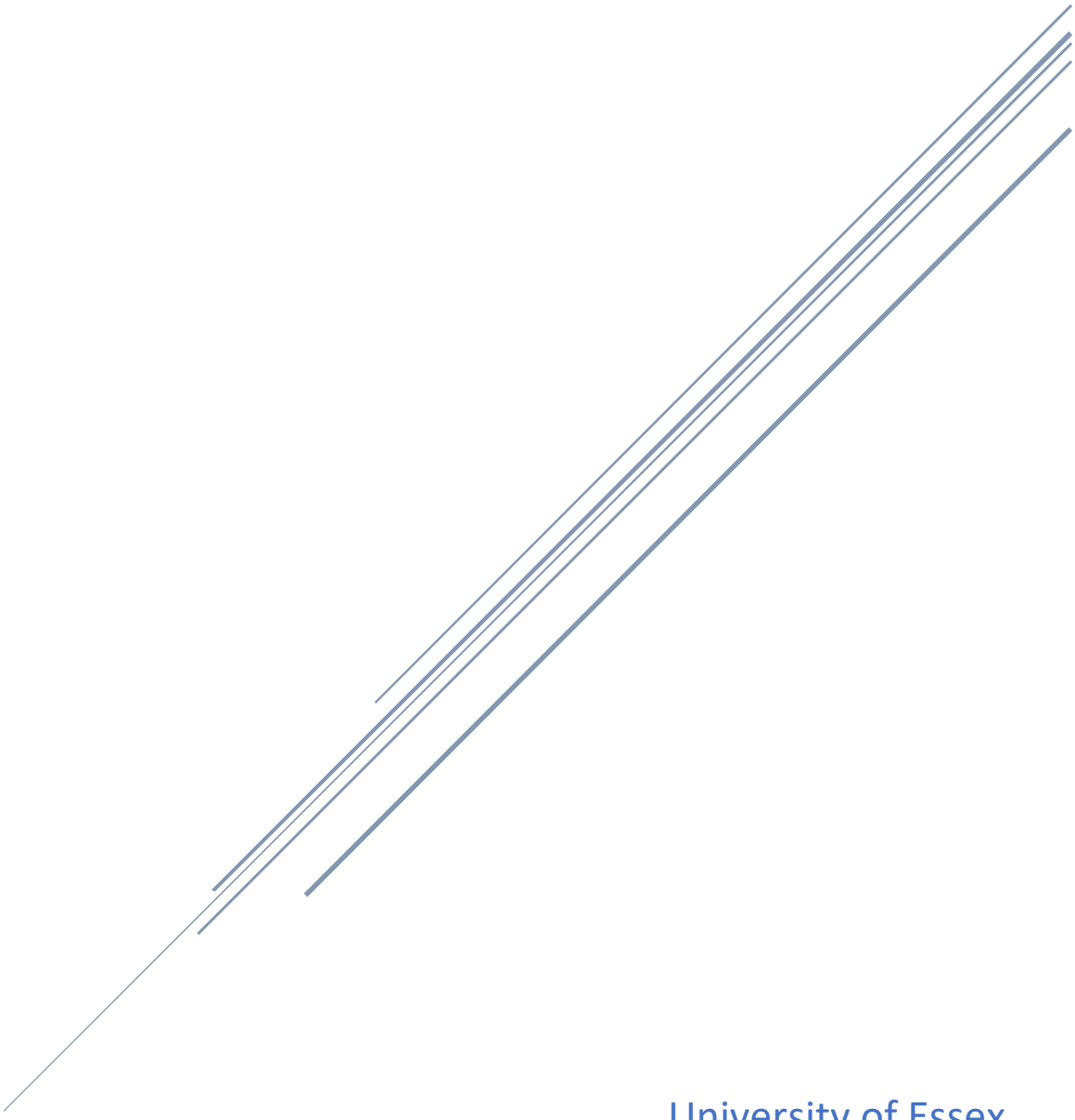
ONLINE SHOPPING SYSTEM (OSS)

Individual Essay Report



University of Essex

Launching into Cyber Security January 2023

In today's fast-paced and increasingly digital world and with the rising use of media applications, consumer behavior, and shopping habits have undergone significant transformations. The number of online shoppers is growing as a convenient and time-saving alternative to traditional brick-and-mortar stores. As a forward-thinking business owner, it is crucial to recognize the immense potential of having an online shopping system, catering to your customers' evolving needs and expanding your market reach. I would like to present a proposal for implementing an Online Shopping System (OSS) for your store. This proposal outlines the benefits and potential challenges, including cyber threats, that may arise from implementing the system. It is crucial to understand these aspects to make an informed decision.

