Threat Modeling Using STRIDE for Web Applications

Name: Ammar Yasser Mohamed
Enterprise Security Department - Summer 2025

Date: August 3, 2025

What is STRIDE?

STRIDE is a threat modeling framework developed by Microsoft that helps identify and classify different types of security threats. It breaks down threats into six categories:

- **Spoofing** – Pretending to be someone or something else.
- **Tampering** – Modifying data or system components.
- **Repudiation** – Denying having performed an action.
- **Information Disclosure** – Exposing sensitive data.
- **Denial of Service (DoS)** – Disrupting service availability.
- **Elevation of Privilege** – Gaining unauthorized access rights.

Applying STRIDE to Web Applications

The following table outlines common threats to a typical web application (e.g., e-commerce site), categorized by STRIDE, with examples and mitigations.

Component	**STRIDE Threat**	**Example**	**Mitigation**
User Login Form	Spoofing	Attacker uses stolen credentials	Multi-factor authentication, strong password policy
	Info Disclosure	Credentials sent over HTTP	Enforce HTTPS/TLS
	Repudiation	User denies login action	Secure, timestamped logs
Web Server	Tampering	HTTP headers or request fields modified	Input validation, WAF
	DoS	Flooding server with HTTP requests	Rate limiting, CAPTCHA, load balancing
Application Server	Elevation of Privilege	User modifies cookie to gain admin access	Secure session handling, RBAC
	Tampering	Modify form data to alter order amount	Server-side validation
Database	Info Disclosure	SQL injection reveals user data	Prepared statements, least privilege access
	Tampering	Malicious query alters product prices	Access control, input sanitization
Admin Interface	Spoofing	Attacker logs in as admin with weak password	MFA, strong password enforcement
	Elevation of Privilege	Unauthorized access to admin panel	Role-based access control
Payment API	Info Disclosure	API key leaked or intercepted	Encryption, API gateway, key management
	Repudiation	User claims no payment initiated	Transaction logging with IP and timestamp