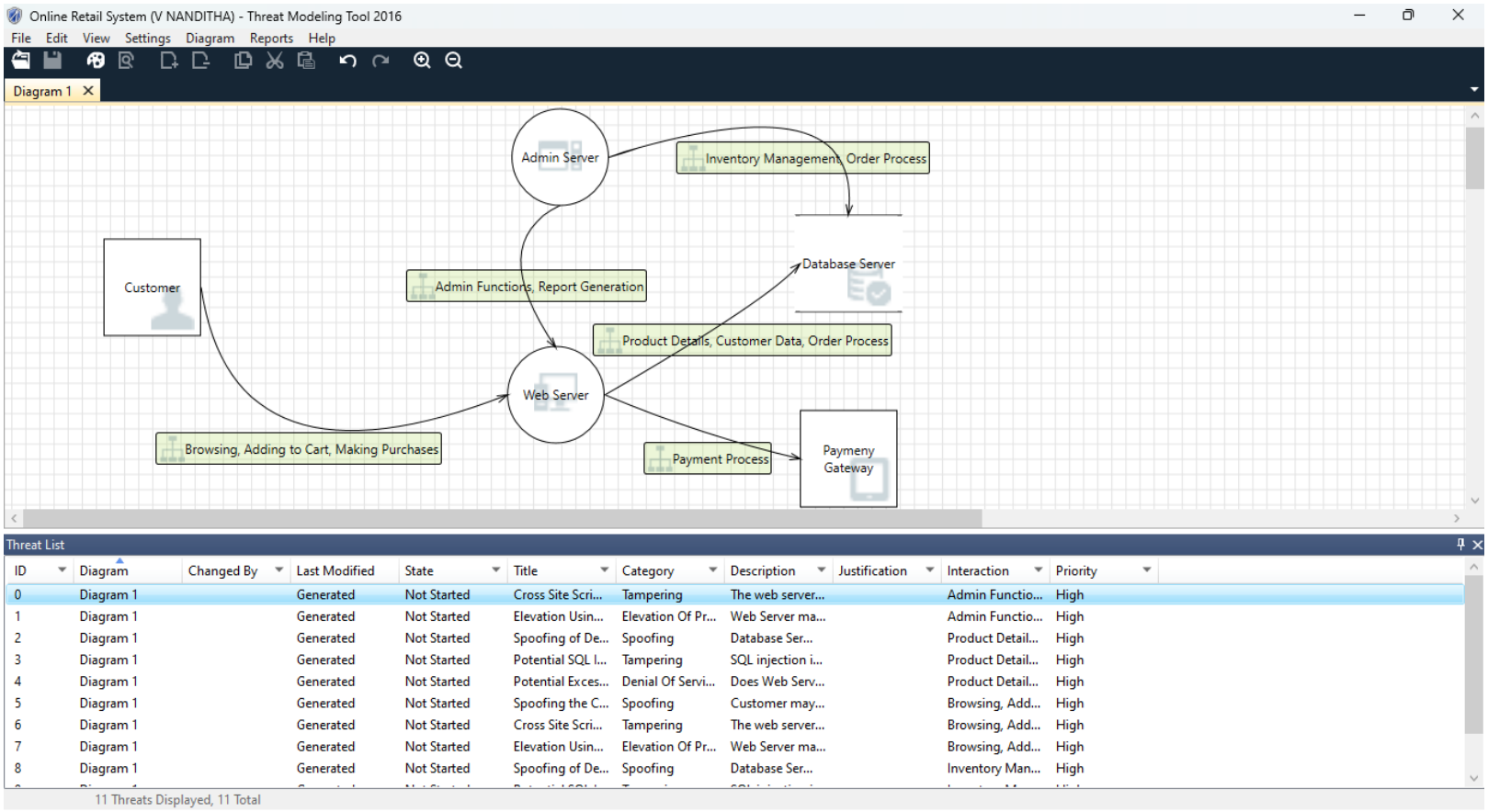
1. Click: NEW MODEL



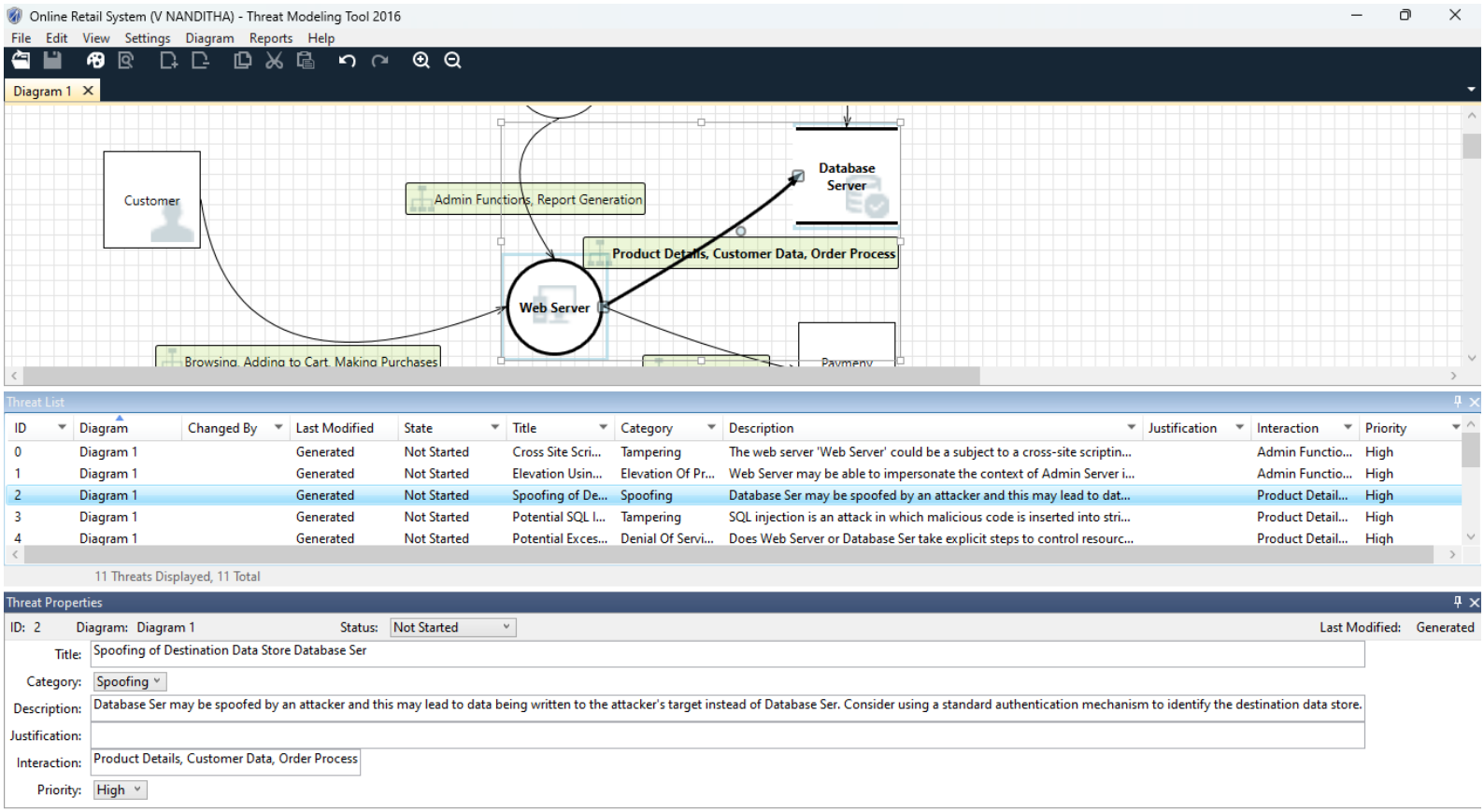
2. Create a new model – Online Retail System



3. Identify & Analyse Threats



- Analyse the Process to find Treats



4. Data Flow Sequence

a. Customer Browses Products

Customer → Web Server: Request to view product catalog.

Web Server → Database Server: Query for product details.

Database Server → Web Server: Send product details.

Web Server → Customer: Display product catalog.

b. Customer Adds Item to Cart

Customer → Web Server: Request to add product to cart.

Web Server → Database Server: Update cart details.

Database Server → Web Server: Confirmation of cart update.

Web Server → Customer: Display updated cart.

c. Customer Makes Purchase

Customer → Web Server: Request to proceed to checkout.

Web Server → Payment Gateway: Send payment details.

Payment Gateway → Web Server: Confirmation of payment.

Web Server → Database Server: Update order details.

Database Server → Web Server: Confirmation of order update.

Web Server → Customer: Display order confirmation.

d. Customer Tracks Order

Customer → Web Server: Request to track order status.

Web Server → Database Server: Query order status.

Database Server → Web Server: Send order status details.

Web Server → Customer: Display order status.

e. Admin Manages Inventory

Admin Server → Database Server: Update inventory details.

Database Server → Admin Server: Confirmation of inventory update.

f. Admin Processes Orders

Admin Server → Database Server: Query and update order processing status.

Database Server → Admin Server: Send order processing details.

