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.

Spoofing – An Attacker can steal the information of a user who is going to log in the server in order to impersonate the user.

Tempering – An Attacker can temper the packet that contains the payment for goods in order to modify the cost down.

Dos – An attacker can not provide service to the requesting user who want to use a service on the server by dropping all packets coming to a specific site(user) from the server. Therefore An attacker compromises Availability for the web server.

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

Repudiation – The attacker can deny that it has received and viewed the user's request mail from the server, but has not received the user's request by deleting the related log records.

Information disclosure - The attacker can view and steal information about the service used by the user, including specific user information of the server.

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

Denial of service - Attacker corrupts data by accessing files fatally to system processes with the aim of destroying the availaablity of certain services.

Elevation of privilege - The attacker records malicious data in a file accessed with root privileges, and when a user executes a process with root privileges, it attempts malicious actions that can be executed with high privileges.

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

Temper - The attacker accesses the web server and manipulates other users' information.

Information disclosure - The server did not hide the user's confidential information by storing it in plaintext. So the attacker can view personal data.

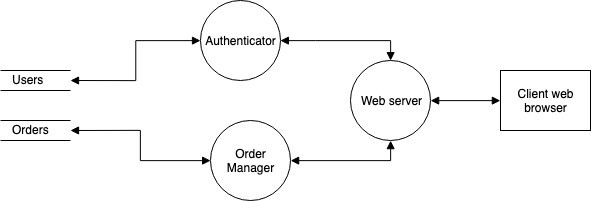
Consider the Data-Flow Diagram (DFD) for an Online Book Ordering System with the following description:

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:

Machine Trust boundary

Internet boundary



Machine Trust boundary

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.

Assumptions

1. The web server is a server that handles client requests, and this webserver is connected to an external MS SQL servers through DSMS.

2. The Authenticator is a process running on MS SQL Server and can be managed by connecting to DB using ODBC connector.

3. The Order Manager is a process running on MS SQL Server and manages the DB by connecting to the DB using the ODBC connector.

|  |  |  |
| --- | --- | --- |
| ID | Category | Threat Description |
| 01 | Spoofing | Client web browser may be spoofed by an attacker and this may lead to unauthorized access to Web Server. |
| 02 | Tampering | The web server 'Web Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input. |
| 03 | Spoofing | Web Server may be spoofed by an attacker and this may lead to information disclosure by Client web browser. |
| 04 | Repudiation | Clients can repudiate the actions they have performed. |
| 05 | Information Disclosure | Data flowing across HTTP may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. |
| 06 | DoS | Web Server runs slowly because the client sends the malicious code that try to occupy the server’s resource. |
| 07 | Elevation Of Privilege | Client web browser may be able to remotely execute code for Web Server. |