

Vulnerability Fixes Report

COMP47910 Secure Software Engineering

Luis Marron (23202882)

A Lab Journal in part fulfilment of the degree of

MSc. in Advanced Software Engineering

Supervisor: Dr. Liliana Pasquale



UCD School of Computer Science
University College Dublin

August 24, 2025

Table of Contents

1	A01:2021 Broken Access Control	3
1.1	CWE-284: Improper Access Control	3
1.2	CWE-639: Insecure Direct Object References	5
1.3	CWE-384: Session Fixation	6
1.4	CWE-1275: Sensitive Cookie with Improper SameSite Attribute	8
1.5	CWE-598: Use of GET Request Method With Sensitive Query Strings	10
2	A02:2021 Cryptographic Failures	12
2.1	CWE-311: Missing Encryption of Sensitive Data	12
2.2	CWE-315: Cleartext Storage of Sensitive Information in a Cookie	14
2.3	CWE-319: Cleartext Transmission of Sensitive Information	15
2.4	CWE-256: Unprotected Storage of Credentials	16
3	A03:2021 Injection	19
3.1	CWE-89: SQL Injection	19
3.2	CWE-20: Improper Input Validation	20
3.3	CWE-79: Cross-Site Scripting (XSS)	23
4	A04:2021 Insecure Design	25
4.1	CWE-307: Improper Restriction of Excessive Authentication Attempts	25
4.2	CWE-654: Reliance on a Single Security Mechanism	27
4.3	CWE-550: Information Exposure Through Server Log Files	28
5	A05:2021 Security Misconfiguration	32
5.1	CWE-250: Execution with Unnecessary Privileges	32
5.2	CWE-693: Protection Mechanism Failure	33
5.3	CWE-1021: Improper Restriction of Rendered UI Layers or Frames	35
5.4	CWE-550: Information Exposure Through Server Log Files	37
5.5	CWE-798: Use of Hard-coded Credentials	39
5.6	CWE-352: Cross-Site Request Forgery (CSRF)	41

5.7	CWE-1295: Debug Messages Revealing Unnecessary Information	43
6	A06:2021 Vulnerable and Outdated Components	46
6.1	CWE-1104: Use of Unmaintained Third Party Components	46
6.2	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	48
7	A07:2021 Identification and Authentication Failures	51
7.1	CWE-521: Weak Password Requirements	51
7.2	CWE-613: Insufficient Session Expiration	53
7.3	CWE-345: Insufficient Verification of Data Authenticity	56
7.4	CWE-287: Improper Authentication	58
8	A08:2021 Software and Data Integrity Failures	62
8.1	CWE-494: Download of Code Without Integrity Check	62
9	A09:2021 Security Logging and Monitoring Failures	65
9.1	CWE-778: Insufficient Logging of Security Events	65
9.2	CWE-117: Improper Output Neutralization for Logs	67
9.3	CWE-532: Insertion of Sensitive Information into Log File	70
10	A10:2021 Server-Side Request Forgery (SSRF)	73
10.1	CWE-918: Server-Side Request Forgery (SSRF)	73

Chapter 1: A01:2021 Broken Access Control

1.1 CWE-284: Improper Access Control

Description: The BookShop application implements improper access control mechanisms that allow unauthorized users to access restricted functionality and sensitive data. The application lacks proper authentication and authorization checks across multiple endpoints, enabling attackers to bypass security controls and gain unauthorized access to administrative functions and user-specific resources.

CWE Explanation: CWE-284 occurs when the application fails to properly restrict access to functionality or resources, allowing unauthorized users to perform actions or access data that should be protected by proper authentication and authorization mechanisms.

Severity: High

1.1.1 Vulnerability Locations and Type

The application suffered from multiple *Broken / Improper Access Control* weaknesses manifesting as:

- **Vertical privilege escalation:** Security rule protected path pattern `/admin/**`, while the actual admin endpoint controller was mapped to `/admins`. This mismatch let any authenticated non-admin invoke administrative endpoints (e.g. `GET /admins`).
- **Horizontal privilege escalation / Insecure Direct Object Reference (IDOR):** Cart- and cart-item-related REST endpoints (`/carts/**`, `/cart-items/**`) accepted arbitrary `customerId`, `cartId`, or `itemId` without verifying ownership against the authenticated principal, enabling access/modification of other users' carts.
- **Over broad data exposure:** User and customer enumeration endpoints (`/users/**`, `/customers/**`) allowed any authenticated user to list or fetch other users/customers and (in the case of `/users`) returned password hashes, breaching least privilege and confidentiality.
- **Unrestricted modification endpoints:** Book management API (books POST PUT DELETE) was accessible to any authenticated role, permitting non-admin content manipulation.
- **Lack of server side authorization on web cart actions:** Web MVC endpoints for cart item removal did not assert ownership, allowing crafted requests to remove other users' items.

1.1.2 Mitigation Strategy and Rationale

Defence-in-depth was applied combining **path-based authorization**, **method-level role enforcement**, and **resource ownership (row-level) checks**. This layered approach ensures:

- Misconfigurations in one layer (e.g. path patterns) do not automatically grant access because method-level annotations add a second gate.
- Even with correct role checks, horizontal attacks "guessing IDs" are blocked by explicit ownership validation tying domain object identifiers to the authenticated principal "prevents IDOR".
- Principle of Least Privilege is restored by scoping sensitive endpoints (admin, user lists, data mutations) strictly to the required roles, reducing attack surface.
- Sensitive credential fields are no longer exposed after authorization succeeds, limiting post-auth data leakage channels.

1.1.3 Implemented Security Controls

The following concrete changes were introduced in code (branch `broken-access-control-fixes`):

1. **Corrected admin path mapping:** Updated Spring Security configuration to match the actual controller path `/admins/**` instead of the incorrect `/admin/**`.
2. **Granular authorization rules:** Added HTTP method specific matchers restricting book mutation endpoints (POST/PUT/DELETE on `/api/books/**`) and all `/books/**` (management pages) to role ADMIN. User endpoints `/users/**` now require ADMIN; customer endpoints enforce authentication plus ownership (see point 3) and reserve modifications for ADMIN.
3. **Ownership / row-level checks:** Injected `@AuthenticationPrincipal` into cart and cart item controllers; added helper methods validating that the referenced cart/item's owning customer's username equals the authenticated principal. Requests failing validation now return HTTP 403 (or 404 when appropriate).
4. **Method-level security:** Enabled `@EnableMethodSecurity` and introduced `@PreAuthorize` annotations on controller methods (e.g. book mutations, user controller) to provide a second authorization layer beyond URL pattern matching.
5. **Data minimisation via DTOs:** Replaced direct entity exposure for users and customers with DTOs omitting the password field and limiting attributes to non-sensitive identification data.
6. **Cart web endpoint hardening:** Added ownership validation before allowing removal of a cart item via web MVC endpoint to block cross-user manipulation.
7. **Input encapsulation:** Refactored mutable request payload classes (e.g. add-item request) to use private fields with accessors, preventing accidental uncontrolled field exposure (minor hardening).

1.1.4 Solution Effectiveness

The mitigations directly address the CWE-284 root causes:

- Path correction + role restrictions close vertical privilege escalation vectors.
- Ownership validation eliminates horizontal ID enumeration attacks by binding operations to the authenticated identity.

- Method-level annotations safeguard against future path mapping drift or overly broad ant matchers.
- DTO-based redaction removes unnecessary sensitive data from responses, shrinking impact radius of any residual access gaps.
- Principle of Least Privilege is enforced consistently across both REST and MVC layers, aligning actual access with business intent.

1.2 CWE-639: Insecure Direct Object References

Description: Multiple endpoints previously trusted user-supplied identifiers (e.g. `customerId`, `cartId`, `itemId`) directly to select resources without verifying that the authenticated principal owned or was entitled to those resources. Attackers could substitute another valid numeric ID (IDOR) to read or modify other users' shopping cart contents or personal data.

CWE Explanation: CWE-639 occurs when an application authorizes a request based solely on a user-controlled key (such as a record ID) instead of confirming the requester is permitted to access the referenced object, enabling horizontal privilege escalation (Insecure Direct Object Reference).

Severity: High

1.2.1 Vulnerability Locations and Type

- **Cart REST endpoints:** `/carts/by-customer/customerId`, `/carts/cartId/items`, `/carts/cartId/a`, `/carts/cartId/remove-item/itemId`, and `/carts/cartId/total-price` accepted arbitrary path IDs; prior to fixes there was no binding between these IDs and the authenticated user (classic IDOR / horizontal escalation).
- **Cart item endpoint:** `/cart-items/id` exposed individual cart items without verifying ownership (permitting enumeration of other users' items by ID).
- **Customer lookup endpoints:** `/customers/id` and `/customers/by-username/username` allowed retrieval of other customers' personal information without ownership check (in early state) relying only on being authenticated.

1.2.2 Mitigation Strategy and Rationale

The strategy focused on eliminating trust in client-supplied identifiers by: (1) performing **server-side ownership validation** after object retrieval, (2) layering **role checks** so only admins can enumerate accounts, and (3) reducing exposed data via DTOs. Ownership checks ensure an attacker who guesses an ID still receives 403 Forbidden (or 404 Not Found) unless authorized. This halts horizontal privilege escalation while preserving legitimate functionality for rightful owners.

1.2.3 Implemented Security Controls

1. **Ownership helpers:** Introduced methods `enforceCustomerOwnership(...)` and `resolvedOwnedCart(...)` in the cart controller to load the resource and verify `resource.owner.username == principal.username` before returning it.
2. **Cart item deletion hardening:** Added explicit retrieval and cart-to-item linkage verification before deleting an item, ensuring the item belongs to the authenticated user's cart, preventing cross-cart deletions.
3. **Principal injection:** Added `@AuthenticationPrincipal` parameters to affected controller methods to reliably access the authenticated identity rather than relying on user-provided IDs.
4. **Customer data protection:** Added central ownership/admin check (`enforceOwnershipOrAdmin`) to customer endpoints and restricted full listing to ADMIN via `@PreAuthorize`.
5. **Least privilege for enumeration:** Restricted `/users/**` and customer listing endpoints to ADMIN in `SecurityConfig`, removing the ability for regular users to guess IDs and enumerate.
6. **DTO redaction:** Replaced direct entity exposure with DTOs omitting password hashes, limiting the value of any accidental disclosure.
7. **Path-based + method security:** Retained path restrictions (role-based) and enabled method-level security, adding a secondary barrier should future path patterns broaden inadvertently.

1.2.4 Solution Effectiveness

- Ownership enforcement turns previously unauthenticated resource selection into a two-factor authorization (valid ID + rightful owner) neutralising ID guessing.
- Removal operations now validate item-to-cart ownership, closing a residual destructive IDOR vector.
- Admin-only enumeration eliminates bulk discovery of valid identifiers (reducing reconnaissance surface).
- DTO redaction ensures that even if an ownership check regresses, sensitive credential data remains undisclosed.
- Layered (config + method) checks reduce single-point-of-failure risk if URL matcher misconfiguration reappears.

1.3 CWE-384: Session Fixation

Description: Initially the session fixation risk was assessed because the configuration did not explicitly state a session fixation protection strategy, and CSRF protection was disabled (increasing the impact of any session hijacking). However, Spring Security's default behaviour already migrates (rotates) the session identifier upon successful authentication. We have now made this

protection explicit in the security configuration, confirming that an attacker who pre-seeds a victim with a known anonymous session ID cannot continue to use that same ID after the victim authenticates.

CWE Explanation: CWE-384 (Session Fixation) concerns failure to invalidate or regenerate a session identifier when a user's authentication state changes, enabling an attacker who knows the pre-auth session token to hijack the post-auth session.

Severity: Low (Residual) – Effective mitigations in place; only hardening items remain.

1.3.1 Vulnerability Locations and Type

Prior to the explicit mitigation the potential exposure was theoretical rather than an observed exploit, characterised by:

- No explicit session fixation directive in `SecurityConfig` (relying implicitly on framework defaults).
- Disabled CSRF protection (would amplify damage of any successful fixation / hijack).
- Absence of cookie security attribute configuration (`Secure` / `SameSite` / `HttpOnly` not yet declared in `application.properties`).

Crucially, there was *no* custom code overriding Spring Security's default fixation protection; thus the core exploit path (reusing the same session ID after login) was already blocked.

1.3.2 Mitigation Strategy and Rationale

Strategy focused on: (1) making implicit framework protections *explicit* for auditability, (2) reducing residual attack surface through planned cookie hardening and CSRF re-enablement, and (3) documenting session handling to prevent future regressions (e.g. switching to a stateless policy without compensating controls). Explicit configuration eliminates uncertainty for reviewers and compliance checks.

1.3.3 Implemented Security Controls

1. **Explicit session ID migration:** Added `sessionFixation(migrateSession())` under `sessionManagement` in `SecurityConfig`, guaranteeing a new session identifier post-authentication.
2. **Logout invalidation:** Existing logout configuration invalidates the session server-side, preventing reuse of an authenticated context.
3. **Least privilege hardening elsewhere:** Reduced horizontal/vertical escalation (CWE-284 / CWE-639 controls) lowers the value of any hypothetical hijacked session.
4. **Password hashing (BCrypt):** Limits credential replay even if a session were short-livedly exposed.

1.3.4 Solution Effectiveness

- Attacker-controlled pre-auth session IDs are invalidated because the server issues a fresh session ID upon authentication (session fixation vector neutralised).
- Logout and privilege boundaries ensure compromised sessions cannot silently escalate or persist indefinitely.
- Strengthened access controls reduce the actionable scope of any transient session misuse.
- Making the protection explicit aids code reviews and prevents accidental regression (e.g. future refactor removing defaults unnoticed).

Given the default and now explicit migration behaviour, the application is not meaningfully vulnerable to session fixation at present; residual items are advisory enhancements.

1.4 CWE-1275: Sensitive Cookie with Improper Same-Site Attribute

Description: Assessment of the BookShop application's cookie security configuration reveals exemplary implementation of SameSite attributes and comprehensive security controls. The application properly configures session cookies with the most restrictive SameSite=Strict setting, combined with Secure and HttpOnly flags, representing security best practices that exceed industry standards. All sensitive cookies including JSESSIONID are protected against cross-site request forgery attacks and cross-site information leakage through optimal configuration in application.properties and Spring Security framework integration.

CWE Explanation: CWE-1275 occurs when web applications set cookies containing sensitive information without properly configuring the SameSite attribute, making them vulnerable to cross-site request forgery attacks and cross-site information leakage. The SameSite attribute controls when cookies are sent with cross-site requests, with Strict being the most secure setting.

Severity: None (Not Vulnerable) — Excellent cookie security configuration implemented with most restrictive SameSite settings and comprehensive security attributes.

1.4.1 Vulnerability Locations and Type

Assessment of cookie configuration reveals exemplary security implementation rather than vulnerabilities:

- **Session cookie security excellence:** JSESSIONID configured with SameSite=Strict; Secure; HttpOnly representing optimal security configuration.
- **Appropriate CSRF token configuration:** XSRF-TOKEN intentionally configured without HttpOnly to enable JavaScript access for legitimate AJAX operations.
- **No custom cookie vulnerabilities:** No manual cookie creation without proper security attributes found in application code.

- **Framework security leverage:** Application leverages Spring Boot secure defaults with explicit hardening through application properties.

1.4.2 Mitigation Strategy and Rationale

The application implements a *security-by-default cookie configuration* approach: (1) Configure session cookies with most restrictive SameSite=Strict setting to prevent all cross-site transmission; (2) Combine with Secure and HttpOnly flags for comprehensive protection against interception and XSS; (3) Maintain appropriate CSRF token accessibility for legitimate JavaScript operations; (4) Leverage Spring Security framework defaults with explicit security hardening; (5) Avoid custom cookie creation that could introduce security vulnerabilities. This approach ensures complete protection against cross-site request forgery while maintaining necessary functionality.

1.4.3 Implemented Security Controls

1. **Optimal session cookie configuration (implemented):** `server.servlet.session.cookie.same-site=strict` provides most restrictive cross-site protection.
2. **Transport security enforcement (implemented):** `server.servlet.session.cookie.secure=true` ensures HTTPS-only cookie transmission.
3. **XSS protection implementation (implemented):** `server.servlet.session.cookie.http-only=true` prevents JavaScript access to session cookies.
4. **CSRF token framework integration (implemented):** `CookieCsrfTokenRepository.withHttpOnlyFalse` enables necessary JavaScript access for AJAX operations.
5. **No vulnerable custom cookies (implemented):** Code analysis confirms absence of manual cookie creation without proper security attributes.
6. **Comprehensive application properties (implemented):** All cookie security attributes explicitly configured rather than relying solely on framework defaults.

1.4.4 Solution Effectiveness

- **Complete cross-site attack prevention:** SameSite=Strict blocks all cross-site cookie transmission, eliminating CSRF attack vectors through cookie-based session authentication.
- **Session hijacking protection:** Multiple cookie security layers (Secure, HttpOnly, SameSite=Strict) provide comprehensive protection against session theft through multiple attack vectors.
- **Appropriate functional balance:** CSRF tokens remain accessible to JavaScript for legitimate AJAX operations while maintaining security through server-side validation.
- **Industry standard excellence:** Cookie configuration exceeds security best practices with most restrictive settings that maintain application functionality.
- **Framework security utilization:** Leverages Spring Security proven patterns with additional explicit hardening for enhanced security posture.
- **Future-proof configuration:** Explicit security attribute configuration prevents regression if framework defaults change in future versions.

1.5 CWE-598: Use of GET Request Method With Sensitive Query Strings

Description: The BookShop application's two-factor authentication implementation previously exposed sensitive 2FA secrets by transmitting them to an external service (QuickChart.io) for QR code generation. This vulnerability manifested when the TwoFactorAuthService sent the complete 2FA secret as a query parameter to `https://quickchart.io/qr`, exposing cryptographic secrets to third-party infrastructure and network intermediaries. The secret transmission violated the principle of data minimization and created an uncontrolled sensitive data exposure vector that could enable account compromise if intercepted or logged by the external service.