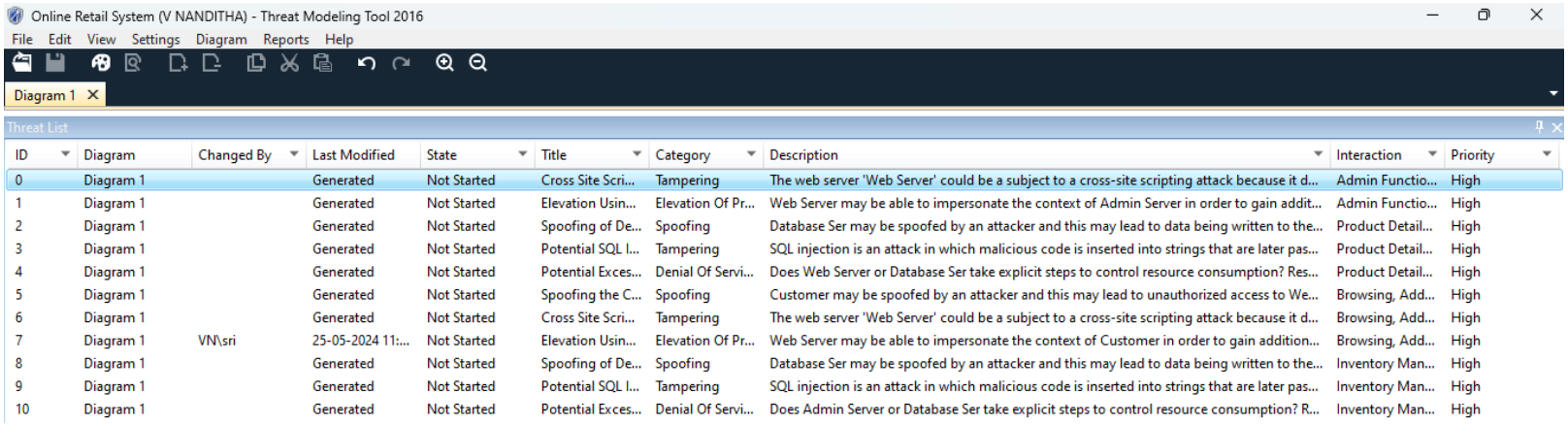
g. Admin Generates Reports

Admin Server → Database Server: Query sales and customer data.

Database Server → Admin Server: Send requested data.

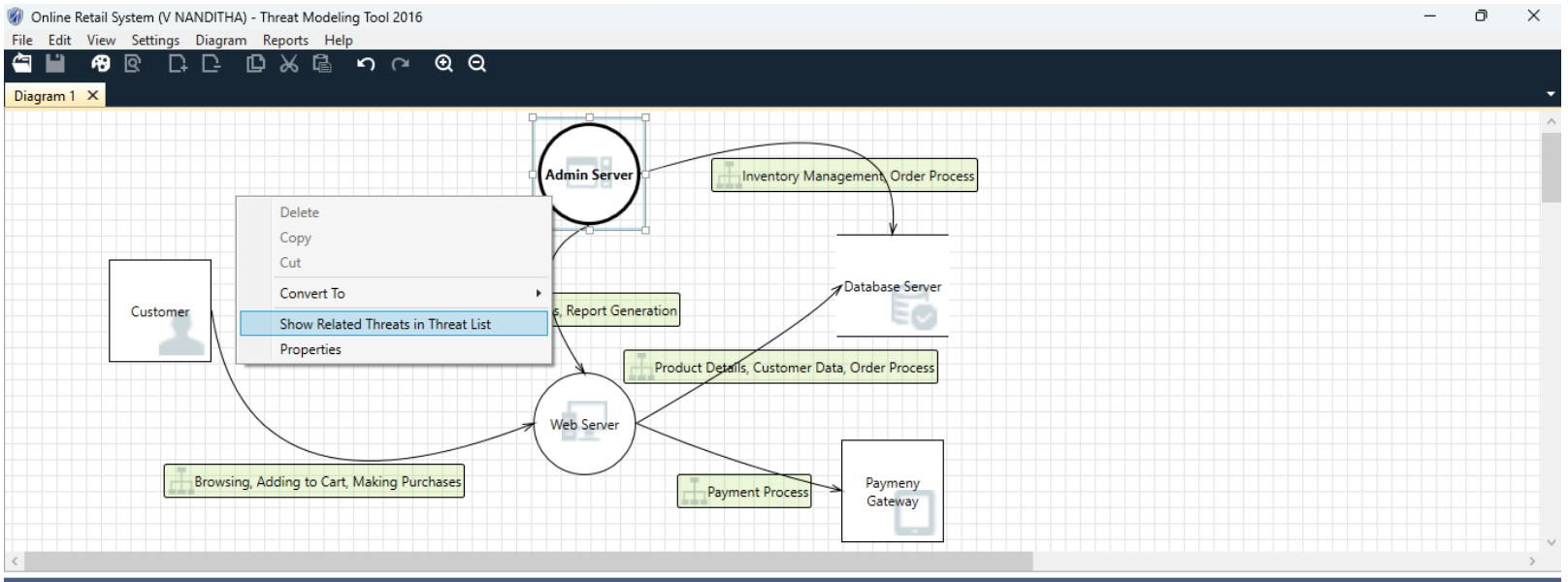
Admin Server: Generate reports and analytics.

