

Live functional test report

Generated 2026-10-17 19:59 UTC against <https://collectsea.com> · release 2026.10.17-seo-visuals · commit b6e5100

Google Chrome (headless) via Playwright, macOS; HTTP suite on Node v26.7.0

137/137

live test cases passed

263/263

unit and integration tests passed

8

defects found and fixed this cycle

17/17

production self-checks (every 2 h)

1. Scope and method

CollectSEA is a public web platform, REST API and Model Context Protocol (MCP) server that matches a proposed software or AI-agent design to documented real-world failures and returns source-linked precedents and safeguards. This report records end-to-end tests run against the **live production site**, not a test copy.

- **HTTP suite** (77 cases): every public page rendered on the server, search-engine features (canonical URLs, structured data, sitemap, redirects, 404s), the analysis engine on representative designs, all MCP tools and error handling, the public API and dataset downloads, security headers and access control, and a concurrency check.
- **Browser suite** (43 cases): real user journeys in Google Chrome on desktop and phone sizes — analysis, exports for coding agents, share links, search and filters, navigation, keyboard access, dark mode, feedback and downloads — with screenshots.
- **Production self-checks**: 17 checks the platform runs on itself every two hours; results are published at collectsea.com/verification.
- Test traffic identifies itself and is excluded from the platform's public usage statistics.

Reproduce: `node scripts/live-test.mjs` and `node scripts/ui-test.mjs` from the CollectSEA source repository.

2. Defects found and fixed

ID	Issue and impact	Fix	Verified by
DEF-01	The home page's own "Cloud cleanup job" example returned no precedents, although GitLab, Atlassian, UniSuper and AWS S3 deletion incidents are in the corpus. Found by HTTP suite probe A-04 (live site). A core example produced an empty result.	Broadened the behavior classifier for deletion wording ("deletes", "tears down", "drops tables"), infrastructure ("virtual machines", "cloud databases") and scheduled jobs ("nightly", "background job"). Internal benchmark recall@5 rose from 0.43 to 0.50.	A-04, U-09, self-check analysis-deletion, unit test

DEF-02	For a shared multi-tenant cache, unrelated breaches (e.g. an unpatched web framework) ranked above cross-tenant precedents. Found by HTTP suite probe A-05 (live site). Less relevant precedents were shown first.	Added a bounded likely-pattern signal: behaviors in the design imply failure patterns (a multi-tenant cache implies cross-tenant access), which re-ranks records that already qualify but can never qualify a record alone. Recall@5 0.50 → 0.525, precision@3 0.47 → 0.50; unrelated designs still return nothing.	A-05, A-06, unit tests
DEF-03	Typing or clicking immediately after a page loaded could be lost, because the page's code was fetched only after the HTML arrived. Found by Browser suite U-11, U-18, U-20 (first run). Fast first interactions could do nothing on slow connections.	The Worker now reads the build manifest and adds modulepreload links for the current page's code, so pages become interactive sooner; the app marks when it is ready.	U-11, U-18, U-20 (re-run)
DEF-04	The edge cache key used only the release name, so for up to five minutes after a deploy, cached pages could reference the previous build's script files. Found by Manual check of preload tags after deploy. Possible broken pages immediately after a deployment.	Cache keys now include a fingerprint of the deployed build.	Post-deploy HTML inspection; P-01 to P-16
DEF-05	Automated test and self-check traffic would have been counted as real visitors and analyses. Found by Test design review. Usage figures would be inflated.	Requests identifying as CollectSEA test or self-check clients, and maintainer browsers carrying an internal cookie, are excluded from all usage counters.	Unit test (telemetry exclusion)
DEF-06	The GitHub advisory feed failed with HTTP 403 and the NVD feed timed out. Found by Service status panel during pre-release QA. New advisories were not being added.	NVD query narrowed to a 7-day window (1.5 s instead of timing out); GitHub requests send the recommended API headers and accept an optional token. All three feeds succeeded on the next sync.	D-01, self-check feeds
DEF-07	Code samples and long labels made the home and analysis pages wider than a phone screen. Found by Mobile overflow scan during pre-release QA. Sideways scrolling on mobile.	Grid columns may now shrink below their content width; long pattern names wrap.	U-24, U-25
DEF-08	An internet-wide security scanner (CensysInspect) was listed as an AI client connected over MCP, and its handshakes counted as MCP calls.	Security scanners are now detected by user agent and counted only as automated traffic, never as visitors, analyses, MCP calls or AI clients; past scanner entries are left out of the client list.	tests/telemetry_scanner.test.ts

Found by review of live usage data (October 17, 2026). The impact page overstated MCP use; all three lifetime MCP calls came from the scanner.

3. Results by suite

Suite	Passed
HTTP suite: pages, search engines, analysis, MCP, API and security	77/77
Browser suite: real user journeys in Google Chrome	43/43
Production self-checks (latest scheduled run)	17/17

HTTP suite: pages, search engines, analysis, MCP, API and security

Every public route, redirect, API endpoint and MCP tool, called over the internet like a client would.

ID	Test	Expected	Observed	Result
P-01	/ renders on the server Pages	HTTP 200, server-rendered content contains "Learn from real software failures"	HTTP 200 in 562 ms, 79 KB of HTML	Pass
P-02	/incidents renders on the server Pages	HTTP 200, server-rendered content contains "How real software and AI systems failed"	HTTP 200 in 109 ms, 179 KB of HTML	Pass
P-03	/incidents/SEA-SEC-003 renders on the server Pages	HTTP 200, server-rendered content contains "CrowdStrike"	HTTP 200 in 98 ms, 46 KB of HTML	Pass
P-04	/incidents/SEA-AI-001 renders on the server Pages	HTTP 200, server-rendered content contains "Replit"	HTTP 200 in 59 ms, 59 KB of HTML	Pass
P-05	/patterns renders on the server Pages	HTTP 200, server-rendered content contains "The 14 ways software keeps failing"	HTTP 200 in 74 ms, 184 KB of HTML	Pass
P-06	/patterns/duplicate-action-after-timeout renders on the server Pages	HTTP 200, server-rendered content contains "Duplicate action after an ambiguous result"	HTTP 200 in 71 ms, 72 KB of HTML	Pass
P-07	/frameworks renders on the server Pages	HTTP 200, server-rendered content contains "Standards, mapped to the incidents behind them"	HTTP 200 in 55 ms, 26 KB of HTML	Pass
P-08	/frameworks/nist-sp-800-53 renders on the server Pages	HTTP 200, server-rendered content contains "SA-15(8)"	HTTP 200 in 60 ms, 144 KB of HTML	Pass

P-09	/impact renders on the server Pages	HTTP 200, server-rendered content contains "Who CollectSEA reaches"	HTTP 200 in 1459 ms, 93 KB of HTML	Pass
P-10	/verification renders on the server Pages	HTTP 200, server-rendered content contains "Does everything actually work?"	HTTP 200 in 239 ms, 222 KB of HTML	Pass
P-11	/integrations renders on the server Pages	HTTP 200, server-rendered content contains "claude mcp add"	HTTP 200 in 41 ms, 38 KB of HTML	Pass
P-12	/docs renders on the server Pages	HTTP 200, server-rendered content contains "API and MCP reference"	HTTP 200 in 69 ms, 54 KB of HTML	Pass
P-13	/methodology renders on the server Pages	HTTP 200, server-rendered content contains "How CollectSEA finds precedents"	HTTP 200 in 155 ms, 66 KB of HTML	Pass
P-14	/dataset renders on the server Pages	HTTP 200, server-rendered content contains "The CollectSEA incident dataset"	HTTP 200 in 64 ms, 83 KB of HTML	Pass
P-15	/changelog renders on the server Pages	HTTP 200, server-rendered content contains "What has changed"	HTTP 200 in 44 ms, 30 KB of HTML	Pass
P-16	/about renders on the server Pages	HTTP 200, server-rendered content contains "Software keeps failing the same ways"	HTTP 200 in 42 ms, 39 KB of HTML	Pass
S-01	Canonical URL, description and Open Graph tags Search engines	Each page has canonical, description, og:image (PNG)	canonical, description and og:image present	Pass
S-02	Structured data on home and incident pages Search engines	FAQPage, SoftwareApplication, Article and BreadcrumbList JSON-LD	All expected schema.org types present	Pass
S-03	Dataset page is discoverable by Google Dataset Search Search engines	schema.org Dataset with license and downloads	Dataset with CC BY 4.0 license and 3 downloads	Pass
S-04	Unknown page returns 404 Search engines	HTTP 404 with noindex	HTTP 404, noindex	Pass
S-05	Unknown incident ID returns 404 Search engines	HTTP 404	HTTP 404	Pass
S-06	https://www.collectsea.com/incidents redirects permanently Search engines	301 → https://collectsea.com/incidents	301 → https://collectsea.com/incidents	Pass
S-07	https://docs.collectsea.com/ redirects permanently Search engines	301 → https://collectsea.com/docs	301 → https://collectsea.com/docs	Pass

S-08	/stats redirects permanently Search engines	301 → /impact	301 → /impact	Pass
S-09	/research redirects permanently Search engines	301 → /methodology#evaluation	301 → /methodology#evaluation	Pass
S-10	/incidents?id=SEA-SEC-003 redirects permanently Search engines	301 → /incidents/SEA-SEC-003	301 → /incidents/SEA-SEC-003	Pass
S-11	/incidents/sea-sec-003 redirects permanently Search engines	301 → /incidents/SEA-SEC-003	301 → /incidents/SEA-SEC-003	Pass
S-12	/patterns/SEA-FM-004 redirects permanently Search engines	301 → /patterns/indirect-prompt-injection	301 → /patterns/indirect-prompt-injection	Pass
S-13	/incidents/ redirects permanently Search engines	301 → /incidents	301 → /incidents	Pass
S-14	Sitemap lists every documented incident, pattern and framework Search engines	Valid XML with ≥ 80 URLs; no advisories or private pages	179 URLs	Pass
S-15	robots.txt points to the sitemap Search engines	Sitemap directive; /review disallowed	Sitemap and Disallow present	Pass
S-16	llms.txt summarises the site for AI assistants Search engines	Lists patterns, frameworks and incidents	160 lines	Pass
S-17	Atom feed of new incidents Search engines	Valid Atom with entries	50 entries	Pass
S-18	Social preview image Search engines	PNG served at 1200×630	PNG 1200×630	Pass
S-19	Product tour video Search engines	Both MP4 renditions and the poster are served; byte ranges return 206 (required by Safari); VideoObject on home	1080p 16.9 MB, 720p 7.7 MB; poster and VideoObject present	Pass
A-01	Refund agent design Analysis	Precedents with idempotency or approval-boundary patterns; coverage strong	6 precedents, coverage strong, 630 ms	Pass
A-02	Agent reading public GitHub issues Analysis	GitHub/Supabase MCP prompt-injection incidents; prompt-injection safeguard	Matched SEA-AI-003, SEA-AI-004, SEA-AI-007, SEA-AI-008	Pass
A-03	Global configuration push Analysis	CDN/edge outage precedents (Cloudflare, Fastly, CrowdStrike)	SEA-SEC-003, SEA-POST-006, SEA-POST-005, SEA-SEC-010	Pass
A-04	Cloud cleanup job Analysis	Deletion-without-recovery precedents (GitLab, Atlassian, UniSuper)	SEA-POST-009, SEA-POST-004, SEA-POST-010, SEA-SEC-012	Pass

A-05	Multi-tenant shared cache Analysis	A cross-tenant precedent in the top 3	SEA-PUB-059, SEA-CVE-2026-108606, SEA-SEC-015	Pass
A-06	Unrelated design is not padded Analysis	No precedents; coverage "none"	coverage none, 0 matches	Pass
A-07	Semantic retrieval active Analysis	retrieval_algorithm reports Workers AI embeddings	Hybrid: Workers AI embeddings (bge-base-en-v1.5) + Weighted Capability Overlap	Pass
A-08	At most one illustrative scenario per result Analysis	≤ 1 SEA-PUB record among matches	1 illustrative of 10	Pass
A-09	Exclusion list for "show more precedents" Analysis	Excluded IDs never returned	SEA-POST-001 excluded	Pass
A-10	Input validation Analysis	Empty → 400, malformed JSON → 400, oversize → 413	400 / 400 / 413	Pass
A-11	Legacy "idea" field still accepted Analysis	HTTP 200 with matches	HTTP 200	Pass
M-01	initialize negotiates the protocol version MCP	Echoes 2025-06-18; serverInfo and instructions present	server 2026.10.17-seo-visuals	Pass
M-02	Notifications acknowledged MCP	HTTP 202 without body	HTTP 202	Pass
M-03	GET for SSE stream refused MCP	HTTP 405 (stateless server)	HTTP 405	Pass
M-04	tools/list MCP	6 read-only tools with input schemas	analyze_design, analyze_existing_app, search_incidents, get_incident, list_failure_patterns, get_safeguards	Pass
M-05	analyze_design MCP	Markdown summary plus structured precedents	4 precedents	Pass
M-06	search_incidents MCP	Keyword search returns CrowdStrike for "channel file"	70 results	Pass
M-07	get_incident MCP	Full record with source for SEA-POST-009	GitLab record returned	Pass
M-08	list_failure_patterns MCP	14 patterns	14 patterns	Pass
M-09	get_safeguards MCP	AGENTS.md content citing precedents	6283 characters	Pass
M-10	Errors are reported correctly MCP	Unknown tool → -32602; unknown method → -32601; bad JSON → 400	-32602 / -32601 / 400	Pass

M-11	Legacy endpoint and tool names MCP	/api/mcp with analyze_architecture_proposal works	works	Pass
D-01	Health endpoint (deployment contract) API & data	status operational with corpus counts	1649 records, feeds healthy	Pass
D-02	Incident list (full and summary views) API & data	incidents array; summary view is smaller	1649 records; summary 927 KB vs full 7631 KB	Pass
D-03	Single record and unknown record API & data	200 for SEA-SEC-003, 404 for unknown	200 / 404	Pass
D-04	Patterns and frameworks endpoints API & data	14 patterns; 7 frameworks	14 patterns, 7 frameworks	Pass
D-05	OpenAPI schema API & data	OpenAPI 3.1 with analyzeDesign operation	11 paths	Pass
D-06	Dataset download (JSON) API & data	Attachment with all served records	7631 KB	Pass
D-07	Dataset download (CSV) API & data	Attachment with all served records	1844 KB	Pass
D-08	Dataset download (JSONL) API & data	Attachment with all served records	2281 KB	Pass
D-09	Impact report and CSV API & data	JSON report with 30 daily points; CSV header	tracking since 2026-10-01	Pass
D-10	Self-check results published API & data	Latest run with all checks passing	17/17 at 2026-10-17T18:40	Pass
D-11	Feedback validation API & data	Missing message → 400; record report needs a valid ID → 400	400 / 400	Pass
D-12	Unknown API route API & data	JSON 404 listing endpoints	JSON 404	Pass
0-01	Security headers on pages Security	CSP with script hash, HSTS, nosniff, frame protection	CSP (no unsafe-inline scripts), HSTS, nosniff, X-Frame-Options	Pass
0-02	Private review API rejects unauthorized requests Security	HTTP 401 without token or 503 when review is disabled	HTTP 401: unauthorized or disabled	Pass
0-03	Manual feed sync requires a token Security	HTTP 401 without token	HTTP 401	Pass
0-04	Record text cannot inject script Security	Record page escapes HTML in data	Embedded data escapes "<"	Pass
0-05	Pages served quickly under concurrency Performance	40 parallel page and API requests succeed; median < 1.5 s	0 failures; median 286 ms, max 693 ms	Pass
A-EX-01	Files-only existing-app analysis Existing apps	Returns source context, app mode and refund behavior	4 precedents; submitted source and evidence limits returned	Pass

M-EX-01	MCP existing-app tool Existing apps	Returns structured app context and safeguards to verify	MCP app review returns precedents, safeguards and evidence limits	Pass
A-EX-02	Public repository context import Existing apps	Returns inspectable files and a pinned public repository revision	3 selected files at dd32ce8; arbitrary host rejected	Pass

Browser suite: real user journeys in Google Chrome

Desktop and mobile flows driven by Playwright, with screenshots as evidence.

ID	Test	Expected	Observed	Result
U-01	Home page loads and hydrates without errors Home	Hero, analyzer and corpus figures visible; no console errors	Hydrated cleanly; figures: Documented incidents0Postmortems, filings, court recordsLive security advisories...	Pass
U-02	Live behavior detection while typing Home	Detected capability chips appear under the input	Runs code or shell commands; Changes infrastructure; Changes data; Handles credentials or secrets; AI agent that calls tools	Pass
U-03	Example prompts run an editable analysis Home	Clicking "Cloud cleanup job" opens results with an editable proposal	A nightly background job that finds unused cloud databases and virtual machines and deletes them to save cost.	Pass
U-04	Run an analysis end to end Analysis	Safeguards, ranked precedents and profile panel render	5 safeguards, 8 precedents; proposal kept out of the URL	Pass
U-05	Score breakdown is inspectable Analysis	"How scored" reveals score components	Composite score 0.80. How scoring works	Pass
U-06	Export AGENTS.md for a coding agent Analysis	Download produces an AGENTS.md citing precedents	AGENTS.md (7429 characters)	Pass
U-07	Mark a safeguard as already in place Analysis	Ticked safeguard moves to "Already in place" in exports	Section jumps, refresh and reading evidence preserve choices; export includes "Already in place"	Pass
U-08	Share link reproduces the analysis Analysis	Copied ?q= link opens the same proposal and results	Shared link restored the proposal and results	Pass
U-09	Edit and re-run Analysis	Edited proposal produces different precedents	Top precedent changed to "Engineer deletes the production database directory and every backup me"	Pass
U-10	Unrelated design shows an honest empty state Analysis	"No close precedent" message, no padded results	Empty state shown	Pass

U-11	Search the incident database Incidents	Typing "redis" filters results and updates the URL	60 → 3 records; URL ?q=outage	Pass
U-12	Evidence-type tabs, pattern filter and AI filter Incidents	Each filter narrows the list	advisories 60, prompt-injection 5, AI systems 15	Pass
U-13	Open an incident by client-side navigation Incidents	Card click opens the record without a full reload; title updates	/incidents/SEA-POST-005 — "Cloudflare bot-management outage (Nov 2025) CollectSEA..."	Pass
U-14	Incident page shows evidence, source, safeguards and citation Incidents	Source link, trust panel, safeguards, related incidents, citation copy	Source, safeguards, related incidents and BibTeX citation present	Pass
U-15	Report-a-problem form validates input Incidents	Empty report is rejected with a message	Validation message shown (no report submitted)	Pass
U-16	Failure pattern page Patterns	Definition, prevention guidance and real incidents	17 incident cards	Pass
U-17	Framework crosswalk deep link Frameworks	Anchor to ASI01 lands on the item with linked incidents	ASI01 shows 5 incidents	Pass
U-18	MCP setup switches per client and copies config Integrations	Cursor tab shows .cursor/mcp.json; copy succeeds	Cursor config copied	Pass
U-19	Command palette search (⌘K) Navigation	Searching "crowdstrike" and pressing Enter opens the record	Opened /incidents/SEA-SEC-003	Pass
U-20	Browser back and forward Navigation	History navigation restores pages	Back and forward restored the right pages	Pass
U-21	Theme toggle persists without a flash Accessibility	Dark mode set before first paint after reload	Dark class applied by inline script on reload	Pass
U-22	Keyboard: skip link and focus Accessibility	First Tab reveals "Skip to content"; Enter moves focus to main	Skip link works	Pass
U-23	Images and controls are labelled Accessibility	Every button and link has an accessible name; one h1 per page	6 pages: no unnamed controls, exactly one h1, all images have alt text	Pass
U-24	Mobile layout and menu	No horizontal scrolling; menu opens and navigates	9 pages fit 390 px; menu navigation works	Pass

Mobile

U-25	Mobile analysis Mobile	Analysis results usable on a phone	Results fit (390 px)	Pass
U-26	Feedback dialog submits Feedback	Message accepted and confirmation shown	Confirmation shown	Pass
U-27	Dataset download from the page Data	CSV download starts from /dataset	collectsea-incidents-2026.10.17.csv (1649 rows)	Pass
U-28	Impact and verification pages render live data Transparency	Charts with table fallback; self-check table	30-day table view and self-check results visible	Pass
U-29	Unknown page Errors	Friendly 404 with navigation	HTTP 404 page with links	Pass
U-31	Scroll animations reveal content without hiding it Motion	On-screen content animates in on arrival; below-the-fold cards reveal on scroll and settle fully visible; with reduced motion nothing moves (fades only)	17 arrival animations; 12 elements revealed on scroll; 0 hidden above the fold; reduced motion: fades only	Pass
U-32	Animated pattern explainer plays and is interactive Patterns	One timeline advances; safeguard steps update the diagram and caption; index previews stay still	One timeline advances, safeguard step 3 shows "The retry reuses the same key, so the API recognises it and returns the first result.", 14 static previews on /patterns	Pass
U-33	Files-only analysis, reload, editing and export Existing apps	Uploaded context stays private, existing-app mode survives reload and edits, exports include source context	Files-only review, reload, editing, export and removal passed; context absent from URL	Pass
U-34	Input errors and mode-specific caching Existing apps	Invalid files are rejected and identical text retains the selected analysis mode	Invalid archive rejected; same description analyzed in both modes with correct labels	Pass
U-35	Quick review without uploads Existing apps	Behavior choices start an app review with no file or description required	Review created from behavior choices, with safeguards and no uploaded files	Pass
U-36	Public GitHub import, source preview and review Existing apps	A repo link imports pinned context and preserves provenance through reload and export	Public repository imported, sources previewed, commit preserved after reload and in export	Pass
U-37	Unfinished review survives refresh and return navigation Existing apps	Notes and behavior choices remain editable after reload and after reviewing	Mode, notes and removable behavior choices survive refresh and return	Pass

U-38	Shared file review preserves sources in a fresh tab Existing apps	Sharing retains file names, contents and app mode without context in the HTTP query	Fresh recipient retains app mode, file name, contents and export provenance	Pass
U-39	Mixed source provenance and file removal Existing apps	Uploaded notes are separate from GitHub files; removing imported files clears the revision	GitHub and uploaded files remain distinct; revision clears with last imported file	Pass
U-40	Narrow phone layout Existing apps	Every analyzer element fits a 320 px screen	All three context paths fit a 320 px dark screen	Pass
U-41	Import error recovery Existing apps	A rejected repository link leaves quick review usable	Actionable import error followed by a successful upload-free review	Pass
U-42	Offline review fallback Existing apps	Browser matching retains existing-app context when the API is unavailable	Browser fallback displays its limitations and retains existing-app mode	Pass
U-43	Malformed shared context Existing apps	Bad share links show an error and allow returning to the analyzer	Invalid share fragment rejected with recovery navigation and no crash	Pass
U-30	No console errors across the site Quality	Zero JavaScript errors recorded during the whole suite	No console errors	Pass

Production self-checks (latest scheduled run)

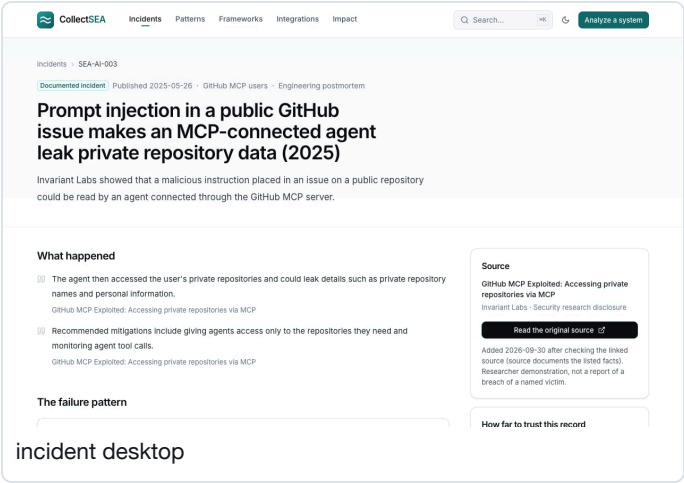
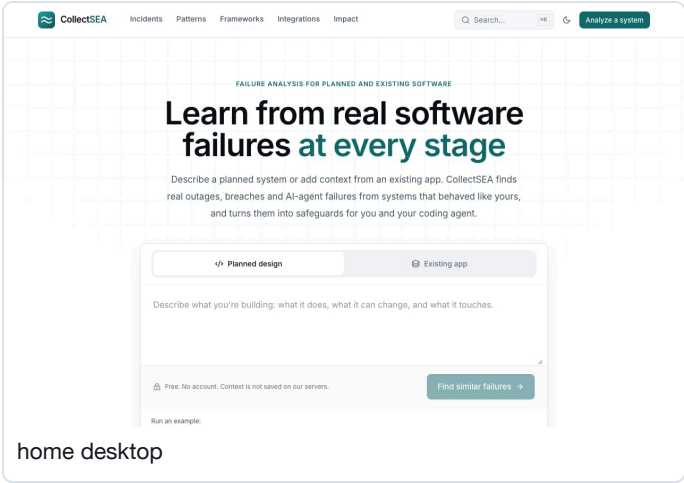
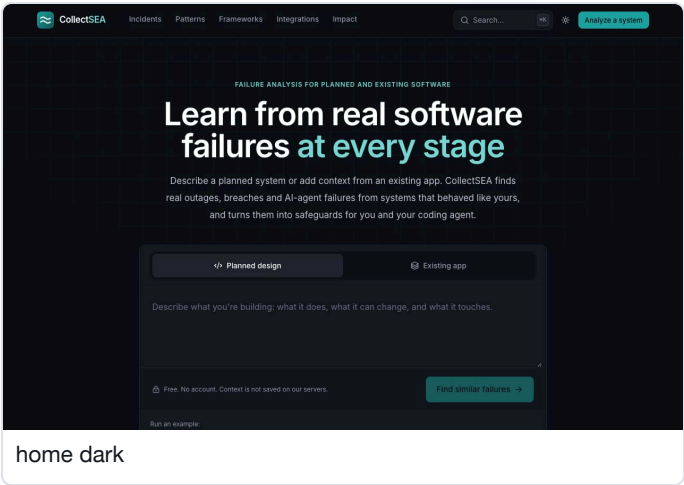
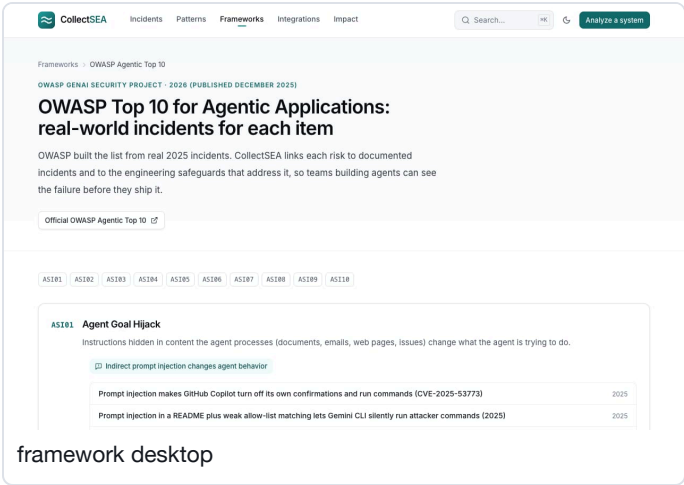
Run by the platform itself every two hours; this run 2026-10-17 18:40 UTC.

ID	Test	Expected	Observed	Result
SC-01	Home page is server-rendered with the analyzer Pages	Pass	Headline, analyzer and hydration data present	Pass
SC-02	Incident page shows the record and its source Pages	Pass	CrowdStrike record with source link	Pass
SC-03	Failure-pattern page lists real incidents Pages	Pass	Prompt-injection pattern links its incidents	Pass
SC-04	Framework crosswalk page renders every item Pages	Pass	OWASP Agentic ASI01-ASI10 present	Pass
SC-05	Unknown pages return a real 404 Search engines	Pass	HTTP 404 with noindex	Pass
SC-06	Old URLs redirect permanently Search engines	Pass	/stats → 301 /impact	Pass
SC-07	Pages carry canonical URLs and structured data Search engines	Pass	Canonical URL and Article JSON-LD	Pass
SC-08	Sitemap lists documented incidents Search engines	Pass	179 URLs	Pass

SC-09	Refund agent → duplicate-charge and approval precedents Analysis	Pass	6 precedents · Hybrid	Pass
SC-10	Agent reading GitHub issues → prompt-injection safeguard Analysis	Pass	Safeguard for indirect prompt injection among 5	Pass
SC-11	Cloud cleanup job → deletion-without-recovery precedents Analysis	Pass	6 precedents	Pass
SC-12	Unrelated design returns no padded results Analysis	Pass	Coverage "none", 0 matches	Pass
SC-13	MCP server negotiates the protocol MCP	Pass	protocolVersion 2025-06-18	Pass
SC-14	MCP analyze_design returns structured precedents MCP	Pass	3 precedents	Pass
SC-15	Public API serves the corpus API & data	Pass	1649 records	Pass
SC-16	Dataset downloads in CSV API & data	Pass	1649 rows	Pass
SC-17	Advisory feeds refreshed recently Operations	Pass	healthy; last full success 2026-10-17 17:05 UTC	Pass

4. Screenshots

Captured automatically by the browser suite on the live site.



 **CollectSEA**



Incidents > SEA-SEC-003

Documented incident

 Incident 2024-07-19 · CrowdStrike · Engineering postmortem

Faulty Channel File 291 content update crashes Windows hosts running CrowdStrike Falcon (2024)

Rapid deployment channel 291 bypassed staged canary rings; out-of-bounds memory read triggered BSOD on 8.5M Windows hosts.

The failure pattern



Global change without a staged rollout

A configuration, content or code change reaches every server at once, so one bad value takes everything down together.

incident mobile

 **CollectSEA** Incidents Patterns Frameworks Integrations Impact

Q Search...

HT

G

Analyze a system

FAILURE ANALYSIS FOR PLANNED AND EXISTING SOFTWARE

Learn from real software failures at every stage

Describe a planned system or add context from an existing app. CollectSEA finds real outages, breaches and AI-agent failures from systems that behaved like yours, and turns them into safeguards for you and your coding agent.

Planned design

Existing app

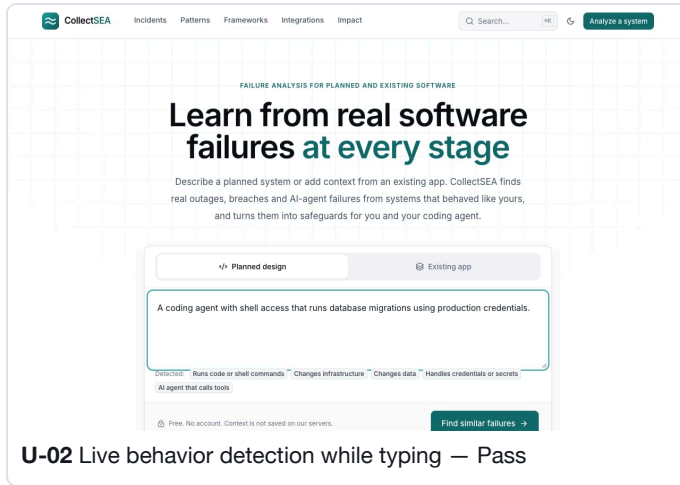
Describe what you're building: what it does, what it can change, and what it touches.

Free. No account. Context is not saved on our servers.

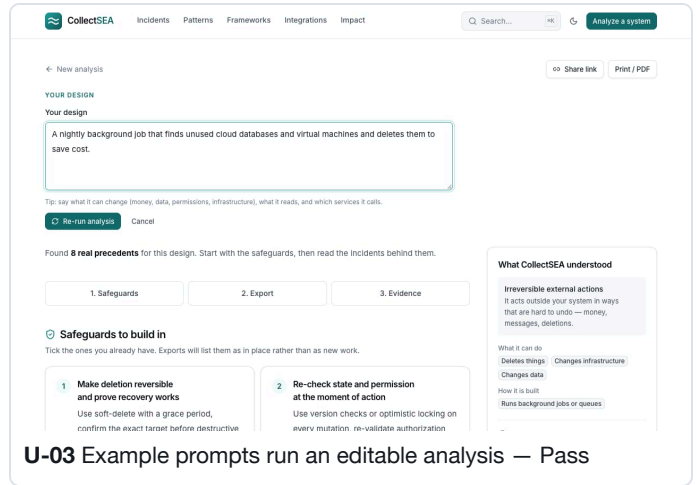
Find similar failures →

Run an example:

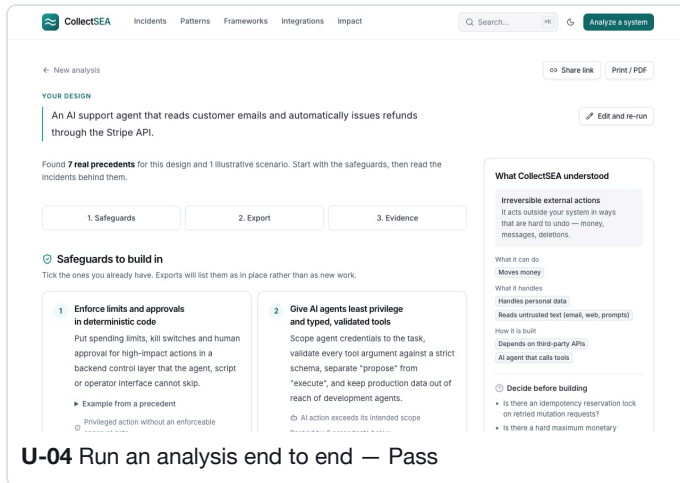
U-01 Home page loads and hydrates without errors — Pass



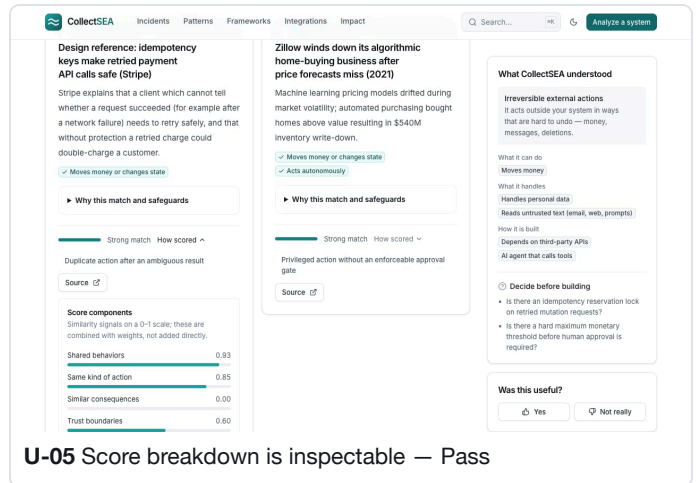
U-02 Live behavior detection while typing — Pass



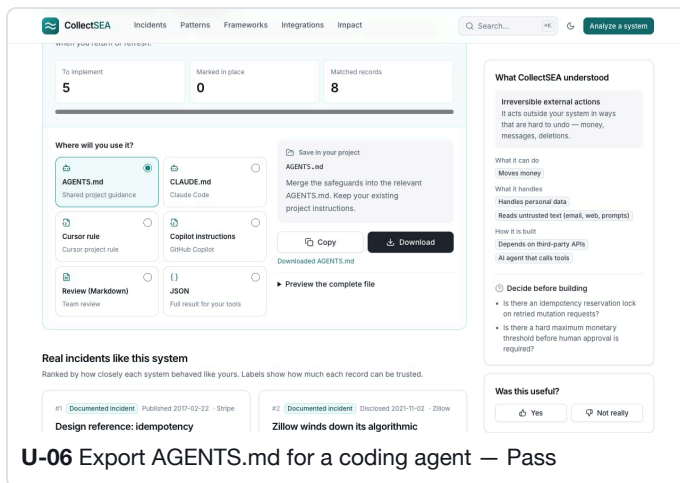
U-03 Example prompts run an editable analysis — Pass



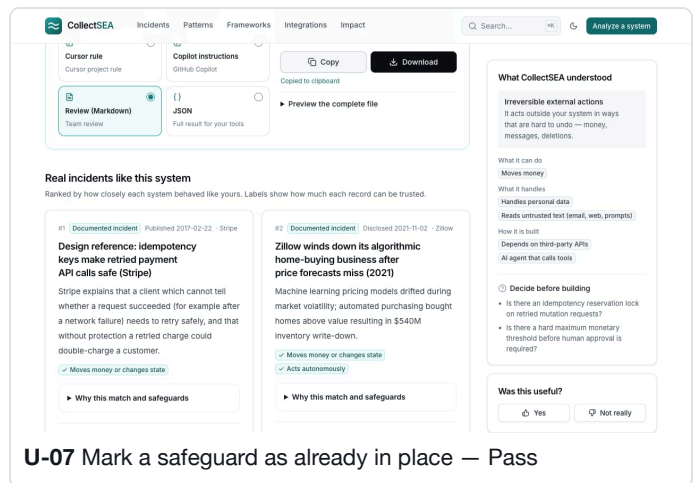
U-04 Run an analysis end to end — Pass



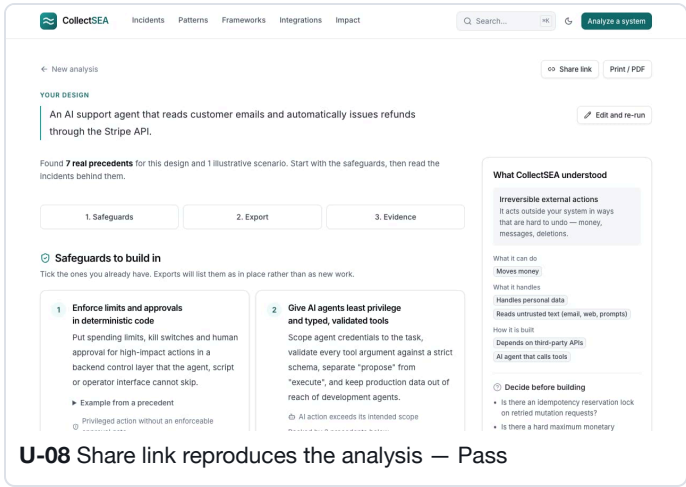
U-05 Score breakdown is inspectable — Pass



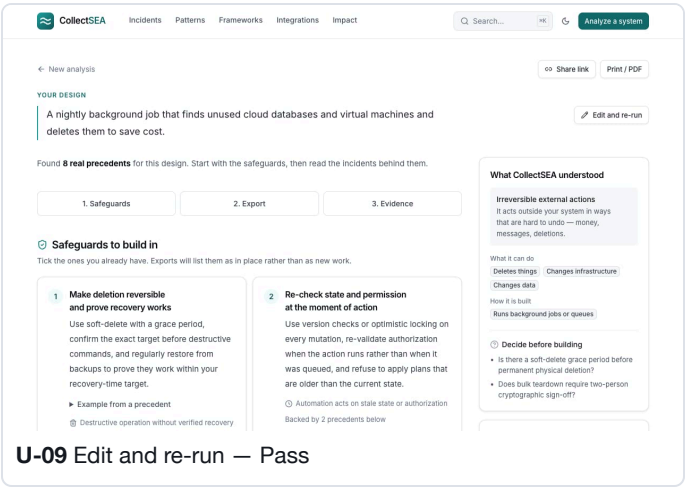
U-06 Export AGENTS.md for a coding agent — Pass



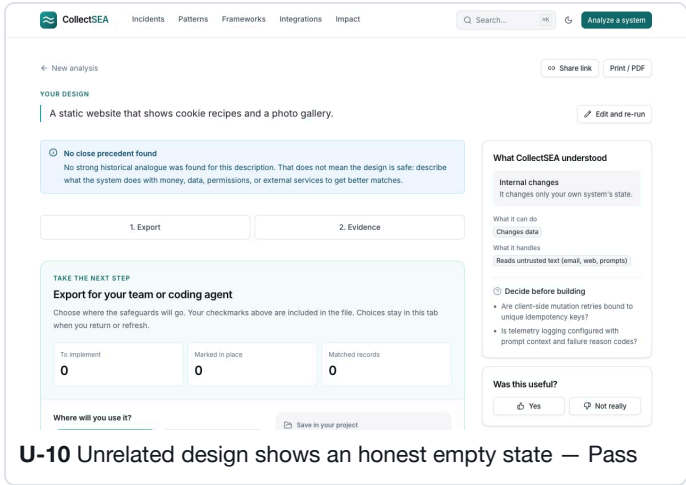
U-07 Mark a safeguard as already in place — Pass



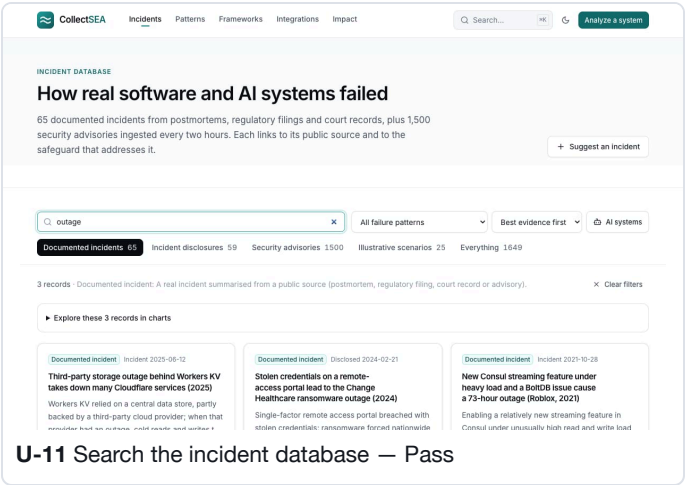
U-08 Share link reproduces the analysis — Pass



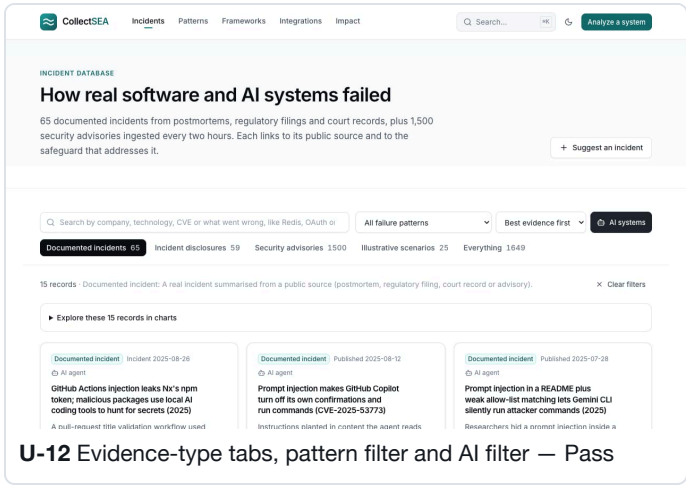
U-09 Edit and re-run — Pass



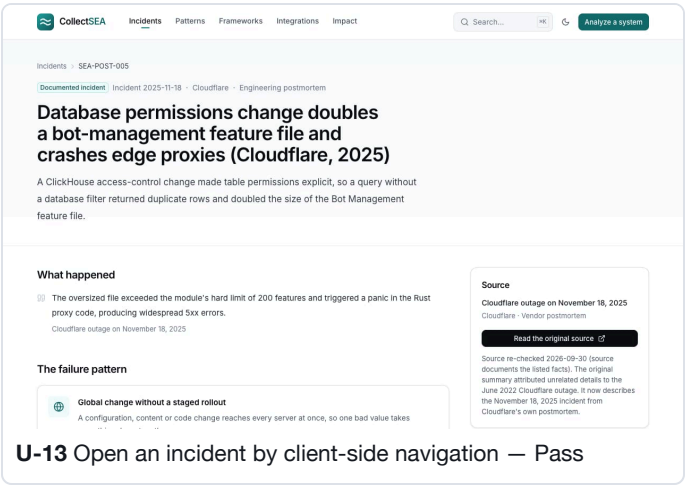
U-10 Unrelated design shows an honest empty state — Pass



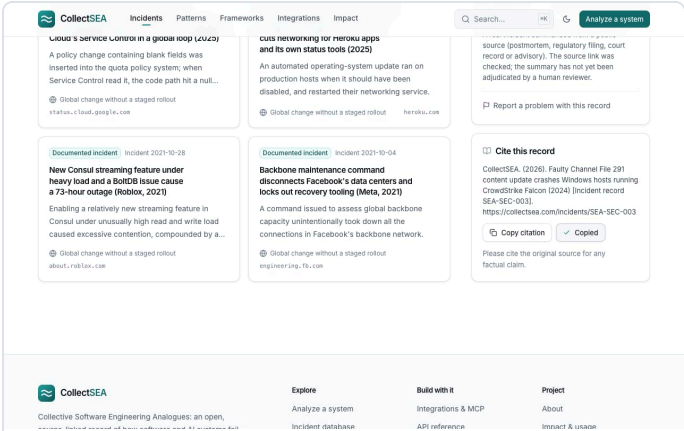
U-11 Search the incident database — Pass



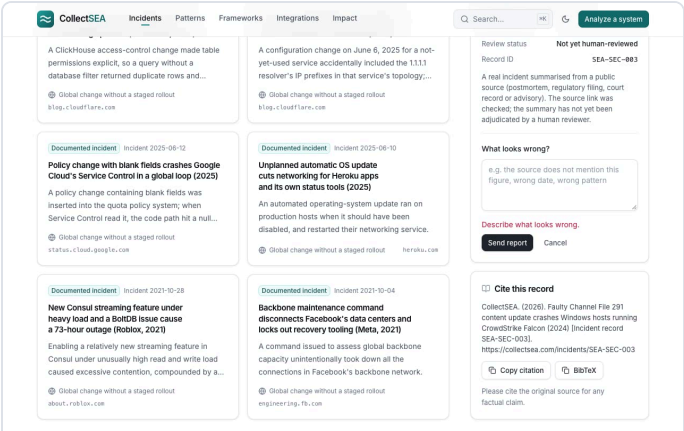
U-12 Evidence-type tabs, pattern filter and AI filter — Pass



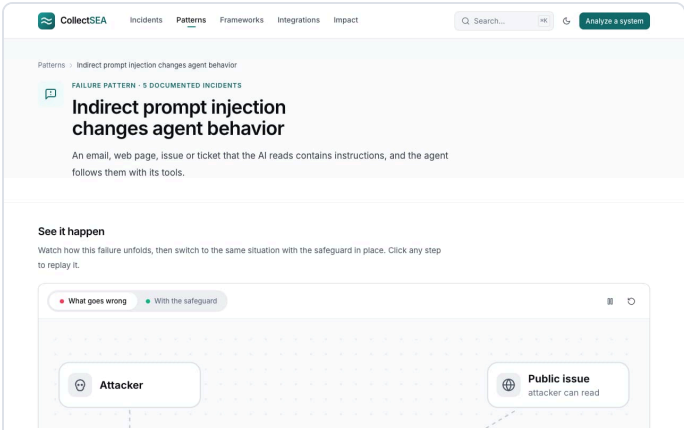
U-13 Open an incident by client-side navigation — Pass



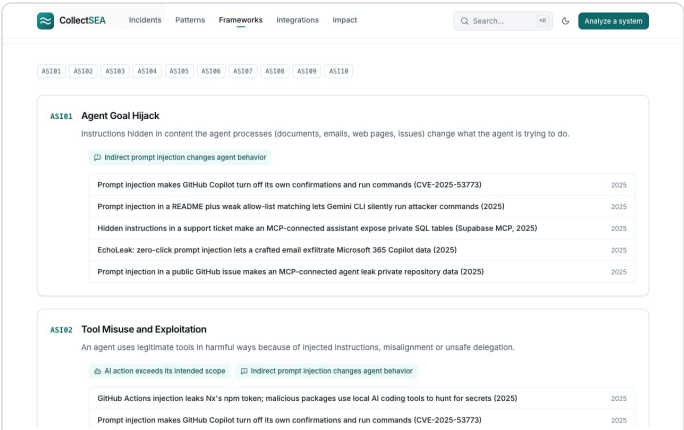
U-14 Incident page shows evidence, source, safeguards and citation — Pass



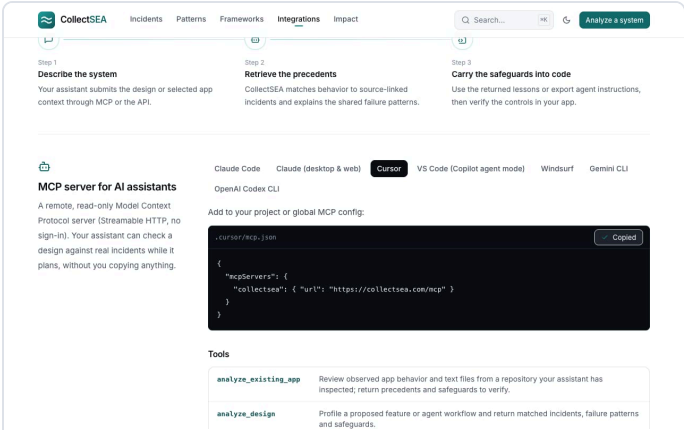
U-15 Report-a-problem form validates input — Pass



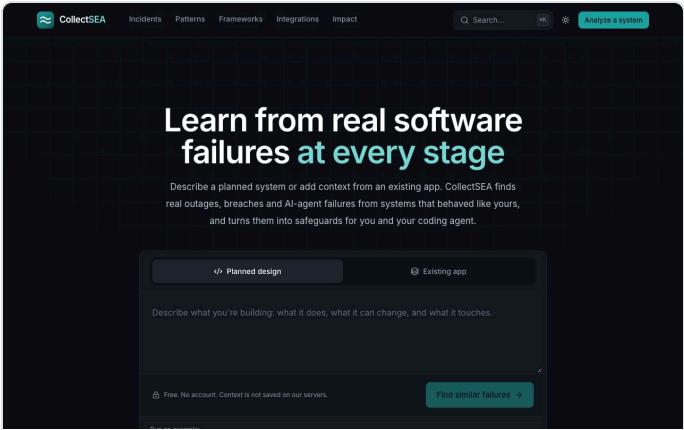
U-16 Failure pattern page — Pass



U-17 Framework crosswalk deep link — Pass



U-18 MCP setup switches per client and copies config — Pass



U-21 Theme toggle persists without a flash — Pass

 CollectSEA



INCIDENT DATABASE

How real software and AI systems failed

65 documented incidents from postmortems, regulatory filings and court records, plus 1,500 security advisories ingested every two hours. Each links to its public source and to the safeguard that addresses it.