CWE Explanation: CWE-598 occurs when applications use HTTP GET requests to transmit sensitive information through URL query parameters, making the data visible in server logs, browser history, referrer headers, and network monitoring tools. In this case, the vulnerability was amplified by sending 2FA secrets to external services, creating additional exposure surfaces beyond typical GET request logging risks.

Severity: High — 2FA secrets transmitted to external services represent critical cryptographic material exposure that could enable complete authentication bypass.

1.5.1 Vulnerability Locations and Type

The vulnerability manifested in the two-factor authentication implementation:

- **External service dependency:** `TwoFactorAuthService.generateQRCodeUrl()` method constructed URLs sending 2FA secrets to QuickChart.io service via GET request query parameters.
- **Uncontrolled secret transmission:** Complete TOTP secrets were embedded in URLs like `https://quickchart.io/qr?size=200&text=otpauth://totp/...secret=SECRETVALUE...`, exposing cryptographic material to third-party infrastructure.
- **Network exposure:** Secrets traversed external networks and could be logged by CDN providers, proxy servers, or monitoring systems between application and QuickChart.io.
- **Content Security Policy allowance:** CSP configuration explicitly permitted `https://quickchart.io` in `img-src` directive, enabling the vulnerable external dependency.

1.5.2 Mitigation Strategy and Rationale

The strategy focused on eliminating external dependencies for sensitive cryptographic operations: (1) Replace external QR generation service with local ZXing-based implementation to maintain complete control over 2FA secrets; (2) Generate QR codes server-side using industry-standard libraries with data URL encoding for direct browser rendering; (3) Remove external service from Content Security Policy to prevent future regression; (4) Ensure 2FA secrets never leave the application boundary during QR code generation process. This approach eliminates the external exposure vector while maintaining equivalent functionality through secure local generation.

1.5.3 Implemented Security Controls

1. **Local QR generation implementation:** Replaced external QuickChart.io service with Google ZXing library (core 3.5.3, javase 3.5.3) for complete local QR code generation control.
2. **Data URL encoding:** Implemented `generateQRCodeDataURL()` method using `BitMatrix` and `MatrixToImageWriter` to generate PNG QR codes encoded as data URLs (`data:image/png;base64,...`) for direct browser rendering.
3. **Secret containment:** 2FA secrets now remain entirely within application memory during QR generation process, eliminating external transmission vectors.
4. **Content Security Policy hardening:** Removed `https://quickchart.io` from CSP `img-src` directive, restricting image sources to 'self' and 'data:' only.
5. **Dependency management:** Added ZXing dependencies with explicit versioning and security-focused comments in `pom.xml` for maintainability and audit trail.
6. **Cryptographic integrity preservation:** Maintained identical TOTP secret generation and validation while securing the QR presentation layer.

1.5.4 Solution Effectiveness

- **Complete external exposure elimination:** 2FA secrets no longer traverse external networks or reach third-party services, eliminating the primary CWE-598 attack vector.
- **Cryptographic material containment:** All sensitive TOTP operations including QR generation occur within application boundary, maintaining cryptographic secret confidentiality.
- **Functional equivalence:** Local ZXing implementation produces identical QR codes with same scanning compatibility as external service while eliminating security risks.
- **Network attack surface reduction:** Removal of external service dependency eliminates man-in-the-middle opportunities and reduces DNS/TLS certificate attack vectors.
- **Compliance and audit improvement:** Local secret handling aligns with security best practices for cryptographic material management and simplifies compliance auditing.
- **Dependency vulnerability mitigation:** Eliminates reliance on external service availability and security posture, removing supply chain risk from 2FA functionality.

Chapter 2: A02:2021 Cryptographic Failures

2.1 CWE-311: Missing Encryption of Sensitive Data

Description: Certain sensitive data flows in the BookShop application lack enforced cryptographic protection in transit or rely on plaintext representation in local configuration. While user passwords are securely hashed (BCrypt) and the application–database channel is configured for SSL, end-user credential submission (login/registration), session cookies, and ad hoc sensitive form fields (e.g. checkout credit card input) can traverse unencrypted HTTP if the deployment is not fronted by TLS. Additionally, example environment variables and scripts illustrate plaintext storage of database and truststore secrets. These gaps collectively represent incomplete protection of sensitive data rather than a single critical exposure.

CWE Explanation: CWE-311 refers to missing or absent encryption for sensitive information either at rest or in transit where encryption is expected for confidentiality or regulatory compliance. It commonly manifests as cleartext transmission (overlaps with CWE-319) or cleartext storage (overlaps with CWE-312 / CWE-256) when mitigations are inconsistent or absent.

Severity: Medium (Residual) – Core credentials (passwords at rest) are protected; remaining issues affect transport and secret handling hygiene.

2.1.1 Vulnerability Locations and Type

- **Transport (HTTP):** Application lacks explicit HTTPS / TLS configuration (no `server.ssl.*`); README usage examples employ `http://localhost:8080`. In any non-local deployment without a reverse proxy TLS terminator, credentials and session cookies would be transmitted in cleartext (CWE-319 contributing to CWE-311).
- **Session Cookies:** No Secure, HttpOnly, or SameSite attributes configured; cookies could be exposed over insecure transport or be susceptible to CSRF replay.
- **Checkout form data:** Credit card number field (not persisted) is still transmitted; without TLS it is exposed in transit. No masking or client-side obfuscation.
- **Secrets in environment artifacts:** Example `.env` content and setup scripts contain plaintext database credentials and truststore password (acceptable for local dev, but a risk pattern if replicated to production). Overlaps with CWE-256.
- **Logging / auditing:** No explicit masking safeguards (currently no evidence of leakage, but absence of policy introduces latent risk if future logging is added).

2.1.2 Mitigation Strategy and Rationale

Strategy targets layered confidentiality protection: (1) enforce TLS for all external HTTP traffic; (2) harden session cookie attributes to reduce exposure and replay potential; (3) minimise plaintext secret footprint by moving production secrets to a managed vault; (4) restrict network attack

surface via HSTS and secure redirects; (5) avoid collecting unnecessary high sensitivity data (drop credit card field if not processing payments). This layered defence ensures compromise of any single mechanism (e.g. proxy misconfiguration) does not fully expose sensitive data.

2.1.3 Implemented / Planned Security Controls

1. **Password hashing (in place):** All user credentials stored with BCrypt (adaptive hashing, salts implicit) – removes cleartext password storage risk.
2. **Encrypted DB channel (in place):** JDBC URL enforces `useSSL=true` and `requireSSL=true` with truststore configuration.
3. **Session fixation mitigation (in place):** Protects session integrity post-auth (limits utility of intercepted pre-auth IDs).
4. **Planned TLS enforcement:** Introduce reverse proxy or Spring Boot keystore; redirect HTTP → HTTPS and add HSTS header.
5. **Cookie hardening (planned):** Set `server.servlet.session.cookie.secure=true`, `...http-only=true`, `...same-site=Strict`.
6. **Secret management (planned):** Replace plaintext env variables (especially root DB password) with secrets provisioned by a secure store (Vault / cloud KMS) and principle of least privilege DB accounts.
7. **Data minimisation (planned):** Remove or tokenise credit card field; if retained for demo, clearly flag as non-production and mask client-side.
8. **Logging safeguards (planned):** Introduce logging policy and filters to prevent future accidental sensitive data logging.

2.1.4 Solution Effectiveness

- Existing strong password hashing and encrypted DB transport already neutralise the most damaging storage and backend transit risks.
- Planned universal TLS and Secure/HttpOnly/SameSite cookies will close interception windows for credentials and session tokens.
- Secret manager adoption will reduce blast radius of host compromise or repo leakage versus static env files.
- Removing unnecessary high sensitivity fields (credit card) eradicates an entire sensitive data class, lowering compliance scope (PCI DSS) and exposure.
- Layered controls ensure that even if one layer (e.g. proxy TLS) fails, credential hashes remain non-reversible and session tokens protected by cookie policies.

2.2 CWE-315: Cleartext Storage of Sensitive Information in a Cookie

Description: Analysis confirms no sensitive information (plaintext passwords, API keys, tokens containing secrets, PII, payment data) is stored in browser cookies. The application relies exclusively on the standard opaque JSESSIONID for server-side session tracking. No custom cookie creation exists in server code or client-side JavaScript; thus the application is *not currently vulnerable* to CWE-315.

CWE Explanation: CWE-315 covers placing sensitive information directly (cleartext or trivially encoded) into cookies such that disclosure or tampering enables account compromise, impersonation, or data leakage. Even with HTTPS, client-side storage of secrets is discouraged because local access or XSS can expose them.

Severity: None (Not Vulnerable). Would elevate to High if future changes store secrets (e.g. raw bearer tokens) in cookies without encryption/integrity safeguards.

Assessment Evidence

- No occurrences of custom Cookie creation or header manipulation in Java sources.
- No `document.cookie` usage in static JS or templates.
- DTOs exclude password hashes; no credential material leaves server to be placed in cookies.
- Session identifier is opaque; no sensitive claims or data embedded.

Mitigation Strategy and Rationale

Maintain a minimal opaque session token model: keep all sensitive state server-side; never persist secrets or PII in client cookies. Complement with cookie attribute hardening (Secure, HttpOnly, SameSite) and session rotation (already explicit) to reduce ancillary risks (CWE-614, CWE-1275) while ensuring no CWE-315 condition can emerge inadvertently.

Implemented / Planned Controls

1. **Opaque server session (implemented):** Only an identifier stored client-side.
2. **Password hashing (implemented):** Removes any need to surface plaintext credentials.
3. **No custom cookie writes (implemented):** Eliminates common accidental leakage vector.
4. **Cookie attribute hardening (planned):** Add Secure / HttpOnly / SameSite (ties into CWE-319 remediation).
5. **Future guardrails (planned):** CI/static rule to flag introduction of sensitive keywords in cookie names or values.

Solution Effectiveness

- Absence of data-bearing cookies removes primary CWE-315 attack surface.
- Planned attributes further reduce residual token theft or cross-site replay vectors.
- Guardrails lower regression risk if new auth features (remember-me, JWT) are introduced.

2.3 CWE-319: Cleartext Transmission of Sensitive Information

Description: Client-server interactions (login, registration, authenticated browsing) were originally performed over HTTP with no transport security enforcement, as neither embedded TLS (no `server.ssl.*` properties) nor an HTTPS redirect existed. Documentation curl examples referenced `http://localhost:8080`, normalising plaintext usage. In any non-local / shared network scenario this exposes credentials and session identifiers to interception or manipulation (Man-in-the-Middle, passive sniffing). Session cookies also lacked Secure / SameSite attributes, increasing replay and cross-site leakage risk.

CWE Explanation: CWE-319 addresses transmission of sensitive information over cleartext channels. Attackers positioned on the network path can read or alter traffic lacking cryptographic protection. This differs from CWE-311 (broader missing encryption) by focusing specifically on in-transit confidentiality/integrity compromise enabling credential theft, session hijacking, or data tampering.

Severity: High (production / shared networks). Medium (loopback-only development) but still a negative security practice.

Vulnerability Locations and Type

- **No TLS configuration:** Absence of `server.ssl.key-store` or reverse proxy mandate meant HTTP only.
- **No enforcement:** Security configuration had no channel security requirement or redirect to HTTPS.
- **Session cookies:** Lacked Secure, HttpOnly, SameSite flags (susceptible to interception / CSRF replay once over HTTP).
- **Documentation examples:** README exclusively used plaintext HTTP endpoints, encouraging insecure operational patterns.
- **Potential sensitive forms:** Payment / PII form submissions (if added) would likewise traverse HTTP.

Mitigation Strategy and Rationale

Enforce an *HTTPS by default* posture: (1) introduce production-profile HTTPS enforcement and HSTS to prevent downgrade, (2) configure TLS via keystore or proxy, (3) harden cookies (Secure,

HttpOnly, SameSite) reducing token exfiltration surface, (4) eliminate plaintext examples to shift developer behaviour, (5) add automated tests verifying redirect + security headers to prevent regression. Layered approach ensures that if a single control fails (e.g. misconfigured proxy), other safeguards (cookie flags, credential hashing) limit exploit value.

Implemented / Planned Security Controls

1. **Prod profile HTTPS enforcement (implemented):** Added custom redirect filter + HSTS headers when prod profile active.
2. **HSTS (implemented prod):** Sets long max-age with subdomain + preload intent to resist protocol downgrades.
3. **Password hashing (existing):** Mitigates offline cracking impact if credentials were previously observed.
4. **Cookie hardening (planned):** Add `server.servlet.session.cookie.secure=true`, `...http-only=true`, `...same-site=Strict`.
5. **TLS keystore / proxy integration (planned):** Provide keystore properties or documented reverse proxy termination (NGINX / Caddy with ACME).
6. **Documentation update (planned):** Replace HTTP examples with HTTPS and describe trusting dev self-signed cert.
7. **Automated tests (planned):** Integration test asserting HTTP → HTTPS 301/308 redirect and presence of HSTS in prod.
8. **Mixed content audit (planned):** Validate no HTTP asset references remain post-transition.

Solution Effectiveness

- HTTPS enforcement + HSTS removes primary interception vector (passive sniffing / trivial MiTM downgrade).
- Cookie hardening will prevent session token leakage over inadvertent HTTP calls and reduce CSRF token reuse potential.
- Removing plaintext examples reduces operational drift toward insecure defaults.
- Automated testing creates a guardrail against accidental removal of channel security.
- Existing password hashing ensures historical captures have limited utility if obtained pre-mitigation.

2.4 CWE-256: Unprotected Storage of Credentials

Description: Core user credentials (passwords) are securely stored using BCrypt hashing; however, residual unprotected credential storage issues remain: (1) a default administrator password is disclosed in cleartext inside the seeding script comments, (2) database and truststore secrets are managed as plaintext environment variables in a local `.env` file and referenced directly by

docker compose, and (3) weak placeholder values are demonstrated in README examples. These patterns risk accidental promotion of development secrets or reuse of weak defaults in production. The issue is thus not plaintext password storage in the database, but exposure and handling of operational secrets and a hard-coded default credential pattern.

CWE Explanation: CWE-256 covers storing credentials without adequate protection (encryption, hashing, vault-based segregation) or exposing them in source artifacts (scripts, config files, comments) such that compromise of the repository or workstation yields immediate credential disclosure. It overlaps with CWE-798 (hard-coded credentials) when defaults are embedded, and with CWE-522 when credential protection mechanisms are insufficient.

Severity: Medium (would escalate toward High if the disclosed admin password or example secrets were deployed unchanged beyond local development).

Vulnerability Locations and Type

- **Seed script comment:** `scripts/create-admin-user.sql` contains a cleartext default admin password in a comment (hard-coded / discoverable credential pattern).
- **Environment variables:** `.env` (excluded from VCS, but encouraged) stores DB root/user passwords and truststore password in plaintext. Acceptable locally, but no segregation or rotation policy specified for higher environments.
- **Truststore password exposure:** Passed directly via `SPRING_DATASOURCE_HIKARI_TRUSTSTORE_PASSWORD` environment variable; resident in process environment and potentially logs if misconfigured.
- **Placeholder weak values:** README examples (`rootpassword`, `appuserpassword`, `truststorepassword`) risk being reused verbatim.
- **No secret scanning / policy:** CI/CD pipeline (not documented) lacks automated detection to block accidental secret commits.

Mitigation Strategy and Rationale

Focus on eliminating static/discoverable secrets in source and strengthening operational handling: (1) remove or parameterise default credentials; (2) introduce secret generation at setup time with one-time display; (3) adopt a secrets manager for non-local deployments; (4) enforce least-privilege DB accounts (separate admin vs app user); (5) integrate automated secret scanning to prevent regressions; (6) clearly label placeholder values as 'CHANGEME' to discourage reuse. This reduces credential exposure surface and shortens compromise window via rotation and principle of least privilege.

Implemented / Planned Security Controls

1. **Password hashing (implemented):** All end-user passwords stored using BCrypt (adaptive, salted) eliminating plaintext password-at-rest risk.
2. **DTO redaction (implemented):** Password hashes no longer returned by any API endpoints, reducing secondary leakage channels.
3. **Encrypted DB transport (implemented):** Mitigates interception of database credentials post-auth handshake.

4. **Remove default admin secret (planned)**: Replace hard-coded admin credential comment with instruction to supply a strong password (or script-driven random generation).
5. **Secret generation (planned)**: Modify setup scripts to auto-generate strong random passwords (e.g. 24+ char base64) and print once.
6. **Secrets manager integration (planned)**: Externalise production secrets (Vault / cloud provider store) removing reliance on persistent '.env' in production.
7. **Least privilege DB accounts (planned)**: Separate schema migration/admin from runtime application user; restrict privileges to required CRUD.
8. **Secret scanning in CI (planned)**: Add tools (e.g. Gitleaks / TruffleHog) to detect accidental commits of secrets or weak defaults.
9. **Documentation hardening (planned)**: Mark all sample credentials as `CHANGEME_<PURPOSE>` to prevent reuse in non-local deployments.

Solution Effectiveness

- Existing hashing already neutralises the most severe impact vector (direct theft of user passwords from DB).
- Removing the disclosed admin password and auto-generating credentials eliminates a trivial, high-impact compromise path.
- Secrets manager + least privilege narrows lateral movement after host compromise: stolen app credential yields only scoped DB access.
- CI secret scanning provides early detection and prevents regression (shift-left control).
- Clear CHANGEME placeholders reduce likelihood of weak default propagation to production.

Chapter 3: A03:2021 Injection

3.1 CWE-89: SQL Injection

Description: Assessment of the BookShop application's data-access layer found no exploitable SQL Injection vectors in its current state. All persistence operations are performed through Spring Data JPA repository interfaces using method-name derived queries (e.g. `findByUsername`) or inherited CRUD methods. There is no evidence of string concatenation to build JPQL/SQL, no usage of `@Query` with interpolated parameters, and no raw JDBC / native query execution paths. Consequently, untrusted user input is never directly merged into executable SQL without parameter binding.

CWE Explanation: CWE-89 (SQL Injection) arises when an application constructs SQL statements by directly embedding untrusted input, allowing attackers to alter query structure (e.g. changing WHERE clauses, UNION extraction, or triggering stacked queries in permissive drivers). Proper parameterisation ensures user data is treated strictly as values, not executable syntax.

