- There exists a 'Host Web Client', which interacts with:  
         - A 'Remote Web Server' via HTTP request/response cycle  
         - An external 'User' via a generic command/service cycle  
         - A 'File System' using a read/write cycle

For the given prompt, perform threat modeling. Which is: build a data flow diagram, and identify threats using STRIDE approach. Proposing mitigations for the identified threats is optional. Verification of the threats and verification of the mitigations is not a requirement.

Perform the threat modeling from the perspective of a system admin for the organization that controls the 'Host Web Client', which would be a website hosted by the company. The file system can be assumed to belong to the company. The threat model should be performed from a company perspective and not an end-user perspective.

Service

Command

Request

Response

Read

write

File System

Remote web server

User

Host Web Client

|  |  |  |
| --- | --- | --- |
| Spoofing | * Threat: Unauthorized users or malicious entities could impersonate legitimate users or servers or gain access to the ‘Host Web Client’, ‘Remote Web Server,’ or ‘File System.’ | * Mitigiation: Implement strong authentication and access control mechanisms, such as MFA and HTTPS/TLS for communication |
| Tampering | Threat: Malicious users may alter data in transit between the ‘Host Web Client,’ or they may modify data in the ‘File System’ | Mitigation: Use data integrity checks (e.g. hashing) to ensure data integrity during transmission. Apply file system permissions to restrict unauthorized access and modifications |
| Repudiation | Threat: Users might deny their actions within system, leading to disputes and accountability issues | Mitigation: implement comprehensive logging and auditing mechanisms to record user activities and interactions with the ‘Host Web Client’, ‘Remote Web Server,’ and the ‘File System.’ Ensure logs cannot be easily tampered with. |
| Information Disclosure | Threat: Sensitive data may be exposed during communication between the ‘Host Web Client’ and the ‘Remote Web Server’ or through unauthorized access to the ‘File system’ | Mitigation: Encrypt sensitive data in transit (using HTTPS/TLS) and at rest (using strong encryption mechanisms). Implement access controls to limit access to sensitive data |
| Denial of service | Threat: Malicious users or automated attacks may overload the ‘Host Web Client’ or the Remote Web Server, causing service disruptions | Mitigations: Implement rate limiting, traffic, traffic monitoring, and resource allocation mechanism to mitigate denial-of-service attacks. Use load balancers for distributing traffic |
| Elevation of Privilege | Threat: Unauthorized users or malicious actors may escalate their privileges within the ‘Host Web Client’ or gain unauthorized access to the ‘File System’ | Mitigation: Enforce the principle of least privilege, ensuring users have only the minimum necessary permissions. Regularly update and patch the ‘Host Web Client’ and ‘Remote Web Sever’ to address security vulnerabilities |

1. Perform the threat modeling from the perspective of a system admin for the organization that controls the 'Host Web Client', which would be a website hosted by the company. The file system can be assumed to belong to the company. The threat model should be performed from a company perspective and not an end-user perspective.
2. Threat Actor Analysis
   1. External attackers: These could be hackers or other threats attempting to compromise the Host Web Client, Remote Web Server or gain access to the File system
   2. Insiders: Current or former employees or contractors with the access to the organizations system
3. Asset Identification:
   1. Host Web Client: data/code and user interactions
   2. Remote Web Server: the server hosting application
   3. File System: sensitive data, configuration and back ups
   4. User Data: users interacting with the website
   5. Company Reputation: company brand
4. Threat Identification:
   1. HTTP-Based Threats:
      1. Injection Attacks: may attempt SQL injection, XSS or other attacks against the Host web Client or server
      2. DoS: overwhelm the remote web server with HTTP requests causing disruption
   2. Command/Service-Based Threats:
      1. Unauthorized Access: insiders or external attackers gain access to host web client
      2. Data Exfiltration: use legitimate commands to steal sensitive data from the File system
   3. File System Threats:
      1. Unauthorized Access: Unauthorized users might attempt to gain access to the File System
      2. Data Loss: Accidental deletion or malicious actions
5. Vulnerability Assessment:
   1. Outdated software
   2. Weak Authentication
   3. Input validation
   4. Insider threats
   5. Lack of access controls
6. Risk Assessment
   1. Access the potential impact and likelihood of each threat based on organizations context
   2. Prioritize threats based on their risk levels
7. Risk Mitigation:
   1. Implement security best practices, including regular software patching and updates
   2. Enforcing strong authentication and access controls
   3. Monitor web traffic and server logs
   4. Implement backups and recovery procedures