5. Analysis View



ID	Diagram	Changed By	Last Modified	State	Title	Category	Description	Interaction	Priority
0	Diagram 1		Generated	Not Started	Cross Site Scri...	Tampering	The web server 'Web Server' could be a subject to a cross-site scripting attack because it d...	Admin Functio...	High
1	Diagram 1		Generated	Not Started	Elevation Usin...	Elevation Of Pr...	Web Server may be able to impersonate the context of Admin Server in order to gain addit...	Admin Functio...	High
2	Diagram 1		Generated	Not Started	Spoofing of De...	Spoofing	Database Ser may be spoofed by an attacker and this may lead to data being written to the...	Product Detail...	High
3	Diagram 1		Generated	Not Started	Potential SQL I...	Tampering	SQL injection is an attack in which malicious code is inserted into strings that are later pas...	Product Detail...	High
4	Diagram 1		Generated	Not Started	Potential Exces...	Denial Of Servi...	Does Web Server or Database Ser take explicit steps to control resource consumption? Res...	Product Detail...	High
5	Diagram 1		Generated	Not Started	Spoofing the C...	Spoofing	Customer may be spoofed by an attacker and this may lead to unauthorized access to We...	Browsing, Add...	High
6	Diagram 1		Generated	Not Started	Cross Site Scri...	Tampering	The web server 'Web Server' could be a subject to a cross-site scripting attack because it d...	Browsing, Add...	High
7	Diagram 1	VN\sri	25-05-2024 11:...	Not Started	Elevation Usin...	Elevation Of Pr...	Web Server may be able to impersonate the context of Customer in order to gain addition...	Browsing, Add...	High
8	Diagram 1		Generated	Not Started	Spoofing of De...	Spoofing	Database Ser may be spoofed by an attacker and this may lead to data being written to the...	Inventory Man...	High
9	Diagram 1		Generated	Not Started	Potential SQL I...	Tampering	SQL injection is an attack in which malicious code is inserted into strings that are later pas...	Inventory Man...	High
10	Diagram 1		Generated	Not Started	Potential Exces...	Denial Of Servi...	Does Admin Server or Database Ser take explicit steps to control resource consumption? R...	Inventory Man...	High