+ Suggest an incident

 Search by company, technology, CVE or wha

All failure patterns

Best evidence first

 AI systems

Documented incidents 65 Incident disclosures

65 records · Documented incident: A real incident summarised from a public source (postmortem, regulatory filing, court record or advisory).

► Explore these 65 records in charts

U-24 Mobile layout and menu — Pass

 CollectSEA



New analysis

Share link

Print / PDF

YOUR DESIGN

An AI support agent that reads customer emails and automatically issues refunds through the Stripe API.

Edit and re-run

Found **7 real precedents** for this design and 1 illustrative scenario. Start with the safeguards, then read the incidents behind them.

1. Safeguards2. Export3. Evidence

 Safeguards to build in

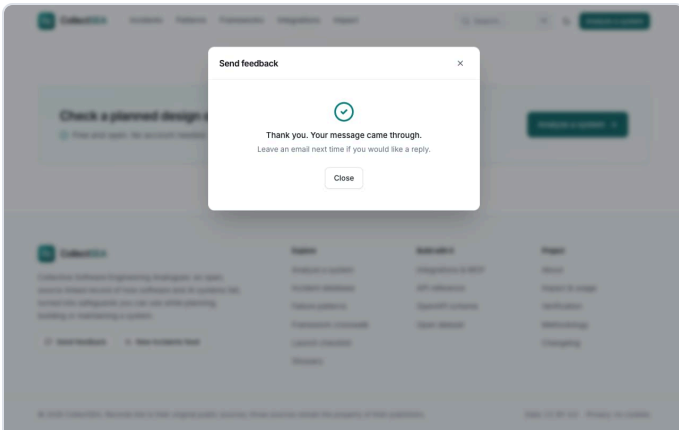
Tick the ones you already have. Exports will list them as in place rather than as new work.

1

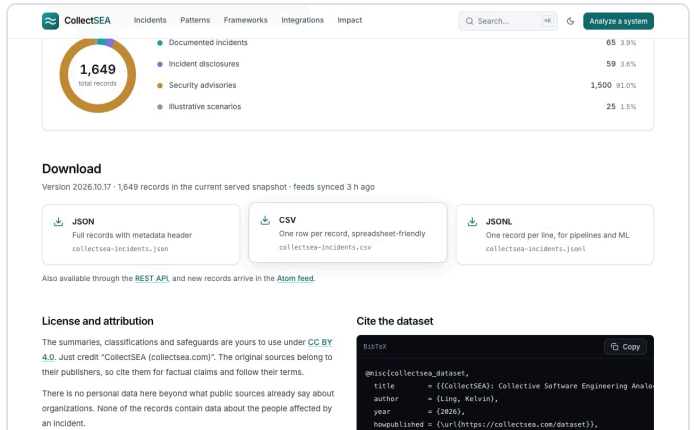
Enforce limits and approvals in deterministic code

Put spending limits, kill switches and human approval for high-impact actions in a backend control layer that the agent, script or operator interface

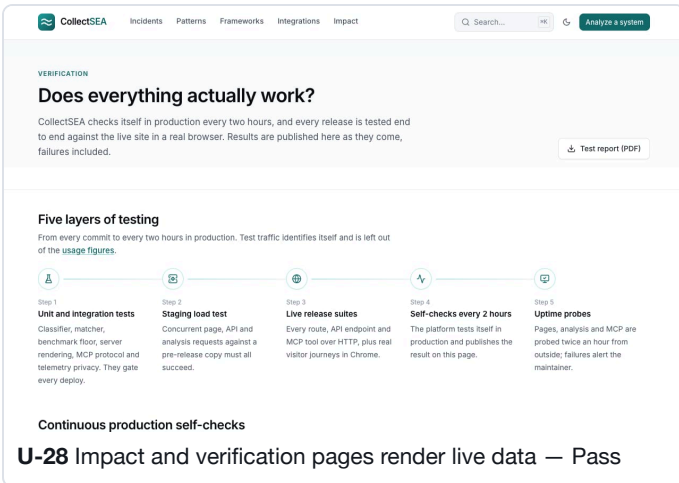
U-25 Mobile analysis — Pass



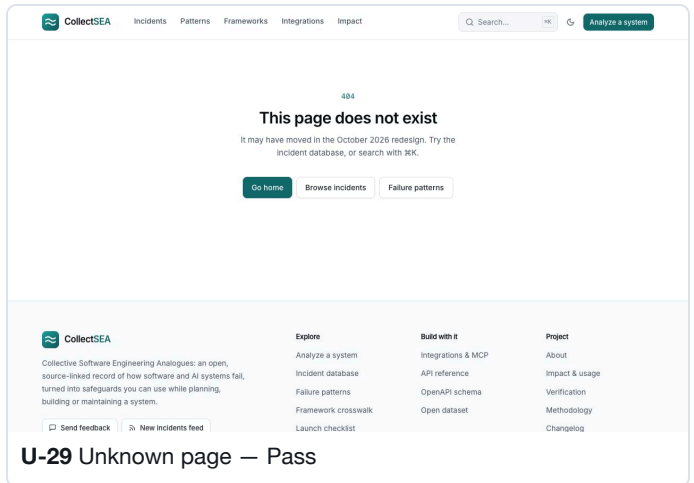
U-26 Feedback dialog submits — Pass



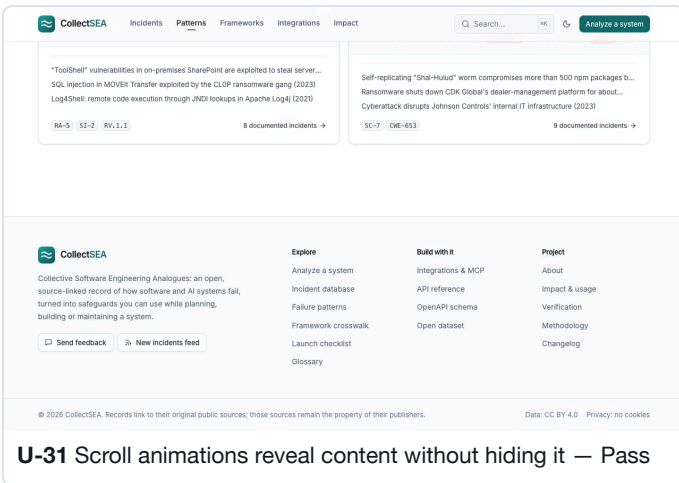
U-27 Dataset download from the page — Pass



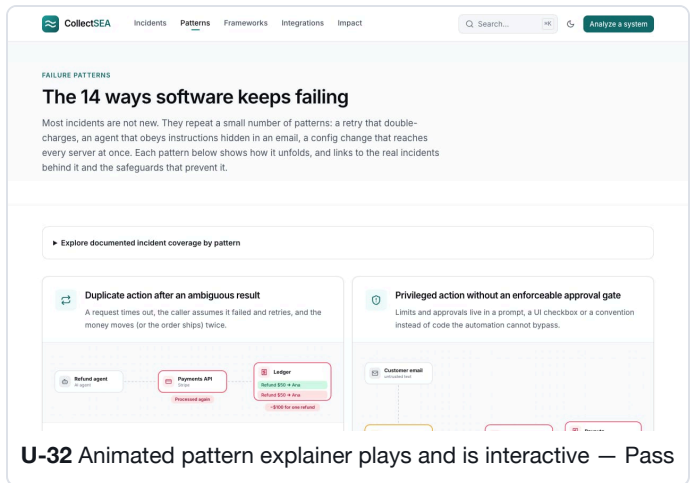
U-28 Impact and verification pages render live data — Pass



