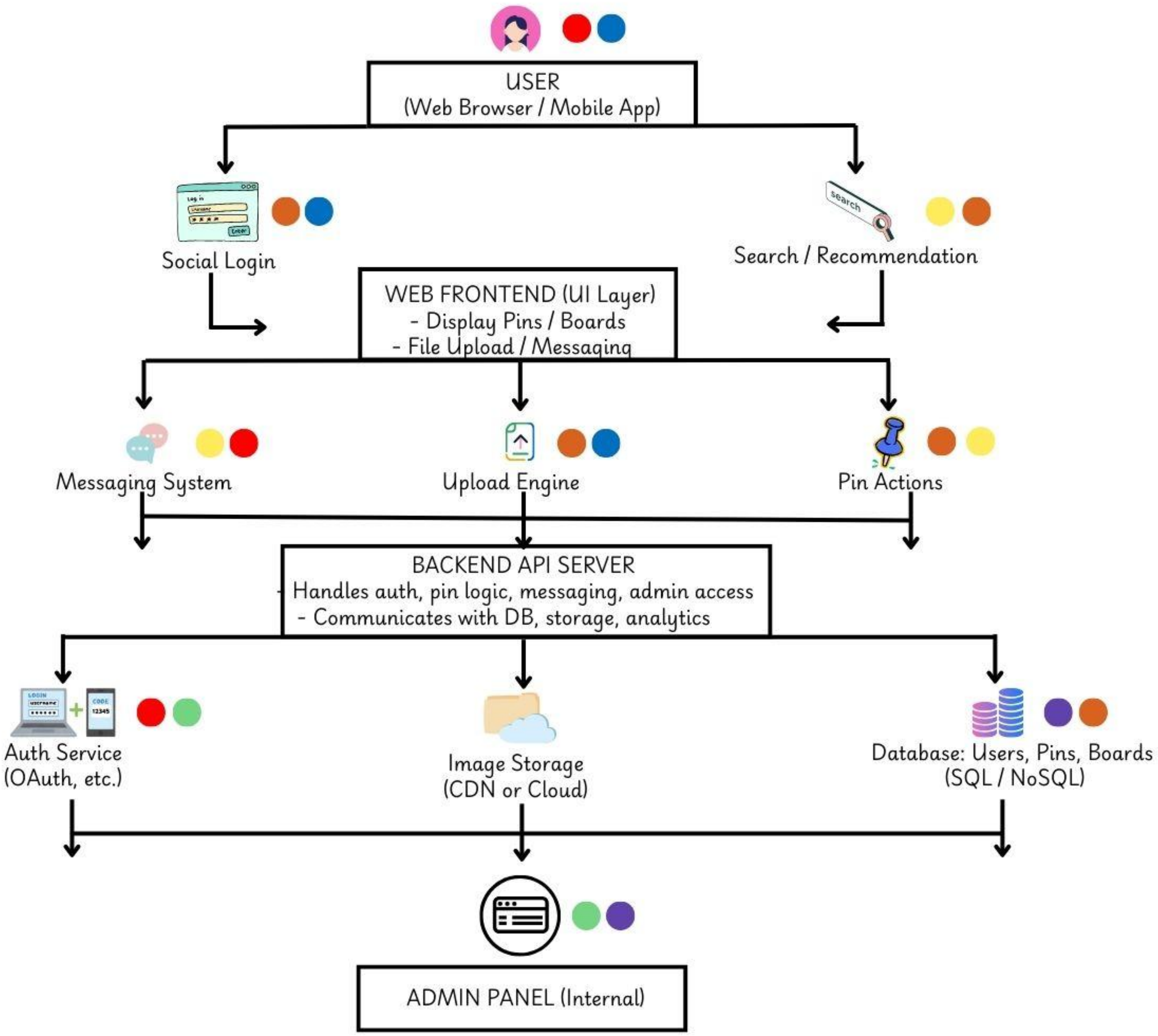
Pinterest Threat Modeling & GRC Risk Assessment

This case study analyzes Pinterest’s system components through the STRIDE threat modeling framework and aligns identified threats with NIST and ISO security controls for GRC-based risk mitigation