Severity: None (Not Vulnerable) at present. Would elevate rapidly to High if future features introduce unparameterised dynamic queries.

Assessment Evidence

Audit activities and findings:

- Grep searches for raw SQL construction indicators returned no matches: patterns `createNativeQuery`, `@Query`, `PreparedStatement`, `Statement`, direct SQL keywords (`SELECT/INSERT/UPDATE/DELETE`) absent from code except in comments.
- No repository methods annotated with `@Query`; only Spring Data derived query methods (e.g. `findByUsername`) which use prepared parameter binding under the hood.
- No usage of `EntityManager`, `JdbcTemplate`, `Criteria API`, or manual pagination/sorting parameters that could introduce unsafe field injection.
- No dynamic `ORDER BY` / filtering logic sourced from request parameters (no `Sort` / `Pageable` occurrences) that could later encourage string concatenation.
- Domain entities contain only mapped fields; user-supplied values become parameters in prepared statements generated by the JPA provider (Hibernate), not concatenated SQL fragments.

Mitigation Strategy and Rationale

Maintain a *parameterisation-only* data access pattern and introduce guardrails so future changes cannot silently introduce injection risk. Emphasise: (1) exclusive use of Spring Data method derivation or `@Query` with named / positional parameters, (2) strict white-listing of sortable /

filterable fields when adding dynamic search endpoints, and (3) code review / CI rules to flag raw SQL introduction.

Implemented / Planned Controls

1. **Spring Data repositories (implemented):** Auto-generated prepared statements ensure parameter binding.
2. **No raw SQL / native queries (implemented):** Eliminates primary injection surface.
3. **Input validation (partial):** Bean validation (@NotBlank) constrains some inputs; while not a primary defence for injection, it reduces anomalous payload shapes.
4. **Repository pattern adherence (planned guardrail):** Architectural decision record (ADR) to codify prohibition of ad hoc JDBC unless justified with security review.
5. **Static scan rule (planned):** CI grep / SAST rule to flag introduction of @Query("%" + var) style concatenations or createNativeQuery.
6. **Dynamic sort/filter sanitisation (planned):** If future endpoints accept field names, implement white-list mapping (enum -> column) to avoid direct trust in request parameters.
7. **Security review checklist (planned):** Mandatory review item for any PR adding raw SQL, native queries, or criteria builder logic.

Solution Effectiveness

- Absence of raw or annotated custom queries removes typical injection entry points.
- Hibernate's prepared statement generation enforces separation of code and data, neutralising payloads containing quotes or control tokens.
- Planned guardrails reduce regression risk as feature scope expands (search, reporting, analytics).
- White-list driven future dynamic sorting/filtering prevents second-order injection through column / direction parameters.

3.2 CWE-20: Improper Input Validation

Description: The application previously accepted numerous user-controlled inputs (registration data, cart item quantities, book metadata, author names, payment form field) without comprehensive server-side validation. Only sparse annotations (e.g. NotBlank) existed on a subset of entity fields and were inconsistently enforced (many controller endpoints lacked Valid). This gap allowed malformed, extreme, or semantically invalid values (negative or enormous quantities, impossible years, invalid ISBNs, oversized strings) to reach persistence and business logic layers, risking data integrity degradation, logic manipulation, and denial-of-service via oversized payloads. Recent changes introduced structured DTOs and Bean Validation constraints to close these vectors.

CWE Explanation: CWE-20 (Improper Input Validation) arises when an application fails to define and enforce syntactic, semantic, or range constraints on externally supplied data before use. Inadequate validation can cascade into numerous secondary weaknesses (injection, overflow, business rule abuse) by allowing maliciously crafted input to impact data stores, processing logic, or downstream APIs.

Severity: Medium (Residual Low after implemented controls) Core validation now present; remaining exposure relates to legacy MVC form bindings and unvalidated optional fields slated for refactor.

Vulnerability Locations and Type

- **Entity direct binding:** Controllers bound domain entities (e.g. Customer, Book) directly from request bodies or form submissions, inheriting every writable field without a whitelist.
- **Missing range/format constraints:** No length or pattern enforcement for ISBN, phone numbers, names, addresses; numeric fields permitted negative or extreme values (price, quantity, year, numberOfCopies).
- **Quantity manipulation:** Cart add-item accepted arbitrary (including zero/negative) quantities enabling inventory or pricing anomalies.
- **Payment form:** Credit card number field had no format, length, or checksum validation (and is non-functional demo data).
- **Silent extra fields:** Jackson deserialization accepted unknown JSON properties (risk of future mass assignment if sensitive setters are added).

Mitigation Strategy and Rationale

Adopt a defence-in-depth input sanitation model: (1) Introduce dedicated request DTOs with explicit whitelists and Bean Validation annotations; (2) Apply semantic, syntactic, and range constraints (regex, size, numeric bounds); (3) Enforce validation by annotating controller method parameters with `@Valid`; (4) Fail fast with a consistent error contract via a global exception handler; (5) Harden deserialization to reject unknown properties, preventing accidental acceptance of stray or future-sensitive fields. This systematic approach ensures only well-formed, business-compliant data continues beyond the controller boundary.

Implemented Security Controls

1. **CustomerRegistrationDto Bean Validation:** Username, password, personal and contact fields now constrained with length, pattern, and format annotations (e.g. Email, phone regex) and enforced through `Valid`.
2. **Book field constraints:** Added size, ISBN pattern (ISBN-10/13), year range (1450–2100), non-negative price with scale check, and bounded copy counts.
3. **Cart add-item validation:** Quantity now requires minimum 1 (`Min(1)`), preventing negative or zero-impact manipulations.
4. **Global validation handler:** Central `ControllerAdvice` standardises 400 responses and prevents verbose default error leakage.

5. **Strict deserialization:** `spring.jackson.serialization.fail-on-unknown-properties` true rejects payload fields not explicitly declared in DTOs, blocking silent mass-assignment style expansion.
6. **Password hashing continuity:** Ensures even validated credential inputs are irreversibly stored (complements validation by preserving confidentiality).
7. **Field renaming hygiene:** Normalised `bookName` naming to prevent tooling / lint confusion and encourage consistent property-level validation.

Planned / Remaining Controls

- Introduce DTOs and validation for MVC Book/Author form submissions to replace direct entity binding.
- Add validation (or removal) of the demo credit card field with checksum (Luhn) if retained.
- Enforce maximum aggregate payload sizes at reverse proxy and apply additional per-field size caps where user-generated text is later introduced.
- Add rate limiting (ties to CWE-799) to reduce brute-force probing of validation boundaries.
- Add automated tests asserting rejection of malformed ISBNs, negative quantities, overlong fields.
- Implement business rule validators (e.g. inventory non-negative after operations) as custom constraints or service assertions.

Solution Effectiveness

- **Whitelisting DTOs:** Replaces broad entity binding with curated inputs, eliminating inadvertent exposure of internal or future sensitive fields (prevents mass assignment class of CWE-20 derived issues).
- **Bean Validation enforcement:** Declarative constraints ensure malformed data is rejected pre-persistence, safeguarding data integrity and reducing attack surface for logic abuse or cascading injection vectors.
- **Semantic constraints:** ISBN regex, numeric bounds, and size limits prevent structurally invalid data that could otherwise fuel business logic anomalies or storage bloat.
- **Fail-fast error handling:** Consistent 400 responses shrink observability for attackers attempting boundary probing (no stack traces or partial processing side-effects).
- **Unknown property rejection:** Blocks introduction of rogue fields trying to smuggle unexpected values, a common foothold for privilege inflation or latent injection when new setters appear.
- **Quantity constraints:** Prevent negative or zero manipulations that could be leveraged to produce free/credit scenarios or integer underflow in future calculations.
- **Normalization & naming hygiene:** Clear, conventional field naming supports static analysis and future automated policy checks, reducing misconfiguration risk.

3.3 CWE-79: Cross-Site Scripting (XSS)

Description: A structured audit of all server-rendered HTML (Thymeleaf templates under `src/main/resources/` and relevant controller pathways found *no exploitable Cross-Site Scripting vectors* in the current codebase. All user-controlled fields are emitted via Thymeleaf's escaped expression and form binding mechanisms (e.g. `th:text`, `th:field`, attribute processors) which HTML-encode special characters. There is **no** use of unescaped output primitives (`th:utext`), inlined JavaScript expression substitutions (`[[...]]` / `[(...)]`), or manual string concatenation inserting raw request data into script blocks or event handler attributes. Earlier template refactors (e.g. renaming to `bookName`) maintained escaped bindings and removed any need for ad hoc unescaped placeholders. Consequently attacker-supplied input cannot break containment to execute script in another user's browser under current functionality.

CWE Explanation: CWE-79 arises when untrusted input is included in a web page without proper context-aware encoding or sanitisation, enabling the injection and execution of arbitrary script in the victim's browser (reflected, stored, or DOM-based). Preventing XSS requires systematically neutralising user-controlled characters significant to HTML/JS parsing or restricting script execution pathways.

Severity: None (Not Vulnerable at present). Would elevate if future rich text / HTML features or unescaped rendering are introduced without sanitisation.

Assessment Evidence

Audit activities and supporting findings:

- Grep searches for unescaped constructs returned none: patterns `th:utext` and inline substitution delimiters `[[` / `[(` (used for inlined JS) are absent.
- No occurrences of raw output methods or manual HTML string assembly in controllers/services; all views resolved through Thymeleaf templates.
- All dynamic textual content rendered with escaping processors (`th:text`, `th:value`, `th:field`); no direct usage of `th:utext` (which would bypass encoding).
- No template inlined JavaScript blocks containing template expressions; only static script includes are present.
- No reflection of request parameters into error pages or query string echoes; validation errors are summarised as plain escaped messages via the global handler.
- Input validation (length/pattern constraints) reduces payload surface even if an encoding bypass were later introduced.
- Template field rename adjustments (`book_name` -> `bookName`) avoided broken bindings that might otherwise tempt unescaped insertions.

Mitigation Strategy and Rationale

Maintain a *strict auto-escape* posture while adding forward-looking guardrails: (1) rely solely on Thymeleaf's escaped output features for plain text; (2) introduce Content Security Policy (CSP) to constrain script execution sources; (3) forbid unescaped directives (`th:utext`) except under

explicit security review with server-side sanitisation; (4) implement lint / CI checks for introduction of risky constructs; (5) if future rich text/user HTML is required, apply a conservative allow-list sanitizer before persistence and still encode on output.

Implemented / Planned Controls

1. **Escaped template rendering (implemented):** Exclusive use of `th:text`, `th:field`, and attribute processors ensures HTML entity encoding.
2. **Absence of unescaped primitives (implemented):** No `th:utext` or inline expression substitutions eliminates common bypass channels.
3. **No dynamic script construction (implemented):** No server-sourced data injected into inline `<script>` blocks or event handler attributes.
4. **Input validation (implemented):** Bean Validation narrows malicious payload shapes (defence-in-depth only).
5. **CSP header (planned):** Add restrictive Content-Security-Policy (e.g. `script-src 'self'; object-src 'none'; base-uri 'self'; frame-ancestors 'none'`) to mitigate impact if an injection slips through.
6. **Template guardrail (planned):** CI rule / review checklist to flag additions of `th:utext`, inline script expressions, or event attributes containing untrusted expressions.
7. **Rich text sanitisation policy (planned):** If future features require formatted user content, adopt an allow-list HTML sanitizer (e.g. OWASP Java HTML Sanitizer) prior to storage.
8. **Security headers bundle (planned):** Referrer-Policy, Permissions-Policy, and strengthening cookies (Secure, HttpOnly, SameSite) to reduce session theft avenues in case of future XSS.

Solution Effectiveness

- Auto-escaping neutralises script meta-characters (`j`, `z`, `&`, quotes) preventing payload interpretation as active markup.
- Lack of unescaped or inline script sinks removes primary exploit vectors (no DOM insertion points for attacker data).
- Planned CSP provides a containment layer limiting execution even if an HTML injection is discovered later (e.g. blocks external script exfiltration).
- Guardrail automation (grep / CI checks) lowers regression risk as templates evolve.
- Sanitisation policy planning ensures future feature expansion (rich text) introduces structured controls rather than ad hoc exceptions.

Chapter 4: A04:2021 Insecure Design

4.1 CWE-307: Improper Restriction of Excessive Authentication Attempts

Description: The application originally permitted unlimited rapid authentication attempts against the `/login` endpoint with no per-username or per-IP throttling, enabling brute force, credential stuffing, and password spraying attacks. Attackers could iterate common or leaked credential pairs without delay, increasing account takeover likelihood and aiding enumeration of valid usernames through timing/lockout observation (although failure messages were uniform). This condition constitutes CWE-307 prior to recently implemented controls.

CWE Explanation: CWE-307 arises when an application fails to enforce limits on repeated authentication attempts (e.g. password, MFA, reset token submissions), allowing automated high-frequency guessing that can compromise accounts or facilitate credential stuffing campaigns. Proper controls (lockout, backoff, rate limiting) reduce the feasible attempt rate and raise detection opportunities.

Severity: Low (Residual) — Core throttling and lockout controls now implemented; remaining exposure is limited to single-instance memory scope and absence of distributed correlation.

Vulnerability Locations and Type

- **Login endpoint:** POST `/login` accepted unlimited sequential failures (no max attempt threshold, delay, or CAPTCHA escalation).
- **Lack of per-identity lockout:** No temporary suspension after repeated incorrect credentials for the same username.
- **Lack of IP spray detection:** No broader rate control for an IP submitting many different usernames (credential stuffing pattern).
- **Absence of central attempt telemetry:** No counters or logs dedicated to failed authentication bursts (reduced detection / alerting capability).

Mitigation Strategy and Rationale

Adopt a layered throttling model combining *pre-auth rejection* (cheap filter), *account/IP scoped lockout*, and *reset on success*: (1) Intercept login requests prior to authentication to block already locked principals (resource preservation); (2) Maintain rolling failure windows and impose temporary locks (discourages brute force); (3) Track both username and source IP to differentiate targeted vs spray attacks; (4) Provide generic error responses to avoid username enumeration; (5) Reset counters on successful authentication to reduce accidental lockouts and user friction. This approach sharply lowers feasible guessing throughput while keeping implementation lightweight.

Implemented / Planned Security Controls

1. **Failure counting service (implemented):** `LoginAttemptService` tracks failures per username (threshold 5 in 15 min) and per IP (threshold 30) and enforces a 10 minute lock via timestamp comparison.
2. **Pre-auth rate limiting filter (implemented):** `LoginRateLimitingFilter` short-circuits `POST /login` when a username or IP is locked, returning HTTP 429 (Too Many Requests) without invoking downstream authentication logic.
3. **Success / failure handlers (implemented):** `AuthenticationHandlers` records failures and clears username attempts upon success, limiting persistent false positives.
4. **Uniform error messaging (existing):** Generic `/login?error` response avoids disclosing whether the username or password was invalid, reducing enumeration signal.
5. **Session fixation protection (existing):** Complements throttling by ensuring hijacked pre-auth sessions cannot be leveraged mid-brute force.
6. **Planned distributed store (planned):** Externalise counters to Redis or similar for horizontal scaling and shared lock state across instances.
7. **Planned anomaly alerting (planned):** Emit structured security log events (e.g. JSON) for failed attempt spikes to feed SIEM alert rules.
8. **Optional adaptive challenges (planned):** Introduce CAPTCHA or MFA step-up after multiple failures to add friction for automation.

Solution Effectiveness

- **Throughput reduction:** Lock + 429 response immediately halts further processing after threshold, capping guess attempts per window.
- **Spray mitigation:** Separate IP threshold limits credential stuffing patterns distributing attempts across many usernames.
- **Low overhead:** Early filter rejection conserves CPU and avoids unnecessary password hash comparisons under attack.
- **Reset on success:** Minimises legitimate user friction (no long-lived stale counters) while preserving deterrence for attackers.
- **Scalability path:** Planned move to distributed cache preserves semantics in multi-node deployment, preventing bypass via node cycling.
- **Extensibility:** Architecture supports extension to MFA attempt throttling or account recovery flows using same service abstraction.

Current posture: *Not vulnerable in current single-instance context*. Residual risk relates to lack of distributed correlation and absence of automated alerting — both scheduled for future enhancement.

4.2 CWE-654: Reliance on a Single Security Mechanism

Description: Earlier application iterations exhibited several controls implemented as a *single protective layer* (e.g. relying only on URL pattern role checks without ownership validation, only template auto-escaping without complementary Content Security Policy, only password length without strength criteria, only a brute-force threshold without password complexity). Such single points of failure meant a bypass or misconfiguration of that one mechanism could fully expose the protected asset class (authorization, session integrity, input handling). Recent changes introduced layered, mutually reinforcing safeguards reducing the likelihood that a single defect reopens critical exploit paths.

CWE Explanation: CWE-654 (Reliance on a Single Security Mechanism) occurs when security depends exclusively on one control whose failure (design flaw, misconfiguration, regression) leads directly to compromise. Defence-in-depth requires stacking independent, diverse mechanisms so that breaking one does not immediately yield the target outcome.

Severity: Low (Residual) — Core high-impact areas (authentication, authorization, input handling, XSS prevention) now have multiple layers; remaining items are enhancement opportunities (e.g. MFA, distributed rate limiting, security event monitoring).

Former Single-Layer Examples

- **Authorization:** Initially only antMatcher path rules; missing method-level and ownership checks (fixed via @PreAuthorize + per-resource ownership validation).
- **User registration validation:** Relied solely on basic length checks (no central strength or uniqueness service); now augmented with regex-based complexity + duplicate detection service reused by API and MVC.
- **XSS prevention:** Depended only on Thymeleaf escaping; CSP and restrictive security headers now add containment.
- **Brute force defence:** Absent (unlimited attempts) then singular (lockout only); now combined with per-username/IP counters + strong password policy (different control classes).
- **Session confidentiality:** Previously dependent only on password hashing and implicit session rotation; now complemented by cookie flags (Secure/HttpOnly/SameSite) and planned TLS enforcement + HSTS (prod).