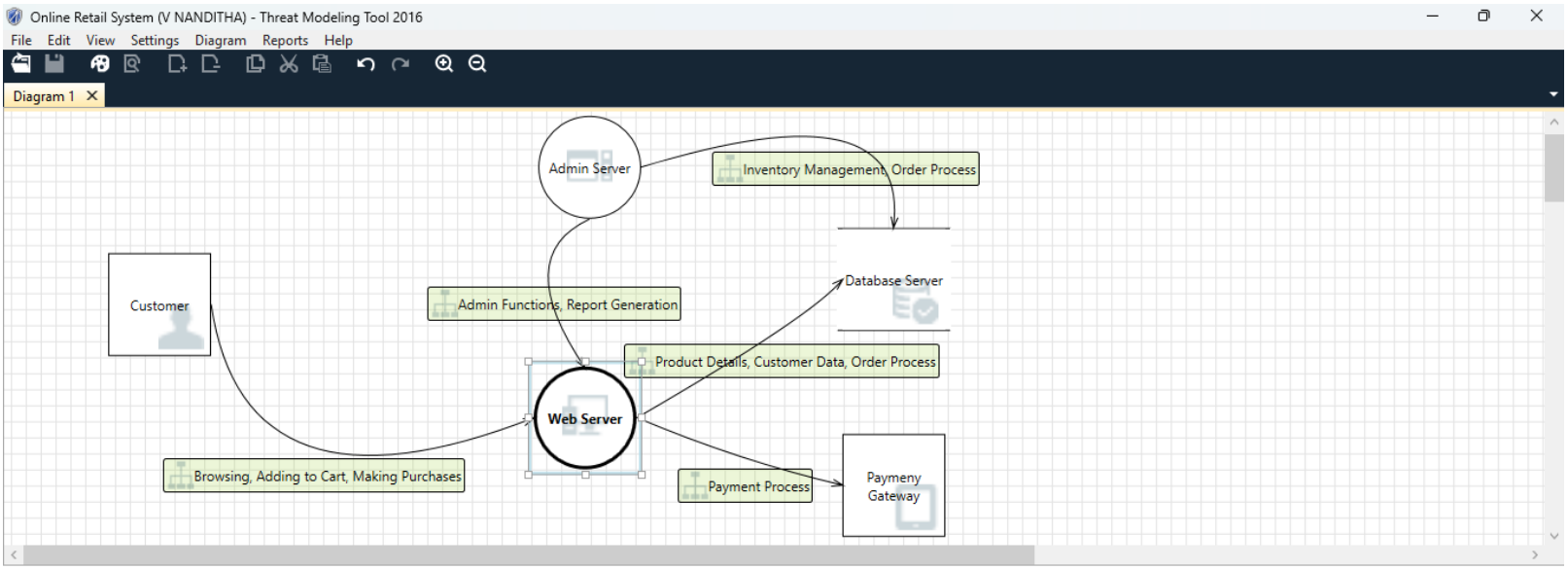
- You can Search for Related Threats



ID	Diagram	Changed By	Last Modified	State	Title	Category	Description	Interaction	Priority
0	Diagram 1		Generated	Not Started	Cross Site Scri...	Tampering	The web server 'Web Server' could be a subject to a cross-site scripting attack because it d...	Admin Functio...	High
1	Diagram 1		Generated	Not Started	Elevation Usin...	Elevation Of Pr...	Web Server may be able to impersonate the context of Admin Server in order to gain addit...	Admin Functio...	High
8	Diagram 1		Generated	Not Started	Spoofing of De...	Spoofing	Database Ser may be spoofed by an attacker and this may lead to data being written to the...	Inventory Man...	High
9	Diagram 1		Generated	Not Started	Potential SQL I...	Tampering	SQL injection is an attack in which malicious code is inserted into strings that are later pas...	Inventory Man...	High
10	Diagram 1		Generated	Not Started	Potential Exces...	Denial Of Servi...	Does Admin Server or Database Ser take explicit steps to control resource consumption? R...	Inventory Man...	High

- Related Threats are Filtered and mentioned.

- Threat ID : 0, 1, 8, 9, 10 are Related to Admin Server.

