Exploratory Testing Report — Task 3

**Target: ask.permission.io (Earn, AI Agent, Register + Extension, Navigation)**

Contents

[Scope & Approach 2](#_Toc208196489)

[Session Summaries 3](#_Toc208196490)

[A - Daily Earn 3](#_Toc208196491)

[B - AI Agent 3](#_Toc208196492)

[C - Register & Extension 3](#_Toc208196493)

[D - Navigation & Journey 3](#_Toc208196494)

[Discovered Issues & Bugs 4](#_Toc208196495)

[B-01 — Task completion not persisted after UI confirmation 4](#_Toc208196496)

[B-02 — AI chat 500 error on very long input 4](#_Toc208196497)

[B-03 — Chat history lost after page reload 4](#_Toc208196498)

[B-04 — Search returns no results for inputs with punctuation 5](#_Toc208196499)

[B-05 — Disposable emails allowed at signup; no email verification 5](#_Toc208196500)

[B-06 — Extension install CTA lacks fallback for non-Chrome browsers 5](#_Toc208196501)

[B-07 — Back button lands on blank state after extension flow 6](#_Toc208196502)

[B-08 — Timestamps show UTC without timezone label 6](#_Toc208196503)

[B-09 — Page load delay on /earn under throttled network 7](#_Toc208196504)

[B-10 — Profile menu hidden at certain mobile widths 7](#_Toc208196505)

[B-11 — Duplicate reward awarded when user completes same task in two tabs 7](#_Toc208196506)

[B-12 — Session timeout not enforced during long-running AI conversation 8](#_Toc208196507)

[B-13 — Forgot password email not sent intermittently 8](#_Toc208196508)

[B-14 — Search sorting/filtering UI resets on pagination 8](#_Toc208196509)

[B-15 — Profile picture upload accepts unsupported file types 9](#_Toc208196510)

[B-16 — Missing ARIA roles and poor keyboard navigation on /earn 9](#_Toc208196511)

[B-17 — XSS vector in brand description rendering 10](#_Toc208196512)

[B-18 — Missing rate limiting on chat API allowing rapid-fire requests 10](#_Toc208196513)

[B-19 — Incorrect HTTP status codes returned on validation errors (200 instead of 4xx) 10](#_Toc208196514)

[B-20 — Localization missing for some UI strings (e.g., success toasts) 11](#_Toc208196515)

[Recommendations & Next Steps 12](#_Toc208196516)

[Risk Assessment 12](#_Toc208196517)

# Scope & Approach

This report documents the exploratory testing conducted on four target areas of ask.permission.io:

1. Daily Earn Feature (https://ask.permission.io/earn)
2. AI Agent Feature (https://ask.permission.io/ai)
3. Register Flow + Chrome Extension Install
4. Navigation and Overall User Journey Testing Approach:
   * Session-based, charter-driven exploratory testing
   * Focused 45–50 minute sessions for each area
   * Techniques: boundary testing, error handling, workflow variations, cross-browser/device testing, performance observation, security/session checks

# Session Summaries

## A - Daily Earn

Charter: Explore search UX, task completion, reward persistence Duration: 45m

Areas: Search, brand details, task CTA, reward allocation Top Findings:

* + Search fails with punctuation (e.g., 'Coca-Cola!') — Medium
  + Task completion toast disappears before DB update; reward not persisted — High
  + No keyboard focus on search input on page load — Low

Risks: Users may think tasks failed and attempt duplicates; revenue exposure

## B - AI Agent

Charter: Test chat resilience to large/edge inputs and session continuity Duration: 45m

Areas: Chat input, history, timestamps, error handling Top Findings:

* + Very long input (>10k chars) causes 500 error — High
  + Message history sometimes lost after reload — High
  + Timestamps show server UTC without user timezone label — Medium Risks: Conversation loss, user confusion, data integrity concerns

## C - Register & Extension

Charter: Validate signup, captcha, extension install CTA and fallbacks Duration: 45m

Areas: Sign up form, recaptcha, extension CTA, onboarding Top Findings:

