Security and Performance Optimisation for Social Networking Platforms

Andrii Matviienko

Date: 20.06.2025

Fontys

UNIVERSITY OF APPLIED SCIENCES

Context

This document explores critical strategies for enhancing security and performance in social networking platforms. It covers three core topics: implementing safe and restricted HTML/CSS customisation to mitigate security risks, applying best practices to secure databases effectively, and optimising system performance for real-time user interactions such as messaging and posting.

Questions

- How to implement safe and restricted HTML/CSS customization to prevent security vulnerabilities?
- What are the best practices for database security in a social networking platform?
- How to optimize performance for real-time interactions (e.g., messaging, posts)?

1. Safe HTML/CSS Customisation in Social Platforms

What

This research addresses how to securely allow user-generated HTML/CSS customization in social networking platforms without introducing cross-site scripting (XSS) or cross-site request forgery (CSRF) vulnerabilities.

Why

User personalization improves engagement, but unrestricted HTML/CSS poses severe security risks. XSS attacks can steal user sessions or inject malicious code, leading to data breaches and platform compromise.

How

To mitigate risks, a strict Content Security Policy (CSP) is enforced to limit external scripts, mixed content, and frame ancestors. Sanitization tools like DOMPurify and HTMLPurifier are applied to clean inputs. A whitelist of safe HTML/CSS is defined. Customizations are executed in sandboxed iframes, and actions are rate-limited and audited before deployment.

2. Securing Database Access in Social Platforms

What

This section focuses on database security techniques for managing sensitive user data, including identities, messages, and access tokens.

Why

Databases are prime targets for attacks. Common threats include SQL injection, stolen credentials, and unauthorized access. Ensuring database integrity is fundamental to maintaining platform trust and regulatory compliance.

How

Security is implemented using parameterized queries to prevent SQL injection (OWASP, 2024). The principle of least privilege limits database access per role. Data is encrypted both at rest (AES-256) and in transit (TLS 1.3). Secure access is enforced through OAuth 2.0, OpenID Connect, and multi-factor authentication (MFA). SIEM tools monitor activity, while tools like HashiCorp Vault manage secrets. Regular backups follow the 3-2-1 strategy.

3. Optimising Real-Time Interaction Performance

What

This topic explores methods to optimize the responsiveness of real-time features such as messaging and news feeds in social platforms.

Why

Users expect instant interaction. Latency, unresponsive UI, and delays in message delivery significantly impact user experience, especially in competitive environments.

How

Persistent connections via WebSockets replace inefficient HTTP polling. Asynchronous processing is handled using RabbitMQ or Kafka queues. In-memory caching (e.g., Redis, Memcached) accelerates data access. CDNs serve static content closer to users. DB queries are optimized and indexed. Compression techniques like Gzip and Brotli reduce payloads, and connection pooling minimizes overhead. Tools such as New Relic provide live performance monitoring.

References

1. BigID. (2023). Principle of least privilege access – why it matters. https://bigid.com/blog/principle-of-least-privilege-access/
2. Curbstone. (2023). What we learned from the 2023 Verizon data breach investigation report. https://curbstone.com/2023-verizon-dbir
3. Mozilla. (2024). The WebSockets API. https://developer.mozilla.org/en-US/docs/Web/API/WebSockets_API
4. NCSC UK. (2024). Data protection guidelines. https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data
5. OWASP. (2024). Content security policy & XSS prevention cheat sheets. https://cheatsheetseries.owasp.org
6. Verizon. (2024). Data breach investigations report 2024. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf