

STUDY NOTES

Severity vs Priority

100 Classified Bug Reports

A practice set of realistic defects across ten common QA modules — each one classified with both a severity and a priority rating, and a one-line reason for the call. Built to make the difference between the two concrete instead of theoretical.

COMPILED JULY 2026 · 10 MODULES, 100 BUGS · REFERENCE EDITION

00

Severity vs. Priority — What's the Difference?

Severity measures how badly a defect damages the system if left alone: data loss, a crash, a security hole, or a cosmetic misalignment. It's a technical judgment and doesn't change based on deadlines or business goals.

Priority measures how urgently the defect needs to be fixed relative to everything else in the backlog. It's a business and scheduling judgment, and it can be influenced by a launch date, a VIP customer, or a compliance deadline — even for a bug that is technically minor.

The two are independent. A bug can be severe but low priority (a rare crash in a feature almost nobody uses), or minor but high priority (a typo in the CEO's name on the homepage the day of a product launch). Every bug in this set is picked to make that independence visible.

The scales used in this set

Critical	System down, data loss/corruption, security breach, or a core flow completely blocked for all users.
High	Major function broken or badly degraded for a large group of users; no reasonable workaround.
Medium	Function impaired but usable, affects a subset of users, or has a workaround.
Low	Cosmetic, rare, or negligible impact on the user's ability to complete their task.
P1 — Urgent	Fix immediately, often same-day; blocks release or causes ongoing active harm.
P2 — High	Fix in the current sprint/cycle; significant but not actively on fire.
P3 — Medium	Fix in an upcoming release; scheduled normally alongside other work.
P4 — Low	Fix when convenient; nice-to-have, backlog groomed opportunistically.

Four combinations worth knowing cold

	High Priority	Low Priority
High Severity	Payment double-charges customers (this set's BUG-011) — technically severe and urgent to fix.	A crash in an admin tool used twice a year (severe if it happens, but nobody's hitting it today).
Low Severity	Placeholder "Lorem ipsum" text live on the production FAQ page (BUG-030) — trivial to fix, embarrassing to leave up.	A favicon that loads 400ms slower than it should (BUG-050) — nobody is waiting on this.

Severity distribution (100 bugs)

Critical	18
High	27
Medium	30
Low	25

Priority distribution (100 bugs)

P1 — Urgent	30
P2 — High	34
P3 — Medium	25
P4 — Low	11

SEVERITY VS PRIORITY — 100 CLASSIFIED BUGS

MODULE 01 / 10

01

Authentication & Authorization

10 example defects from this area, each with a reasoned severity and priority call.

ID	DESCRIPTION	SEV.	PRI.	WHY
BUG-001	Password reset email never arrives for Gmail addresses with a '+' alias	Critical	P1	Blocks account recovery entirely for a common address pattern; support tickets spike.
BUG-002	Session does not expire after the configured 30-minute idle timeout	Critical	P1	Shared/public computers stay logged in indefinitely — direct security exposure.
BUG-003	Logging in with correct credentials sometimes returns 'Invalid password' on first attempt	High	P1	Intermittent but blocks legitimate users from a core flow; retry usually works, which delays detection.
BUG-004	Admin role checkbox has no effect — users can still access /admin without it	Critical	P1	Privilege escalation; any authenticated user can reach admin-only pages.
BUG-005	Two-factor authentication code accepted after the 5-minute expiry window	High	P2	Weakens 2FA's time-boxing guarantee but still requires a valid code, not a full bypass.
BUG-006	'Remember me' checkbox is ignored — session always ends when the browser closes	Low	P3	Annoying but has a trivial workaround (log in again); no data or security impact.
BUG-007	Password strength meter shows 'Strong' for the password 'password1'	Medium	P3	Misleading UX that encourages weak passwords, but doesn't itself weaken enforcement.
BUG-008		Low	P4	

Logout button on the mobile nav requires two taps to register

Minor friction, single component, easy manual workaround.

BUG-009 **Account lockout after 5 failed attempts never resets, even after 24 hours**

Medium

P2

Locks out legitimate users long-term with no self-service recovery path.

BUG-010 **Social login (Google) creates a duplicate account if the user's email casing differs**

Medium

P3

Confusing but doesn't lose data; both accounts are still individually usable.

pdfsent.com

02

Payments & Checkout

10 example defects from this area, each with a reasoned severity and priority call.

ID	DESCRIPTION	SEV.	PRI.	WHY
BUG-011	Customers are charged twice when clicking 'Pay Now' twice in quick succession	Critical	P1	Direct financial harm to customers at scale; every double-click is a real overcharge.
BUG-012	Discount code stacks with itself if applied twice, doubling the discount	High	P1	Direct revenue loss and easily discoverable/exploitable by any user.
BUG-013	Order confirmation page shows the wrong shipping address for gift orders	High	P2	Risk of packages going to the wrong place, but affects a narrower gift-order flow only.
BUG-014	Currency symbol shows '\$' for EUR-priced items in the UK storefront	Medium	P2	Confusing and trust-damaging, but the underlying charge amount is still correct.
BUG-015	Cart total briefly flashes \$0.00 before recalculating after adding an item	Low	P4	Purely cosmetic; final total is always correct before checkout.
BUG-016	Saved credit card expiry dropdown allows selecting a year in the past	Medium	P3	Leads to a confusing decline at charge time rather than validating up front.
BUG-017	Refund requests older than 90 days silently fail with no error shown to the agent	High	P2	Support agents believe the refund succeeded; customer never gets their money without follow-up.
BUG-018	Tax is calculated using the billing address instead of the shipping address	High	P1	Produces incorrect tax collection, which is a compliance issue in several jurisdictions.
BUG-019	Checkout button label still reads 'Continue' instead of 'Pay \$49.00' on Safari	Low	P3	Cosmetic label issue isolated to one browser; checkout itself still functions.
BUG-020	Gift-wrap option resets to unchecked if the user edits the shipping address after selecting it	Low	P4	Minor annoyance with an easy re-click fix; no financial or data impact.

03

UI / UX & Visual

10 example defects from this area, each with a reasoned severity and priority call.

ID	DESCRIPTION	SEV.	PRI.	WHY
BUG-021	Company logo in the footer links to a 404 page	Low	P3	Broken link looks unpolished and is easy to fix, but has no functional impact on the app.
BUG-022	Dark mode toggle makes all body text the same colour as the background	Critical	P1	Makes the entire application unreadable for any user who enables the feature.
BUG-023	Modal dialog cannot be closed on iOS Safari — the X button is unresponsive	High	P1	Traps the user in a dead-end on a widely used platform with no way to proceed.
BUG-024	Tooltip text overflows its container on long product names	Low	P4	Visually messy in an edge case (very long names) but text remains legible.
BUG-025	Table columns misalign by a few pixels when the window is resized below 1024px	Low	P3	Cosmetic layout shift; all data remains correct and readable.
BUG-026	Primary 'Submit' button and 'Cancel' button are the same colour, easy to misclick	Medium	P2	Design ambiguity that can cause accidental data loss or unwanted cancellations.
BUG-027	Loading spinner never disappears on slow connections, even after content has loaded	Medium	P2	Makes users think the page is broken and prompts unnecessary refreshes/support tickets.
BUG-028	Font renders as a fallback serif instead of the brand typeface on Android Chrome	Low	P4	Brand inconsistency only; no functional or readability issue.
BUG-029	Error toast notifications stack indefinitely instead of replacing the previous one	Medium	P3	Clutters the screen over time in error-prone sessions but doesn't block any action.
BUG-030	Placeholder text ('Lorem ipsum') is visible in the production FAQ page	High	P1	Publicly visible unfinished content damages credibility and looks unshipped.

04

Performance & Load

10 example defects from this area, each with a reasoned severity and priority call.