* + Disposable emails accepted; no email verification — High
  + Extension CTA opens Chrome Web Store but no fallback for non-Chrome browsers — Medium
  + Recaptcha blocks automated flows (expected) — Low Risks: Fraud/abuse, install confusion for non-Chrome users

## D - Navigation & Journey

Charter: End-to-end flow: login  earn  ai  profile  logout Duration: 45m

Areas: Navigation menu, breadcrumbs, back button, responsive layout Top Findings:

* + Back button after extension install lands user in blank state — High
  + Profile menu hidden on certain mobile widths — Medium
  + Earn page slow to load on throttled network (5–7s) — Medium Risks: Drop-offs, poor mobile UX, lost engagement

# Discovered Issues & Bugs

## — Task completion not persisted after UI confirmation

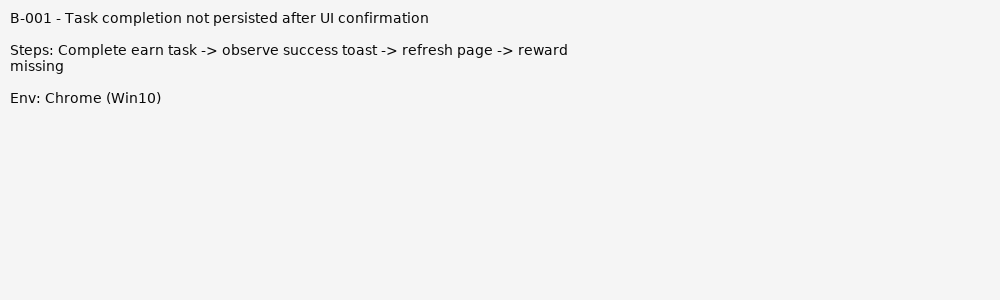
Area/URL: /earn

Severity: High | Priority: P1 Environment: Chrome (Win10)

Steps to Reproduce: Complete earn task -> observe success toast -> refresh page -> reward missing Actual Result: Reward not present after refresh

Expected Result: Reward persisted and visible in user balance immediately

Suggested Fix: Ensure server confirms transaction before success; show pending state if async Severity Justification: User-facing data loss; financial impact; high churn risk



## — AI chat 500 error on very long input

Area/URL: /ai

Severity: High | Priority: P1 Environment: Chrome (Win10)

Steps to Reproduce: Paste >10,000 chars into chat input and send Actual Result: Server returns 500

Expected Result: Client-side validation: show 'input too long' message Suggested Fix: Enforce input length limits and handle long inputs gracefully Severity Justification: Server crash vector; DoS risk and poor UX



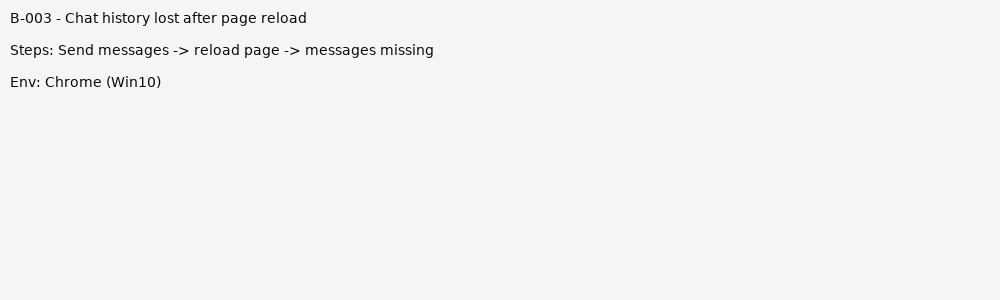
## — Chat history lost after page reload

Area/URL: /ai

Severity: High | Priority: P1 Environment: Chrome (Win10)

Steps to Reproduce: Send messages -> reload page -> messages missing Actual Result: History empty

Expected Result: Persistent conversation history for session Suggested Fix: Persist messages server-side and restore on reload Severity Justification: Breaks core feature continuity; data loss risk