Benefits of an Online Shopping System:

1. Increased Reach: By embracing an OSS, your store can reach a wider audience without geographical limitations. This can lead to a significant increase in sales and customer base.
2. Convenience for Customers: Online shopping allows customers to browse and purchase products from the comfort of their homes 24/7. This can lead to increased customer satisfaction and loyalty.
3. Improved Inventory Management: An OSS can help you efficiently manage and track inventory levels, reducing stockouts and overstocking.
4. Better Data Collection and Analytics: The system can provide insights into customer behavior, preferences, and purchasing patterns. This data can be used to make better-informed decisions regarding product offerings, pricing, and promotions.
5. Cost-effective marketing: Digital marketing can be more targeted and cost-effective than traditional methods. An OSS allows you to take advantage of these opportunities and promote your store to a broader audience.

Potential Problems and Cyber Threats:

1. Data Breaches: Implementing an OSS involves handling sensitive customer data, such as payment information and personal details. A data breach could lead to financial loss and damage to your store's reputation.
2. Online Fraud and Scams: Your online store could be targeted by fraudsters and scammers, resulting in chargebacks and lost revenue.
3. Website Downtime: Technical issues or cyber-attacks can take your website offline, disrupting sales and negatively affecting customer trust.
4. Legal and Compliance Issues: Additional legal and regulatory requirements may be associated with operating an online store, such as privacy policies and taxation rules.
5. Increased Competition: Transitioning to an online platform can expose your store to increased competition from other online retailers.

Mitigation strategies:

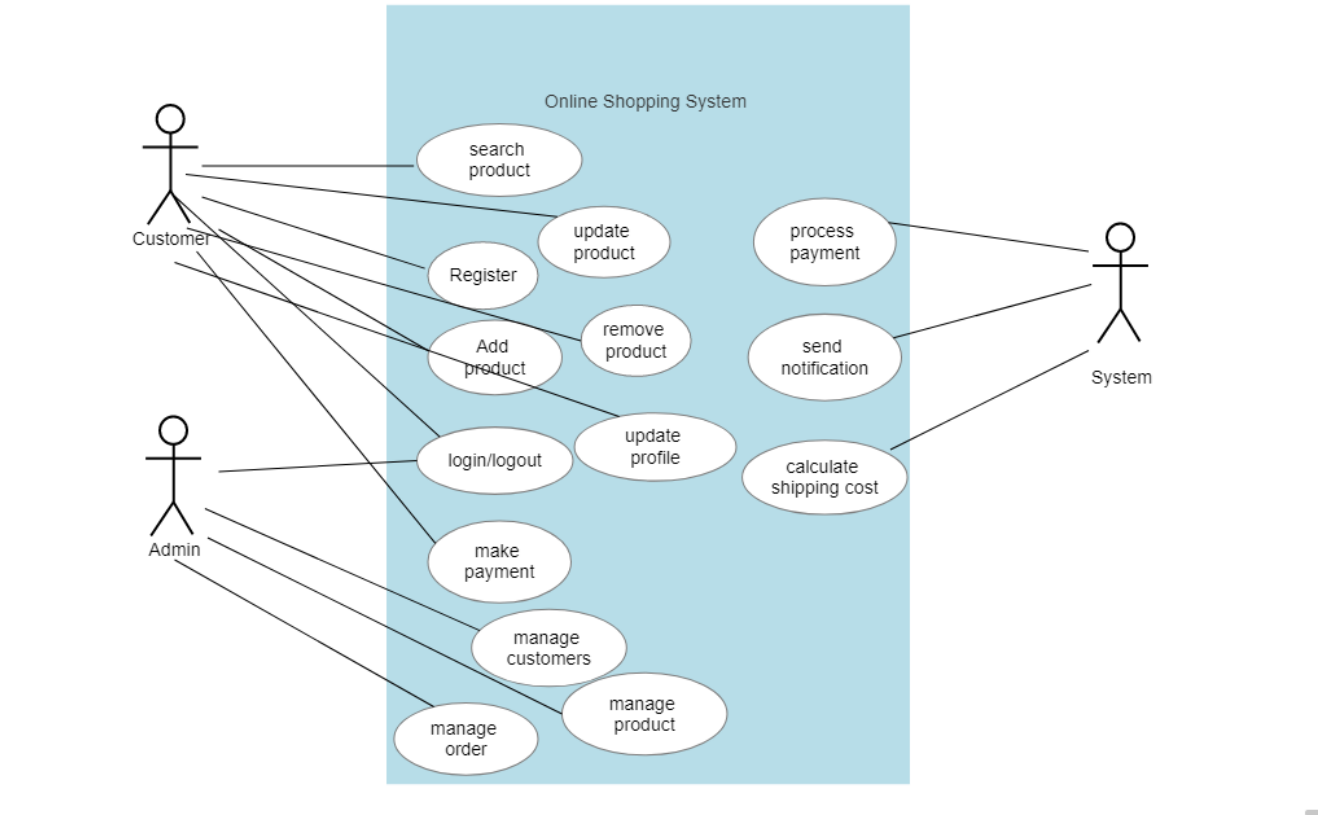
1. To protect sensitive customer data, invest in robust security measures, such as encryption, secure socket layer (SSL) certificates, and firewalls.
2. Partner with a reliable payment gateway provider to minimize fraud and chargeback risk.
3. Implement regular website maintenance, updates, and backups to minimize downtime risk.