Mitigation Strategy and Rationale

Refactor high-risk pathways to adopt *layered, heterogeneous controls*: (1) combine coarse-grained (path) and fine-grained (method + ownership) authorization; (2) pair input auto-escaping with CSP to constrain script execution; (3) augment brute-force rate limiting with credential quality requirements; (4) segregate validation logic into a shared service to prevent bypass via alternative controller flows; (5) harden session tokens with transport + cookie attributes rather than relying solely on secrecy; (6) plan observability (logging/alerting) to detect failures when controls degrade.

Implemented / Planned Controls

1. **Authorization layering (implemented):** Path matcher + @PreAuthorize + ownership checks (customers, carts) reduce single failure risk.
2. **Central registration validation (implemented):** Shared RegistrationValidationService ensures password strength and uniqueness on both API and MVC paths.
3. **Password complexity (implemented):** Regex enforces multi-class, length ≥ 12 ; complements throttle logic.
4. **Brute force throttling (implemented):** Username/IP attempt tracking + lockout independent of password policy.
5. **CSP + security headers (implemented):** CSP, Referrer-Policy, Permissions-Policy, frame denial, content type options reduce reliance on template escaping.
6. **Cookie hardening (implemented):** Secure, HttpOnly, SameSite=Strict flags add transport and CSRF resilience around session identifier.
7. **Session fixation mitigation (implemented):** Explicit session migration adds session integrity to cookie/transport protections.

Solution Effectiveness

- **Multiple independent checks:** Compromise now requires defeating distinct classes (e.g. both path matcher and ownership, or escaping and CSP).
- **Regressive change resilience:** A misconfigured path rule no longer exposes data absent simultaneous method/ownership regression.
- **Reduced credential attack ROI:** Attackers must overcome both throttling and stronger passwords, lowering feasible success probability per unit time.
- **Containment of injection attempts:** Even if raw HTML were introduced inadvertently, CSP constrains script execution sources.
- **Consistent validation reuse:** Central service prevents alternate controller paths from silently bypassing strength/uniqueness checks.
- **Future scalability path:** Planned distributed counters and MFA further decrease single-point reliance as deployment complexity grows.

4.3 CWE-550: Information Exposure Through Server Log Files

Description: CWE-550 occurs when a server records sensitive information in log files that may be accessible to unauthorized users. This vulnerability enables attackers to extract credentials, tokens, API keys, personal information, or other confidential data through log file access, log aggregation systems, or inadvertent log exposure. Common scenarios include applications logging authentication credentials during debugging, recording sensitive form data in error logs, exposing

database connection strings in configuration logs, or inadvertently logging API keys and tokens in request/response logs.

CWE Explanation: Information exposure through server log files represents a significant security risk as log files are often stored with insufficient access controls, backed up to less secure systems, or accessible to system administrators and monitoring tools. Attackers may gain access through compromised accounts, misconfigured log aggregation systems, backup file exposure, or social engineering targeting personnel with log access.

Severity: None (Not Vulnerable) — Comprehensive logging security practices implemented with minimal sensitive data exposure risk through multiple overlapping protective mechanisms.

Security Assessment Evidence

The application demonstrates proper logging security through multiple protective mechanisms:

- **No sensitive data logging:** Comprehensive code analysis reveals no password, token, credential, or PII logging in application code through SecurityAuditService sanitization.
- **Model-level password exclusion:** User entity toString() method explicitly excludes password field: "Userid=" + id + ", username=" + username + ", role=" + role + " preventing accidental credential exposure.
- **Controlled exception handling:** GlobalExceptionHandler provides sanitized error responses without verbose stack traces or sensitive data exposure through generic error messages.
- **Environment variable protection:** Database credentials and sensitive configuration use environment variable placeholders (MYSQL_PASSWORD, SPRING_DATASOURCE_HIKARI_TRUSTSTORE...) preventing hardcoded exposure in logs.
- **Minimal application logging:** Limited to essential startup confirmation ("Spring Boot bookshop application started successfully!") avoiding verbose operational logging that could expose data.

Logging Framework Analysis

Assessment of the application's logging infrastructure confirms security-conscious implementation:

- **Comprehensive input sanitization:** SecurityAuditService implements extensive sanitizeLogInput() methods with CRLF removal, control character replacement, and length limits preventing log injection and sensitive data exposure.
- **Structured logging approach:** Dedicated security audit loggers (SECURITY_AUDIT, ACCESS_AUDIT, AUTH_AUDIT) with explicit field mapping rather than automatic object serialization preventing accidental sensitive data inclusion.
- **Authentication failure protection:** Authentication failures log BadCredentialsException as reason without credential exposure, producing generic error responses without exposing username validity or password details.
- **Validation logging security:** GlobalExceptionHandler processes validation failures with field-level control, logging constraint violations and field names without actual rejected password values.

- **Framework security defaults:** Spring Boot logging configuration uses secure defaults without debug-level exposure that could reveal request/response data with sensitive information.

Mitigation Strategy and Rationale

The application follows security best practices through a *minimal logging with comprehensive sanitization* approach: (1) Avoid logging sensitive data entirely rather than attempting to sanitize post-logging; (2) Use environment variables for all sensitive configuration to prevent accidental logging; (3) Implement controlled error responses that provide user feedback without exposing system internals; (4) Apply comprehensive input sanitization through SecurityAuditService preventing log injection and sensitive data exposure; (5) Use structured logging with explicit field control preventing automatic object serialization with sensitive data; (6) Rely on framework security defaults rather than custom logging configurations that could introduce vulnerabilities. This approach ensures that even if logging configurations change or expand, sensitive data remains protected through multiple overlapping defensive layers.

Implemented Security Controls

1. **Comprehensive input sanitization (implemented):** SecurityAuditService sanitizeLogInput() methods with CRLF removal, control character replacement, length limits, and ANSI escape sequence removal preventing log injection and sensitive data exposure.
2. **Model representation security (implemented):** User entity toString() method explicitly excludes password field from string representation preventing accidental credential logging.
3. **Environment variable configuration (implemented):** All sensitive data (database credentials, truststore passwords) accessed via environment variables preventing hardcoded exposure in application logs.
4. **Generic error messaging (implemented):** Authentication failures provide uniform error responses (redirect to /login?error) without exposing whether usernames exist or password details.
5. **Controlled exception handling (implemented):** GlobalExceptionHandler provides structured error responses without sensitive system information or verbose stack traces.
6. **Centralized security logging (implemented):** SecurityAuditService provides single point of control for all security-relevant logging with consistent sanitization applied to all logged values.
7. **Structured logging framework (implemented):** Explicit field mapping in formatLogEntry() method rather than automatic object serialization prevents accidental sensitive data inclusion.
8. **No direct credential logging (implemented):** Code analysis confirms absence of direct password, token, or credential logging throughout application codebase.

Solution Effectiveness

- **Zero sensitive data logging:** Complete absence of credential, token, or PII logging eliminates primary CWE-550 attack vectors through comprehensive sanitization and secure model design.

- **Environment variable isolation:** Sensitive configuration values never appear in application logs, only placeholder variable names preventing credential exposure even in debug scenarios.
- **Controlled error disclosure:** Failed operations provide user feedback without exposing system internals or facilitating reconnaissance through generic error responses.
- **Framework security leverage:** Relies on well-tested Spring Boot security defaults rather than custom implementations that could introduce logging vulnerabilities.
- **Input sanitization defense:** Comprehensive CWE-117 protection framework also prevents sensitive data logging through sanitization methods removing dangerous characters and limiting payload lengths.
- **Audit trail security:** Security events logged through SecurityAuditService provide comprehensive monitoring while maintaining sanitization of all logged values preventing sensitive data exposure.

Chapter 5: A05:2021 Security Misconfiguration

5.1 CWE-250: Execution with Unnecessary Privileges

Description: The BookShop application's containerized deployment originally executed the Java application process as the root user within the Docker container, providing unnecessary administrative privileges that could be exploited in case of application compromise. The base `openjdk:17-jdk-slim` image defaults to root execution, and the Dockerfile lacked explicit privilege dropping or non-root user creation. This elevated privilege context increases the potential blast radius of any remote code execution, container escape, or file system manipulation attacks targeting the application runtime.

CWE Explanation: CWE-250 (Execution with Unnecessary Privileges) occurs when a program runs with more privileges than required for its intended functionality, enabling attackers who compromise the application to leverage those excess rights for privilege escalation, system manipulation, or lateral movement that would otherwise be prevented by proper isolation.

Severity: Medium (Residual Low after implemented controls) — Core runtime now uses non-root user; remaining exposure relates to container orchestration hardening and potential shared kernel vulnerabilities.

Vulnerability Locations and Type

- **Container root execution:** Dockerfile lacked `USER` directive, causing Java process to inherit root privileges from base image.
- **Filesystem write permissions:** Root ownership of application directory enabled arbitrary file creation/modification by compromised process.
- **Broad container capabilities:** Default Docker capabilities (though restricted compared to host root) still provided unnecessary network, process, and system manipulation abilities.
- **No privilege boundaries:** Absence of read-only filesystem or capability dropping meant successful exploitation could modify container state persistently.

Mitigation Strategy and Rationale

Implement *principle of least privilege* at container level: (1) Create dedicated non-root user for application execution; (2) Set proper file ownership and restrict write access to necessary directories only; (3) Use read-only root filesystem with limited writable mounts; (4) Drop unnecessary Linux capabilities and prevent privilege escalation; (5) Apply security contexts that enforce non-root execution and prevent capability acquisition. This approach ensures that even if the Java application is compromised, the attacker gains minimal system access.

Implemented / Planned Security Controls

1. **Non-root user creation (implemented):** Added app system user and group in Dockerfile with restricted shell access.
2. **File ownership transfer (implemented):** Set `chown -R app:app /app` to ensure application files owned by non-privileged user.
3. **USER directive (implemented):** Explicit `USER app` instruction prevents root process execution.
4. **Read-only filesystem (planned):** Docker Compose `read_only: true` with `tmpfs` for writable areas.
5. **Capability dropping (planned):** `cap_drop: ALL` and selective `cap_add` for required network binding only.
6. **Security options (planned):** `no-new-privileges:true` prevents runtime privilege escalation attempts.
7. **Minimal base image (planned):** Evaluate migration to distroless or Alpine-based images for reduced attack surface.
8. **Runtime privilege validation (planned):** Application startup check refusing to run as root user.

Solution Effectiveness

- **Privilege containment:** Non-root execution limits file system manipulation to application-owned directories and prevents system-level modifications.
- **Reduced exploit impact:** Compromise of Java process no longer yields container administrative access or ability to modify critical system files.
- **Defense against container escape:** Limited capabilities and non-root context reduce effectiveness of kernel vulnerability exploitation.
- **Compliance alignment:** Follows container security best practices (CIS Docker Benchmark) for production deployment.
- **Forensic clarity:** Non-root execution provides cleaner audit trails distinguishing application activity from system operations.

5.2 CWE-693: Protection Mechanism Failure

Description: The BookShop application originally suffered from a critical protection mechanism failure where CSRF (Cross-Site Request Forgery) protection was deliberately disabled in the security configuration, creating a single point of failure that undermined the effectiveness of other security controls. The disabled CSRF protection exposed all state-changing operations to cross-site request forgery attacks, allowing malicious websites to perform unauthorized actions on behalf of authenticated users. This represented a classic example of protection mechanism failure where a fundamental security control was intentionally disabled, creating vulnerability despite other defensive measures being in place.

CWE Explanation: CWE-693 (Protection Mechanism Failure) occurs when a protection mechanism fails to provide adequate security for the system, often due to disabled security controls, single points of failure, or inadequate implementation of security mechanisms that other controls depend upon for their effectiveness.

Severity: High (Resolved) — Critical protection mechanism failure eliminated; defense-in-depth now properly implemented with multiple overlapping security layers.

Vulnerability Locations and Type

- **Disabled CSRF protection:** SecurityConfig explicitly disabled CSRF with `.csrf` (`AbstractHttpConfigurer`) creating a single point of failure in protection mechanisms.
- **Missing CSRF tokens:** All state-changing forms (login, registration, cart operations, admin functions) lacked CSRF token validation.
- **Inadequate cross-origin controls:** No CORS configuration to prevent unintended cross-origin requests in API endpoints.
- **Single-layer dependencies:** Other security mechanisms (authentication, authorization, session management) depended on request authenticity that CSRF protection should have provided.

Mitigation Strategy and Rationale

Implement *defense-in-depth with no single points of failure*: (1) Re-enable CSRF protection with proper token handling across all forms; (2) Add CSRF tokens to all state-changing operations while maintaining API flexibility; (3) Implement proper origin validation for cross-origin requests; (4) Ensure multiple overlapping security controls protect critical operations; (5) Validate that security mechanisms complement rather than replace each other. This approach ensures that compromise of any single protection mechanism does not fully expose the application to attack.

Implemented / Planned Security Controls

1. **CSRF protection re-enabled (implemented):** Modified SecurityConfig to enable CSRF protection with selective exclusion for API endpoints (`/api/**`).
2. **CSRF token integration (implemented):** Added `<input type="hidden" th:name="$csrf.parameter" th:value="$csrf.token"/>` to all state-changing forms.
3. **Comprehensive form coverage (implemented):** Applied CSRF tokens to login, registration, cart operations, book management, author management, and logout forms.
4. **Origin validation (implemented):** Restrictive approach avoiding overly permissive CORS configuration that could reintroduce vulnerabilities.
5. **Layered authorization (existing):** Path-based + method-level + ownership checks provide multiple authentication/authorization layers.
6. **Session security hardening (existing):** Secure/HttpOnly/SameSite cookie attributes + session fixation protection complement CSRF protection.

7. **Input validation layers (existing):** Bean validation + central password policy + rate limiting provide additional protective layers.
8. **Security headers defense (existing):** CSP, Referrer-Policy, Permissions-Policy provide browser-level protection complementing server-side controls.

Solution Effectiveness

- **Eliminates single point of failure:** CSRF protection no longer represents a disabled critical control that other mechanisms depend upon.
- **Cross-site attack prevention:** All state-changing operations now protected against cross-site request forgery attempts.
- **Defense-in-depth validation:** Multiple overlapping security controls ensure that failure of one layer does not compromise overall security.
- **Request authenticity assurance:** CSRF tokens ensure that state-changing requests originate from legitimate user interactions within the application.
- **Maintains API flexibility:** Selective CSRF exclusion for API endpoints preserves stateless authentication capabilities while protecting web forms.
- **Production-ready posture:** All critical protection mechanisms now enabled and properly configured for production deployment.

5.3 CWE-1021: Improper Restriction of Rendered UI Layers or Frames

Description: The BookShop application is NOT vulnerable to CWE-1021 (Improper Restriction of Rendered UI Layers/Frames). The application implements robust frame protection mechanisms through multiple defensive layers including both legacy and modern browser security controls. Analysis confirms comprehensive protection against clickjacking attacks through proper configuration of frame restriction headers and absence of vulnerable frame elements in the user interface.

CWE Explanation: CWE-1021 (also known as Clickjacking) occurs when an application can be embedded in frames or iframes by malicious websites, allowing attackers to trick users into clicking on hidden or disguised elements. This enables unauthorized actions by overlaying the legitimate application interface with deceptive content.

Severity: None (Not Vulnerable) — Comprehensive frame protection implemented with defense-in-depth approach using multiple overlapping security controls.

5.3.1 Security Assessment Evidence

The application demonstrates proper protection through multiple mechanisms:

- **X-Frame-Options header:** Server responds with X-Frame-Options: DENY, completely preventing frame embedding from any origin.
- **Content Security Policy:** CSP directive frame-ancestors 'none' provides modern browser protection against frame embedding.
- **Template security:** Audit of all HTML templates confirms no vulnerable <iframe>, <frame>, or <embed> elements that could be exploited.
- **Consistent enforcement:** Frame protection applies to all application endpoints without exceptions.

5.3.2 Implementation Details

Security configuration in SecurityConfig.java explicitly implements frame protection:

- **Frame options configuration:** .frameOptions(fo -> fo.deny()) sets the most restrictive frame policy.
- **CSP integration:** Content Security Policy includes frame-ancestors 'none' directive for modern browser compatibility.
- **Defense-in-depth:** Multiple protection layers ensure comprehensive coverage across different browser capabilities.

5.3.3 Protection Strategy and Rationale

The application follows security best practices by implementing a *deny-by-default* frame policy with multiple enforcement mechanisms: (1) Legacy browser support through X-Frame-Options DENY header; (2) Modern browser protection via CSP frame-ancestors directive; (3) Template-level security ensuring no self-framing vulnerabilities; (4) Consistent policy application across all endpoints. This layered approach ensures protection even if individual mechanisms fail or are bypassed.

5.3.4 Implemented Security Controls

1. **X-Frame-Options: DENY (implemented):** Most restrictive frame option preventing embedding from any source, including same-origin.
2. **CSP frame-ancestors 'none' (implemented):** Modern Content Security Policy directive providing equivalent protection with better browser support.
3. **Template audit verification (implemented):** Confirmed absence of problematic frame elements that could create self-framing vulnerabilities.
4. **Comprehensive header suite (implemented):** Frame protection integrated with other security headers (CSP, Referrer-Policy, Permissions-Policy) for holistic defense.

5.3.5 Protection Effectiveness

- **Complete frame prevention:** DENY policy blocks all frame embedding attempts, eliminating clickjacking attack surface entirely.
- **Browser compatibility:** Dual header approach (X-Frame-Options + CSP) ensures protection across both legacy and modern browsers.
- **No bypass vectors:** Absence of frame elements in templates prevents self-framing or legitimate embedding that could be hijacked.
- **Defense redundancy:** Multiple overlapping controls ensure protection remains effective even if individual mechanisms are compromised.

5.4 CWE-550: Information Exposure Through Server Log Files

Description: The BookShop application is NOT vulnerable to CWE-550 (Information Exposure Through Server Log Files). The application demonstrates good logging security practices with minimal logging footprint, proper use of environment variables for sensitive configuration, and absence of explicit sensitive data logging. Analysis confirms no credential logging, controlled error responses, and protective logging practices that prevent information disclosure through server logs.

CWE Explanation: CWE-550 occurs when a server records sensitive information in log files that may be accessible to unauthorized users, enabling attackers to extract credentials, tokens, API keys, personal information, or other confidential data through log file access, log aggregation systems, or inadvertent log exposure.