ID	DESCRIPTION	SEV.	PRI.	WHY
BUG-031	Homepage takes 11 seconds to become interactive on a throttled 3G connection	High	P2	Drives users away before the page is usable, but the page does eventually load correctly.
BUG-032	Memory usage grows unbounded on the analytics dashboard, crashing the tab after ~20 minutes	Critical	P1	Makes a core feature entirely unusable for any extended session.
BUG-033	Search-as-you-type fires a new API request on every keystroke instead of debouncing	Medium	P2	Unnecessary backend load and cost at scale, though functionally search still works.
BUG-034	Bulk CSV export of 100k+ rows times out and returns a blank file	High	P1	A core reporting feature is completely broken for the exact users who need it most.
BUG-035	Product image thumbnails are served at full resolution, slowing the catalogue page	Medium	P3	Degrades load time noticeably but the page still functions end to end.
BUG-036	Database connection pool exhausts under moderate concurrent load, returning 500s	Critical	P1	Whole application becomes unavailable to all users during peak traffic.
BUG-037	Animations stutter on low-end Android devices during page transitions	Low	P4	Cosmetic performance issue affecting a device tier, no functional breakage.
BUG-038	Autosave in the document editor blocks the UI thread for ~2 seconds every save	Medium	P2	Frequent, noticeable interruption to a core editing workflow.
BUG-039	Background sync job silently retries every second on failure, spiking server CPU	High	P1	Runaway retry loop degrades performance for every user on the shared infrastructure.
BUG-040	Favicon takes an extra 400ms to load due to an uncompressed image	Low	P4	Negligible, cosmetic-adjacent performance detail with no user-facing consequence.

05

API & Backend

10 example defects from this area, each with a reasoned severity and priority call.

ID	DESCRIPTION	SEV.	PRI.	WHY
BUG-041	DELETE /api/users/:id returns 200 even when the user ID does not exist	Medium	P3	Misleading response code, but no actual data is deleted or corrupted.
BUG-042	Pagination 'next page' cursor repeats the same page indefinitely past page 20	High	P2	Breaks a core browsing pattern for any dataset large enough to paginate deeply.
BUG-043	Rate limiting returns a raw stack trace instead of a 429 response	Medium	P2	Leaks internal implementation details and gives integrators a confusing error to debug.
BUG-044	Webhook retries are not idempotent, causing duplicate order-created events downstream	Critical	P1	Causes duplicate real-world side effects (e.g., duplicate fulfillment) for integrated partners.
BUG-045	API returns dates in the server's local timezone instead of UTC as documented	High	P2	Breaks any client doing correct timezone math, though data itself isn't lost.
BUG-046	Health-check endpoint returns 200 even while the database connection is down	Critical	P1	Defeats the entire purpose of the health check, masking real outages from monitoring.
BUG-047	Optional 'notes' field is silently truncated at 255 characters with no error	Medium	P3	Silent data loss on a non-critical field; user has no way to know it happened.
BUG-048	API versioning header is ignored — v1 and v2 clients get identical v2 responses	High	P2	Breaks the contract for any client still expecting v1 behaviour, without warning.
BUG-049	CORS headers missing on the /export endpoint only, blocking browser-based access	Medium	P2	Single endpoint unusable from browser clients; server-to-server calls still work.
BUG-050	Swagger/OpenAPI docs describe a field that was	Low	P3	Confusing for integrators but discoverable quickly and doesn't affect running systems.

removed from the API two
releases ago

pdfsent.com

06

Database & Data Integrity

10 example defects from this area, each with a reasoned severity and priority call.

