Threat modelling

Spoofing (S)

1. **Threat: Spoofing (Admin Login)**
    - Risk: High
    - Impact: Unauthorized access to admin privileges.
    - Possibility: Moderate

Tampering (T)

1. **Threat: Tampering (Material Management)**
    - Risk: Moderate
    - Impact: Unauthorized modification or deletion of training materials.
    - Possibility: Moderate

Elevation of Privilege (E)

1. **Threat: Elevation of Privilege (Coach Access Control)**
    - Risk: High
    - Impact: Unauthorized individuals gaining administrator-level access.
    - Possibility: Low to Moderate

Information Disclosure (I)

1. **Threat: Data Exposure (Content Customization)**
    - Risk: Moderate
    - Impact: Sensitive training materials exposed to unauthorized users.
    - Possibility: Moderate
2. **Threat: SQL Injection (Data Validation)**
    - Risk: High
    - Impact: Attackers manipulating input fields to execute malicious SQL queries.
    - Possibility: Moderate to High
3. **Threat: Cross-Site Scripting (XSS) (Data Validation)**
    - Risk: High
    - Impact: Attackers injecting malicious scripts into web pages viewed by other users.
    - Possibility: Moderate
4. **Threat: Inadequate Data Encryption (Data Encryption)**
    - Risk: High
    - Impact: Sensitive data transmitted or stored without proper encryption.
    - Possibility: Moderate

Denial of Service (D)

1. **Threat: Lack of Rate Limiting (Authentication and Authorization)**
    - Risk: Moderate
    - Impact: Attackers performing brute force or denial-of-service attacks.
    - Possibility: Moderate

Repudiation (R)

1. **Threat: Lack of Audit Trails (Logging and Monitoring)**
    - Risk: Moderate
    - Impact: Inability to track and investigate security incidents.
    - Possibility: Moderate

Escalation of Privilege (E)

1. **Threat: Insecure Session Management (Session Management)**
    - Risk: High
    - Impact: Weak session management leading to session fixation, hijacking, or unauthorized access.
    - Possibility: Moderate to High
2. **Threat: Insufficient Input Validation (Data Validation)**
    - Risk: Moderate
    - Impact: Lack of input validation allowing attackers to submit malicious data.
    - Possibility: Moderate
3. **Threat: Lack of Security Patch Management (Security Updates)**

- Risk: High
- Impact: Failing to apply security patches leaving the system vulnerable to known vulnerabilities.
- Possibility: Moderate to High

4. **Threat: Insecure File Uploads (Secure File Upload)**
    - Risk: High
    - Impact: Malicious file uploads leading to code execution, data breaches, or malware distribution.
    - Possibility: Moderate
5. **Threat: Insider Threats (User Training)**
    - Risk: Moderate
    - Impact: Malicious or negligent actions by administrators or coaches.
    - Possibility: Low to Moderate
6. **Threat: Lack of Two-Factor Authentication (Authentication and Authorization)**
    - Risk: Moderate
    - Impact: Compromised credentials leading to unauthorized access.
    - Possibility: Moderate
7. **Threat: Cross-Site Request Forgery (CSRF) (Authentication and Authorization)**
    - Risk: Moderate
    - Impact: Attackers tricking administrators into performing unwanted actions on the system.
    - Possibility: Low to Moderate
8. **Threat: Inadequate Backup and Recovery (Backup and Disaster Recovery)**
    - Risk: High
    - Impact: Data loss or system compromise without recovery options.
    - Possibility: Moderate to High