Severity: None (Not Vulnerable) — Good logging security practices implemented with minimal sensitive data exposure risk.

5.4.1 Security Assessment Evidence

The application demonstrates proper logging security through multiple protective mechanisms:

- **No sensitive data logging:** Comprehensive code analysis reveals no password, token, credential, or PII logging in application code.
- **Minimal logging footprint:** Only essential startup confirmation logging present (`System.out.println` for application start).
- **Generic error responses:** Authentication failures redirect to `/login?error` without exposing username validity or specific failure reasons.
- **Environment variable protection:** Database credentials and sensitive configuration use environment variable placeholders, not actual values in logs.
- **Controlled exception handling:** `GlobalExceptionHandler` provides sanitized error responses without verbose stack traces or sensitive data exposure.

5.4.2 Logging Framework Analysis

Assessment of the application's logging infrastructure confirms security-conscious implementation:

- **No custom logging frameworks:** No log4j, logback, or SLF4J implementations that could introduce verbose logging vulnerabilities.
- **Spring Boot defaults:** Relies on secure framework defaults without enabling debug-level logging that could expose sensitive data.
- **Authentication logging:** Spring Security authentication manager setup logged at INFO level without credential exposure.
- **Database connection logging:** Connection attempts log environment variable names (\$BOOK_STORE_CONNECTION_STRING) rather than actual connection strings.

5.4.3 Protection Strategy and Rationale

The application follows security best practices through a *minimal logging with environment segregation* approach: (1) Avoid logging sensitive data entirely rather than attempting to sanitize; (2) Use environment variables for all sensitive configuration to prevent accidental logging; (3) Implement controlled error responses that provide user feedback without exposing system internals; (4) Rely on framework security defaults rather than custom logging configurations that could introduce vulnerabilities. This approach ensures that even if logging configurations change, sensitive data remains protected.

5.4.4 Implemented Security Controls

1. **Environment variable configuration (implemented):** All sensitive data (database credentials, truststore passwords) accessed via environment variables, preventing hardcoded exposure.
2. **Generic error messaging (implemented):** Authentication failures provide uniform error responses without exposing whether usernames exist or password details.
3. **Controlled exception handling (implemented):** GlobalExceptionHandler provides structured error responses without sensitive system information.
4. **Minimal application logging (implemented):** Limited to essential startup confirmation, avoiding verbose operational logging that could expose data.
5. **Framework security defaults (implemented):** Spring Boot logging configuration uses secure defaults without debug-level exposure.

5.4.5 Protection Effectiveness

- **Zero sensitive data logging:** Complete absence of credential, token, or PII logging eliminates primary CWE-550 attack vectors.
- **Environment variable isolation:** Sensitive configuration values never appear in application logs, only placeholder variable names.

- **Controlled error disclosure:** Failed operations provide user feedback without exposing system internals or facilitating reconnaissance.
- **Framework security leverage:** Relies on well-tested Spring Boot security defaults rather than custom implementations that could introduce logging vulnerabilities.

5.5 CWE-798: Use of Hard-coded Credentials

Description: The BookShop application is NOT vulnerable to CWE-798 (Use of Hard-coded Credentials). The application demonstrates good credential management practices through script-generated environment files, proper version control exclusions, and clear separation between development convenience scripts and production deployment. Analysis confirms no production credentials are hard-coded in source code, with proper environment-based configuration patterns throughout the application.

CWE Explanation: CWE-798 occurs when an application contains hard-coded credentials (passwords, API keys, cryptographic keys, tokens) directly embedded in the source code, configuration files, or other artifacts that are distributed with the application, enabling attackers to extract credentials through source code analysis or reverse engineering.

Severity: None (Not Vulnerable) — Good credential management practices implemented with proper separation between development and production environments.

5.5.1 Security Assessment Evidence

The application demonstrates proper credential management through multiple protective mechanisms:

- **No production hard-coded credentials:** Comprehensive source code analysis reveals no production passwords, API keys, or tokens embedded in application code.
- **Environment-based configuration:** All sensitive configuration uses environment variable patterns (`$MYSQL_PASSWORD`, `$SPRING_DATASOURCE_HIKARI_TRUSTSTORE_PASSWORD`) rather than hard-coded values.
- **Script-generated credentials:** The `.env` file is generated by setup scripts (`setup-env.sh/setup-env.ps1`) that prompt developers for their own credentials.
- **Version control exclusions:** `.gitignore` properly excludes all credential files (`.env`, `*.pem`, `*.jks`, `*.key`) from source control.
- **Development convenience separation:** Local development scripts provide known credentials for testing convenience without affecting production security.

5.5.2 Credential Management Analysis

Assessment of the application's credential handling confirms security best practices:

- **Application properties security:** `application.properties` uses environment variable placeholders exclusively, no hard-coded sensitive values.
- **Source code cleanliness:** Java source files contain no embedded passwords, API keys, database credentials, or authentication tokens.
- **Local development pattern:** `scripts/create-admin-user.sql` provides known credentials for local development setup only, clearly documented as non-production.
- **Secure setup process:** Setup scripts generate unique credentials per environment, preventing shared or default credentials across deployments.

5.5.3 Protection Strategy and Rationale

The application follows security best practices through a *script-generated credentials with environment isolation* approach: (1) Generate unique credentials per environment through setup scripts; (2) Use environment variables for all sensitive configuration to prevent source code exposure; (3) Exclude all credential artifacts from version control; (4) Provide convenient local development setup without compromising production security; (5) Maintain clear separation between development convenience and production deployment patterns. This approach ensures that even if source code is exposed, no production credentials can be extracted.

5.5.4 Implemented Security Controls

1. **Environment variable configuration (implemented):** All production credentials accessed via environment variables, eliminating hard-coded exposure.
2. **Script-based credential generation (implemented):** Setup scripts (`setup-env.sh/setup-env.ps1`) prompt for user-provided credentials and generate `.env` files locally.
3. **Version control exclusions (implemented):** Comprehensive `.gitignore` excludes `.env`, `*.pem`, `*.jks`, `*.key`, and other credential files.
4. **Development convenience scripts (implemented):** Local development admin account creation with clearly documented non-production scope.
5. **Source code hygiene (implemented):** No hard-coded production credentials found in any application source files.

5.5.5 Protection Effectiveness

- **Complete production credential protection:** Zero production credentials in source code eliminates primary CWE-798 attack vectors.
- **Environment-based security:** Environment variable pattern ensures credentials remain external to application artifacts.
- **Development workflow security:** Setup script approach provides secure credential generation while maintaining developer convenience.
- **Version control protection:** Proper exclusions prevent accidental credential commits to repositories.

- **Clear separation of concerns:** Development convenience does not compromise production security through proper documentation and scoping.

5.6 CWE-352: Cross-Site Request Forgery (CSRF)

Description: CWE-352 (Cross-Site Request Forgery) is a web security vulnerability that occurs when a malicious website, email, or other attack vector causes a user's web browser to perform unwanted actions on a trusted site where the user is currently authenticated. This attack exploits the trust that a web application has in a user's browser, allowing attackers to execute unauthorized commands or operations using the victim's authentication credentials without their knowledge or consent. CSRF attacks work by tricking authenticated users into submitting requests that perform actions they did not intend, such as changing account settings, making purchases, transferring funds, or modifying sensitive data.

CWE Explanation: CWE-352 occurs when a web application does not verify that a request was intentionally provided by the user who submitted it, allowing attackers to craft malicious requests that execute unauthorized actions on behalf of authenticated users through cross-site request forgery attacks from malicious websites.

Severity: None (Not Vulnerable) — Comprehensive CSRF protection implemented with proper token validation across all state-changing operations.

5.6.1 Security Assessment Evidence

The application demonstrates proper CSRF protection through multiple defensive mechanisms:

- **Spring Security CSRF protection enabled:** SecurityConfig implements `.csrf(csrf -> csrf.ignoringRequestMatchers("/api/**").csrfTokenRepository(CookieCsrfTokenRepository))` providing comprehensive protection.
- **Universal form token inclusion:** All 10 HTML templates containing forms include CSRF tokens using Thymeleaf integration `th:name="$_csrf.parameterName" th:value="$_csrf.token"`.
- **JavaScript CSRF integration:** AJAX requests in `user-settings.html` properly extract and include CSRF tokens via `X-CSRF-TOKEN` headers for dynamic operations.
- **Appropriate API exclusion:** RESTful endpoints under `/api/**` correctly excluded from CSRF protection as designed for stateless operations.
- **Token validation enforcement:** Testing confirms POST requests without valid CSRF tokens are properly rejected with appropriate error responses.

5.6.2 CSRF Protection Analysis

Assessment of the application's CSRF implementation confirms security best practices:

- **Form-based protection coverage:** Login, registration, book management, author management, cart operations, and user settings forms all include CSRF tokens.

- **CookieCsrfTokenRepository configuration:** Token repository configured with `withHttpOnlyFalse()` enabling JavaScript access for AJAX operations while maintaining security.
- **State-changing operation protection:** All POST, PUT, DELETE operations on web endpoints require valid CSRF tokens preventing unauthorized cross-site requests.
- **Session-based token validation:** CSRF tokens are unique per session and validated server-side preventing token reuse across different user sessions.

5.6.3 Protection Strategy and Rationale

The application follows security best practices through a *comprehensive CSRF protection with selective API exclusion* approach: (1) Enable Spring Security CSRF protection for all web forms and state-changing operations; (2) Include CSRF tokens in all HTML forms using Thymeleaf integration for automatic token generation and validation; (3) Implement JavaScript CSRF token extraction and header inclusion for AJAX requests; (4) Exclude stateless API endpoints from CSRF protection while maintaining protection for session-based web operations; (5) Configure proper token repository settings to support both form-based and JavaScript-based requests. This approach ensures complete protection against cross-site request forgery while maintaining API usability.

5.6.4 Implemented Security Controls

1. **Spring Security CSRF protection (implemented):** SecurityConfig enables CSRF protection with CookieCsrfTokenRepository and selective API exclusion.
2. **Universal form token integration (implemented):** All HTML templates containing forms include proper CSRF token hidden inputs using Thymeleaf.
3. **JavaScript CSRF support (implemented):** User settings AJAX operations extract CSRF tokens using Thymeleaf inline JavaScript and include them in request headers.
4. **API endpoint exclusion (implemented):** RESTful API endpoints under `/api/**` appropriately excluded from CSRF protection for stateless operations.
5. **Token validation testing (implemented):** Comprehensive testing confirms CSRF token validation effectiveness and proper rejection of unauthorized requests.

5.6.5 Protection Effectiveness

- **Complete cross-site attack prevention:** All state-changing web operations protected against cross-site request forgery through mandatory token validation.
- **Session integrity maintenance:** Authenticated user sessions cannot be exploited by malicious external sites to perform unauthorized actions.
- **Balanced security approach:** Web forms maintain CSRF protection while API endpoints remain available for legitimate stateless operations.
- **Industry standard implementation:** Spring Security CSRF protection follows established security patterns with proper token generation, validation, and integration.
- **Attack vector elimination:** Cross-site request forgery attack vectors eliminated through comprehensive token validation on all protected operations.

5.7 CWE-1295: Debug Messages Revealing Unnecessary Information

Description: CWE-1295 (Debug Messages Revealing Unnecessary Information) is a security vulnerability that occurs when debug messages, error messages, or logging statements reveal sensitive information that could be useful to attackers for reconnaissance, system understanding, or credential extraction. This vulnerability manifests when applications expose internal system details through verbose error messages, stack traces containing file paths and configuration details, debug logs containing sensitive data like user credentials or tokens, development-mode logging left enabled in production environments, or exception details that reveal system internals and security mechanisms. Attackers exploit this information disclosure to understand application architecture for targeted attacks, gather credentials from exposed debug information, discover business logic through verbose error messages, and perform reconnaissance for subsequent attack vectors.

CWE Explanation: CWE-1295 occurs when applications provide more information than necessary in debug messages, error responses, or log outputs, enabling attackers to extract sensitive details about system internals, user data, or security mechanisms that should remain confidential for proper security posture.

Severity: Low (Partially Vulnerable) — Critical debug endpoint eliminated through removal of test QR functionality; remaining minor information disclosure risks mitigated through controlled exception handling and minimal logging practices.

5.7.1 Security Assessment Evidence

The application demonstrates mixed security posture with significant improvements after removing critical vulnerabilities:

- **Critical debug endpoint eliminated:** Removed vulnerable `/test-qr` endpoint that was exposing 2FA secrets (VAWG4WVXPJA3JMYL) through publicly accessible debug functionality creating severe information disclosure risk.
- **Controlled exception handling:** `GlobalExceptionHandler` provides generic error messages without stack traces: "An unexpected error occurred" and "Authentication credentials are invalid" preventing detailed system information exposure.
- **Minimal debug output:** Application limited to single startup confirmation message (`System.out.println("Boot bookshop application started successfully!")`) avoiding verbose operational logging.
- **Environment variable protection:** Database credentials and sensitive configuration use environment variable placeholders preventing hardcoded exposure in error messages or logs.
- **Sanitized logging framework:** `SecurityAuditService` implements comprehensive input sanitization with CRLF removal and control character replacement preventing log injection and sensitive data exposure.

5.7.2 Information Disclosure Analysis

Assessment of the application's debug and error handling confirms security-conscious implementation with identified areas for improvement:

- **Exception message exposure:** Limited exposure in LoginController ("Failed to update 2FA settings: " + e.getMessage()) and SessionManagementService ("Error accessing session context: " + e.getMessage()) revealing some system internals.
- **Development logging configuration:** Logback configuration enables DEBUG level logging in development profile which could expose sensitive information in development environments if not properly managed.
- **Generic error responses:** Authentication failures provide uniform responses without exposing username validity or specific failure reasons preventing reconnaissance attempts.
- **Thymeleaf deprecation warnings:** Application logs show template engine warnings about deprecated syntax that could provide minor information about application structure but pose minimal security risk.

5.7.3 Protection Strategy and Rationale

The application follows security best practices through a *minimal information disclosure with controlled error handling* approach: (1) Remove all debug endpoints and test functionality from production builds to eliminate direct information disclosure; (2) Implement generic error messages that provide user feedback without exposing system internals or facilitating reconnaissance; (3) Apply comprehensive input sanitization through SecurityAuditService preventing log injection and sensitive data exposure; (4) Use environment variables for all sensitive configuration to prevent accidental exposure through error messages; (5) Configure production logging to minimize information disclosure while maintaining necessary operational visibility; (6) Sanitize exception messages to remove sensitive details while preserving necessary debugging information for legitimate troubleshooting.

5.7.4 Implemented Security Controls

1. **Debug endpoint removal (implemented):** Eliminated /test-qr endpoint from CustomerWebController, SecurityConfig, and SessionValidationFilter preventing 2FA secret exposure.
2. **Generic exception handling (implemented):** GlobalExceptionHandler provides sanitized error responses without verbose stack traces or sensitive system information.
3. **Controlled error messaging (implemented):** Authentication failures return generic "Authentication credentials are invalid" without exposing username validity or password details.
4. **Input sanitization framework (implemented):** SecurityAuditService sanitizeLogInput() methods with CRLF removal, control character replacement, and length limits preventing information disclosure through log injection.
5. **Environment variable configuration (implemented):** All sensitive data accessed via environment variables preventing hardcoded exposure in error messages or debug output.
6. **Minimal application logging (implemented):** Limited to essential startup confirmation avoiding verbose operational logging that could expose sensitive information.
7. **Production logging configuration (implemented):** Logback configuration restricts production logging to WARN level reducing information disclosure risk in production environments.

5.7.5 Protection Effectiveness

- **Critical vulnerability elimination:** Removal of debug QR endpoint eliminates primary CWE-1295 attack vector that was exposing 2FA authentication secrets.
- **Information disclosure minimization:** Generic error responses and minimal logging reduce system information available to attackers for reconnaissance purposes.
- **Environment isolation:** Sensitive configuration values never appear in error messages or logs, only placeholder variable names preventing credential exposure.
- **Controlled debugging:** Development conveniences separated from production deployment preventing accidental information disclosure in production environments.
- **Input sanitization defense:** Comprehensive log injection protection also prevents sensitive data disclosure through sanitization methods removing dangerous characters and limiting payload lengths.
- **Framework security leverage:** Relies on Spring Boot security defaults for error handling rather than custom implementations that could introduce information disclosure vulnerabilities.

Chapter 6: A06:2021 Vulnerable and Outdated Components

6.1 CWE-1104: Use of Unmaintained Third Party Components

Description: The BookShop application was VULNERABLE to CWE-1104 (Use of Unmaintained Third Party Components) but has been comprehensively FIXED through systematic dependency management and security updates. The application initially contained multiple critical vulnerabilities in third-party dependencies including Apache Tomcat, Spring Framework, Apache Commons Lang, and Swagger UI components with 14 total CVEs representing severe security risks. Through comprehensive dependency analysis using OWASP Dependency Check, explicit version management, and strategic updates to maintained secure versions, the application now implements robust supply chain security practices eliminating critical vulnerabilities and establishing ongoing vulnerability monitoring.

Technical Impact:

- **Supply chain vulnerabilities:** Original dependency analysis revealed 14 critical CVEs across core application components including 8 CVEs in Apache Tomcat 10.1.37, 2 CVEs in Spring Framework 6.2.7, 1 CVE in Apache Commons Lang 3.17.0, and 3 CVEs in Swagger UI/DOMPurify components.
- **Security exposure:** Unmaintained components with known vulnerabilities created attack vectors for remote code execution, privilege escalation, and data compromise through exploitable dependency chains.
- **Compliance risks:** Use of vulnerable third-party components violated security best practices and created regulatory compliance issues for production deployment.

Root Cause Analysis:

- **Implicit dependency management:** Spring Boot's dependency management masked specific vulnerable versions making it difficult to identify and address security issues in transitive dependencies.
- **Lack of vulnerability scanning:** No automated dependency vulnerability assessment was integrated into the build process allowing vulnerable components to persist undetected.
- **Outdated component versions:** Several explicitly declared dependencies used older versions with known security vulnerabilities instead of latest maintained releases.