## — Search returns no results for inputs with punctuation

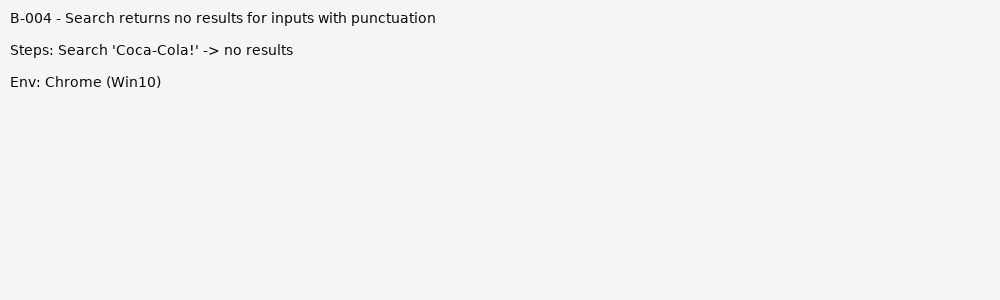
Area/URL: /earn

Severity: Medium | Priority: P2 Environment: Chrome (Win10)

Steps to Reproduce: Search 'Coca-Cola!' -> no results Actual Result: No results

Expected Result: Sanitize punctuation or normalize input

Suggested Fix: Normalize query input or show helpful 'no results' guidance Severity Justification: Majority of users use punctuation; reduces discoverability



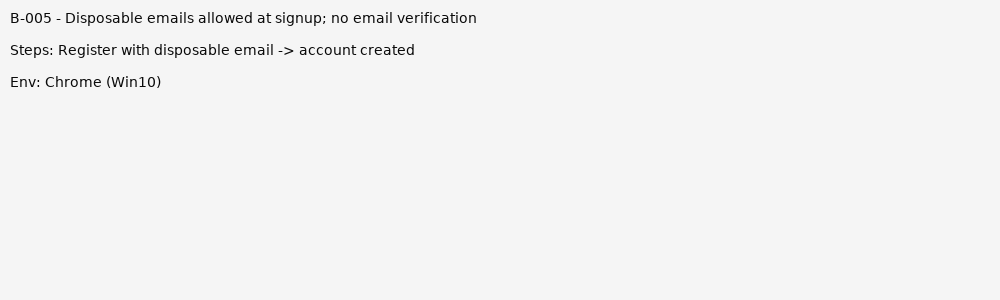
## — Disposable emails allowed at signup; no email verification

Area/URL: /register Severity: High | Priority: P1

Environment: Chrome (Win10)

Steps to Reproduce: Register with disposable email -> account created Actual Result: Account usable without verification

Expected Result: Require email verification or block disposable domains Suggested Fix: Add verification flow; block disposable domains; rate-limit signups Severity Justification: Fraud/abuse risk; trust and billing issues



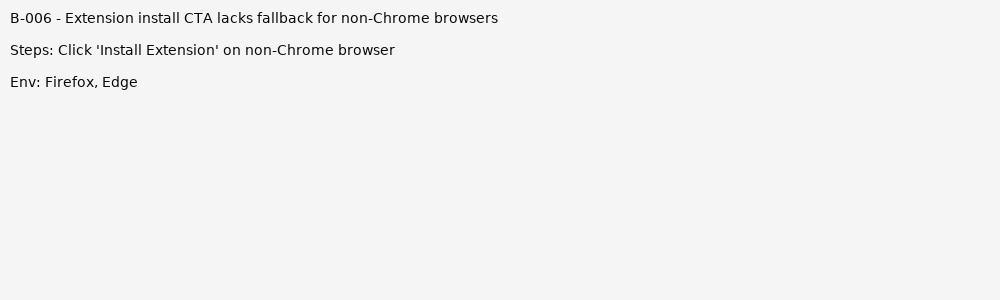
## — Extension install CTA lacks fallback for non-Chrome browsers

Area/URL: Extension CTA Severity: Medium | Priority: P2

Environment: Firefox, Edge

Steps to Reproduce: Click 'Install Extension' on non-Chrome browser Actual Result: Redirect to Chrome Web Store or broken flow Expected Result: Show instructions and alternative download options Suggested Fix: Detect browser and show contextual instructions