Prepared by: Purva Naresh Rumde
Cybersecurity Analyst | GRC | Security+
March 2025
📧 rumde.purva21@gmail.com | 📞 (850) 966-2894
🌐 Portfolio
🔗 LinkedIn

Pinterest Threat Model



USER
(Web Browser / Mobile App)

Social Login

Search / Recommendation

WEB FRONTEND (UI Layer)
- Display Pins / Boards
- File Upload / Messaging

Messaging System

Upload Engine

Pin Actions

BACKEND API SERVER
- Handles auth, pin logic, messaging, admin access
- Communicates with DB, storage, analytics

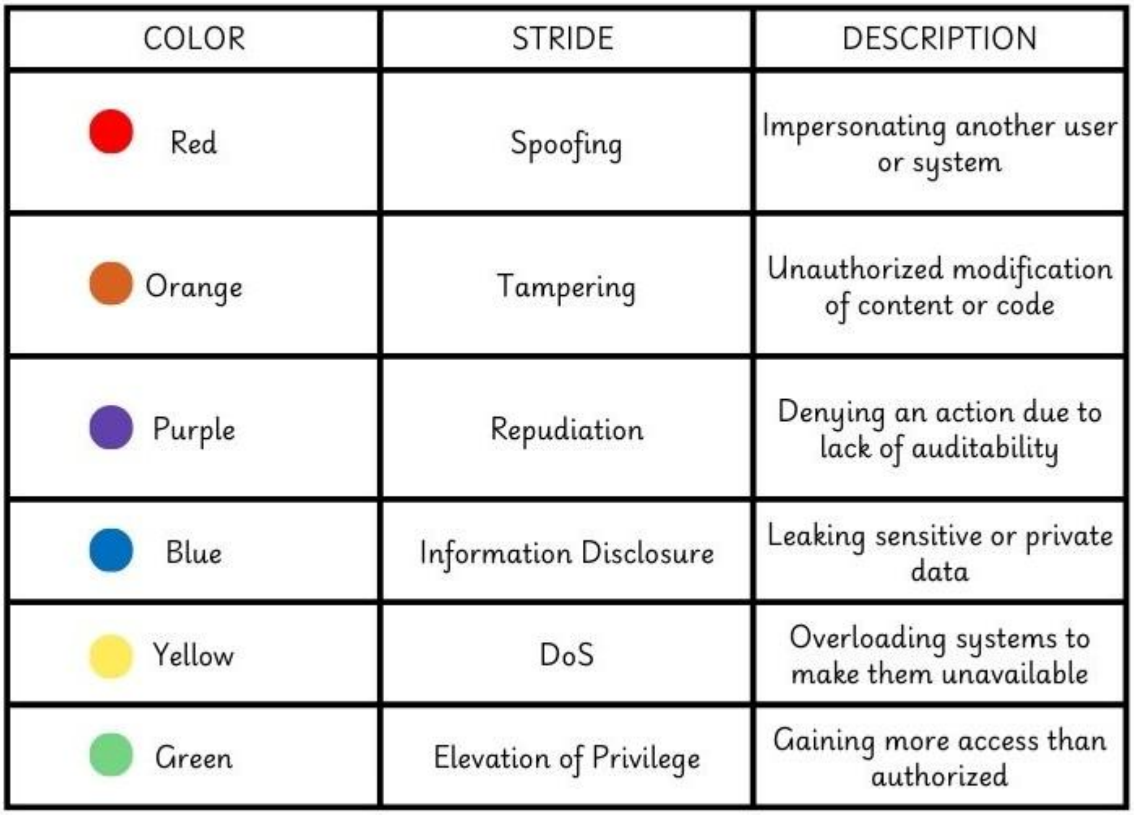
Auth Service
(OAuth, etc.)