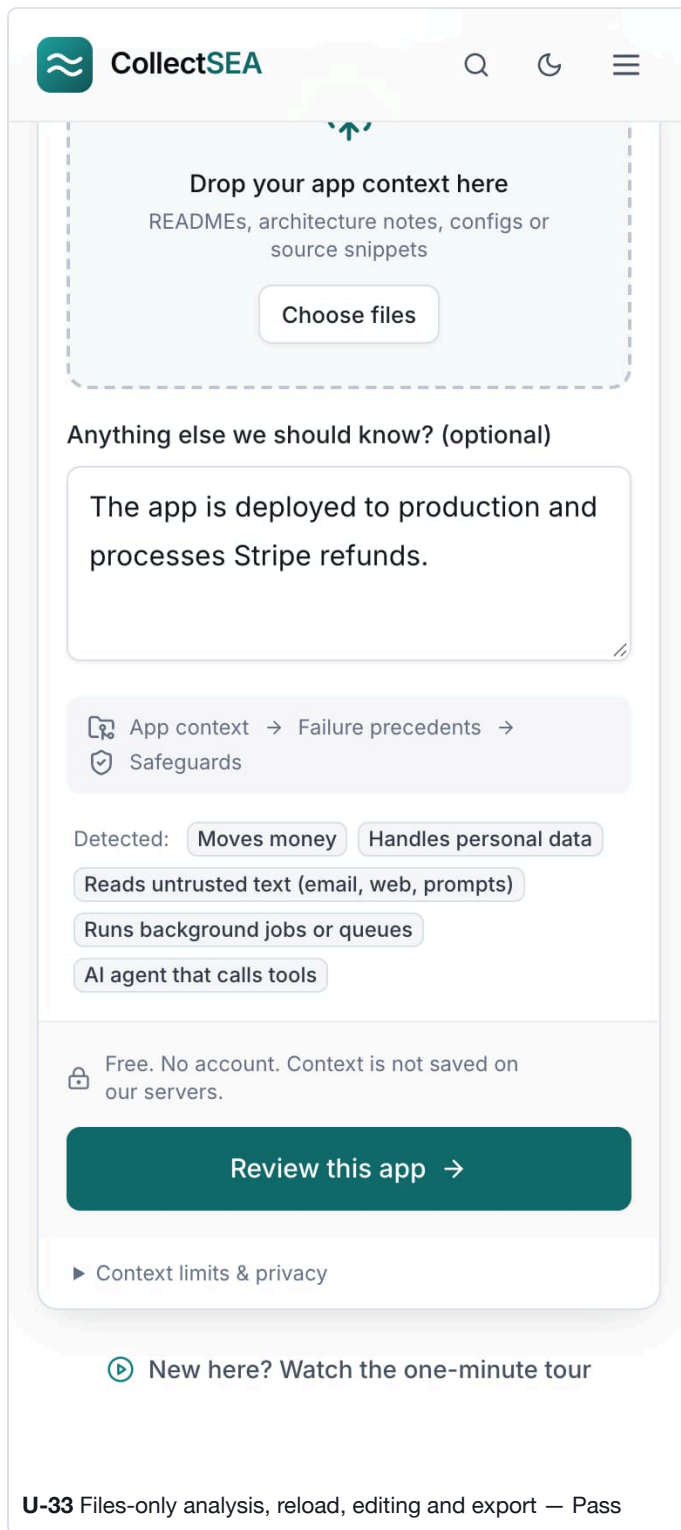
U-29 Unknown page — Pass



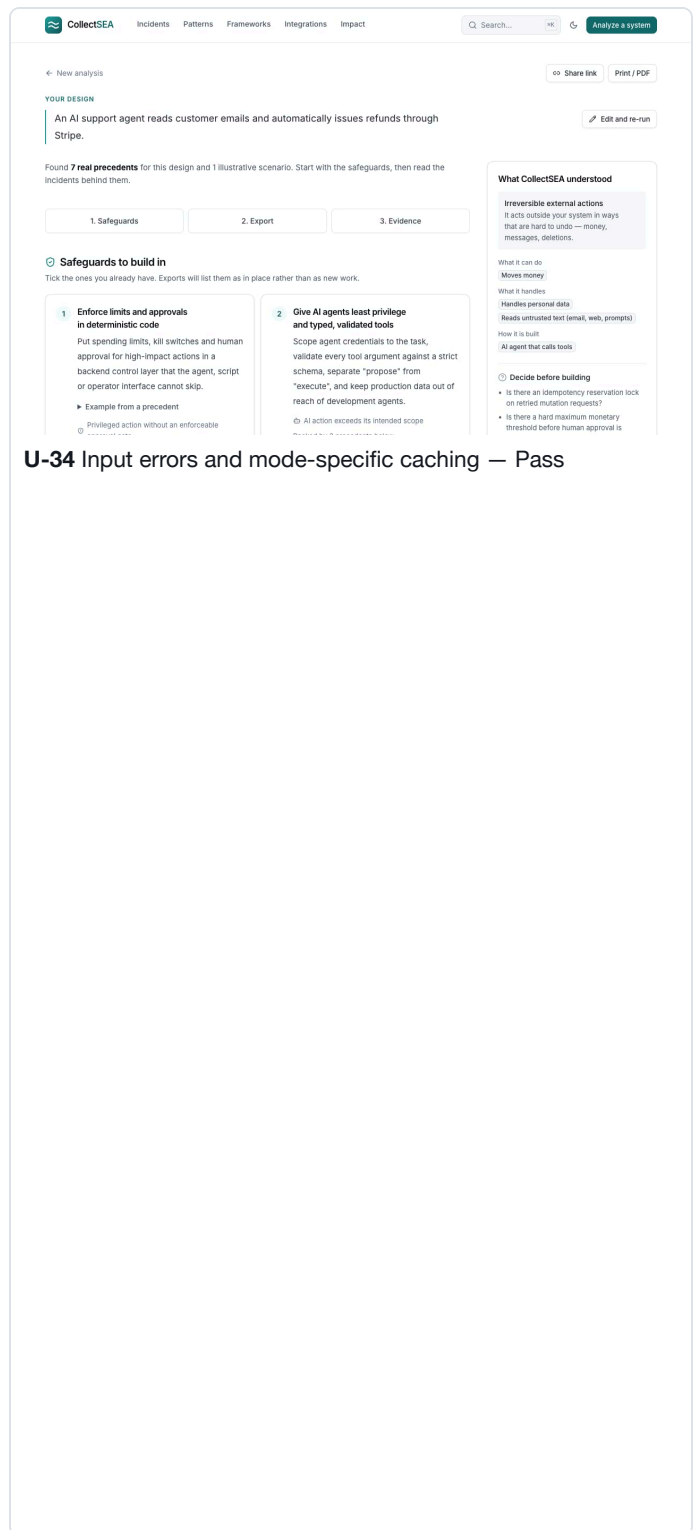
U-31 Scroll animations reveal content without hiding it — Pass



U-32 Animated pattern explainer plays and is interactive — Pass



U-33 Files-only analysis, reload, editing and export — Pass



U-34 Input errors and mode-specific caching — Pass



CollectSEA



 New analysis

 Share link

Print / PDF

YOUR APP REVIEW

The app processes payments and issues refunds through a payment API. An AI agent reads untrusted user messages and external content and calls tools.

 Edit and re-run

Based only on submitted descriptions and text files. Detected behaviors are signals to verify against the running app; code paths, deployed configuration and safeguards have not been verified. No repository or live app was crawled, executed or scanned.

Found **7 real precedents** for this app and 1 illustrative scenario. Start with the safeguards, then read the incidents behind them.

1. Safeguards

2. Export

3. Evidence

 **Safeguards to verify**

Tick the ones you already have. Exports will list them as in place rather than as new work.

U-35 Quick review without uploads — Pass

CollectSEA

IncidentsPatternsFrameworksIntegrationsImpact

Q Search...HEGAnalyze a system

308

Where will you use it?

AGENTS.md

Shared project guidance

CLAUDE.md

Claude Code

Cursor rule

Cursor project rule

Copilot instructions

GitHub Copilot

Review (Markdown)

Team review

()

JSON

Full result for your tools

Your file

collectsea-design-review.md

Attach this review to your design document or pull request. Discuss which safeguards apply.

Copy

Download

Downloaded collectsea-design-review.md

Preview the complete file

Real incidents like this system

Ranked by how closely each system behaved like yours. Labels show how much each record can be trusted.

#1 Documented incident Disclosed 2024-05-24

Google Cloud (unSapier)

Blank provisioning parameter leads to automatic deletion of a customer's private cloud

#2 Documented incident Incident 2022-04-05

Atlassian

Deletion script given site IDs instead of app IDs removes 775 customers' data (Atlassian 2022)

What CollectSEA understood

Inevitable external actions

It acts outside your system in ways that are hard to undo — money, messages, deletions.