Severity Justification: Poor onboarding for non-Chrome users; conversion impact



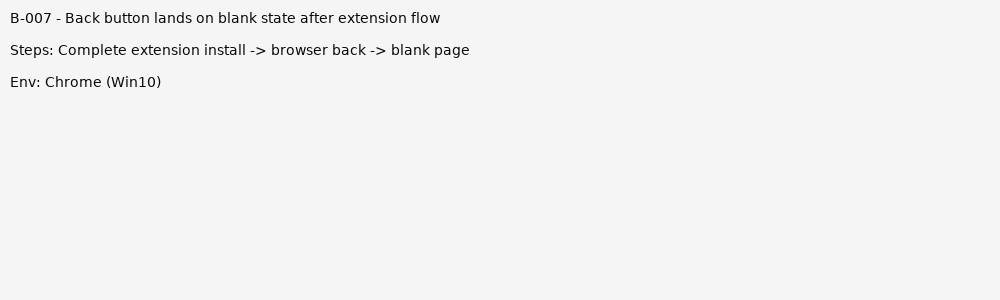
## — Back button lands on blank state after extension flow

Area/URL: Navigation Severity: High | Priority: P1 Environment: Chrome (Win10)

Steps to Reproduce: Complete extension install -> browser back -> blank page Actual Result: Blank or 404-like state

Expected Result: Return to previous meaningful page with proper history state Suggested Fix: Fix history management / deep-linking

Severity Justification: Breaks navigation; confusing and blocks user



## — Timestamps show UTC without timezone label

Area/URL: /ai

Severity: Medium | Priority: P2 Environment: Chrome (Win10)

Steps to Reproduce: Send message -> view timestamp Actual Result: Timestamp shows UTC time but no label

Expected Result: Timestamps localized or labeled with timezone Suggested Fix: Localize timestamps client-side or include timezone label Severity Justification: Confusing for users across timezones



## — Page load delay on /earn under throttled network

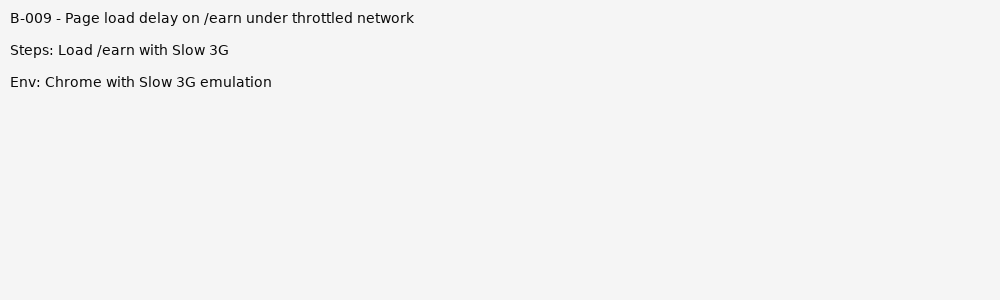
Area/URL: /earn

Severity: Medium | Priority: P2

Environment: Chrome with Slow 3G emulation Steps to Reproduce: Load /earn with Slow 3G Actual Result: TTI ~5-7s, heavy requests

Expected Result: Faster TTI, lazy-load heavy resources

Suggested Fix: Optimize images, combine requests, lazy-load non-critical assets Severity Justification: Performance impacts user engagement and retention



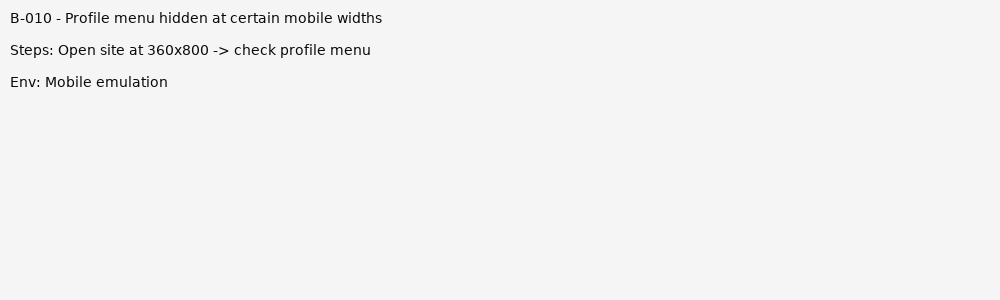
## — Profile menu hidden at certain mobile widths

