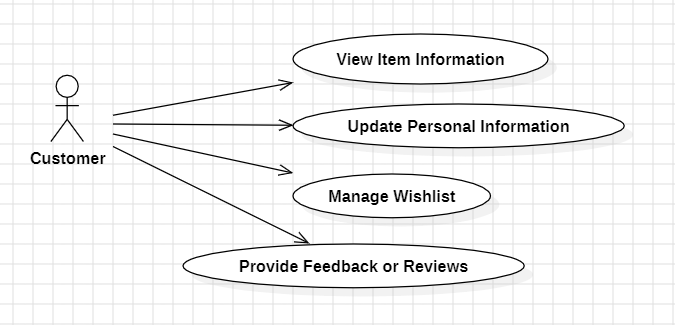
ascbascaUse cases:



1. View item Information:

Use case:

The customer can browse through the available items in the store and view detailed information about each item, including name, price, description, and availability.

Misuse case:

An attacker gains unauthorized access to the customer's browsing history or viewed items, leading to targeted advertising or phishing attempts based on the customer's interests.

|  |  |
| --- | --- |
| Misuse Case ID |  |
| Misuse Case Name | Exploit browsing history for targeted attacks |
| Description | The attacker gains access to the customer's browsing history within the POS software to target the customer with personalized phishing attempts or advertising. |
| Preconditions | The attacker has unauthorized access to the customer's browsing history. |
| Postconditions | The attacker successfully executes targeted attacks against the customer. |
| Normal Flow | 1. The attacker gains unauthorized access to the customer's browsing history data. 2. The attacker analyzes the browsing history to identify the customer's interests and preferences. 3. The attacker crafts phishing emails or targeted advertisements based on the customer's browsing history. |
| Mitigation | 1. Implement encryption and access controls to protect customer browsing history data. 2. Regularly audit access to browsing history data to detect unauthorized access attempts. 3. Train customers to recognize phishing attempts and encourage them to report suspicious emails or advertisements. |

1. Update Personal Information:

Use case:

The customer can update their personal information stored in the system, such as contact details, shipping address, or preferred payment methods.

Misuse case:

A hacker compromises the POS system and alters the customer's personal information, such as shipping address or contact details, resulting in misdirected shipments or identity theft.

|  |  |
| --- | --- |
| Misuse Case ID |  |
| Misuse Case Name | Manipulate customer's personal information |
| Description | The attacker gains unauthorized access to the customer's personal information |
| Preconditions | The attacker has unauthorized access to the customer's personal information. |
| Postconditions | The attacker successfully modifies the customer's personal information. |
| Normal Flow | 1. The attacker gains unauthorized access to the customer's account within the POS software. 2. The attacker modifies the customer's personal information, such as contact details or shipping address. 3. The attacker saves the changes, potentially causing confusion or disruption to the customer's transactions. |
| Mitigation | 1. Implement strong authentication mechanisms, such as multi-factor authentication, to protect customer accounts from unauthorized access. 2. Encrypt sensitive customer data stored within the POS software to prevent unauthorized modification. 3. Monitor account activity for suspicious behavior, such as multiple failed login attempts or unusual changes to account information. |

A diagram of a login information

Description automatically generated

1. Create and Manage Wishlists:

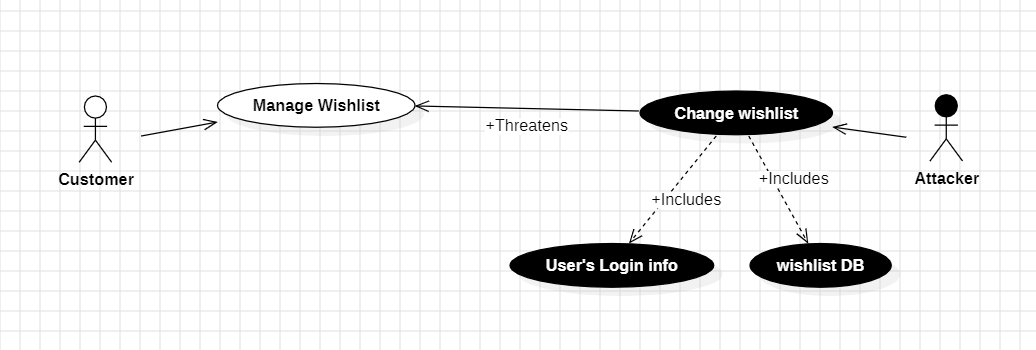
Use case:

The customer can create and manage wishlists within the POS software, allowing them to save items for future purchase or reference.