Image Storage
(CDN or Cloud)

Database: Users, Pins, Boards
(SQL / NoSQL)

ADMIN PANEL (Internal)

Threat Tags



COLOR	STRIDE	DESCRIPTION
🔴 Red	Spoofing	Impersonating another user or system
🟠 Orange	Tampering	Unauthorized modification of content or code
🟣 Purple	Repudiation	Denying an action due to lack of auditability
🔵 Blue	Information Disclosure	Leaking sensitive or private data
🟡 Yellow	DoS	Overloading systems to make them unavailable
🟢 Green	Elevation of Privilege	Gaining more access than authorized

STRIDE Threat Table – Pinterest

Component	**Threat**	**STRIDE Category**	**Description**	**Impact**
User Authentication	Credential stuffing	Spoofing	Reusing leaked credentials to gain access	Account takeover
Messaging System	Impersonation/spoofed messages	Spoofing	Sending messages pretending to be another user	Trust issues, phishing
Image Upload	Malicious file upload	Tampering	Uploading images with embedded malware or scripts	Malware spread, server compromise
Boards/Pins	Tampered metadata or links	Tampering	Pins with altered redirect links or content	Phishing, misinfo, brand harm
User Deletion of Logs	Lack of audit trail	Repudiation	No way to prove actions were taken by a user	Legal, compliance, forensic gaps
Public Boards	Exposed private content	Information Disclosure	Misconfigured board exposes private pins	Privacy breach, GDPR risk
APIs (unauthenticated)	Data scraping	Information Disclosure	Public API endpoints leaking sensitive metadata	Data leakage, bot abuse
Notifications System	Spam pins or messages	Denial of Service	Mass spam campaigns to overload inbox/feed	System performance, user annoyance
Search/Recommendation Engine	Abuse via bot accounts	Denial of Service	Automated pin creation floods trending topics	Feed pollution, brand manipulation
Admin Panel	Privilege escalation	Elevation of Privilege	User gains unauthorized admin access	Total compromise
Social Login	Token reuse or hijack	Elevation of Privilege	Intercepted auth token used on Pinterest	Account hijacking

GRC Control Mapping Table

(NIST 800-53 + ISO 27001)

Threat	NIST 800-53 Control(s)	ISO 27001 Control(s)	Mitigation Strategy
Credential stuffing	IA-5 (Authenticator Mgmt), AC-7	A.9.4.3	MFA, rate limiting, login alerts
Impersonation/spoofed messages	AC-10 (Concurrent Session Control), SC-23	A.13.2.3	Session integrity, digital signatures
Malicious file upload	SI-10, SC-28 (Data Protection)	A.14.2.6	File scanning, MIME type validation, sandboxing
Tampered metadata or links	SI-7 (Software, Firmware, and Info Integrity)	A.12.2.1	Metadata validation, link filtering
Lack of audit trail	AU-2, AU-12	A.12.4.1	Immutable logs, log monitoring
Exposed private content	AC-4, SC-12 (Encryption)	A.9.1.1	Privacy settings, access controls
Data scraping	AC-17, SC-7	A.13.1.1	API key auth, rate limiting, CAPTCHA
Spam pins or messages	SC-5 (DoS Protection), SI-4	A.13.1.2	Anti-bot measures, abuse detection systems
Abuse via bot accounts	IR-4, SI-4	A.12.1.1	Behavioral anomaly detection
Privilege escalation	AC-6, AC-2	A.9.2.3	RBAC, privilege auditing, code review
Token reuse or hijack	IA-2, SC-23	A.9.4.2	OAuth best practices, token expiration, secure transmission

Risk Register – Pinterest Threats

Threat	**Likelihood (1–5)**	**Impact (1–5)**	**Risk Score**	**Risk Level**	**Response**	**Status**
Credential stuffing	4	4	16	High	Mitigate	MFA & alerts enabled
Impersonation/spoofed messages	3	4	12	Medium-High	Mitigate	Planned
Malicious file upload	4	5	20	High	Mitigate	In Progress
Tampered metadata or links	3	3	9	Medium-High	Mitigate	In Review
Lack of audit trail	2	5	10	Medium	Mitigate	Design discussion
Exposed private content	4	5	20	High	Mitigate	Planned
Data scraping	4	3	12	Medium-High	Mitigate	Planned
Spam pins or messages	3	3	9	Medium	Mitigate	WAF rules updated
Abuse via bot accounts	3	4	12	Medium-High	Mitigate	Monitoring enabled
Privilege escalation	2	5	10	Medium	Mitigate	Code audit started
Token reuse or hijack	3	4	12	Medium-High	Mitigate	Secure token config done