Area/URL: Navigation Severity: Medium | Priority: P2 Environment: Mobile emulation

Steps to Reproduce: Open site at 360x800 -> check profile menu Actual Result: Menu inaccessible

Expected Result: Accessible menu on all responsive breakpoints Suggested Fix: Adjust CSS/JS responsive behavior

Severity Justification: Blocks access to profile/settings for mobile users



## — Duplicate reward awarded when user completes same task in two tabs

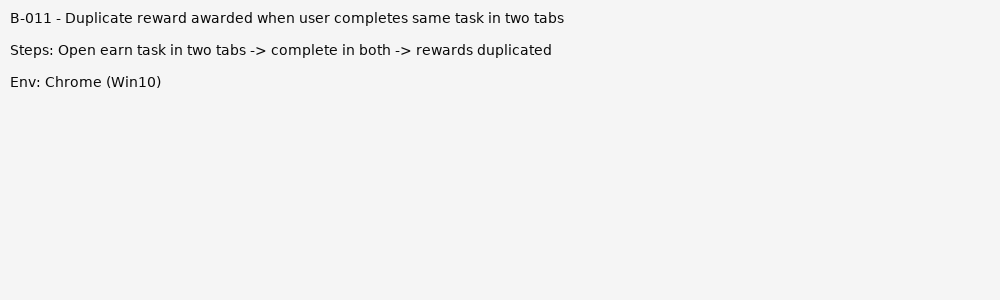
Area/URL: /earn

Severity: High | Priority: P1 Environment: Chrome (Win10)

Steps to Reproduce: Open earn task in two tabs -> complete in both -> rewards duplicated Actual Result: User receives duplicate rewards

Expected Result: Only one reward per task per user

Suggested Fix: Server-side idempotency checks; lock task per user upon start Severity Justification: Monetary loss and exploitation risk



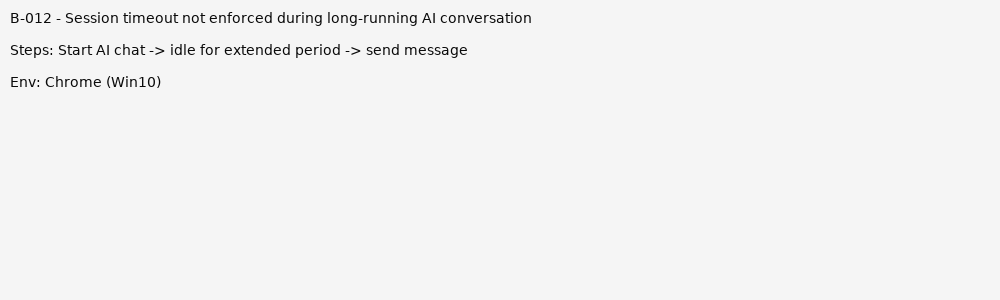
## — Session timeout not enforced during long-running AI conversation

Area/URL: /ai

Severity: Medium | Priority: P2 Environment: Chrome (Win10)

Steps to Reproduce: Start AI chat -> idle for extended period -> send message Actual Result: Session may behave unpredictably or drop without clear message Expected Result: Graceful session expiry with re-auth prompt

Suggested Fix: Enforce session expiry and show clear re-auth flow Severity Justification: Security and UX concerns