Misuse case:

An attacker gains access to the customer's wishlist and uses it to identify valuable or desired items for targeted theft or fraudulent transactions.

|  |  |
| --- | --- |
| Misuse Case ID |  |
| Misuse Case Name | Manipulate customer's wishlist for targeted attacks |
| Description | The attacker gains unauthorized access to the customer's wishlist within the POS software and manipulates it for malicious purposes. |
| Preconditions | The attacker has unauthorized access to the customer's wishlist data. |
| Postconditions | The attacker successfully manipulates the customer's wishlist. |
| Normal Flow | 1. The attacker gains unauthorized access to the customer's wishlist data within the POS software. 2. The attacker modifies the customer's wishlist, adding or removing items to deceive or exploit the customer. 3. The attacker saves the changes, potentially leading to the customer making unintended purchases or falling victim to targeted attacks. |
| Mitigation | 1. Implement strong authentication mechanisms and access controls to protect customer wishlist data from unauthorized access. 2. Encrypt sensitive customer data stored within the POS software, including wishlist information, to prevent unauthorized modification. 3. Monitor wishlist activity for suspicious behavior, such as rapid changes or unusual item additions, indicating potential manipulation. |



1. Provide Feedback or Reviews:

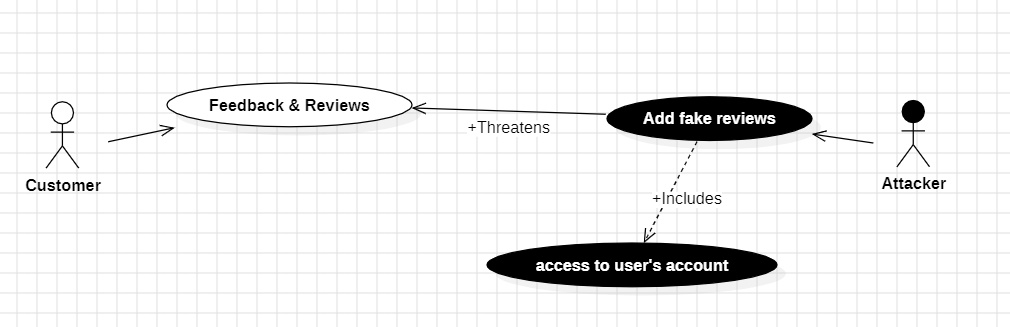
Use case:

The customer can submit feedback or reviews for items they have purchased, helping other customers make informed decisions and providing valuable insights to the store.

Misuse case:

Fake reviews submitted by the attacker manipulate the customer's perception of products or services, leading to misguided purchasing decisions or dissatisfaction.

|  |  |
| --- | --- |
| Misuse Case ID |  |
| Misuse Case Name | Fabricate feedback or reviews for malicious purposes |
| Description | The attacker gains access to the customer's feedback or review submissions within the POS software and fabricates them for malicious purposes. |
| Preconditions | The attacker has unauthorized access to the customer's feedback or review data. |
| Postconditions | The attacker successfully fabricates feedback or reviews for malicious purposes. |
| Normal Flow | 1. The attacker gains unauthorized access to the customer's feedback or review data within the POS software. 2. The attacker fabricates feedback or reviews, posting false or misleading information to manipulate other customers' perceptions or damage the store's reputation. 3. The attacker submits the fabricated feedback or reviews, potentially influencing purchasing decisions or causing reputational harm to the store. |
| Mitigation | 1. Implement stringent access controls and encryption to protect customer feedback and review data from unauthorized access. 2. Regularly audit feedback and review submissions to detect and prevent unauthorized modifications or fabrications. |



Customer Requirements:

1. Encrypt customer’s personal information
2. Secure authentication
3. Strict access control
4. Logging user’s activities