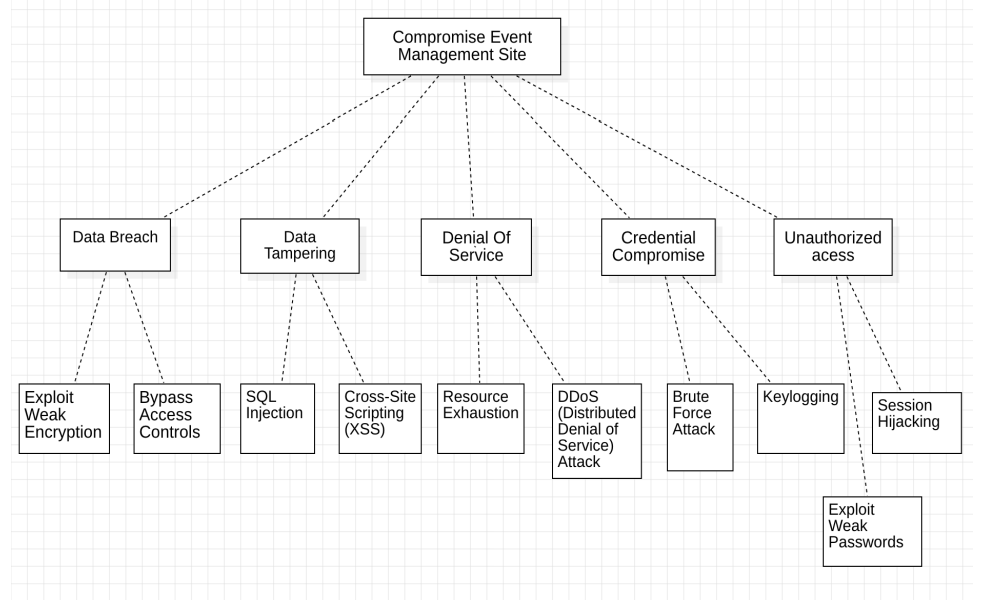
Attack Tree

2022BCY0034

K.Sai Sidhartha



# Security Objectives of Our Project:

## Secrecy:

Description: Secrecy safeguards sensitive information from unauthorized disclosure.

Example Measures: Encryption, access controls, data classification, and implementation of secure communication protocols.

## Data Trustworthiness:

Description: Ensuring the accuracy and unaltered state of data, maintaining trust throughout its lifecycle.

Example Measures: Implementation of hash functions, digital signatures, version control, and adherence to secure coding practices.

## Accessibility:

Description: Guaranteeing that information and resources are accessible and available as needed.

Example Measures: Incorporating redundancy, regular backups, disaster recovery planning, and deploying distributed systems.

## User Verification:

Description: Confirming the identity of users or systems prior to granting access to resources.

Example Measures: Passwords, multi-factor authentication, biometrics, and smart card implementation.

## Access Control:

Description: Determining the permissions and resources accessible to an authenticated entity.

Example Measures: Utilizing role-based access control (RBAC), access control lists (ACLs), and adhering to the principle of least privilege.

## Undeniable Accountability:

Description: Ensuring that a party cannot disown the authenticity of their actions or transmitted data.

Example Measures: Leveraging digital signatures, maintaining audit trails, and employing tamper-evident logs.

## Adaptability and Recovery:

Description: Focusing on the ability to adapt and recover from security incidents or disruptions.

Example Measures: Formulating incident response plans, conducting penetration testing, and establishing continuous monitoring processes.