
Cyber Security

Capstone Project Problem Statement





Capstone Project: Threat Modeling

Background of the problem statement:

BigMart has a chain of retail stores, selling daily groceries and home requirements across the country.

Lately, it has been losing market share to online competitors who are providing a better customer experience than BigMart's brick and mortar establishments.

BigMart wants to secure #1 market leader position for daily groceries and home requirements by adopting a digital strategy.

The company plans to provide a secure, uninterrupted, and enhanced user experience to its existing and prospective customers.


BigMart, Inc., has contracted your organization to perform a threat modeling exercise for its online strategy.

BigMart provides the following requirements:

- Customers should be able to search for products and place their orders using the online web store.
- Customer needs to create an account prior to placing an order.
- Customers can pay with their credit card, debit card, online banking or digital wallet.
- Sales team can view customer order details in order to process and deliver it.
- Administrators can modify product information.

The requirements study results in the following statements and requirements:

- The web store will need to be accessible from the Intranet as well as the Internet.

- 
- The web store will need to be designed with a distributed architecture for scalability reasons.
 - Users will need to authenticate to the web store with the user account credentials which in turn will authenticate to the backend database (deployed internally) via a web services interface.
 - Credit card processing will be outsourced to a third-party processor.
 - User interactions with the web store will need to be tracked.
 - The database will need to be backed up periodically to a third-party location for disaster recovery (DR) purposes.
 - Programming language used is Python and the backend database can be either Oracle or Microsoft SQL Server. The Web Server used is Nginx.

You have been tasked to perform the threat modeling of the application.

Task 1

Before you dive into the process of threat modeling, first identify the business and security objectives.


Once the security objectives are identified and understood, you can threat model the software.

This includes the following phases with specific activities inside each phase.

- Identify Assets
- Create Architecture Overview
- Decompose Architecture
- Identify Threats
- Document Threats
- Rate Threats

Phase 1 – Identify Assets

Task 2

- 
- Identify human and non-human actors of the systems
 - Identify data elements
 - Identify technologies that will be used to develop the application
 - Identify external dependencies
 - Identify threat actors

Phase 2 – Create Architecture Overview

Task 3

Create a physical network topology using the following information:

- Use Firewall for boundary protection
- Use Web application Firewall to protect the application
- Use security solutions such as IDS to monitor for malicious traffics
- Application server is placed in the DMZ
- Database server is placed in the Internal network

Phase 3 – Decompose Architecture

Task 4

Create a logical topology using the following information:

- Customers use SSL/TLS to access the web store
- There is a trust boundary between the web server and application
- There is a trust boundary between the application and database
- Connection between application is via a secure VPN

Phase 4 – Identify Threats

Task 5

- Apply the STRIDE model to identify relevant threats (minimum 1 per element). Use OWASP Top 10 list as reference.

Phase 5 – Document Threats

Task 6

Use the following threat template for the threats identified in Phase 4.

Threat description	
Threat target	
Attack techniques	
Controls/ Countermeasures	

Phase 6 – Rate Threats

Task 7

Use the DREAD model to rate each threat. Each element of DREAD can have a threat rating of 1, 2 or 3 (1=Low, 2=Medium, 3=High).

Threat	D	R	E	A	D	Total	Rating
Threat1							



Threat2							
---------	--	--	--	--	--	--	--

Threat Rating

Low – Total between 5 and 7

Medium – Total between 7 and 10

High – Total more than 10

Task 8

- Include the threat rating for each threat in the template created in Phase 5.