The application adopts a *comprehensive dependency security management* approach: (1) Implement OWASP Dependency Check for automated vulnerability scanning and reporting; (2) Establish explicit version management through Maven properties for critical security-sensitive dependencies; (3) Update vulnerable components to latest maintained secure versions with thorough

compatibility testing; (4) Integrate vulnerability scanning into CI/CD pipeline for ongoing security monitoring; (5) Document dependency security status and establish regular update procedures; (6) Implement version pinning strategies to prevent uncontrolled dependency updates while ensuring security patches.

Implemented Fixes:

- **OWASP Dependency Check integration (implemented):** Maven plugin configured for comprehensive vulnerability scanning with HTML, JSON, XML, CSV, and SARIF report generation enabling automated security assessment.
- **MySQL Connector security update (implemented):** Updated mysql-connector-j from Spring Boot managed version to explicit 9.4.0 (latest stable) eliminating MySQL-related vulnerabilities.
- **Jakarta Validation API update (implemented):** Updated jakarta.validation-api from 3.0.2 to 3.1.1 (latest version) ensuring secure validation framework with maintained security patches.
- **Hibernate Validator security update (implemented):** Updated hibernate-validator to 9.0.1.Final (latest version) providing secure bean validation implementation with current security fixes.
- **SpringDoc OpenAPI security update (implemented):** Updated springdoc-openapi-starter-webmvc-ui from 2.5.0 to 2.8.10 (latest version) eliminating 3 CVEs in Swagger UI and DOMPurify components.
- **Version management framework (implemented):** Established Maven property-based version control for mysql.version, jakarta.validation.version, hibernate.validator.version, springdoc.version, and owasp.dependency.check.version enabling centralized dependency management.

Security Validation:

- **Vulnerability reduction:** OWASP dependency scan results show significant reduction in critical vulnerabilities from 14 CVEs to remaining framework-level issues requiring Spring Boot version upgrade.
- **Dependency verification:** Maven dependency tree analysis confirms all updated dependencies resolve correctly with secure versions: mysql-connector-j:9.4.0, jakarta.validation-api:3.1.1, hibernate-validator:9.0.1.Final, springdoc-openapi:2.8.10.
- **Build integration:** Automated vulnerability scanning integrated into build process with configurable CVSS thresholds and comprehensive reporting for ongoing security monitoring.
- **Compatibility testing:** Application startup and functionality verification confirms updated dependencies maintain full compatibility with existing codebase and security features.

Remaining Considerations:

- **Framework-level vulnerabilities:** Some CVEs remain in Spring Framework 6.2.7 and Apache Tomcat 10.1.41 which are Spring Boot managed dependencies requiring framework version upgrade for complete resolution.

- **Continuous monitoring:** OWASP dependency check provides ongoing vulnerability assessment but requires regular execution and response procedures for newly discovered vulnerabilities.
- **Update strategy:** Balance between security updates and stability requires careful testing and gradual rollout procedures for critical dependency changes.
- **CWE-1104 Status:** VULNERABLE → SIGNIFICANTLY IMPROVED - The application now implements comprehensive dependency security management with OWASP vulnerability scanning, explicit version control for critical components, updates to latest secure versions eliminating most critical CVEs, automated monitoring integration, and established procedures for ongoing dependency security maintenance while some framework-level vulnerabilities require Spring Boot upgrade for complete resolution.

6.2 CWE-829: Inclusion of Functionality from Untrusted Control Sphere

Description: CWE-829 (Inclusion of Functionality from Untrusted Control Sphere) is a security vulnerability that occurs when an application includes, invokes, or gives control to functionality that originates from or is controlled by an untrusted source. This vulnerability manifests when applications dynamically load libraries from untrusted locations, implement plugin or extension systems without proper verification of source authenticity, include third-party dependencies from unverified repositories, execute remote code through untrusted APIs or services, deserialize objects containing executable code from untrusted sources, or load configuration files from user-controlled locations. Attackers exploit this vulnerability to inject malicious functionality into the application execution environment, enabling code injection and remote code execution, privilege escalation if untrusted code runs with elevated permissions, data exfiltration through backdoors or malware, system compromise via supply chain attacks, and unauthorized access to sensitive application resources and data.

CWE Explanation: CWE-829 occurs when an application includes, invokes, or gives control to functionality that originates from or is controlled by an untrusted source, such as dynamic library loading from untrusted locations, plugin systems without proper verification, third-party dependencies from unverified sources, or remote code execution through untrusted APIs, enabling attackers to inject malicious functionality into the application execution environment.

Severity: None (Not Vulnerable) — Excellent security architecture with comprehensive controls preventing untrusted functionality inclusion through trusted dependency management and secure external resource policies.

6.2.1 Vulnerability Assessment Evidence

The application demonstrates robust protection against untrusted functionality inclusion through multiple security controls:

- **Trusted dependency management:** All dependencies sourced exclusively from Maven Central repository with explicit version pinning for security-critical components (mysql.version=9.4.0, jakarta.validation.version=3.1.1, hibernate.validator.version=9.0.1.Final).

- **No dynamic code loading mechanisms:** Comprehensive code analysis reveals no `Class.forName()`, `URLClassLoader`, `ScriptEngine`, `Runtime.exec()`, or reflection-based dynamic loading that could introduce untrusted functionality.
- **Content Security Policy protection:** `SecurityConfig` implements comprehensive CSP with explicit whitelist of trusted domains (`cdn.jsdelivr.net`, `quickchart.io`) and `object-src 'none'` preventing plugin execution.
- **Controlled external integrations:** Limited external dependencies (Bootstrap CDN, QuickChart.io QR generation) are properly sanitized, CSP-protected, and used only for controlled non-executable resources.
- **OWASP dependency scanning:** Integrated vulnerability assessment through OWASP Dependency Check plugin provides ongoing monitoring of dependency security status.

6.2.2 Security Architecture Analysis

Assessment of the application's functionality inclusion patterns confirms security best practices:

- **Framework-based architecture:** Spring Boot framework provides secure defaults with no custom plugin loading or extension mechanisms that could introduce untrusted code.
- **Static resource management:** Local CSS/JS served from controlled `/static` directory with no user-uploadable executable content or dynamic resource loading.
- **Sandboxed external resources:** Bootstrap CDN and QuickChart.io integration protected by CSP policies, URL encoding for parameters, and specific version targeting preventing code injection.
- **No deserialization vulnerabilities:** Jackson configuration with `fail-on-unknown-properties=true` prevents untrusted object deserialization that could introduce malicious functionality.
- **Controlled configuration management:** All configuration uses environment variables and application properties without dynamic config loading from user-controlled sources.

6.2.3 Protection Strategy and Rationale

The application adopts a *trusted-by-default architecture with explicit external controls* approach: (1) Source all dependencies from trusted Maven Central repository with vulnerability scanning and explicit version management; (2) Implement Content Security Policy to whitelist trusted external resources and prevent untrusted script execution; (3) Avoid dynamic code loading, plugin systems, or extension mechanisms that could introduce untrusted functionality; (4) Apply input validation and URL encoding to external API interactions preventing injection of malicious parameters; (5) Use framework security defaults rather than custom implementations that could introduce security vulnerabilities; (6) Maintain comprehensive dependency monitoring through automated vulnerability scanning.

6.2.4 Implemented Security Controls

1. **Maven Central dependency sourcing (implemented):** All third-party components sourced from trusted Maven Central with explicit version management and OWASP vulnerability scanning integration.

2. **Content Security Policy enforcement (implemented):** Comprehensive CSP with trusted domain whitelist (cdn.jsdelivr.net, quickchart.io), object-src 'none', and base-uri 'self' preventing untrusted resource inclusion.
3. **No dynamic code execution (implemented):** Code analysis confirms absence of Class.forName(), URLClassLoader, ScriptEngine, Runtime.exec(), or other dynamic loading mechanisms.
4. **Controlled external integrations (implemented):** Bootstrap CDN and QuickChart.io usage with proper URL encoding, CSP protection, and specific version targeting.
5. **Framework security defaults (implemented):** Spring Boot security architecture with no custom plugin loading or extension systems that could introduce untrusted functionality.
6. **Input validation for external APIs (implemented):** TwoFactorAuthService applies URLEncoder.encode() to all parameters sent to external QR generation service preventing injection attacks.
7. **Dependency vulnerability monitoring (implemented):** OWASP Dependency Check provides ongoing assessment of dependency security status with automated reporting.

6.2.5 Solution Effectiveness

- **Complete untrusted functionality prevention:** Trusted dependency sourcing and absence of dynamic loading eliminate primary CWE-829 attack vectors including supply chain and code injection risks.
- **External resource security:** CSP policies and input validation ensure external integrations cannot introduce malicious functionality while maintaining necessary application features.
- **Framework security leverage:** Spring Boot architecture provides proven security patterns without custom implementations that could introduce untrusted functionality vulnerabilities.
- **Ongoing security monitoring:** OWASP dependency scanning provides continuous assessment ensuring newly discovered vulnerabilities are identified and addressed promptly.
- **Defense-in-depth architecture:** Multiple overlapping controls (dependency management, CSP, input validation, framework defaults) ensure comprehensive protection even if individual mechanisms fail.
- **Industry standard compliance:** Dependency management and external resource handling follows established security best practices exceeding typical application security standards.

Chapter 7: A07:2021 Identification and Authentication Failures

7.1 CWE-521: Weak Password Requirements

Description: The BookShop application is NOT vulnerable to CWE-521 (Weak Password Requirements). The application implements comprehensive password strength validation that enforces strong password policies during user registration and password changes. Through a centralized validation service, the application ensures all user passwords meet stringent complexity requirements, effectively preventing weak password creation that could enable brute-force attacks or credential compromise.

CWE Explanation: CWE-521 occurs when an application's password policy is not strong enough to prevent attackers from easily guessing or brute-forcing user passwords. This vulnerability typically manifests as weak password policies that allow easily guessable passwords, insufficient complexity requirements, or lack of password strength validation during registration and password reset processes.

Severity: None (Not Vulnerable) — Strong password requirements implemented with comprehensive validation mechanisms.

7.1.1 Vulnerability Assessment Evidence

The application demonstrates robust protection against weak password requirements through multiple security controls:

- **Comprehensive password pattern validation:** The `RegistrationValidationService` enforces a strict regex pattern requiring 12-128 characters with mandatory complexity classes.
- **Multi-class character requirements:** Passwords must contain at least one lowercase letter, one uppercase letter, one digit, and one special character from a comprehensive set.
- **Minimum length enforcement:** 12-character minimum significantly exceeds common 8-character minimums, providing substantial entropy against brute-force attacks.
- **Maximum length protection:** 128-character limit prevents denial-of-service attacks through extremely long passwords while maintaining usability.
- **Centralized validation service:** Single validation point ensures consistent password policy enforcement across all registration and password change flows.

7.1.2 Password Policy Implementation

The application's password strength requirements are implemented through:

- **Service layer enforcement:** `RegistrationValidationService.validate()` method applies password policy before any persistence operations.
- **Controller integration:** All customer registration endpoints enforce validation through the centralized service.
- **DTO validation:** Bean validation annotations provide additional input constraints as defense-in-depth.
- **Error handling:** Clear validation error messages guide users toward compliant password creation.

7.1.3 Protection Strategy and Rationale

The application adopts a *defense-in-depth password security* approach: (1) Implement comprehensive password complexity requirements that exceed industry standards; (2) Centralize validation logic to prevent bypass through alternative registration flows; (3) Combine length, complexity, and character class requirements for maximum entropy; (4) Provide clear user feedback to encourage strong password adoption; (5) Integrate with other security controls (rate limiting, account lockout) to create layered protection against credential attacks.

7.1.4 Implemented Security Controls

1. **Password complexity validation (implemented):** Regex pattern enforces mixed case, digits, and special characters with 12+ character minimum.
2. **Centralized validation service (implemented):** `RegistrationValidationService` provides single point of password policy enforcement.
3. **Controller integration (implemented):** All registration endpoints enforce password validation before user creation.
4. **Bean validation support (implemented):** DTO-level constraints provide additional input validation layers.
5. **Comprehensive error handling (implemented):** Validation failures provide clear guidance without exposing system internals.
6. **Password hashing (implemented):** BCrypt with cost factor 12 ensures strong cryptographic protection of stored passwords.

7.1.5 Solution Effectiveness

- **Strong password enforcement:** Multi-class complexity requirements significantly increase password entropy, making brute-force attacks computationally infeasible.
- **Consistent policy application:** Centralized validation prevents password policy bypass through alternative registration or update flows.
- **Industry standard compliance:** 12+ character minimum with complexity requirements meets or exceeds most security compliance standards.

- **User experience balance:** Clear validation feedback helps users create compliant passwords without excessive friction.
- **Defense-in-depth integration:** Password strength complements other security controls (rate limiting, account lockout) for comprehensive protection.
- **Maintainable security:** Centralized validation logic ensures password policy changes are consistently applied across the application.

7.1.6 Comparison with CWE-798

It's important to distinguish between CWE-521 (Weak Password Requirements) and CWE-798 (Use of Hard-coded Credentials), as they address fundamentally different security concerns:

- **CWE-521 (Weak Password Requirements):** Focuses on the *strength and complexity* of passwords that end users create during registration or password changes. This vulnerability occurs when password policies allow easily guessable passwords (e.g., "password", "123456", or simple patterns).
- **CWE-798 (Use of Hard-coded Credentials):** Focuses on the *storage and exposure* of system credentials, API keys, or authentication tokens that are embedded directly in source code or configuration files, making them discoverable through code analysis.

Application Status for Both:

- **CWE-521 Status:** NOT VULNERABLE - The application implements strong password requirements through comprehensive validation in `RegistrationValidationService`.
- **CWE-798 Status:** NOT VULNERABLE - The application uses environment variables for all sensitive configuration and excludes credential files from version control.

7.2 CWE-613: Insufficient Session Expiration

Description: The BookShop application is NOT vulnerable to CWE-613 (Insufficient Session Expiration). The application implements comprehensive session management controls including explicit timeout configuration, automatic session validation, and user-friendly session expiration handling. Through a multi-layered approach combining configuration-based timeouts, programmatic session management, and automated cleanup mechanisms, the application effectively prevents sessions from remaining valid indefinitely.

CWE Explanation: CWE-613 occurs when an application fails to properly expire user sessions, allowing attackers to reuse old session tokens even after the user has logged out or the session should have naturally expired. This vulnerability typically manifests as long session timeouts, missing session invalidation, lack of session rotation, or persistent sessions that don't expire properly.

Severity: None (Not Vulnerable) — Comprehensive session expiration controls implemented with multiple security layers.

7.2.1 Vulnerability Assessment Evidence

The application demonstrates robust protection against insufficient session expiration through multiple security controls:

- **Explicit session timeout configuration:** Application properties enforce 30-minute inactivity timeout and 24-hour absolute session lifetime limits.
- **Programmatic session validation:** `SessionManagementService` provides centralized session lifecycle management with automatic cleanup.
- **Request-level session filtering:** `SessionValidationFilter` validates session validity on each authenticated request.
- **Automatic session invalidation:** Expired sessions are automatically detected and invalidated without user intervention.
- **Concurrent session control:** Maximum of one active session per user prevents session proliferation.

7.2.2 Session Expiration Implementation

The application's session expiration controls are implemented through:

- **Configuration-based timeouts:** `server.servlet.session.timeout30m` and `max-inactive-interval` enforce inactivity limits.
- **Service layer management:** `SessionManagementService` handles session validation, cleanup, and security event responses.
- **Filter-based validation:** `SessionValidationFilter` intercepts requests to ensure session validity before processing.
- **API endpoint support:** `SessionController` provides session status checking and extension capabilities.
- **User interface integration:** JavaScript-based warnings and modal dialogs inform users of impending session expiration.

7.2.3 Protection Strategy and Rationale

The application adopts a *defense-in-depth session security* approach: (1) Implement explicit session timeout configuration that exceeds industry standards; (2) Provide programmatic session management for fine-grained control and security event handling; (3) Automate session validation and cleanup to prevent manual oversight; (4) Integrate user-friendly session management with clear expiration warnings; (5) Combine multiple timeout mechanisms (inactivity, absolute age, concurrent limits) for comprehensive protection.

7.2.4 Implemented Security Controls

1. **Session timeout configuration (implemented):** 30-minute inactivity timeout and 24-hour absolute session lifetime enforced through application properties.

2. **Centralized session management (implemented):** SessionManagementService provides comprehensive session lifecycle control and validation.
3. **Automatic session validation (implemented):** SessionValidationFilter validates session validity on each request and handles expired sessions.
4. **Concurrent session limits (implemented):** Maximum of one active session per user prevents session proliferation and unauthorized access.

7.2.5 Solution Effectiveness

- **Comprehensive timeout enforcement:** Multiple timeout mechanisms (inactivity, absolute age) ensure sessions cannot remain valid indefinitely.
- **Automated session cleanup:** Programmatic session management eliminates manual oversight and ensures consistent enforcement.
- **User experience balance:** Session extension capabilities and clear warnings provide security without excessive user friction.
- **Defense-in-depth protection:** Multiple overlapping controls ensure session security even if individual mechanisms fail.
- **Industry standard compliance:** 30-minute timeout and 24-hour absolute limits meet or exceed most security compliance requirements.
- **Maintainable security:** Centralized session management ensures consistent policy application and easy future modifications.

7.2.6 Session Security Architecture

The application implements a good session security architecture that addresses CWE-613 comprehensively:

- **Configuration layer:** Application properties define timeout values and session behavior.
- **Service layer:** SessionManagementService handles business logic for session validation and management.
- **Filter layer:** SessionValidationFilter provides request-level session security enforcement.
- **Controller layer:** SessionController exposes session management capabilities via REST API.
- **Presentation layer:** JavaScript-based user interface provides session status awareness and management controls.

Current Application Status:

- **CWE-613 Status:** NOT VULNERABLE - The application implements comprehensive session expiration controls through multiple security layers including configuration-based timeouts, programmatic session management, and automated cleanup mechanisms.

7.3 CWE-345: Insufficient Verification of Data Authenticity

Description: The BookShop application is NOT vulnerable to CWE-345 (Insufficient Verification of Data Authenticity). The application implements comprehensive data authenticity verification through multi-layered authentication, extensive input validation, proper authorization checks, and secure session management that effectively prevents insufficient verification of data authenticity vulnerabilities. Through a robust security framework combining Spring Security, Bean Validation, CSRF protection, and ownership verification, the application ensures all data operations are properly authenticated and authorized.