4. Consult with legal professionals to ensure compliance with all relevant laws and regulations.
5. Develop a robust digital marketing strategy to differentiate your store from competitors and attract customers.

I will use two UML diagrams in my proposal: a use case diagram and a class diagram.

Use case diagrams are essential for visually capturing and prioritizing user requirements, facilitating effective communication and collaboration among stakeholders, and ensuring a system meets its intended purpose by focusing on user interactions. In contrast, class diagrams are crucial for representing the structure, relationships, and attributes of a system's components, providing a clear understanding of the system's organization.(Shoval, Yampolsky and Last, no date)

Use case diagram:

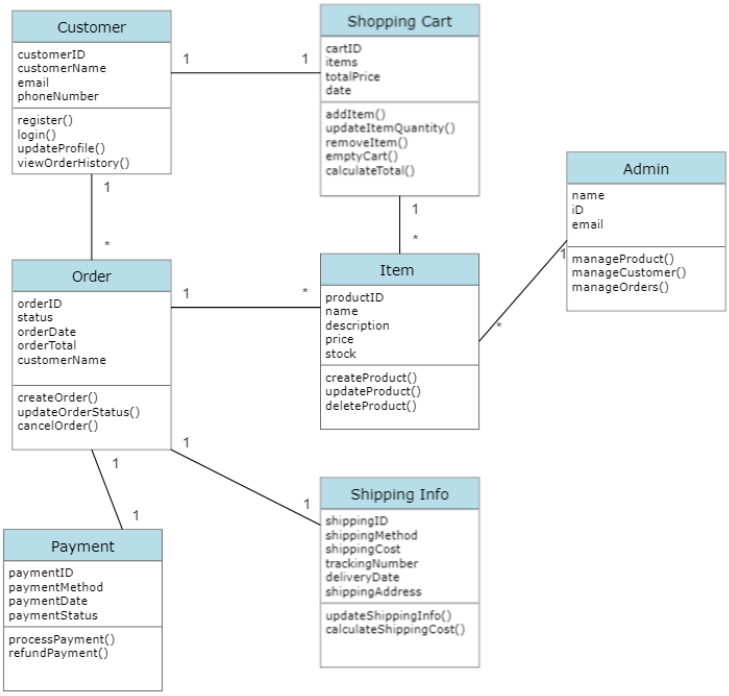


(*SmartDraw - Create Flowcharts, Floor Plans, and Other Diagrams on Any Device*, no date)

Use case summary:

Use case	Brief description
Login/logout	The customer and admin can log in / log out of the system
Register	The customer registers his details in the system
Search Product	The system provides the customer with all quires related to his requirements and displays them.
Update product	The customer can change the product requirements
Remove product	The customer can delete the product he selected
Update profile	The customer can edit his profile details
Make payment	The customer can make a payment after adding all products
Manage customer	Admin can View/Edit/Delete the customer
Manage product	Admin can Add/Edit/Delete a product
Manage order	Admin can View/Update status /cancel the order
Process payment	The system processes payment made by customer
Calculate shipping cost	The system calculates the cost of shipping
Send notification	The system can send order confirmation, shopping updates etc.

Class diagram:



(*SmartDraw - Create Flowcharts, Floor Plans, and Other Diagrams on Any Device*, no date)

Class summary:

Classes	**Relationship and associations**	**Attributes**	**Methods**
Customer	ShoppingCart (1:1) – A customer can have one shopping cart.	customerID, customerName, email, phoneNumber	register(), login(), updateProfile(), viewOrderHistory()
ShoppingCart	Order (1:*) – A customer can have multiple orders.	cartID, items (list of Product objects with quantity), totalPrice, date	addItem(), removeItem(), updateItemQuantity(), emptyCart(), calculateTotal()
Product	Product (1:*) – A shopping cart can contain multiple items.	productID, name, description, price, stock	createProduct(), updateProduct(), deleteProduct()

Order	Item (1:*) – An order can consist of multiple items.	orderID, orderDate, status, orderTotal, customerName	createOrder(), updateOrderStatus(), cancelOrder()
Payment	Payment (1:1) – An order has one payment.	paymentID, paymentMethod, paymentDate, paymentStatus	processPayment(), refundPayment()
Shipping	Shipping (1:1) – An order has one shipping method.	shippingID, shippingMethod, shippingCost, trackingNumber, deliveryDate, shippingAddress	updateShippingInfo(), calculateShippingCost()
Admin	Item (1:*) – An admin can consist of many items	name , ID , email	manageProduct(), manageCustomer(), manageOrders()

In my proposal, I will use two threat modeling techniques: STRIDE and PASTA.

1.

STRIDE is a threat modeling technique developed by Microsoft. It focuses on identifying threats based on the following categories: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege.

By incorporating STRIDE into OSS security processes, you will be better equipped to:

1. Understand the various types of threats that could impact your systems, enabling you to develop targeted and effective countermeasures.
2. Proactively identify and remediate vulnerabilities before they can be exploited, reducing cyber-attack damage.
3. Facilitate communication and collaboration among stakeholders, such as developers, security teams, and management, by providing a common language and framework for discussing potential threats.
4. Foster a security-focused culture within your organization by raising awareness of potential risks and encouraging secure development practices.

Also, STRIDE has some limitations: The concept of 'mitigation' cannot be addressed. Identifying and designing strong countermeasures for identified threats is essential to complete threat modelling. Furthermore, this technique does not document the appropriate implementation of countermeasures (secure coding guidelines) – (Krishnan, no date)

We can apply the STRIDE method to our online shopping system as follows:

Attack property	**Threat scenario**	**Mitigation**	**Security theme**
Spoofing	○ Customer account spoofing ○ Administrator account spoofing ○ Spoofing the payment gateway	○ Implement strong authentication mechanisms like multi-factor authentication (MFA) ○ Use secure connections (HTTPS) for all web pages. ○ Limit login attempts and implement account lockout policies. ○ Validate and verify third-party integrations.	Authentication
Tampering	○ Tampering with product prices or inventory data	○ Implement input validation and output encoding.	Integrity

	○ Tampering with customer data or payment information ○ Tampering with shipping costs and address	○ Use secure data transmission and storage (encryption) ○ Implement integrity checks for critical data. ○ Control access to sensitive data and functionalities	
Repudiation	○ Customers denying, they made a purchase. ○ Administrators denying, they performed a certain action. ○ Attacker adding entries to server logs.	○ Implement comprehensive logging and monitoring of user and system activities. ○ Use digital signatures for critical transactions. ○ Enforce non-repudiation controls in contracts and terms of service.	Non-Repudiation
Information Disclosure	○ Exposure of user data, such as email or ID or addresses or passwords. ○ Exposure of payment information, such as credit card numbers	○ Use encryption for data at rest and in transit. ○ Implement access controls and data classification. ○ Perform regular vulnerability assessments and penetration testing.	Confidentiality
Denial Of Service	○ Overwhelming the web application with traffic ○ Crashing the database server ○ Exhausting the checkout service	○ Implement rate limiting and traffic filtering. ○ Use a Content Delivery Network (CDN) and Web Application Firewall (WAF)	Availability

		○ Design the system for scalability and fault tolerance.	
Elevation Of Privilege	○ Gaining administrative access to the system ○ Gaining unauthorized access to user accounts	○ Implement the principle of least privilege for user accounts and system components. ○ Conduct regular access reviews and audits. ○ Apply strong authentication and authorization mechanisms. ○ Patch and update software and systems regularly	Authorization

2.

