Classify the following threats using the STRIDE (Spoofing of user identity, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) categories. Explain why did you choose each category.

1. An attacker stands up a malicious web server to intercept and respond to requests.

2. An attacker deletes or modifies a system’s audit logs.

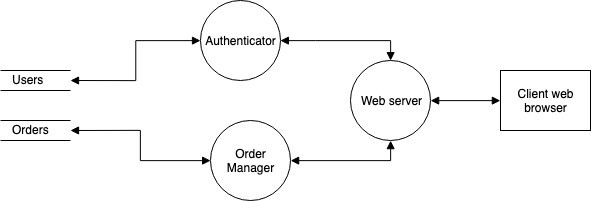
3. An attacker writes data to a file that is read by a root-level process.

4. An adversary accesses user credentials for a social media website, which are stored as plaintext on a web server.

Consider the Data-Flow Diagram (DFD) for an Online Book Ordering System with the following description:

The book ordering system is a web-based application to order books. It is composed of three processes: An authenticator to validate user credentials, an order manager to process books orders and payment information, and a web server to host web-pages. The system uses two databases: The Users database contains user authentication credentials and the Orders database contains information about user book orders (including payment information). Database queries are carried out via standard ODBC connectors. The system is accessed via a user’s web browser over HTTP. Session information is managed via HTTP cookies.

Identify and label the trust boundaries in this DFD:



Assume that system designers want to prevent unintended disclosure of user credentials. Using the Data-Flow Diagram as a guide, analyze one data flow, discuss a possible threat against this objective and classify that threat using STRIDE. State any assumptions that you make.