ID	DESCRIPTION	SEV.	PRI.	WHY
BUG-051	Deleting a parent record does not cascade, leaving orphaned child rows	High	P2	Data inconsistency accumulates over time and can surface as confusing bugs elsewhere.
BUG-052	Unique constraint missing on email column allows duplicate account registration	Critical	P1	Breaks a fundamental data-integrity guarantee used throughout the login system.
BUG-053	Migration script silently drops a column's default value on existing rows	Critical	P1	Irreversible, silent data change across the entire existing dataset.
BUG-054	Timestamps stored inconsistently — some rows in UTC, some in server local time	High	P2	Corrupts any time-based sorting or reporting until reconciled, but no rows are lost.
BUG-055	Soft-deleted records still appear in full-text search results	Medium	P2	Confusing but doesn't expose sensitive data beyond what search already indexes.
BUG-056	A database index intended for the search table was applied to the logs table instead	Low	P3	Wastes storage and a bit of write performance; doesn't affect correctness.
BUG-057	Backup job has been silently failing for 12 days with no alert configured	Critical	P1	Any incident in that window would be unrecoverable — a latent, severe risk.
BUG-058	Trailing whitespace in imported CSV data causes exact-match lookups to fail	Medium	P3	Breaks a specific lookup pattern but the underlying data itself is intact.
BUG-059	Foreign key constraint missing lets orders reference a non-existent product ID	High	P2	Can produce broken order-detail pages, though it's recoverable via cleanup.
BUG-060	Audit log records the wrong 'updated_by' user when an admin edits on behalf of support	Medium	P3	Incorrect attribution in logs, relevant for investigations but not blocking operations.

07

Security

10 example defects from this area, each with a reasoned severity and priority call.

ID	DESCRIPTION	SEV.	PRI.	WHY
BUG-061	Stored XSS in the product review field executes arbitrary script for every viewer	Critical	P1	Full client-side compromise potential for anyone who views the affected page.
BUG-062	Password reset tokens do not expire and can be reused indefinitely	Critical	P1	A single leaked token grants permanent account takeover capability.
BUG-063	Internal admin API is reachable from the public internet with no authentication	Critical	P1	Complete unauthenticated access to administrative functionality.
BUG-064	Verbose error pages in production expose full stack traces and file paths	High	P2	Aids attackers in reconnaissance, though it isn't itself a direct exploit.
BUG-065	CSRF token is validated on POST but not on PUT requests	High	P2	Leaves state-changing PUT endpoints exploitable via cross-site request forgery.
BUG-066	Uploaded profile pictures are not scanned or restricted, allowing .html file uploads	High	P1	Can enable stored XSS or phishing pages hosted on the platform's own domain.
BUG-067	Session cookie is missing the Secure flag, sent over plain HTTP if requested	High	P2	Exposes session cookies to interception on insecure networks.
BUG-068	Clickjacking is possible — the login page can be framed by an external site	Medium	P2	Enables UI-redress attacks against login, though it requires a targeted setup.
BUG-069	Internal version numbers of dependencies are exposed in HTTP response headers	Low	P3	Minor information disclosure that aids reconnaissance but isn't directly exploitable.
BUG-070	Rate limiting on the login endpoint can be bypassed by rotating the X-Forwarded-For header	High	P1	Effectively removes brute-force protection on the most security-sensitive endpoint.

08

Mobile & Responsive

10 example defects from this area, each with a reasoned severity and priority call.

ID	DESCRIPTION	SEV.	PRI.	WHY
BUG-071	App crashes on launch for all users on iOS 15 after the latest release	Critical	P1	Total, immediate loss of access to the app for an entire OS version's user base.
BUG-072	Keyboard covers the input field on the sign-up form on smaller Android screens	High	P2	Blocks task completion on a subset of devices, with an awkward but possible workaround (scrolling).
BUG-073	Pull-to-refresh gesture sometimes triggers a duplicate API call	Medium	P3	Wastes a request and could show a brief flicker, but doesn't corrupt any data.
BUG-074	Push notifications arrive up to 20 minutes late on Android battery-saver mode	Medium	P2	Degrades a key feature's usefulness for a meaningful subset of users, platform-dependent.
BUG-075	Landscape orientation is not supported and the layout breaks if rotated	Low	P3	Confined to an orientation most users don't use for this app; portrait works fully.
BUG-076	Biometric login (Face ID) prompt appears twice in a row on cold app start	Low	P3	Minor annoyance; a second successful attempt always logs the user in.
BUG-077	Deep link from an SMS opens the app but not the specific intended screen	Medium	P2	Breaks a specific conversion path (e.g., from marketing links) but the app itself works.
BUG-078	App icon badge count doesn't clear after reading all notifications	Low	P4	Cosmetic annoyance with no functional consequence.
BUG-079	Offline mode silently discards edits made while disconnected instead of queuing them	Critical	P1	Irrecoverable user data loss with no warning that anything was lost.
BUG-080	Tablet layout stretches a phone-sized UI instead of using available screen space	Low	P4	Purely cosmetic underuse of screen real estate; fully usable as-is.