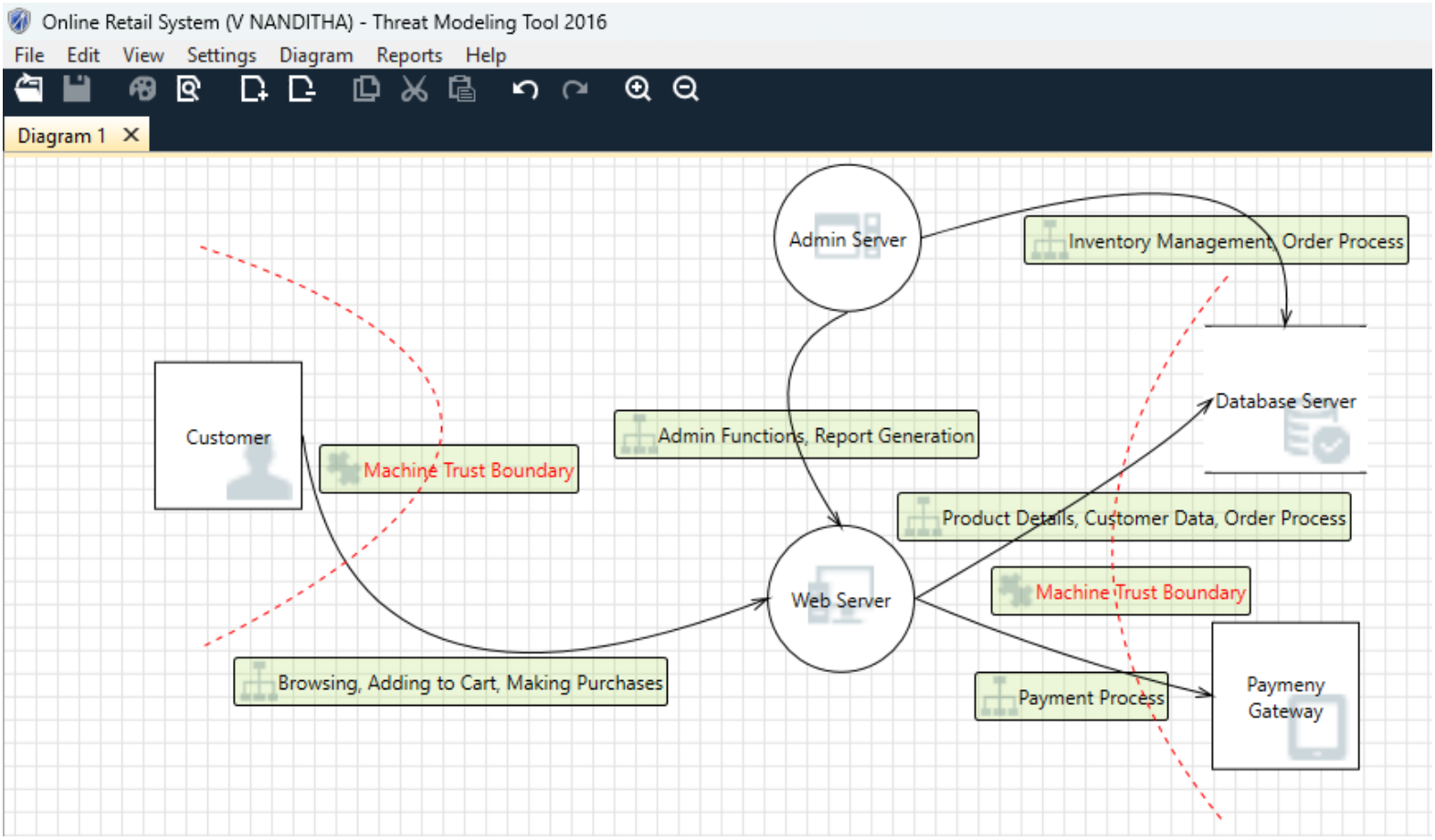


Threat List

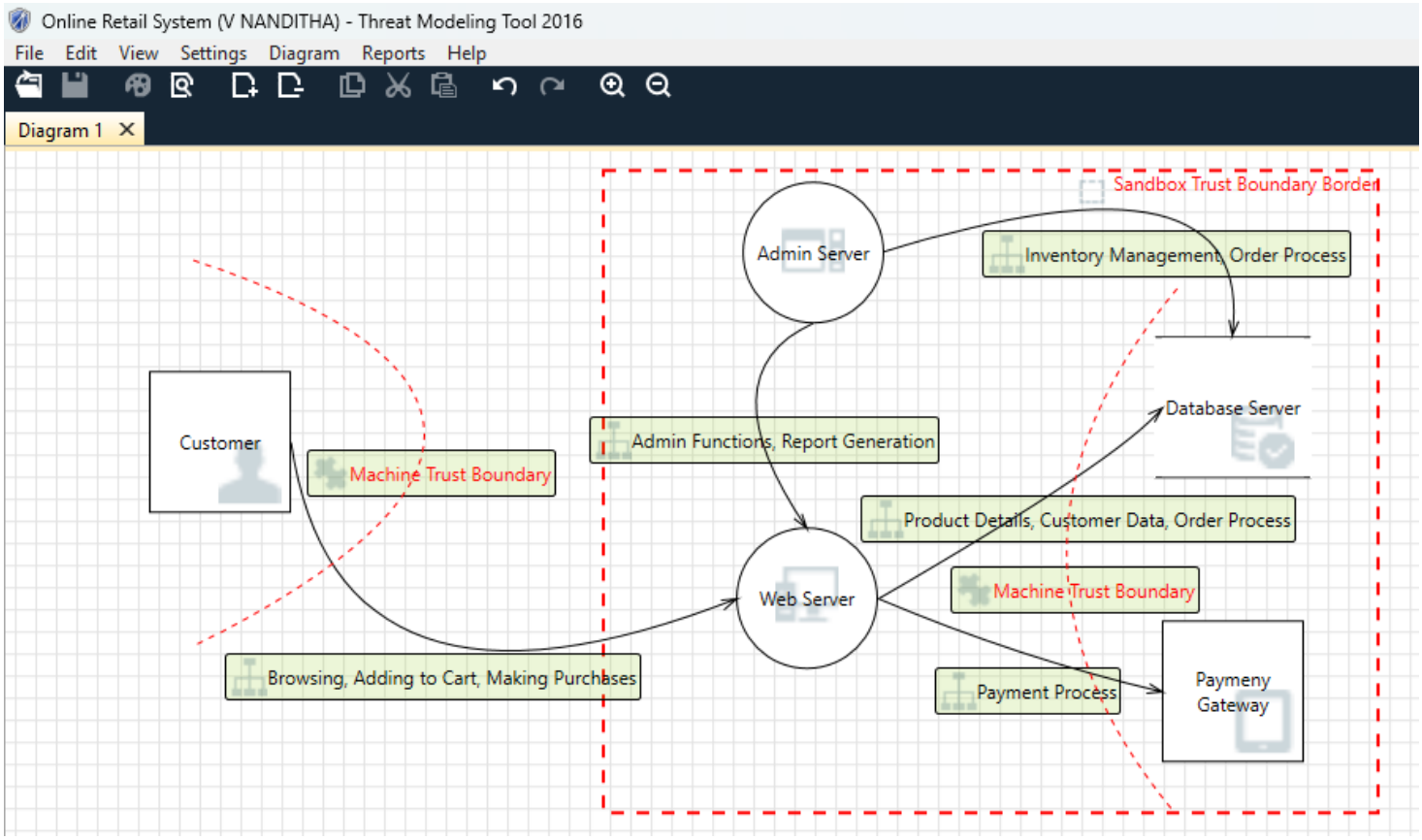
ID	Diagram	Changed By	Last Modified	State	Title	Category	Description	Interaction	Priority
0	Diagram 1		Generated	Not Started	Cross Site Scri...	Tampering	The web server 'Web Server' could be a subject to a cross-site scripting attack because it d...	Admin Functio...	High
1	Diagram 1		Generated	Not Started	Elevation Usin...	Elevation Of Pr...	Web Server may be able to impersonate the context of Admin Server in order to gain addit...	Admin Functio...	High
2	Diagram 1		Generated	Not Started	Spoofing of De...	Spoofing	Database Ser may be spoofed by an attacker and this may lead to data being written to the...	Product Detail...	High
3	Diagram 1		Generated	Not Started	Potential SQL I...	Tampering	SQL injection is an attack in which malicious code is inserted into strings that are later pas...	Product Detail...	High
4	Diagram 1		Generated	Not Started	Potential Exces...	Denial Of Servi...	Does Web Server or Database Ser take explicit steps to control resource consumption? Res...	Product Detail...	High
5	Diagram 1		Generated	Not Started	Spoofing the C...	Spoofing	Customer may be spoofed by an attacker and this may lead to unauthorized access to We...	Browsing, Add...	High
6	Diagram 1		Generated	Not Started	Cross Site Scri...	Tampering	The web server 'Web Server' could be a subject to a cross-site scripting attack because it d...	Browsing, Add...	High
7	Diagram 1	VN\sri	25-05-2024 11:...	Not Started	Elevation Usin...	Elevation Of Pr...	Web Server may be able to impersonate the context of Customer in order to gain addition...	Browsing, Add...	High