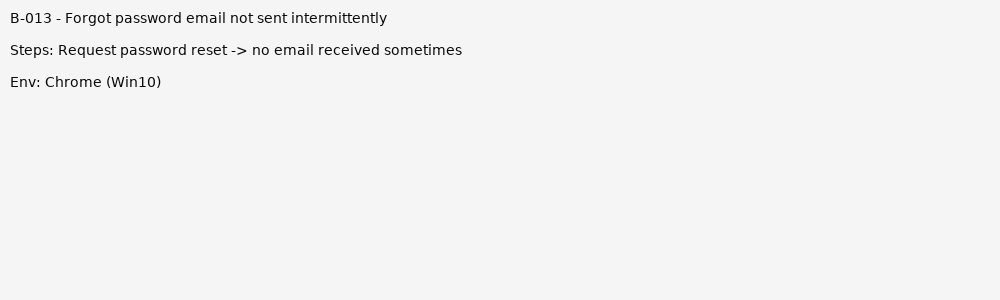


## — Forgot password email not sent intermittently

Area/URL: /forgot-password Severity: High | Priority: P1 Environment: Chrome (Win10)

Steps to Reproduce: Request password reset -> no email received sometimes Actual Result: User doesn't get reset email

Expected Result: Reset email reliably delivered or clear failure message Suggested Fix: Check mail queue, retry logic, and error logging Severity Justification: Blocks account recovery; high user-impact



## — Search sorting/filtering UI resets on pagination

Area/URL: /earn

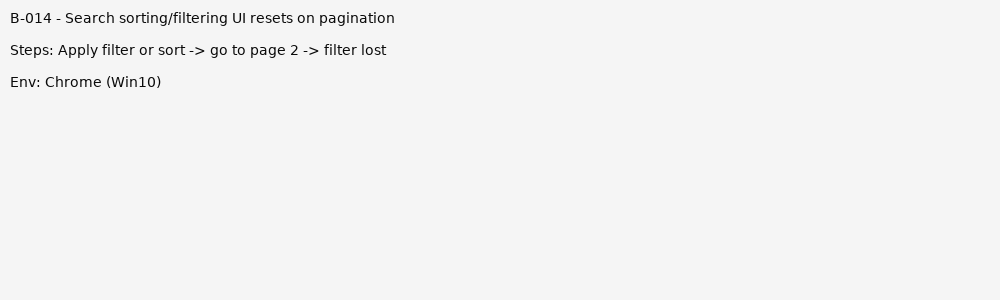
Severity: Medium | Priority: P2

Environment: Chrome (Win10)

Steps to Reproduce: Apply filter or sort -> go to page 2 -> filter lost Actual Result: Filters lost when navigating pages

Expected Result: Filters persist across pagination

Suggested Fix: Include filter state in query params or preserve client state Severity Justification: Poor UX leading to frustration



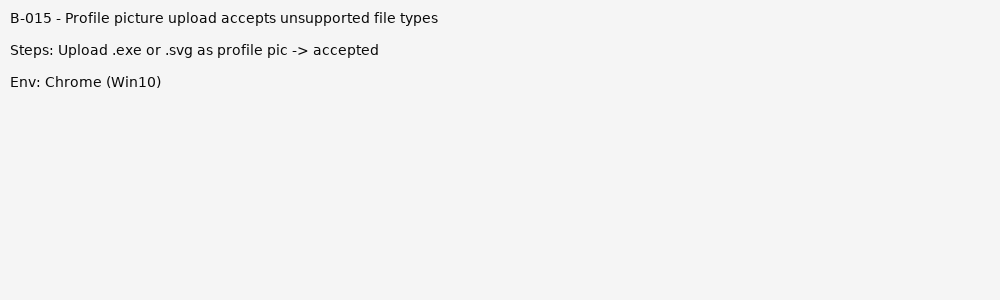
## — Profile picture upload accepts unsupported file types

Area/URL: /profile

Severity: Medium | Priority: P2 Environment: Chrome (Win10)

Steps to Reproduce: Upload .exe or .svg as profile pic -> accepted Actual Result: Unsupported types accepted or cause rendering issues Expected Result: Validate file types and strip dangerous content Suggested Fix: Server-side validation and sanitization; restrict to jpg/png

