Threat Model Report – Every View of Life (EVOL)

System: EVOL (Every View of Life) – Hypothetical E-Commerce Clothing Website
Methodologies Applied: STRIDE (categorization) + DREAD (scoring and prioritization)

---

1. Introduction

Every View of Life (EVOL) is a clothing brand's online store. The website manages sensitive customer data, user accounts, payments, and shipping records. Because of the financial and reputational risks of compromise, a structured threat model is required. This report uses **STRIDE** to classify threats and **DREAD** to score them for prioritization.

---

2. Assets

* Customer credentials and personal information (emails, addresses, phone numbers).
* Payment and transaction data (through integrated payment gateway).
* Order and shipping records.
* Administrative accounts and privileges.
* Website uptime and availability.

---

3. Attacker Profiles

* **Script Kiddie:** runs automated tools to find common web vulnerabilities (SQL injection, XSS).
* **Credential Abuser:** performs credential stuffing to take over accounts.
* **Fraudster:** exploits checkout or payment systems to steal or misuse goods.
* **Competitor/Disruptor:** launches DDoS during product drops to damage reputation.
* **Insider Threat:** employee with privileged access misusing or exfiltrating sensitive data.

---

4. Threats, STRIDE Mapping, DREAD Scores, and Mitigations

| Threat | STRIDE Category | DREAD Avg | Severity | Vulnerabilities | Recommended Mitigations |
|

| ---------- | ---------- | --------- | -------- | ---------- | ---------- |
SQL Injection	Tampering, Information Disclosure, Elevation of Privilege, DoS	**8.8**	Critical	Unparameterized SQL, dynamic queries, missing input validation	Use parameterized queries, ORM safely, WAF rules, least privilege DB user
Credential Stuffing / Account Takeover	Spoofing, Repudiation, Information Disclosure	**8.6**	Critical	Weak passwords, no MFA, no rate-limiting, reused credentials	Rate limiting, MFA, breached-password checks, CAPTCHA thresholds
Session/Token Theft	Spoofing, Tampering, Information Disclosure	**7.6**	High	Insecure cookies, long-lived tokens, XSS stealing tokens	Secure/HttpOnly cookies, short-lived tokens, rotation/revocation, CSP
DDoS / Availability Attacks	Denial of Service	**7.6**	High	No CDN, no WAF, no rate-limiting on endpoints	CDN + WAF, autoscaling, caching, checkout queuing
Cross-Site Scripting (XSS)	Tampering, Information Disclosure, Spoofing	**7.0**	High	Unsanitized inputs, missing CSP	Output encoding, sanitization, CSP headers
Payment Fraud / Checkout Manipulation	Tampering, Repudiation	**6.2**	High	Client-side pricing, weak promo logic	Server-side pricing, payment tokenization, fraud detection
Insider Data Exfiltration	Information Disclosure, Repudiation	**5.4**	Medium	Excessive admin privileges, poor logging	Least privilege, audit logging, secrets manager, access reviews

---

5. Prioritized Risk Remediation Plan

Immediate (0–2 weeks)

1. Fix SQL Injection vulnerabilities with parameterized queries.
2. Implement MFA for admins, enforce stronger passwords, add rate-limiting.
3. Secure session cookies and enforce HTTPS.

Near-Term (2–8 weeks)

4. Rotate and shorten token lifetimes, enforce revocation lists.
5. Add CDN + WAF to mitigate DDoS.
6. Patch XSS with sanitization and CSP.
7. Move all checkout logic server-side; implement payment fraud checks.

Medium to Long-Term (2–12 months)

8. Enforce least privilege and perform quarterly access reviews.
9. Integrate SAST/DAST into CI/CD pipelines.
10. Conduct regular penetration tests and red team exercises.
11. Build incident response playbooks for data breaches and DDoS.

---

6. Conclusion

By applying STRIDE and DREAD, we identified and scored key threats against EVOL. **SQL Injection and Credential Stuffing** are the most urgent issues to remediate. Once those are resolved, the focus should shift to securing sessions, preventing DDoS, and strengthening payment systems. This prioritized roadmap helps EVOL protect sensitive data, maintain availability, and safeguard customer trust.