Mini Threat Model Project: EVOL (Every View of Life) Website

# Introduction

This report presents a mini threat model for EVOL (Every View of Life), a hypothetical clothing brand’s e-commerce website. The analysis uses both STRIDE and DREAD frameworks to identify, evaluate, and prioritize potential threats to the website’s security, functionality, and reputation.

# STRIDE Threat Modeling

The STRIDE model helps classify potential threats into six categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.

* Spoofing: Fake user accounts, credential stuffing, or stolen admin logins.
* Tampering: Altering product prices in the database or manipulating discount codes.
* Repudiation: Users denying fraudulent transactions without sufficient logging.
* Information Disclosure: Sensitive customer data (addresses, credit cards) leaked.
* Denial of Service: Bots or DDoS attacks making the site unavailable.
* Elevation of Privilege: Hackers escalating from normal user to admin control.

# DREAD Threat Scoring

The DREAD model is used to score the risk level of each threat based on five factors: Damage Potential, Reproducibility, Exploitability, Affected Users, and Discoverability. Each factor is rated on a scale of 1–10, and the average produces the overall DREAD score.

## Threat Analysis Table (STRIDE + DREAD)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Threat | Damage | Reproducibility | Exploitability | Affected Users | Discoverability | DREAD Score | Vulnerabilities | Mitigations |
| Spoofing (Fake Accounts) | 8 | 7 | 7 | 8 | 7 | 7.4 | Weak login security, no MFA | Enable MFA, CAPTCHA, stronger hashing |
| Tampering (Price Manipulation) | 9 | 8 | 6 | 7 | 6 | 7.2 | Weak input validation, DB insecure | Validate inputs, use parameterized queries, WAF |
| Repudiation (Transaction Denial) | 7 | 6 | 6 | 6 | 7 | 6.4 | Poor logging | Implement audit logs, non-repudiation controls |
| Information Disclosure (Data Leak) | 10 | 8 | 7 | 9 | 8 | 8.4 | Unencrypted sensitive data | TLS, database encryption, secure storage |
| Denial of Service (DDoS) | 8 | 8 | 7 | 9 | 7 | 7.8 | No DDoS protection | CDN, WAF, rate limiting |
| Elevation of Privilege (Admin Escalation) | 10 | 7 | 6 | 8 | 6 | 7.4 | Excessive permissions, unpatched software | Principle of least privilege, patch mgmt |

# Risk Prioritization

Based on the DREAD scoring, the following threats require the highest priority:

- Information Disclosure (Data Leak): Highest score (8.4), critical due to potential exposure of sensitive customer data.  
- Denial of Service (DDoS): High score (7.8), as downtime directly impacts sales and reputation.  
- Spoofing & Elevation of Privilege: Both scored 7.4, representing significant account takeover and admin risks.

# CSV Export

A CSV file containing the same threat data (STRIDE categories, DREAD scores, vulnerabilities, and mitigations) has also been generated for potential use in spreadsheets or risk-tracking tools.