VIA University College
Software Technology Engineering

Threat Model - Learnify

Semester Project - Group 3

3rd Semester

Last Update: December 18, 2025
Version: 1.6

1 System Description

Learnify is a distributed e-learning platform that is designed to provide users with access to a wide range of educational resources and courses. The system consists of multiple components, including a database, data server, logic server, client web server, and more. The system is built for people seeking education, sharing knowledge, and administrators managing the platform.

2 Security Objectives

The security goals for this system based on the CIA triad.

- **Confidentiality:** Protect user passwords and personal data from unauthorized disclosure.
- **Integrity:** Ensuring that data can not be altered or tampered with by unauthorized parties.
- **Availability:** Ensure the system remains accessible during high traffic or denial-of-service attempts.
- **Accountability:** Actions must be uniquely traceable to a specific entity.
- **Authenticity:** Verify that data inputs and users are genuine.

Accountability and Authenticity can also be considered subsets of Integrity. (Samonas & Coss, 2014)

3 Adversary Model

Who the attackers are and where they are attacking from based on EIOO.

3.1 Who is attacking?

- **External:** Hackers, Competitors
- **Internal:** Administrators, Teachers, Project Members

3.2 Where is the attack occurring?

- **Network:** Interception of traffic, man-in-the-middle attacks
- **Online:** Attacks on the database, data server, logic server, or client web server
- **Offline:** Physical access to servers, social engineering attacks, stealing data saved on local machines (e.g., JWT tokens, cached passwords)

4 Threat Categorization

Potential threats based on the attacker's goal based on STRIDE.

Category	Definition	Potential Threats to Learnify
Spoofing Identity	Impersonating another person or system.	Attacker uses stolen credentials to log in as another user (most importantly as an administrator or teacher)
Tampering	Modifying data without detection.	Modifying database records directly or through the dataserver
Repudiation	Denying having performed an action.	A teacher claims they did not submit a draft, or edit course content. Admin claims they did not alter the user data (roles)
Information Disclosure	Accessing restricted data.	Leaking user personal information, course content that should be restricted
Denial of Service	Denying access to valid users.	Flooding the server with requests to crash it, e.g. bug in the client app that could cause a recursive call to the rest api or intentional attack
Elevation of Privilege	Gaining higher rights than authorized.	A normal user exploits a bug to gain administrator privileges.

5 Attack Surfaces and Vectors

The means and entry points used by attackers.

5.1 Attack Surfaces

- **Network:** Open ports, Wi-Fi, Firewalls, Intranet, VPNs
- **Software:** API endpoints, Database interfaces, IDEs and browsers
- **Human:** Social engineering, Phishing, Human error, Insider threats, Physical access, Lost devices

5.2 Attack Means

- **Passive Attacks:**
  - *Eavesdropping:* Monitoring transmissions for sensitive data.
  - *Traffic Analysis:* Observing patterns/frequency of communication.
  - *Shoulder Surfing:* Observing user input directly (e.g., passwords).
  - *Dumpster Diving:* Searching through physical trash for sensitive information.
  - *Wiretapping:* Intercepting communication lines to capture data. (cables, etc.)
- **Active Attacks:**
  - *Masquerade:* Pretending to be a different entity.
  - *Replay:* Resending old messages to produce unauthorized effects.
  - *Modification:* Altering portions of a legitimate message.
  - *Denial of Service:* Preventing normal use of communications facilities.
  - *Release of Information:* Exposing sensitive data to unauthorized parties.
  - *Injection Attacks:* Inserting malicious code into input fields (e.g., SQL Injection, XSS).

6 Vulnerability Analysis

Potential failures based on their source:

- **Threat Model:** Are there threats we ignored, underestimated, misunderstood or intentionally left out? e.g., insider threats, advanced persistent threats.
- **Assumption:** Are there invalid assumptions about the system? e.g., assuming all users are trustworthy, that network is secure, or that software is bug-free.
- **Policy:** Does the policy allow unsafe actions? e.g., allowing weak passwords, not enforcing safe communication or data storage practices.
- **Mechanism:** Can the security mechanism be bypassed? e.g., software bug in the login code, misconfigured firewall, or unpatched vulnerabilities.

7 Risk Assessment & Mitigation

Threat ID	Threat Description	Likelihood	Impact	Risk Level	Mitigation Strategy
T-01	SQL Injection into an input field	High	High	**Critical**	Implement Input Validation and Parameterized Queries.
T-02	Admin Password Phishing	Low	High	**Medium**	Implement MFA for all admin accounts.
T-03	DDoS Attack	Low	Medium	**Low**	Configure Firewall. Tools like Fail2ban or Cloudflare.
T-04	Insider Threat - Data Leakage by Admin	Low	High	**Medium**	Monitor user activities, rotate credentials, and enforce secure storage policies.
T-05	Man-in-the-Middle Attack on Data Transmission	Medium	High	**High**	Use TLS/SSL for all communications. Enforce HSTS.
T-06	Cross-Site Scripting (XSS)	Medium	Medium	**Medium**	Implement Content Security Policy (CSP) and sanitize user inputs.

Threat ID	Threat Description	Likelihood	Impact	Risk Level	Mitigation Strategy
T-07	Weak Passwords	High	Medium	**High**	Enforce strong password policies and implement password strength meters. Using proper password storage and verification algorithms.
T-08	Unpatched Software Vulnerabilities	High	High	**Critical**	Regularly update and patch all software components. Use automated vulnerability scanning tools. Use auto-update tools for unattended patching. (0-day protection tools and similar)
T-09	Physical Theft or access to devices	Low	High	**Medium**	Encrypt sensitive data on devices. Educate admins on physical security.

The risk level is determined by the following table:

Likelihood \ Impact	Low	Medium	High
Low	Minimal	Low	Medium
Medium	Low	Medium	High
High	Medium	High	Critical

8 Conclusion

This threat model provides an overview of the potential security threats to Learnify, assesed through various frameworks and methodologies. By identifying these threats and implementing the recommended mitigation strategies, Learnify should be able to enhance its security posture and protect its users' data and privacy effectively. Regular reviews and updates to this threat model are essential to adapt to the evolving threat landscape.

9 Glossary

- CIA Triad: Confidentiality, Integrity, Availability
- EIOO: External/Internal, Online/Offline
- STRIDE: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
- TPM: Threat Model, Assumption, Policy, Mechanism
- MFA: Multi-Factor Authentication

10 References

- Biba, K. J. Integrity Considerations for Secure Computer Systems. Bedford, Massachusetts, The MITRE Corporation, Apr. 1977, apps.dtic.mil/sti/tr/pdf/ADA039324.pdf. Accessed 14 Dec. 2025.
- Samonas, Spyridon, and David Coss. "The Cia Strikes Back: Redefining Confidentiality, Integrity and Availability in Security." 2014.
- "Threat Modeling Process | OWASP." Owasp.org, owasp.org/www-community/Threat_Modeling_Process#stride-threat–mitigation-techniques.