**Question 1**

Misuse cases Customers

Create Account

* Steal credit card info

Login/Authenticate

* Brute force
* Social engineering

Searches Products

* False product pricing
* False seller details
* Product not found although I should have been queried by the database
* Unauthorized personnel (customer) listing promotions for products

Order Products

* Address information stolen
* Address is a P.O box location
* Item received isn’t what customer thought we was ordering

Review Products

* Customer has not bought the book reviewing the book

Bids on Auction

* Unauthorized person(customer) listing products for auction
* Customer data being leaked or stolen by 3rd party company ebid.com
* The non-highest bidder wins the auction and the product

Misuse cases Staff

Login

* Brute force attacks
* Social engineering
* Shoulder surfing

Update “current promo” page

* Unauthorized staff updating the page
* Authorized staff updating page with false information

List Products for auction

* Unauthorized staff listing products for auction
* Listing auction item with wrong starting price

**Question 2**

Assist the project team in deriving the security requirement that needs to be incorporated into the software development project.

|  |  |  |
| --- | --- | --- |
| S/N | Software Requirement | Security Requirement |
| 1 | Customers must register with the sBooks portal before they are allowed to purchase ebooks with their credit cards | Identity management – Authentication. Users have to have an account created and be logged in before they can buy an ebook |
| 2 | eBooks are copyrighted, hence, customers should not be able to reproduce or distribute them in an unauthorized manner | Originator Controlled – Confidentiality, integrity. Users should not be able to download the online ebook so that it cannot be easily distributed. |
| 3 | P.O Box addresses will not be accepted as a valid shipping location | Data Input Validation - Integrity  Valid shipping address/location – Availability, confidentiality |
| 4 | Customers must be allowed to search for eBooks | Data Input Validation – Integrity, Availability  Errors should have general message - Error management |
| 5 | Customers can provide ratings & reviews only about the products they have purchased | Data input validation (only purchased products) - Authorization |
| 6 | Customers should be allowed to view an excerpt from the ebook | Customer should be restricted to only view the excerpt from the book.  Content of excerpt must have integrity and confidentiality |
| 7 | Customers can purchase the entire book or just selected chapters | Customers must receive what they actually bought. No cases where they buy the whole book but receive selected chapters only (integrity). |
| 8 | Only specific staff from the Marketing department of sBooks should be able to update the “current promotions” page and list products for auction | Role-Based Access Control (least privilege) - Confidentiality, integrity. Only staff accounts that have been enabled should have access to the “current promotions” page. |
| 9 | Customers for sBooks need not create a new account on eBid.com | Customer details must be securely and accurately transferred from sbooks database to ebid. |
| 10 | The highest bidder at the end of the auction period will be the winner of the product | Identity management – Authentication. |
| 11 | The portal will be developed in-house | Physical protection (access cards, security personnel, equipment tagging) - Confidentiality |