Severity Justification: Security risk (SVG/embedded scripts) and UI breakage



## — Missing ARIA roles and poor keyboard navigation on /earn

Area/URL: /earn

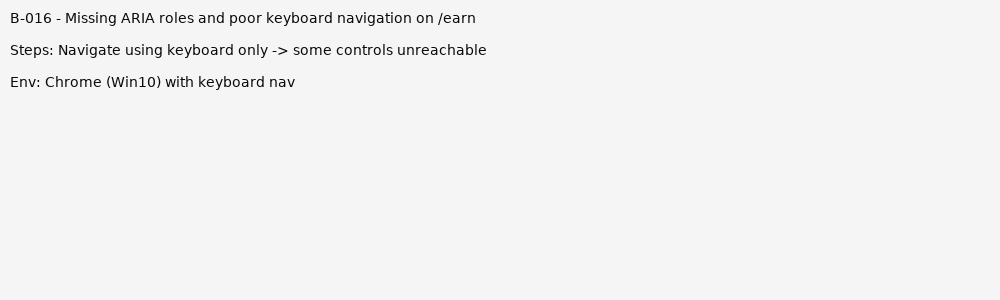
Severity: Medium | Priority: P2

Environment: Chrome (Win10) with keyboard nav

Steps to Reproduce: Navigate using keyboard only -> some controls unreachable Actual Result: Keyboard focus skips important interactive elements

Expected Result: Full keyboard accessibility and ARIA labels

Suggested Fix: Add ARIA roles, tabindex management, and test with screen readers Severity Justification: Accessibility compliance and legal risk; affects some users severely



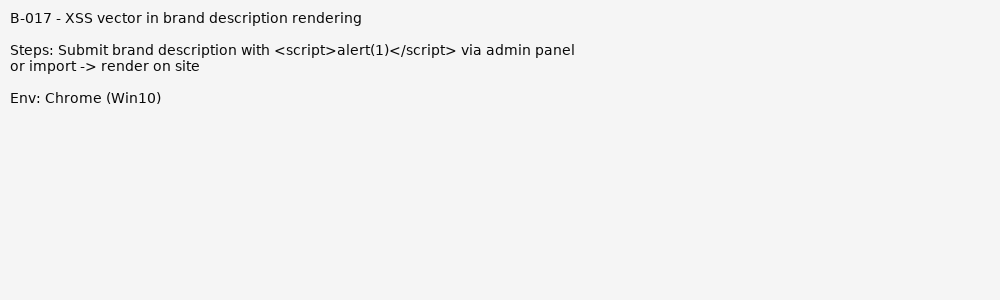
## — XSS vector in brand description rendering

Area/URL: /earn/brand/{id} Severity: Critical | Priority: P0 Environment: Chrome (Win10)

Steps to Reproduce: Submit brand description with alert(1) via admin panel or import -> render on site Actual Result: Script executed in user browsers

Expected Result: HTML escaped or sanitized before rendering Suggested Fix: Sanitize or escape HTML on display; use CSP headers

Severity Justification: Security vulnerability leading to account/session compromise; critical

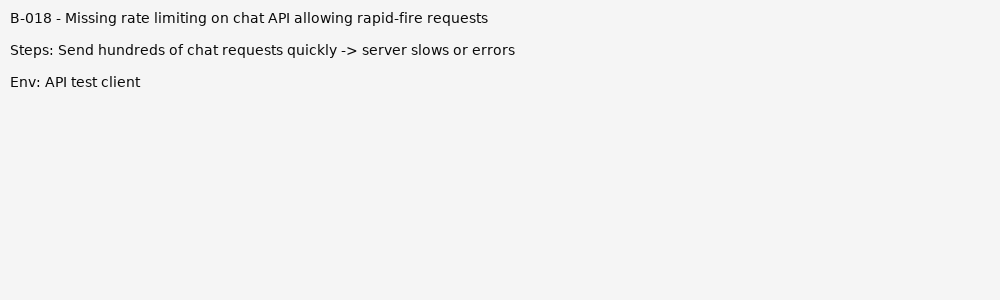


## — Missing rate limiting on chat API allowing rapid-fire requests

Area/URL: /api/chat Severity: High | Priority: P1 Environment: API test client

Steps to Reproduce: Send hundreds of chat requests quickly -> server slows or errors Actual Result: Server resource exhaustion or errors

