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

Introduction

This report looks at possible security problems for **EVOL (Every View of Life)**, a clothing brand's online store. The goal is to spot weaknesses, understand what attackers might do, and figure out which problems should be fixed first.

STRIDE Threat Modeling

The STRIDE model puts threats into six groups:

- **Spoofing**: Fake accounts, stolen logins.
- **Tampering**: Changing product prices or discount codes.
- **Repudiation**: Users denying bad purchases without proof.
- **Information Disclosure**: Private customer data leaked.
- **Denial of Service**: Attackers flooding the site so it crashes.
- **Elevation of Privilege**: Hackers getting admin powers they shouldn't have.

DREAD Threat Scoring

The DREAD model gives each threat a score based on:

- **Damage**: How bad it is.
- **Repeatability**: How easy it is to repeat the attack.
- **Ease of Attack**: How easy it is to pull off.
- **Users Affected**: How many people it impacts.
- **Easy to Find?**: How easy it is for hackers to notice.

Each is scored 1–10. The average is the total score.

Threat Analysis Table (STRIDE + DREAD)

Threat	Damage	Repeatability	Ease of Attack	Users Affected	Easy to Find?	DREAD Score	Weakness	Fix
Spoofing (Fake Accounts)	8	7	7	8	7	7.4	Weak logins, no MFA	Add MFA, CAPTCHA, stronger password rules
Tampering (Price Changes)	9	8	6	7	6	7.2	Weak checks, bad DB security	Check inputs, use safe queries, add WAF
Repudiation (Deny Transactions)	7	6	6	6	7	6.4	No good logging	Add audit logs, keep strong records
Info Disclosure (Data Leak)	10	8	7	9	8	8.4	No encryption on data	Use TLS, encrypt DB, secure storage
Denial of Service (DDoS)	8	8	7	9	7	7.8	No protection	Use CDN, WAF, rate limits
Elevation of Privilege (Admin Hack)	10	7	6	8	6	7.4	Too many permissions, old software	Least privilege, update software

---

What to Fix First

Looking at the scores, the main problems to fix first are:

- **Data leaks (8.4)**: Very serious because customer info could be stolen.

- **DDoS attacks (7.8)**: Would crash the store and stop sales.
- **Fake accounts & Admin hacks (7.4 each)**: Big risks for account theft and full site takeover.