**TASK 1: Smith and Co Second-Hand Bookshop**

1. **Normalized table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Unnormalized | UNF Level | 1NF | 2NF | 3NF |
| Book ID | 1 | Book ID(pk)  Book Name  Author ID  Author Name | Book ID(pk)  Book Name  Author ID  Author Name | Book ID(pk)  Book Name  Author ID |
| Book Name | 1 |
| Author ID | 1 |
| Author Name | 1 |  |
| Price | 2 |  |  | Book ID(pk)  Book Name |
| Publisher | 2 |  |  |
| Book Condition | 2 | Author ID(fk)  Price  Publisher  Book Condition  Purchase Date  Sale Date  Customer ID | Author ID(fk)  Price  Publisher  Book Condition  Purchase Date |  |
| Purchase Date | 2 | Author ID (fk)  Book Condition  Price |
| Sale Date | 2 |
| Customer ID | 2 |
| Sale Price | 2 | Publisher  Book Condition(pk) |

1. Short Report (500words)

Database attacks are becoming more and more common, as malicious actors seek to exploit vulnerabilities in online databases (Brett, 2020). The Smith and Co Second-Hand Bookshop database could potentially be targeted for various reasons. It could contain valuable customer information, including email addresses, credit card numbers, and other personal data. Additionally, the database may contain records of sales, which could be used to identify trends in customer behaviour, or to track the movements of specific customers (Brett, 2020). This makes the Smith and Co Second-Hand Bookshop database an attractive target for malicious actors.

The type of attack that could be used against the Smith and Co Second-Hand Bookshop database includes SQL injection (Ferrari, 2020). This is a type of attack where an attacker attempts to gain access to the database by entering malicious code into a web form that is then executed by the database (Ferrari, 2020). An attacker could use this technique to gain access to the book records, customer information, and sale data stored in the database.

Another type of attack that could be used against the Smith and Co Second-Hand Bookshop database is a Distributed Denial of Service (DDoS) attack (Ferrari, 2020). This type of attack involves flooding the database server with large amounts of traffic, which can cause the server to become overloaded and become unavailable. This type of attack could be used to prevent legitimate users from accessing the database, or to disrupt the normal operation of the database.

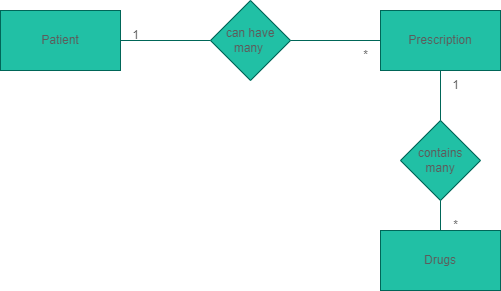
The type of data that could be extracted from the Smith and Co Second-Hand Bookshop database in an attack depends on the type of attack used. For example, if the attack is an SQL injection, then the attacker could extract customer information such as names, email addresses, and credit card numbers. If the attack is a DDoS attack, then the attacker could extract data related to the sale of books, such as when a book was purchased, who purchased it, and how much it was sold for.

In conclusion, the Smith and Co Second-Hand Bookshop database is vulnerable to various types of attacks, such as SQL injection and DDoS attacks. The type of data that could be extracted in an attack depends on the type of attack used, but could include customer information, sale data, and book records. It is important to ensure that the database is properly secured to prevent malicious actors from gaining access to the data.

**TASK 2: St. John’s Hospital**

Entity-Relationship Diagram (ERD)

**Assumption:** The patient can have multiple prescriptions and the prescription can have multiple drugs.



Data dictionary

**Patient Table**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Attribute Name | Data Type | Length | Required | Validation | Format | PK | FK | Comments |
| Patient\_ID | INTEGER | N/A | Y |  | Y |  |  | Unique identifier for each patient |
| Name | VARCHAR | 256 | Y |  |  |  |  |  |
| Address | VARCHAR | 256 | Y |  |  |  |  |  |
| Date\_of\_Birth | DATE | N/A | Y |  | DD-MON-YYYY |  |  |  |
| ID\_Number | INTEGER | N/A | Y |  |  |  |  |  |
| Telephone\_Number | VARCHAR | 256 | Y |  |  |  |  |  |

**Prescription Table**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Attribute Name | Data Type | Length | Required | Validation | Format | PK | FK | Comments |
| Prescription\_Number | INTEGER | N/A | Y |  | Y |  |  | Unique identifier for each patient |
| Date\_Prescribed | DATE | N/A | Y |  | DD-MON-YYYY |  |  |  |
| Doctor | VARCHAR | 256 | Y |  |  |  |  |  |
| Pharmacist | VARCHAR | 256 | Y |  |  |  |  |  |
| Issue\_Date | DATE | N/A | Y |  | DD-MON-YYYY |  |  |  |
| Patient\_ID | INTEGER | N/A | Y |  | Y |  |  | Foreign key related to patient table |

**Drugs Table:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Attribute Name | Data Type | Length | Required | Validation | Format | PK | FK | Comments |
| Drug\_Name | VARCHAR | 256 | Y |  |  |  |  | Unique identifier for each patient |
| Item\_Cost | INTEGER | N/A | Y |  |  |  |  |  |
| Quantity\_Prescribed | INTEGER | N/A | Y |  |  |  |  |  |
| Quantity\_Issued | INTEGER | N/A | Y |  |  |  |  |  |
| Prescription\_Number | INTEGER | N/A | Y |  | Y |  |  | Foreign key related to prescription table |