09

Search & Filtering

10 example defects from this area, each with a reasoned severity and priority call.

ID	DESCRIPTION	SEV.	PRI.	WHY
BUG-081	Search returns zero results for queries containing an apostrophe (e.g., "men's")	High	P2	Silently breaks a common query pattern with no visible error to explain why.
BUG-082	Applying a price filter resets the previously selected category filter	Medium	P2	Frustrating loss of filter state, but the user can simply reapply both filters.
BUG-083	Sort-by-price-ascending actually sorts descending	High	P1	Core sorting logic is inverted, silently giving every user wrong ordering.
BUG-084	Search results pagination shows 'Page 1 of 1' even when more results exist	Medium	P2	Hides available results from the user with no obvious way to see more.
BUG-085	Autocomplete suggestions include out-of-stock and discontinued products	Low	P3	Minor relevance issue; users can still complete a search and see the real inventory.
BUG-086	Filter counts (e.g., 'Red (12)') don't update after applying a second filter	Low	P3	Cosmetic inaccuracy in a secondary UI element; actual filtered results are correct.
BUG-087	Searching in all lowercase misses results that are indexed with mixed case	Medium	P2	Case-sensitivity bug that silently omits valid, relevant results from most queries.
BUG-088	Recently viewed items list on the search page shows items from a different logged-out user	Critical	P1	Cross-account data leakage — a serious privacy issue even if browsing history is 'minor' data.
BUG-089	Typo-tolerant search doesn't correct common one-letter typos in brand names	Low	P4	A missed nice-to-have improvement rather than a functional defect.
BUG-090	Filter panel keeps a stale 'Loading...' state after results have already rendered	Low	P3	Cosmetic inconsistency; the actual results shown are accurate and up to date.

10

Notifications & Email

10 example defects from this area, each with a reasoned severity and priority call.

ID	DESCRIPTION	SEV.	PRI.	WHY
BUG-091	Order confirmation emails are sent to the billing email instead of the account email	High	P1	Customers may never see confirmation of their own order if the two addresses differ.
BUG-092	Unsubscribe link in marketing emails returns a 404 error	High	P1	Legal/compliance risk in several jurisdictions requiring functioning opt-out mechanisms.
BUG-093	Password-changed notification email is sent before the change is actually saved	Medium	P2	Confusing if the save then fails, but doesn't cause security or data harm by itself.
BUG-094	In-app notification bell shows an unread count that never reaches zero	Low	P3	Cosmetic counter bug; the underlying notifications themselves are all readable.
BUG-095	Digest emails are sent twice on Mondays due to a duplicated cron schedule entry	Medium	P2	Annoying duplicate communication at volume, but no data loss or security concern.
BUG-096	Email templates render broken layout in Outlook desktop due to unsupported CSS	Medium	P3	Degrades brand presentation for one client but the message content is still readable.
BUG-097	SMS verification codes occasionally arrive containing a stray null character	Medium	P2	Can cause exact-match verification to fail intermittently, blocking sign-up for some users.
BUG-098	Notification preferences page shows toggles that don't match the user's actual saved settings	Medium	P2	Users may believe they've opted out of emails they're still receiving — a trust issue.
BUG-099	Push notification tapped from a locked screen opens the app to the wrong tab	Low	P3	Minor navigation inconvenience; one extra tap gets the user to the right place.
BUG-100	Email 'From' name displays the internal service name ('svc-notify-prod') instead of the brand	Low	P4	Unpolished but purely cosmetic; delivery and content are otherwise correct.