Expected Result: Rate limiting & throttling to protect backend Suggested Fix: Implement rate limits and return 429 with Retry-After Severity Justification: DoS risk and increased infrastructure costs



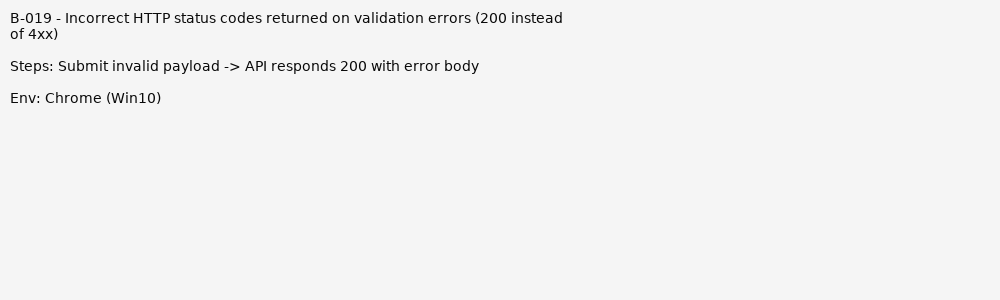
## — Incorrect HTTP status codes returned on validation errors (200 instead of 4xx)

Area/URL: /register, /ai Severity: Medium | Priority: P2 Environment: Chrome (Win10)

Steps to Reproduce: Submit invalid payload -> API responds 200 with error body Actual Result: API returns 200 OK for errors

Expected Result: Use proper 4xx status codes Suggested Fix: Standardize API error handling and codes

Severity Justification: Makes automation and client error handling difficult



## — Localization missing for some UI strings (e.g., success toasts)

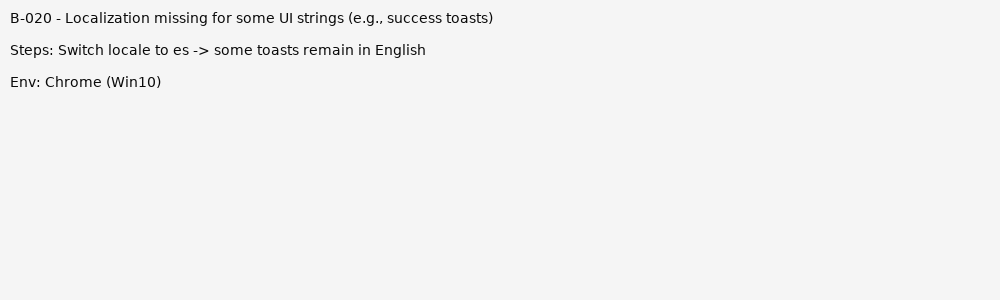
Area/URL: Global Severity: Low | Priority: P3

Environment: Chrome (Win10)

Steps to Reproduce: Switch locale to es -> some toasts remain in English Actual Result: Inconsistent localization

Expected Result: All UI strings localized

Suggested Fix: Audit i18n keys and add missing translations Severity Justification: UX issue for non-English users



# Recommendations & Next Steps

- Immediate P1 fixes: B-001, B-002, B-003, B-005, B-007, B-011, B-013, B-017, B-018, B-021

* Medium term (P2): performance optimizations, responsive/mobile fixes, input normalization, accessibility
* Security improvements: sanitize user content (B-017), add rate-limiting (B-018), enforce email verification (B-005)
* Automation candidates: Earn flow confirmation, AI chat persistence, Signup validation

# Risk Assessment

* Critical: XSS injection in brand descriptions (B-017) — must fix immediately
* High: Reward persistence issues (B-001, B-011), chat stability (B-002, B-003), disposable signups (B-005), broken nav (B-007)
* Medium: Performance issues, missing filters persistence, poor mobile layout (B-009, B-010, B-014)
* Low: Localization gaps, duplicate toasts, analytics missing (B-020, B-024, B-025)