Clear Filters 8 Threats Displayed, 11 Total

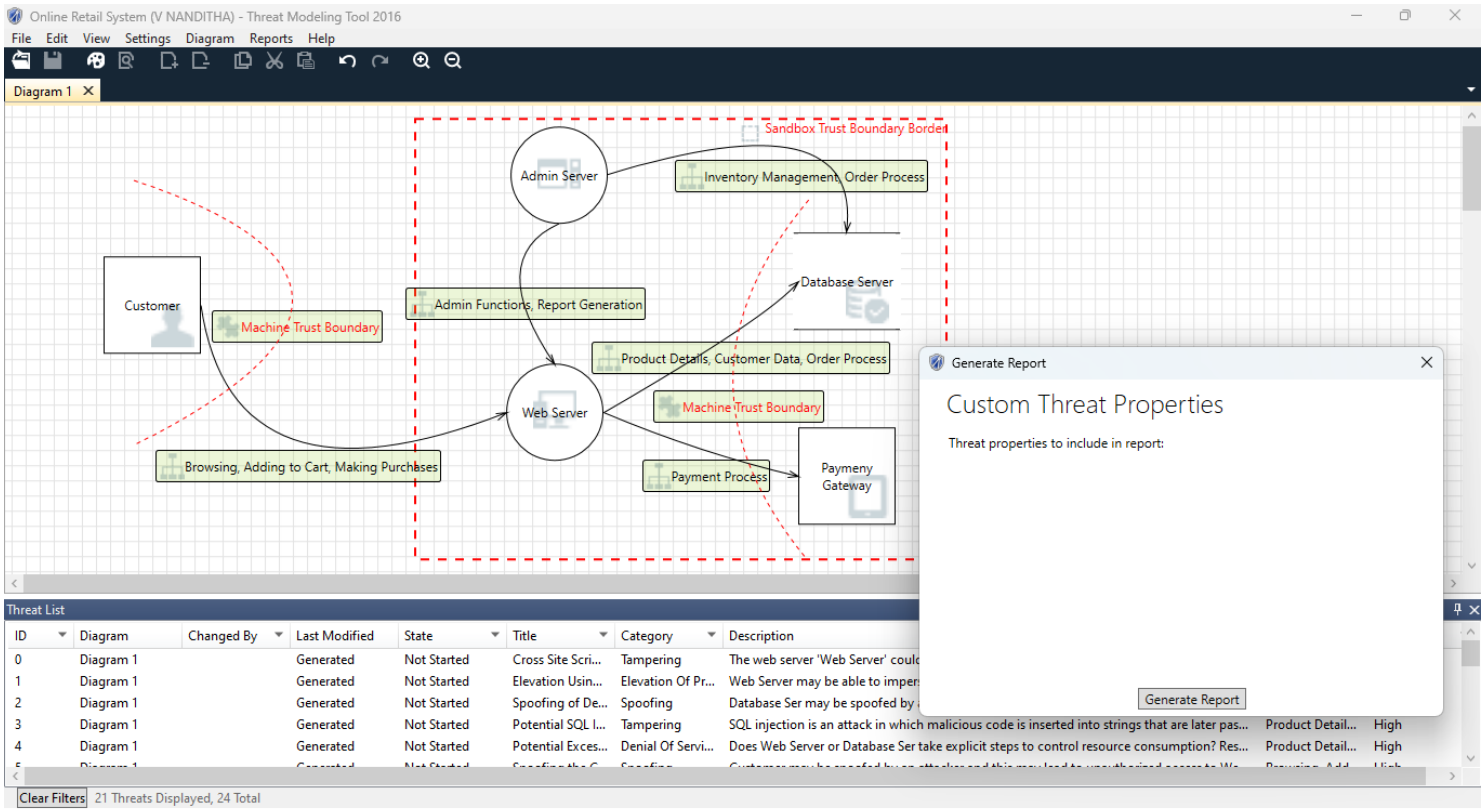
6. Trust Boundaries



7. Sandbox Trust Boundary

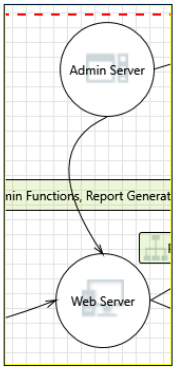


8. Create Full Report



9. Generated Report

Interaction: Admin Functions, Report Generation



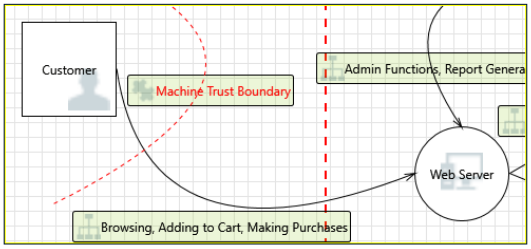
1. Cross Site Scripting [State: Not Started] [Priority: High]

Category: Tampering
Description: The web server 'Web Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
Justification: <no mitigation provided>

2. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: Web Server may be able to impersonate the context of Admin Server in order to gain additional privilege.

Interaction: Browsing, Adding to Cart, Making Purchases



3. Spoofing the Customer External Entity [State: Not Started] [Priority: High]

Category: Spoofing
Description: Customer may be spoofed by an attacker and this may lead to unauthorized access to Web Server. Consider using a standard authentication mechanism to identify the external entity.
Justification: <no mitigation provided>

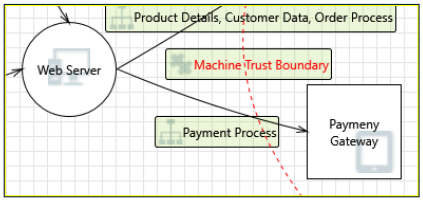
4. Cross Site Scripting [State: Not Started] [Priority: High]

Category: Tampering
Description: The web server 'Web Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
Justification: <no mitigation provided>

5. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Interaction: Payment Process



14. Spoofing of the Paymeny Gateway External Destination Entity [State: Not Started] [Priority: High]

Category: Spoofing
Description: Paymeny Gateway may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Paymeny Gateway. Consider using a standard authentication mechanism to identify the external entity.
Justification: <no mitigation provided>

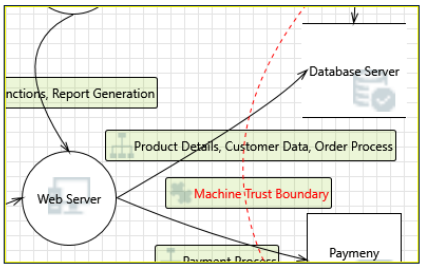
15. External Entity Paymeny Gateway Potentially Denies Receiving Data [State: Not Started] [Priority: High]

Category: Repudiation
Description: Paymeny Gateway claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: <no mitigation provided>

16. Data Flow Payment Process Is Potentially Interrupted [State: Not Started] [Priority: High]

Category: Denial Of Service

Interaction: Product Details, Customer Data, Order Process



17. Spoofing of Destination Data Store Database Ser [State: Not Started] [Priority: High]

Category: Spoofing
Description: Database Ser may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Database Ser. Consider using a standard authentication mechanism to identify the destination data store.
Justification: <no mitigation provided>

18. Potential SQL Injection Vulnerability for Database Ser [State: Not Started] [Priority: High]

Category: Tampering
Description: SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.
Justification: <no mitigation provided>

Generated Report Link :

https://drive.google.com/file/d/1zein2IE_AT7hk8qSWGsCr7BpJZeMgCiL/view?usp=sharing