PASTA is a seven-step, risk-centric threat modeling technique. It focuses on simulating attacks and analyzing threats to the system. The benefits of using PASTA as a threat modeling technique include comprehensive analysis, proactive security measures, improved communication and collaboration among stakeholders, and adaptability to various systems and industries. By incorporating PASTA into your organization's security processes, you will be able to better identify your system's potential vulnerabilities and develop appropriate countermeasures to mitigate risk.

However, PASTA comes with some limitations, with PASTA, organizations can align threat modelling with their strategic objectives. PASTA incorporates business impact analysis into its process, which extends security responsibilities to the entire organization. Using PASTA can be an issue due to the training and education required by the key stakeholders.(Nweke and Wolthusen, 2020)

Here's how to apply PASTA to an online shopping system:

(Process for Attack Simulation and Threat Analysis)

Stages	
1- Define objectives	To protect customer data, ensuring secure payment processing, and maintaining system availability.

	Components and boundaries of the system: user interfaces, databases, and third-party integrations and web servers. Compliance requirements: industry standards, and applicable regulations that may impact the security posture.
2- Define the technical scope	Including the web application, backend database, user authentication, payment processing, and third-party integrations like shipping services.
3- Application Decomposition	Components and interactions, such as user registration, login, product catalog, shopping cart, user authentication, payment processing, shipping services and order fulfill.
4- Threat Analysis	Including cybercriminals, malicious insiders, disgruntled employees, unauthorized access and nation-state actors. Attack vectors such as SQL injection, cross-site scripting, credential theft or social engineering.
5- Vulnerability analysis	Such as code reviews, penetration testing, vulnerability scanning, unpatched software, insecure configurations, or weak authentication mechanisms. Use vulnerability scanners, manual testing, and code reviews to identify potential weaknesses.
6- Attack modelling simulation	Data breaches, payment fraud, or denial-of-service attacks
7- Risk and countermeasure analysis	Such as stronger authentication mechanisms, encryption, input validation, and monitoring/logging. Continuously update and improve the system's security posture based on the findings from these simulations and analyses. Also, secure coding practices, and regularly patching software components.

In summary, as E-Commerce initiatives grow in popularity worldwide, it reflects their compelling advantages, such as improved government performance, lowered costs, increased flexibility, a broader scope of services, and enhanced transparency. (Kabango and Asa, no date). Also, applying threat modeling techniques is essential for several reasons, as they help organizations proactively identify, assess, and address potential security risks within their systems and applications. Moreover, adopting the STRIDE methodology can play a pivotal role in strengthening your organization's security posture and protecting your valuable assets. It can also build trust among customers, partners, and stakeholders. Additionally, by applying the PASTA methodology to an online shopping system, you can systematically identify, analyze, and address potential security risks. This results in a

more secure and resilient application. Lastly, UML, as a visual representation, provides a ready-to-use, formal language for developing and exchanging models.(Hurme, no date)

References:

Hurme, J. (no date) ‘THE BENEFITS OF USING UML- MODELING TOOLS IN EVALUATION AND TESTING OF ETM SOFTWARE’.

Kabango, C.M. and Asa, A.R. (no date) ‘Factors influencing e-commerce development: Implications for the developing countries’.

Krishnan, S. (no date) ‘A Hybrid Approach to Threat Modelling’.

Nweke, L. and Wolthusen, S. (2020) ‘A Review of Asset-Centric Threat Modelling Approaches’, *International Journal of Advanced Computer Science and Applications*, 11, pp. 1–6. Available at: https://doi.org/10.14569/IJACSA.2020.0110201.

Shoval, P., Yampolsky, A. and Last, M. (no date) ‘Class Diagrams and Use Cases - Experimental Examination of the Preferred Order of Modeling’.

SmartDraw - Create Flowcharts, Floor Plans, and Other Diagrams on Any Device (no date). Available at: https://www.smartdraw.com/?id=104607&gclid=CjwKCAjw_YShBhAiEiwAMomsENasPM_qoK2_pxqYAV1JIGDvo2hpWoG3zvreqaW_-xngUTJi0cl9VxoCLhYQAvD_BwE (Accessed: 27 March 2023).