2022 Cyber Group - 2

2022BCY0002 - Dania Eram, 2022BCY0013 – Raghavendra, 2022BCY0024 – Gayatri, 2022BCY0035 – Suraj, 2022BCY0046 – Sanjay, 2022BCY0057 - Shresth

Security Goals For Books' Data

Confidentiality: *This means that only authorized users should be able to access book data. This includes protecting data from unauthorized access, both internal and external.*

- ***Control access to book data:*** *Implement access controls to restrict who can view, edit, or delete book data. This may involve using passwords, roles, and permissions.*
- ***Encrypt book data:*** *Encrypt book data at rest and in transit to protect it from unauthorized access if it is intercepted.*
- ***Pseudonymize or anonymize sensitive data:*** *If possible, pseudonymize or anonymize sensitive data, such as author information or personal details mentioned in the book, to reduce the risk of privacy breaches.*

Integrity: *This means that book data should be accurate and complete, and that it should not be tampered with.*

- ***Implement data integrity checks:*** *Use data integrity checks to verify that book data has not been modified or corrupted. This could involve using checksums, hash functions, or digital signatures.*
- ***Log changes to book data:*** *Keep a log of all changes made to book data, so that you can track who made the changes and when.*
- ***Use intrusion detection and prevention systems:*** *Implement intrusion detection and prevention systems to monitor and prevent unauthorized access to or modification of book data.*

Availability: *This means that authorized users should be able to access book data when they need it.*

- ***Back up book data regularly:*** *Back up book data regularly to ensure that it is available in the event of a disaster.*

- ***Use redundant systems:*** *Use redundant systems to ensure that book data is available even if one system fails.*
- ***Implement disaster recovery plans:*** *Have a disaster recovery plan in place to restore book data and systems in the event of a disaster.*

Non-repudiation: *This means that it should be possible to prove who created or modified book data.*

- ***Use digital signatures:*** *Use digital signatures to ensure that book data cannot be repudiated.*
- ***Maintain audit logs:*** *Keep audit logs of all actions taken on book data, so that you can track who did what and when.*

Authentication:

- ***Ensures only authorized users can access book data:*** *This involves verifying the identity of users through strong passwords, multi-factor authentication, or other secure methods.*
- ***Limits unauthorized access:*** *By verifying identity, unauthorized attempts to access book data can be detected and prevented.*
- ***Supports accountability:*** *By logging who accessed the data, accountability for actions is established.*

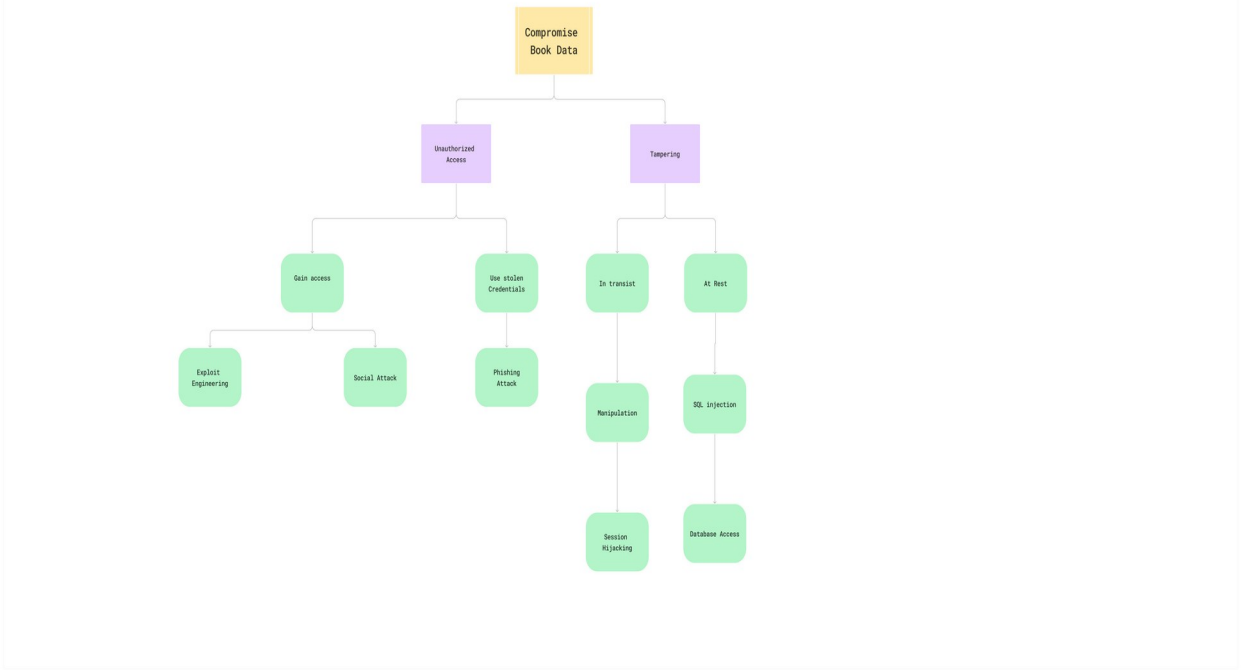
Authorization:

- ***Defines user permissions:*** *Sets clear rules for what each user can do with book data (view, edit, delete, etc.).*
- ***Protects sensitive information:*** *Restricts access to sensitive information based on user roles and needs.*
- ***Minimizes risk of data breaches:*** *By limiting access, the potential for accidental or malicious misuse is reduced.*

Auditing:

- ***Tracks user activity:*** *Logs all actions taken on book data, including who accessed it, what they did, and when.*
- ***Enables forensic analysis:*** *Allows for investigation of suspicious activity or potential security incidents.*
- ***Supports compliance:*** *Helps demonstrate adherence to data security regulations and policies.*

Attack Tree:


Compromise Book Data
Unauthorized Access
Tampering
Gain access
Use stolen Credentials
In transist
At Rest
Exploit Engineering
Social Attack
Phishing Attack
Manipulation
SQL injection
Session Hijacking
Database Access