What it can do

Moves money · Deletes things · Changes infrastructure · Changes data

What it handles

Publishes content publicly · Handles personal data

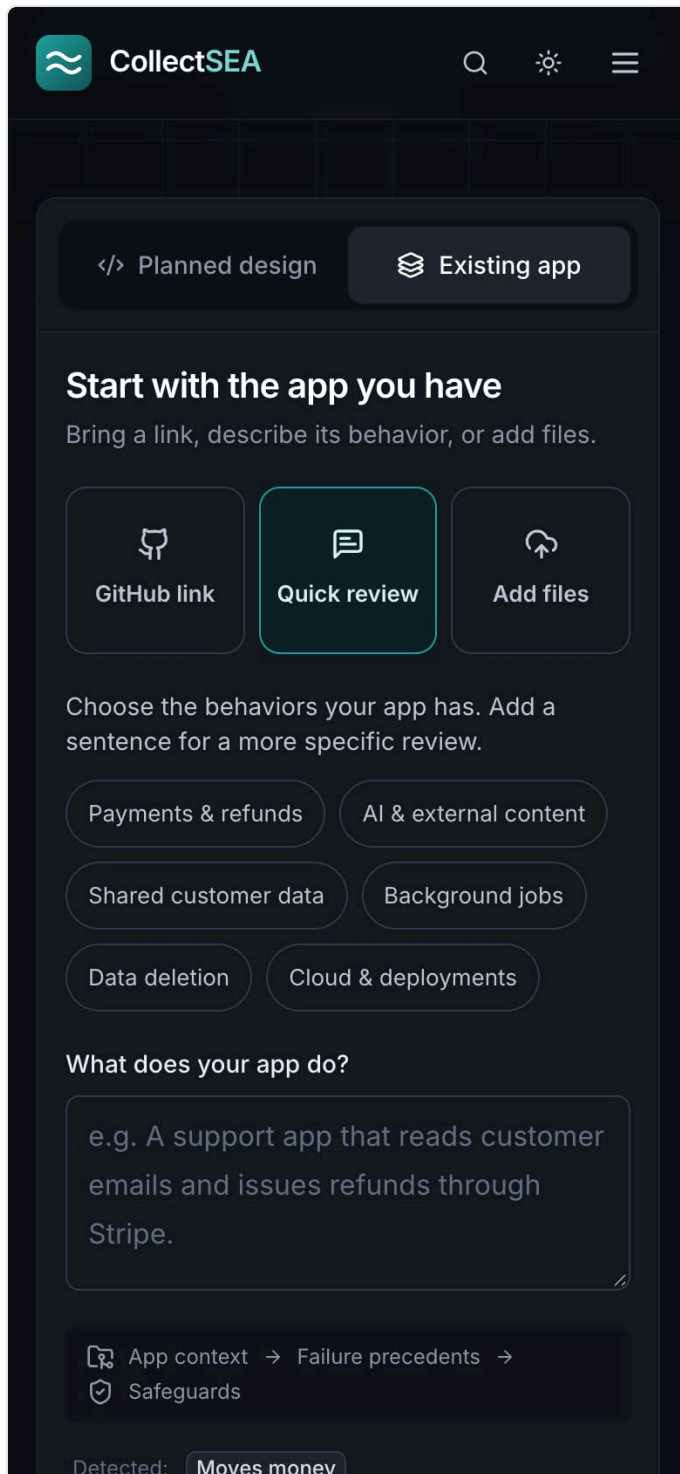
How it is built

Runs background jobs or queues · Reacts to webhooks or events

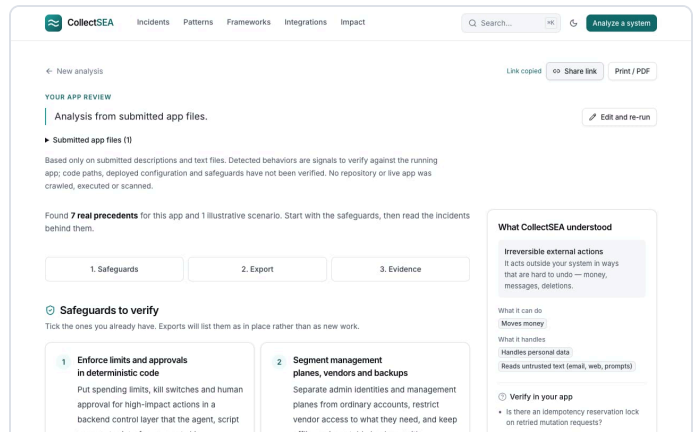
Verify in your app

- Is there an idempotency reservation lock on retried mutation requests?
- Is there a hard maximum monetary threshold before human approval is required?
- Is there a soft-delete grace period before permanent physical deletion?
- Does bulk teardown require two-person cryptographic sign-off?

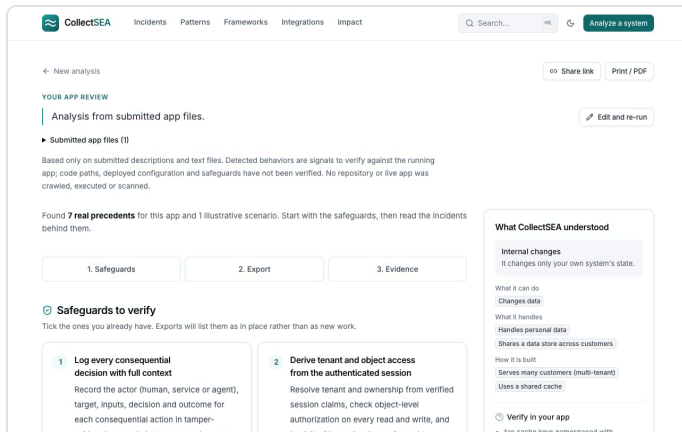
U-36 Public GitHub import, source preview and review — Pass



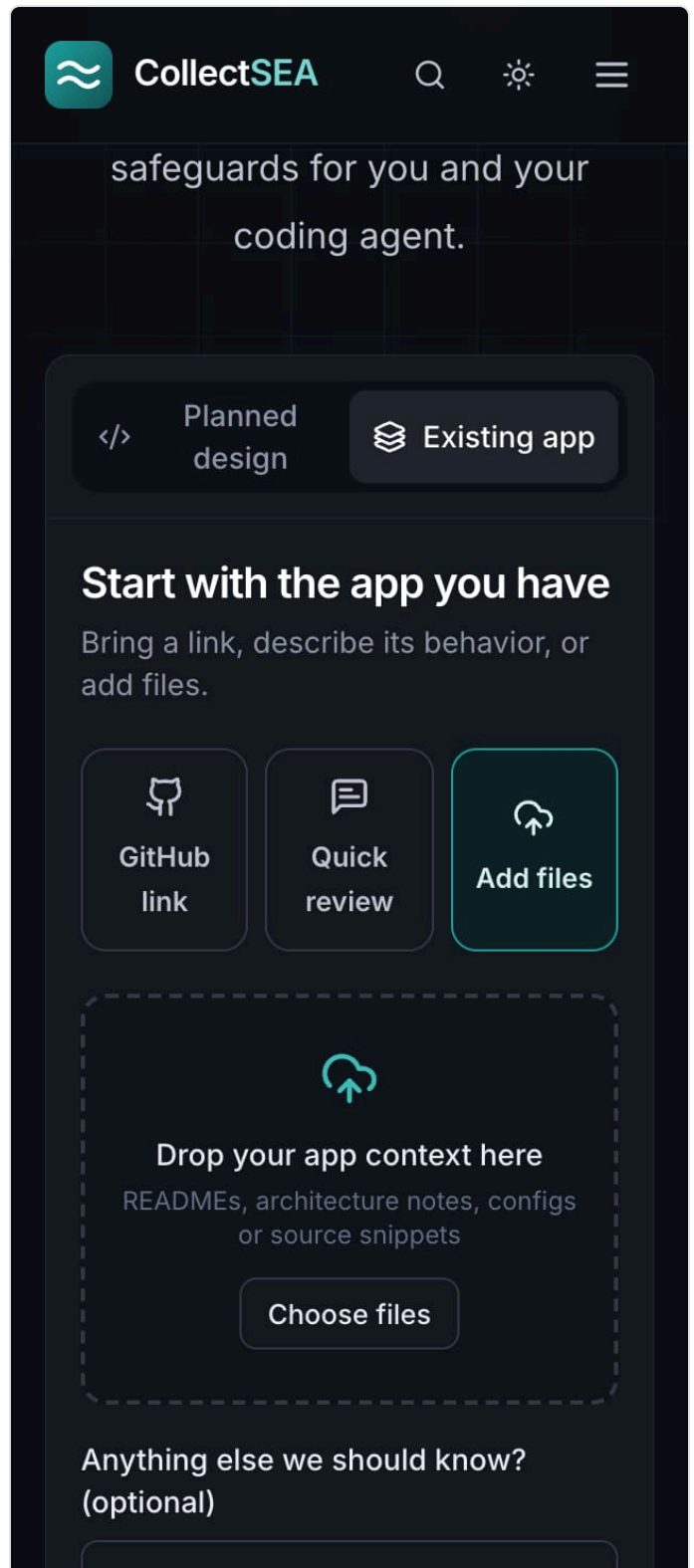
U-37 Unfinished review survives refresh and return navigation — Pass



U-38 Shared file review preserves sources in a fresh tab — Pass



U-39 Mixed source provenance and file removal — Pass



U-40 Narrow phone layout — Pass

CollectSEAIncidentsPatternsFrameworksIntegrationsImpact

Q Search...Analyze a system

< New analysis

Share linkPrint / PDF

YOUR APP REVIEW

Background workers process queued tasks with retries.

Edit and re-run

Based only on submitted descriptions and test files. Detected behaviors are signals to verify against the running app; code paths, deployed configuration and safeguards have not been verified. No repository or live app was crawled, executed or scanned.

Found 1 real precedent for this app and 1 illustrative scenario. Matches are partial overlaps. Treat them as prompts for design questions, not proof of risk.

1. Safeguards2. Export3. Evidence

Safeguards to verify

Tick the ones you already have. Exports will list them as in place rather than as new work.

1. Bound retries, loops and expensive work

Use capped exponential backoff with jitter, retry budgets and circuit breakers, and put hard limits on iterations, cost and CPU per request.

Example from a precedent

2. Design multi-step workflows to converge

Use an outbox or saga with compensating steps, order and version events so stale ones are ignored, and reconcile against the system of record on a schedule.

* Partial success leaves systems out of sync

What CollectSEA understood

Read-only

It observes but does not change anything.

How it is built

Runs background jobs or queues

Verify in your app

Are client-side mutation retries bound to unique idempotency keys?
Is telemetry logging configured with prompt context and failure reason codes?

Was this useful?

U-41 Import error recovery — Pass

CollectSEAIncidentsPatternsFrameworksIntegrationsImpact

Q Search...Analyze a system

< New analysis

Share linkPrint / PDF

YOUR APP REVIEW

An AI agent reads untrusted user messages and external content and calls tools.

Edit and re-run

Based only on submitted descriptions and test files. Detected behaviors are signals to verify against the running app; code paths, deployed configuration and safeguards have not been verified. No repository or live app was crawled, executed or scanned.

Found 6 real precedents for this app and 1 illustrative scenario. Start with the safeguards, then read the incidents behind them.

1. Safeguards2. Export3. Evidence

Offline analysis

The CollectSEA service could not be reached, so this analysis ran in your browser with keyword matching only. Results may be less relevant; try again later for semantic matching against the live corpus.

Found 6 real precedents for this app and 1 illustrative scenario. Start with the safeguards, then read the incidents behind them.

Safeguards to verify

Tick the ones you already have. Exports will list them as in place rather than as new work.

1. Give AI agents least privilege and typed, validated tools

Scope agent credentials to the task.

2. Treat content the model reads as data, never as instructions

Keep untrusted content out of instruction

What CollectSEA understood

Read-only

It observes but does not change anything.

How it handles

Handles personal data
Reads untrusted text (email, web, prompts)
How it is built
AI agent that calls tools

Verify in your app

Are client-side mutation retries bound to unique idempotency keys?
Is telemetry logging configured with prompt context and failure reason codes?

U-42 Offline review fallback — Pass

CollectSEAIncidentsPatternsFrameworksIntegrationsImpact

Q Search...Analyze a system

FAILURE ANALYSIS FOR PLANNED AND EXISTING SOFTWARE

Learn from real software failures at every stage

Describe a planned system or add context from an existing app. CollectSEA finds real outages, breaches and AI-agent failures from systems that behaved like yours, and turns them into safeguards for you and your coding agent.

Planned designExisting app

Describe what you're building: what it does, what it can change, and what it touches.

Free. No account. Context is not saved on our servers.

Find similar failures →

Run an example

U-43 Malformed shared context — Pass