DVPATS- Product Spec

Security Assessment Report

1. Baseline Assessment

Business Importance
Stride Electronics is a dual-sided online marketplace for electronics with social features. It manages payments, commissions, a credit wallet, seller KYC verification, and an admin panel. The platform is **business-critical** due to handling of payments, PII, and compliance obligations (GDPR, PCI-DSS).

Document Coverage

- **Strengths:** Clear product features, user flows, revenue model.
- **Security Mentions:** SSL, PCI-DSS compliance, GDPR, login lockout, email verification, password reset expiry.
- **Gaps:** No detail on MFA, role-based access, fraud prevention, monitoring, session security, or logging.

Design Document Ratings (1–10):

- **Security Information:** 4 — Mentions standards but lacks specifics.
- **Technical Depth:** 5 — Strong on product flows, weak on architecture/controls.
- **Business Criticality:** 8 — Core to revenue, compliance, and trust.

2. Asset Inventory

Sensitive Assets:

- User profile data (PII)

- Authentication identifiers (email, social logins)
- Payment methods (cards, gift cards)
- StrideCredit balances
- Order history & invoices
- Seller KYC data (identity documents)
- Transaction records
- Admin & analytics data

Non-Sensitive Assets:

- Product listings & images
- Social interactions (likes, comments, follows)
- Notification preferences

---

3. Component Inventory

- **Interactors:** Buyer UI, Seller UI
- **Core Services:** Authentication, Catalog, Search, Checkout & Payments, StrideCredit Wallet, Order Management, Notifications
- **Supporting Services:** KYC Verification, Admin Panel, Analytics, Customer Support

4. Concise Security Review

Overall Risk Rating: HIGH

1. **MFA Missing** – No MFA for buyers, sellers, or admins, leaving accounts vulnerable to takeover.

2. **Weak Session Management** – Only persistence noted; no timeouts, rotation, or secure cookie flags documented.
3. **No Rate Limiting** – Login, reset, search, and comments are unprotected from brute force and automated scraping.
4. **PCI-DSS Unclear** – Compliance claimed, but tokenization and vaulting boundaries are unspecified.
5. **KYC Data Risk** – Identity documents collected with no mention of encryption, retention, or access controls.
6. **Content Security Absent** – Comments and listings can include unvalidated input, risking XSS and injection.
7. **Admin Panel Exposure** – Broad privileges without RBAC, audit logging, or workflow controls.
8. **StrideCredit Fraud Risk** – Wallet system lacks fraud-prevention mechanisms.

5. Confirmed Threats & Mitigations

Threat	Severity	Description	Mitigation
Account takeover without MFA	High	Without MFA, stolen or guessed credentials could let attackers access buyer, seller, or admin accounts, leading to fraudulent transactions and platform abuse.	Enforce MFA for admin accounts by default; enable step-up MFA for sensitive user actions like payouts and address changes.
Credential stuffing / brute force	High	No evidence of rate limiting on login or password reset endpoints. Attackers can automate credential stuffing or brute force attempts to compromise accounts.	Introduce per-IP/user rate limits, CAPTCHAs on suspicious traffic, and device/risk scoring to block automated attacks.
Stored/Reflected XSS	High	User-supplied comments, descriptions, and images are accepted without sanitization. Attackers could inject malicious scripts impacting other users.	Implement input sanitization, output encoding, and enforce CSP to prevent script execution; validate and restrict file uploads.

Missing RBAC in Admin Panel	Critical	The Admin Panel allows banning users, approving KYC, and managing disputes. Without RBAC, any admin could access all functions, risking abuse or insider threats.	Design and enforce RBAC roles; apply least-privilege principles and dual approval workflows for sensitive actions.
KYC data breach	Critical	Seller verification involves sensitive identity documents. No mention of encryption, retention, or access restrictions raises significant privacy and compliance risks.	Encrypt KYC data at rest, enforce short retention, limit access through ABAC, and redact data for customer support.
Weak session controls	High	Sessions persist without timeout, rotation, or secure cookie attributes. This leaves sessions vulnerable to hijacking.	Apply idle and absolute timeouts, rotate sessions on login/privilege changes, and enforce secure cookie attributes.
PCI scope creep	High	PCI-DSS is claimed but card tokenization or vaulting is not documented. Full cardholder data may pass through or be stored incorrectly, increasing compliance risk.	Ensure all card handling is via PCI-compliant provider; tokenize PAN; keep application out of PCI scope through hosted fields.
StrideCredit fraud	High	StrideCredit balances can be earned and spent partially. Without fraud checks, attackers may exploit refund loops or abuse promotions.	Introduce velocity and per-order caps, anomaly detection, and manual reviews for suspicious credit use.

6. Open Questions (Information Needed to Close Risks)

Authentication & Access

- Will **Multi-Factor Authentication (MFA)** be mandated for admin accounts and optionally enforced for buyers/sellers?

- How will **social login accounts** be linked to existing users to prevent hijacking (re-authentication, email confirmation, or alerts)?
- What **role-based access model** (RBAC) is planned for the Admin Panel to prevent privilege abuse?

Session & Application Security

- What are the **session timeout rules** (idle and absolute) and will sessions rotate on login or privilege changes?
- What **cookie protections** (HttpOnly, Secure, SameSite) will be enforced to mitigate hijacking?
- Are there **input sanitization** and **Content Security Policy (CSP)** controls planned for user-generated content (comments, product descriptions, uploads)?

Fraud & Abuse Prevention

- What **rate-limiting thresholds** will be applied to login, password reset, search, and comment endpoints?
- What safeguards will prevent **StrideCredit abuse** (velocity caps, per-order maximums, anomaly detection)?

Sensitive Data Handling

- How will **KYC documents** be protected at rest (encryption, access restrictions, redaction for support staff)?
- What is the planned **retention period** for KYC and order data to align with GDPR and compliance needs?
- Which **PCI-compliant payment provider** will be used, and what level of **tokenization or hosted fields** will remove PAN from our systems?

Monitoring & Compliance

- Which **security events** (admin actions, payout approvals, KYC access) will be audited and monitored?
- How will **user consent** for notifications be captured and tracked, and what is the process for fulfilling **GDPR data subject requests** (access, deletion, export)?