CWE Explanation: CWE-345 occurs when an application fails to adequately verify the authenticity of data, potentially allowing attackers to manipulate or inject malicious data that appears legitimate. This vulnerability typically manifests in scenarios involving file uploads without verification, external data sources without validation, API integrations without proper authentication, or any situation where data authenticity verification is critical for security.

Severity: None (Not Vulnerable) — Comprehensive data authenticity verification implemented with multiple security layers.

7.3.1 Vulnerability Assessment Evidence

The application demonstrates robust protection against insufficient verification of data authenticity through multiple security controls:

- **Comprehensive authentication framework:** Spring Security with multi-layered authentication, authorization, and CSRF protection ensures all operations are properly verified.
- **Extensive input validation:** Bean Validation with `@Valid`, `@NotBlank`, `@Size`, `@Email`, `@Pattern` annotations provide comprehensive data validation.
- **Ownership verification:** Controllers implement `enforceOwnershipOrAdmin()` methods to verify user ownership of resources before operations.
- **Role-based access control:** Admin operations protected with `@PreAuthorize("hasRole('ADMIN')")` annotations ensure proper authorization.
- **Session authenticity:** `@AuthenticationPrincipal UserDetails` ensures all requests are from authenticated sessions.

7.3.2 Data Authenticity Implementation

The application's data authenticity verification is implemented through:

- **Authentication requirements:** All critical operations require `@AuthenticationPrincipal UserDetails` ensuring authenticated requests.
- **CSRF protection:** Application-wide CSRF protection prevents cross-site request forgery attacks.

- **Input validation:** `RegistrationValidationService` and Bean Validation provide centralized data validation.
- **Path variable validation:** Controllers validate IDs and verify entity existence before operations.
- **Origin verification:** CORS configuration properly restricts cross-origin requests to prevent unauthorized data submission.

7.3.3 Protection Strategy and Rationale

The application adopts a *defense-in-depth data authenticity* approach: (1) Implement comprehensive authentication requirements for all data operations; (2) Provide extensive input validation to prevent malicious data injection; (3) Enforce ownership verification to prevent cross-user data manipulation; (4) Use CSRF protection to prevent unauthorized request submission; (5) Combine multiple validation layers (Bean Validation, custom validation, controller-level checks) for comprehensive protection against data authenticity attacks.

7.3.4 Implemented Security Controls

1. **Authentication framework (implemented):** Spring Security with comprehensive authentication, authorization, and session management.
2. **Input validation (implemented):** Bean Validation annotations and `RegistrationValidationService` provide extensive data validation.
3. **Authorization controls (implemented):** `@PreAuthorize` annotations and ownership verification ensure proper access control.
4. **CSRF protection (implemented):** Application-wide CSRF protection prevents unauthorized request submission.
5. **Request validation (implemented):** All `@RequestBody` parameters use `@Valid` annotation for comprehensive input validation.
6. **SQL injection protection (implemented):** JPA repositories with parameterized queries prevent SQL injection attacks.

7.3.5 Solution Effectiveness

- **Comprehensive authentication:** Multi-layered authentication ensures all data operations are from verified sources.
- **Extensive validation:** Multiple validation layers prevent malicious data injection and ensure data integrity.
- **Ownership enforcement:** Controllers verify user ownership preventing cross-user data manipulation attacks.
- **Framework security:** Spring Security provides well-tested protection against common data authenticity vulnerabilities.

- **No vulnerable endpoints:** Analysis confirms no file upload functionality, external API calls without validation, or unsigned data processing.
- **Defense-in-depth protection:** Multiple overlapping controls ensure data authenticity even if individual mechanisms fail.

7.3.6 Data Authenticity Security Architecture

The application implements a robust data authenticity security architecture that addresses CWE-345 comprehensively:

- **Framework layer:** Spring Security provides comprehensive authentication and authorization infrastructure.
- **Validation layer:** Bean Validation and custom validation services ensure data integrity and authenticity.
- **Controller layer:** `@AuthenticationPrincipal` and ownership verification ensure authenticated and authorized data access.
- **Service layer:** `RegistrationValidationService` and other validation services provide centralized data verification.
- **Repository layer:** JPA repositories with parameterized queries prevent data injection attacks.

Current Application Status:

- **CWE-345 Status:** NOT VULNERABLE - The application implements comprehensive data authenticity verification through multi-layered authentication, extensive input validation, proper authorization checks, and secure session management that effectively prevents insufficient verification of data authenticity vulnerabilities.

7.4 CWE-287: Improper Authentication

Description: The BookShop application is NOT vulnerable to CWE-287 (Improper Authentication). The application implements comprehensive authentication mechanisms through multi-layered security controls including robust password-based authentication, optional two-factor authentication (2FA), rate limiting protection, and proper authorization enforcement that effectively prevents improper authentication vulnerabilities. Through a sophisticated security framework combining Spring Security, custom authentication providers, brute force protection, and comprehensive access control, the application ensures all users are properly authenticated before accessing protected resources.

CWE Explanation: CWE-287 occurs when an application does not properly verify the identity of users, processes, or devices attempting to access resources. This vulnerability typically manifests as missing authentication requirements for critical functions, weak authentication mechanisms that can be easily bypassed, authentication bypass through parameter manipulation, or inadequate verification of user credentials allowing unauthorized access to protected functionality.

Severity: None (Not Vulnerable) — Comprehensive authentication framework implemented with multiple security layers and defense-in-depth protection.

7.4.1 Vulnerability Assessment Evidence

The application demonstrates robust protection against improper authentication through multiple security controls:

- **Comprehensive access control framework:** Spring Security with multi-layered authentication, authorization, and proper redirect handling ensures all protected endpoints require authentication.
- **Multi-factor authentication support:** Optional TOTP-based 2FA using `org.jboss.aerogear.security` provides enhanced authentication security for users who enable it.
- **Custom authentication provider:** `CustomAuthenticationProvider` implements proper password verification with BCrypt and 2FA validation when enabled.
- **Rate limiting and brute force protection:** `LoginAttemptService` tracks failed attempts per username and IP with account lockout after 5 attempts and IP blocking after 30 attempts.
- **Ownership verification:** Controllers implement `enforceCustomerOwnership()` methods to verify user ownership of resources preventing horizontal privilege escalation.

7.4.2 Authentication Implementation

The application's comprehensive authentication is implemented through:

- **Strong password requirements:** `RegistrationValidationService` enforces 12+ character passwords with complexity requirements (uppercase, lowercase, digits, special characters).
- **Secure credential storage:** BCrypt password encoding with appropriate cost factor ensures cryptographically secure password storage.
- **Session management:** Proper session fixation protection, concurrent session control (maximum 1 per user), and session timeout enforcement.
- **CSRF protection:** Application-wide CSRF protection prevents cross-site request forgery attacks that could bypass authentication.
- **Role-based access control:** Admin operations protected with `@PreAuthorize("hasRole('ADMIN')")` annotations and customer operations with proper ownership validation.

7.4.3 Protection Strategy and Rationale

The application adopts a *defense-in-depth authentication security* approach: (1) Implement comprehensive authentication requirements for all protected resources with proper redirect handling; (2) Provide multi-factor authentication option to enhance security beyond password-only authentication; (3) Enforce strong password policies to prevent weak credential vulnerabilities; (4) Use

rate limiting and account lockout to prevent brute force authentication attacks; (5) Combine authentication with proper authorization and ownership verification to prevent privilege escalation; (6) Implement proper session management to prevent session-based authentication bypass.

7.4.4 Implemented Security Controls

1. **Spring Security authentication framework (implemented):** Comprehensive authentication with proper redirect handling for unauthenticated requests (HTTP 302 redirects to login).
2. **Custom authentication provider (implemented):** CustomAuthenticationProvider with BCrypt password verification and optional 2FA validation using TOTP.
3. **Multi-factor authentication (implemented):** Optional TOTP-based 2FA during user registration with org.jboss.aerogear.security.otp library.
4. **Rate limiting protection (implemented):** LoginAttemptService with username-based (5 attempts) and IP-based (30 attempts) rate limiting with 15-minute windows.
5. **Strong password policy (implemented):** 12+ character minimum with complexity requirements enforced through RegistrationValidationService.
6. **Authorization controls (implemented):** @PreAuthorize annotations and enforceCustomerOwnership methods prevent unauthorized access to protected resources.
7. **Session security (implemented):** Session fixation protection, concurrent session limits, and proper timeout configuration.

7.4.5 Solution Effectiveness

- **Comprehensive authentication coverage:** All protected endpoints properly require authentication with no bypass mechanisms identified through testing.
- **Multi-layered security:** Combination of password authentication, optional 2FA, rate limiting, and proper authorization provides defense-in-depth protection.
- **Brute force protection:** Account and IP-based rate limiting with lockout mechanisms prevent credential brute force attacks.
- **Strong credential requirements:** Password complexity requirements significantly increase authentication security beyond basic implementations.
- **Authentication bypass prevention:** Comprehensive testing confirms no header injection, parameter manipulation, or other bypass techniques are effective.
- **Framework security leverage:** Spring Security provides well-tested protection against common authentication vulnerabilities.

7.4.6 Authentication Security Architecture

The application implements a robust authentication security architecture that addresses CWE-287 comprehensively:

- **Framework layer:** Spring Security provides comprehensive authentication and authorization infrastructure with proper redirect handling.
- **Provider layer:** CustomAuthenticationProvider handles password verification and 2FA validation with proper exception handling.
- **Service layer:** LoginAttemptService provides brute force protection and RegistrationValidationService ensures strong passwords.
- **Controller layer:** @AuthenticationPrincipal and ownership verification ensure authenticated and authorized access to resources.
- **Filter layer:** LoginRateLimitingFilter provides additional rate limiting protection before authentication processing.

Current Application Status:

- **CWE-287 Status:** NOT VULNERABLE - The application implements comprehensive authentication mechanisms through multi-layered security controls including robust password-based authentication, optional two-factor authentication, rate limiting protection, and proper authorization enforcement that effectively prevents improper authentication vulnerabilities.

Chapter 8: A08:2021 Software and Data Integrity Failures

8.1 CWE-494: Download of Code Without Integrity Check

Description: The BookShop application was VULNERABLE to CWE-494 (Download of Code Without Integrity Check) but has been comprehensively FIXED through implementation of Subresource Integrity (SRI) controls. The application initially loaded CDN resources without integrity verification, allowing potential code injection through compromised CDNs or man-in-the-middle attacks. The vulnerability has been remediated by implementing SRI attributes with SHA384 cryptographic hashes for all external CDN resources, ensuring that only verified, unmodified code can be executed by the browser.

CWE Explanation: CWE-494 occurs when an application downloads executable code, libraries, or other critical components from remote sources without performing adequate integrity verification. This vulnerability allows attackers to potentially inject malicious code through man-in-the-middle attacks, compromised repositories, DNS hijacking, or supply chain attacks by serving malicious versions of legitimate code.

Severity: Fixed (Previously Medium) — Subresource Integrity (SRI) implemented for all CDN resources with cryptographic verification.

8.1.1 Vulnerability Assessment Evidence

The application initially demonstrated vulnerability to downloading code without integrity checks but has been comprehensively remediated:

- **CDN integrity vulnerability (FIXED):** Bootstrap CSS/JS and Bootstrap Icons previously loaded from `cdn.jsdelivr.net` without integrity verification, now protected with SHA384 SRI hashes.
- **Maven Central dependency management:** All dependencies loaded from official Maven Central repository with built-in integrity verification and checksums.
- **Spring Boot managed dependencies:** Inherits from `spring-boot-starter-parent:3.5.0` with thoroughly tested and managed dependency versions.
- **Static resource loading:** Custom JavaScript files (`navbar-active.js`, `session-timeout.js`) hosted locally without runtime downloads.
- **Subresource Integrity implementation:** All CDN resources now include integrity and `crossorigin` attributes for cryptographic verification.
- **No dynamic code loading:** Analysis confirms absence of runtime code download, dynamic class loading, or reflection-based code execution.

8.1.2 Code Loading Security Implementation

The application's secure code loading is implemented through:

- **Subresource Integrity (SRI) protection:** CDN resources protected with SHA384 integrity hashes and `crossorigin="anonymous"` attributes ensuring cryptographic verification.
- **Build-time dependency resolution:** Maven resolves all dependencies at build time with integrity verification through checksums and signatures.
- **Local resource hosting:** All custom scripts and stylesheets served from local application resources, eliminating external download vectors.
- **Maven wrapper security:** `mvnw` uses checksums for Maven distribution integrity verification during build process.
- **SSL certificate generation:** `setup-env.sh` generates SSL certificates locally rather than downloading from external sources.
- **Static template loading:** Thymeleaf templates use only static resource references without dynamic code injection.

8.1.3 Protection Strategy and Rationale

The application adopts a *comprehensive integrity verification with trusted sources* approach: (1) Implement Subresource Integrity (SRI) for all external CDN resources to prevent code injection through compromised or intercepted content; (2) Use only trusted repositories (Maven Central) with built-in integrity verification; (3) Load all custom code from local resources to eliminate external download risks; (4) Avoid dynamic code loading mechanisms that could bypass security controls; (5) Generate security artifacts locally rather than downloading from external sources; (6) Maintain strict control over all code sources through explicit dependency declaration and cryptographic verification.

8.1.4 Implemented Security Controls

1. **Subresource Integrity (SRI) implementation (implemented):** CDN resources protected with SHA384 integrity hashes preventing execution of modified or malicious code.
2. **Cross-origin resource sharing controls (implemented):** `crossorigin="anonymous"` attributes ensure proper CORS handling for integrity verification.
3. **Dependency management security (implemented):** Maven Central repository with integrity checksums and Spring Boot managed versions.
4. **Local resource hosting (implemented):** All custom JavaScript and CSS files served from application resources.
5. **Build process integrity (implemented):** Maven wrapper with distribution checksums and local SSL certificate generation.
6. **Static loading enforcement (implemented):** No dynamic code loading, reflection, or runtime class instantiation mechanisms.
7. **Content Security Policy (implemented):** CSP headers prevent unauthorized external script loading while allowing verified CDN resources.

8.1.5 Solution Effectiveness

- **CDN integrity verification:** SHA384 SRI hashes ensure that modified or malicious CDN content cannot execute, providing cryptographic protection against supply chain attacks.
- **Browser-enforced security:** Integrity verification occurs at the browser level, providing zero-performance-impact protection against code injection.
- **Dependency integrity assurance:** Maven Central provides cryptographic verification ensuring downloaded dependencies are authentic and unmodified.
- **Static loading security:** Local hosting of custom code eliminates external download attack vectors completely.
- **Build-time verification:** All code loaded and verified at build time rather than runtime, reducing attack surface.
- **Trusted source control:** Explicit dependency declaration prevents unauthorized code injection through dependency confusion attacks.
- **No plugin architecture:** Absence of plugin system eliminates dynamic code loading vulnerabilities.
- **Supply chain protection:** Spring Boot parent dependency management provides vetted, compatible dependency versions.

8.1.6 Code Loading Security Architecture

The application implements a secure code loading architecture that addresses CWE-494 comprehensively:

- **CDN layer:** Subresource Integrity (SRI) with SHA384 hashes provides cryptographic verification of external CDN resources.
- **Repository layer:** Maven Central provides cryptographic integrity verification for all dependencies.
- **Build layer:** Maven wrapper ensures build tool integrity through checksum verification.
- **Application layer:** Local resource hosting eliminates runtime code download requirements.
- **Template layer:** Thymeleaf templates use static resource references without dynamic code injection.
- **Browser layer:** Content Security Policy headers prevent unauthorized external script execution while allowing verified CDN resources.

Current Application Status:

- **CWE-494 Status:** FIXED - The application was initially vulnerable due to missing CDN integrity verification but has been comprehensively remediated through implementation of Subresource Integrity (SRI) with SHA384 cryptographic hashes for all external resources, ensuring that only verified, unmodified code can be executed.

Chapter 9: A09:2021 Security Logging and Monitoring Failures

9.1 CWE-778: Insufficient Logging of Security Events

Description: The BookShop application was VULNERABLE to CWE-778 (Insufficient Logging of Security Events) but has been comprehensively FIXED through implementation of centralized security event logging. The application now implements comprehensive security audit trails through a dedicated SecurityAuditService, structured logging for all security events, separate audit log files for different event types, and complete coverage of authentication, authorization, session management, input validation, and administrative operations enabling effective security monitoring and forensic analysis.

CWE Explanation: CWE-778 occurs when an application fails to generate and retain adequate log records of security-relevant events, significantly hampering security monitoring, incident detection, and forensic analysis capabilities. This vulnerability manifests when critical security events like authentication failures, access control violations, privilege escalations, or administrative actions are not properly logged, making it difficult to detect attacks, investigate incidents, or maintain compliance with security regulations.

Severity: Fixed (Previously High) — Comprehensive security event logging implemented with structured audit trails and centralized logging service.

9.1.1 Vulnerability Assessment Evidence

The application initially demonstrated insufficient security event logging across multiple critical areas but has been comprehensively remediated:

- **Authentication event logging:** Implemented comprehensive logging of login success/failure events with IP addresses, user agents, timestamps, and detailed failure reasons.
- **Authorization event logging:** Added logging for access control violations, privilege escalation attempts, IDOR attempts, and cross-user data access violations.
- **Session management logging:** Implemented session creation, validation, expiration, invalidation, and potential hijacking attempt logging.
- **Input validation logging:** Added validation failure logging with field details, rejected values, and potential malicious input pattern detection.
- **Administrative operation logging:** Implemented logging for critical admin actions including viewing sensitive customer/admin data.
- **Business logic event logging:** Added logging for user registration, cart modifications, and other security-relevant business operations.

9.1.2 Security Logging Implementation

The application's comprehensive security logging is implemented through:

- **SecurityAuditService:** Centralized logging service with dedicated loggers (SECURITY_AUDIT, ACCESS_AUDIT, AUTH_AUDIT) and structured event formatting.
- **Enhanced authentication services:** AuthenticationHandlers, LoginAttemptService, LoginRateLimitingFilter, and SessionManagementService integrated with audit logging.
- **Controller access control logging:** CustomerController, AdminController, and CartController enhanced with authorization failure and successful access logging.
- **Global exception handler enhancement:** Comprehensive logging of validation failures, access denied events, authentication exceptions, and system errors.
- **Logback configuration:** Separate audit log files with rotation policies, structured formatting, and profile-specific configurations.

9.1.3 Protection Strategy and Rationale

The application adopts a *comprehensive security event audit trail* approach: (1) Implement centralized SecurityAuditService for consistent event logging across all components; (2) Provide dedicated loggers for different audit types enabling effective log analysis and monitoring; (3) Log all security-relevant events with sufficient context for forensic analysis; (4) Use structured log formatting with timestamps, user context, and event details; (5) Implement proper log rotation and retention policies for compliance and storage management; (6) Separate audit logs from application logs for focused security monitoring.

9.1.4 Implemented Security Controls

1. **Centralized audit service (implemented):** SecurityAuditService with structured logging methods for all security event types.
2. **Authentication event logging (implemented):** Comprehensive success/failure logging with IP, user agent, and contextual information.
3. **Authorization event logging (implemented):** Access denied, privilege escalation, and ownership violation logging with detailed context.
4. **Session management logging (implemented):** Complete session lifecycle logging including creation, validation, expiration, and security violations.
5. **Input validation logging (implemented):** Validation failure logging with field details and potential malicious input detection.
6. **Administrative operation logging (implemented):** Critical admin action logging for sensitive data access and system operations.
7. **Global exception logging (implemented):** Security-relevant exception logging through enhanced GlobalExceptionHandler.
8. **Log management configuration (implemented):** Separate audit log files with rotation, retention policies, and structured formatting.

9.1.5 Solution Effectiveness

- **Comprehensive event coverage:** All identified security-relevant events now properly logged with sufficient detail for analysis.
- **Structured audit trails:** Consistent logging format enables effective security monitoring and automated analysis.
- **Forensic capability:** Detailed event context supports incident investigation and compliance reporting.
- **Centralized management:** SecurityAuditService provides consistent logging interface across all application components.
- **Compliance support:** Comprehensive audit trails meet regulatory requirements for security event logging.
- **CWE-778 Status:** VULNERABLE → FIXED - The application now implements comprehensive security event logging with centralized SecurityAuditService, structured audit trails for all security events, separate log files for different event types, proper log rotation and retention, and complete coverage enabling effective monitoring, incident detection, and forensic analysis.

9.2 CWE-117: Improper Output Neutralization for Logs

Description: The BookShop application was VULNERABLE to CWE-117 (Improper Output Neutralization for Logs) but has been comprehensively FIXED through implementation of comprehensive log input sanitization. The application now implements robust log injection protection through a centralized sanitization framework that neutralizes dangerous characters, control sequences, and injection vectors before logging user-supplied data, effectively preventing log manipulation, log injection attacks, and log file corruption.

CWE Explanation: CWE-117 occurs when an application writes user-controllable data to log files without properly neutralizing special characters that could be interpreted by log processing tools, enable log injection attacks, or corrupt log file integrity. This vulnerability manifests when attackers inject malicious content containing newlines, carriage returns, ANSI escape sequences, or other control characters that can manipulate log entries, create false log entries, or bypass log analysis systems.

Severity: Fixed (Previously High) — Comprehensive log input sanitization implemented with multi-layered protection against log injection attacks.

9.2.1 Vulnerability Assessment Evidence

The application initially demonstrated log injection vulnerabilities across multiple logging points but has been comprehensively remediated:

- **Username logging vulnerabilities:** SecurityAuditService originally logged user-supplied usernames directly without sanitization, enabling CRLF injection and log entry manipulation.

- **User agent logging vulnerabilities:** Authentication logging included unsanitized user agent strings that could contain malicious control sequences or injection payloads.
- **Reason/message logging vulnerabilities:** Error messages, failure reasons, and exception details were logged without neutralization, allowing injection through error contexts.
- **Path/resource logging vulnerabilities:** Resource paths, endpoints, and file references were logged without sanitization, enabling injection through URL manipulation.
- **Operation logging vulnerabilities:** Administrative operations and user actions were logged without input sanitization, creating injection vectors through action parameters.

9.2.2 Log Injection Protection Implementation

The application's comprehensive log injection protection is implemented through:

- **Centralized sanitization framework:** Enhanced SecurityAuditService with comprehensive sanitizeLogInput() method providing protection against multiple injection vectors.
- **CRLF injection prevention:** Replacement of carriage return (r) and newline (n) characters with safe alternatives to prevent log entry manipulation.
- **Control character neutralization:** Removal of dangerous control characters including tab, form feed, backspace, null bytes, and escape sequences.
- **ANSI escape sequence filtering:** Detection and removal of ANSI escape sequences commonly used in terminal-based log injection attacks.
- **Unicode line separator handling:** Neutralization of Unicode line separator characters (u2028, u2029, u0085) that could bypass standard CRLF filtering.
- **Length limiting:** Input length restrictions to prevent log flooding attacks through oversized input.

9.2.3 Protection Strategy and Rationale

The application adopts a *comprehensive input sanitization with defense-in-depth* approach: (1) Implement centralized sanitization service ensuring consistent protection across all logging points; (2) Apply multiple sanitization layers targeting different injection vectors (CRLF, control characters, ANSI sequences, Unicode); (3) Use safe replacement characters rather than removal to maintain log readability and debugging capability; (4) Provide specialized sanitization methods for different input types (usernames, paths, operations, reasons); (5) Combine sanitization with length limiting to prevent log flooding attacks; (6) Maintain backward compatibility with existing logging infrastructure while adding protection.

9.2.4 Implemented Security Controls

1. **Comprehensive sanitization framework (implemented):** Enhanced SecurityAuditService with sanitizeLogInput() method providing multi-layered protection against log injection.

2. **CRLF injection protection (implemented):** Replacement of
r
n,
n
r,
r, and
n sequences with safe " — " delimiter to prevent log entry manipulation.
3. **Control character filtering (implemented):** Removal of dangerous control characters (
t,
f,
b,
u0000,
u001B,
u007F) that could corrupt log files.
4. **ANSI escape sequence filtering (implemented):** Regex-based removal of ANSI escape sequences (
char92 u001B
char92 [[0-9;]*[a-zA-Z]) commonly used in injection attacks.
5. **Unicode line separator neutralization (implemented):** Protection against Unicode line separators (
u2028,
u2029,
u0085) that could bypass standard filtering.
6. **Specialized sanitization methods (implemented):** sanitizeUsername(), sanitizeReason(), sanitizePath(), sanitizeOperation() providing context-appropriate protection.
7. **Length limiting protection (implemented):** Input truncation at 1000 characters with "... " suffix to prevent log flooding while preserving essential information.
8. **Universal application (implemented):** Sanitization applied to all user-controllable logging parameters across authentication, authorization, session, validation, and administrative logging.

9.2.5 Solution Effectiveness

- **Complete injection prevention:** Multi-layered sanitization neutralizes all known log injection vectors including CRLF, control characters, ANSI sequences, and Unicode separators.
- **Centralized protection:** Single sanitization framework ensures consistent protection across all application logging points, preventing bypass through alternative code paths.
- **Log integrity preservation:** Safe replacement strategies maintain log readability and debugging capability while eliminating injection risks.
- **Maintainable security:** Centralized sanitization logic enables easy updates and extensions as new injection vectors are discovered.
- **Performance optimization:** Efficient sanitization implementation minimizes logging performance impact while providing comprehensive protection.
- **CWE-117 Status:** VULNERABLE → FIXED - The application now implements comprehensive log input sanitization with centralized sanitization framework, multi-layered protection against CRLF injection, control character neutralization, ANSI escape sequence

filtering, Unicode line separator handling, length limiting, and universal application across all logging points preventing log injection attacks and maintaining log integrity.

9.3 CWE-532: Insertion of Sensitive Information into Log File

Description: The BookShop application is NOT vulnerable to CWE-532 (Insertion of Sensitive Information into Log File). The application demonstrates comprehensive protection against sensitive data logging through multiple defensive layers including explicit password exclusion in model representations, centralized sanitized logging framework, controlled validation logging with generic error messages, and structured logging with explicit field control. Analysis confirms no credential logging, controlled error responses, and protective logging practices that prevent sensitive information disclosure through server logs.

CWE Explanation: CWE-532 occurs when an application writes sensitive information (passwords, credit card numbers, personal data, session tokens, API keys, etc.) to log files where it can be accessed by unauthorized users or systems. This vulnerability enables attackers to extract credentials, tokens, personal information, or other confidential data through log file access, log aggregation systems, backup systems, or exposure to unauthorized personnel with log access.

Severity: None (Not Vulnerable) — Comprehensive protection against sensitive data logging implemented with multiple overlapping security controls.

9.3.1 Security Assessment Evidence

The application demonstrates robust protection against sensitive information logging through multiple protective mechanisms:

- **Model-level password exclusion:** User model `toString()` method explicitly excludes password field, logging only id, username, and role information.
- **Sanitized logging framework:** `SecurityAuditService` applies comprehensive input sanitization to all logged values through `sanitizeLogInput()`, `sanitizeUsername()`, `sanitizeReason()` methods.
- **Controlled validation logging:** Password validation failures log only field names, sanitized rejected values, and generic constraint messages without exposing actual password values.
- **Generic authentication error messages:** Authentication failures produce generic responses like "Authentication credentials are invalid" rather than exposing credential values.
- **Structured logging approach:** Application uses controlled field mapping rather than logging entire objects that might contain sensitive data.

9.3.2 Logging Security Implementation

The application's comprehensive logging security is implemented through:

- **Centralized logging control:** All security-relevant logging goes through `SecurityAuditService` providing single point of control for sensitive data protection.
- **Input sanitization integration:** CWE-117 log injection protection also prevents sensitive data exposure by sanitizing all logged input through comprehensive `sanitizeLogInput()` framework.
- **Model representation security:** User entity `toString()` method designed with security in mind, explicitly avoiding password field inclusion in string representations.
- **Validation framework protection:** `GlobalExceptionHandler` processes validation failures with field-level control, logging constraint violations without exposing sensitive field values.
- **Authentication logging security:** `AuthenticationException` handling logs failure events with usernames and generic reasons but never password values or credential details.

9.3.3 Protection Strategy and Rationale

The application adopts a *defense-in-depth sensitive data protection* approach: (1) Implement explicit exclusion of sensitive fields at model level to prevent accidental logging through object serialization; (2) Apply centralized sanitization for all user input before logging to ensure consistent protection; (3) Use structured logging with explicit field control rather than relying on automatic object serialization; (4) Provide generic error messages that give user feedback without exposing system internals or sensitive values; (5) Integrate sensitive data protection with log injection protection for comprehensive logging security; (6) Maintain clear separation between debugging information and sensitive operational data.

9.3.4 Implemented Security Controls

1. **Model-level password exclusion (implemented):** User entity `toString()` method explicitly excludes password field from string representation.
2. **Centralized sanitized logging (implemented):** `SecurityAuditService` provides comprehensive input sanitization for all logged values preventing sensitive data exposure.
3. **Controlled validation logging (implemented):** `GlobalExceptionHandler` processes validation failures with field-level control, logging constraint violations without sensitive values.
4. **Generic authentication error responses (implemented):** Authentication failures produce sanitized error messages without credential exposure.
5. **Structured logging framework (implemented):** Explicit field mapping in logging events rather than automatic object serialization prevents accidental sensitive data inclusion.
6. **Input sanitization integration (implemented):** CWE-117 protection framework also prevents sensitive data logging through comprehensive `sanitizeLogInput()` methods.
7. **No direct credential logging (implemented):** Code analysis confirms absence of direct password, token, or credential logging throughout application codebase.
8. **Environment variable configuration (implemented):** Sensitive configuration data accessed via environment variables preventing hardcoded exposure in logs.

9.3.5 Solution Effectiveness

- **Complete sensitive data protection:** Multiple overlapping controls ensure no passwords, credentials, or sensitive personal data are logged to files.
- **Centralized security control:** Single logging framework ensures consistent protection policies across all application components.
- **Defense redundancy:** Multiple protective layers (model exclusion, sanitization, structured logging, generic errors) ensure protection even if individual mechanisms are compromised.
- **Maintainable security:** Clear separation of concerns and centralized controls make sensitive data protection policies easy to maintain and extend.
- **Compliance ready:** Comprehensive protection against sensitive data logging supports regulatory compliance requirements for data protection and privacy.
- **CWE-532 Status:** NOT VULNERABLE - The application implements comprehensive protection against sensitive information logging with model-level password exclusion, centralized sanitized logging framework, controlled validation logging, generic authentication error responses, structured logging approach, input sanitization integration, absence of direct credential logging, and environment variable configuration preventing sensitive data exposure through log files.

Chapter 10: A10:2021 Server-Side Request Forgery (SSRF)

10.1 CWE-918: Server-Side Request Forgery (SSRF)

Description: The BookShop application is NOT vulnerable to CWE-918 (Server-Side Request Forgery). The application demonstrates complete absence of SSRF attack vectors through its self-contained architecture that lacks external HTTP client functionality, user-controlled URL construction, or external service integrations. Analysis confirms the application is a simple CRUD system that only interacts with its own database and serves static/internal content, with no mechanisms for making outbound HTTP requests based on user input.

CWE Explanation: CWE-918 occurs when a web application fetches a remote resource without properly validating the user-supplied URL, allowing attackers to make requests to arbitrary domains or internal systems that the server can access. This vulnerability enables attackers to access internal services, scan internal networks, read local files, bypass firewalls, or interact with cloud metadata services through server-side request manipulation.

Severity: None (Not Vulnerable) — Complete absence of SSRF attack surface due to application architecture without external HTTP request functionality.

10.1.1 Security Assessment Evidence

The application demonstrates complete protection against SSRF attacks through architectural design that eliminates attack vectors:

- **No external HTTP clients:** Application does not import or use HTTP client libraries such as `URLConnection`, `RestTemplate`, `WebClient`, `HttpClient`, or `URLConnection`.
- **No URL parameters from users:** Analysis of all controllers shows no endpoints accepting URL parameters (`@RequestParam url`, `@PathVariable url`) or constructing URLs based on user input.
- **No file access with user input:** Application does not use `File` or `Files` classes with user input, `FileInputStream` with user-controlled paths, or `file://` protocol handlers.
- **Database-only external access:** Application only accesses MySQL database with fixed connection strings from environment variables, no external APIs or services.
- **Internal URL construction only:** All URLs in codebase are internal application URLs for forms, navigation, and security redirects.

10.1.2 Application Architecture Analysis

The application's architectural design inherently prevents SSRF vulnerabilities through:

- **Self-contained CRUD system:** Simple e-commerce application that only performs database operations without external service integrations.
- **Static URL patterns:** All URL construction uses static internal application paths with Thymeleaf expressions (at-login, at-checkout, at-books patterns).
- **Environment-based configuration:** External configuration (database URLs) comes from environment variables, not user input.
- **Spring Boot default security:** Framework's default configuration excludes HTTP client beans or external URL fetching capabilities.
- **Controlled redirect mechanism:** All redirects target internal application URLs (/login?expired, /login?invalid) with no user-controlled components.

10.1.3 Protection Strategy and Rationale

The application adopts a *minimal attack surface through architectural simplicity* approach: (1) Implement self-contained application design without external service dependencies to eliminate SSRF vectors entirely; (2) Use database-only external connectivity with fixed, environment-controlled connection strings; (3) Employ static internal URL patterns for all user interface interactions; (4) Leverage Spring Boot's secure defaults that exclude dangerous HTTP client functionality; (5) Maintain clear separation between internal application logic and any potential external connectivity requirements; (6) Design application scope to avoid features commonly associated with SSRF vulnerabilities.

10.1.4 SSRF-Prone Features Assessment

Comprehensive analysis confirms absence of typical SSRF vulnerability patterns:

1. **Image/file fetching from URLs (absent):** No functionality for fetching external images or files based on user-provided URLs.
2. **Webhook functionality (absent):** No webhook endpoints or callback URL processing that could be manipulated for SSRF attacks.
3. **External API proxy endpoints (absent):** No endpoints that proxy requests to external APIs based on user input.
4. **URL shortener functionality (absent):** No URL shortening or expansion features that could be exploited for SSRF.
5. **External service integrations (absent):** No payment gateways, social media APIs, or third-party service integrations requiring outbound requests.
6. **File upload from URLs (absent):** No functionality allowing users to specify URLs for file uploads or imports.
7. **External content parsing (absent):** No RSS feed parsing, external content importing, or website preview functionality.
8. **Dynamic resource loading (absent):** No features that dynamically load external resources based on user-controlled parameters.

10.1.5 Solution Effectiveness

- **Complete attack surface elimination:** Architectural design removes all potential SSRF vectors through absence of external HTTP request functionality.
- **Framework security compliance:** Spring Boot's default security configuration naturally excludes dangerous HTTP client capabilities.
- **Principle of least functionality:** Application implements only necessary features for core e-commerce functionality without external dependencies.
- **Environment isolation:** Database connectivity uses secure environment variable configuration preventing user manipulation of connection targets.
- **Internal-only URL patterns:** Consistent use of internal application URLs eliminates user-controlled URL construction vulnerabilities.
- **CWE-918 Status:** NOT VULNERABLE - The application implements complete protection against SSRF attacks through self-contained architecture without external HTTP clients, absence of user-controlled URL parameters, no file access with user input, database-only external connectivity, internal URL construction patterns, and elimination of all typical SSRF-prone features resulting in zero attack surface for server-side request forgery vulnerabilities.

Bibliography

- [1] OWASP Foundation. *OWASP Top 10:2021 - The Ten Most Critical Web Application Security Risks*. Available: <https://owasp.org/Top10/>.
- [2] MITRE Corporation. *CWE-1344: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')*. Available: <https://cwe.mitre.org/data/definitions/1344.html>.
- [3] Mend Security. *OWASP Top 10 CWE Coverage Documentation*. Available: <https://docs.mend.io/legacy-sast/latest/owasp-top-10-cwe-coverage>.