

# Security Audit Summary

## Scope

Review of the public conversion flow, waitlist capture, and technical event logging for NEXO Free.

## Findings Snapshot

Area	Severity	Status
Conversion payload validation	Medium	Mitigated
Waitlist duplicate protection	Low	Mitigated
Secret handling in local environments	High	Needs follow-up

## Key Findings

### 1. Conversion API validation

The conversion endpoint validates file counts, payload size, attachment size, and logo constraints before rendering.

### 2. Waitlist duplicate handling

The waitlist flow guards against duplicate e-mails and returns a clear response for already-registered users.

### 3. Local secret exposure risk

Local development can become unsafe if service-role or provider keys are committed into tracked environment files.

## Recommended Actions

1. Move production secrets to deployment environment variables only
2. Add a pre-release checklist for environment hygiene
3. Keep free-tier logging as best-effort, never blocking the core conversion flow

## Executive Summary

The product is in a solid position for public validation, with the highest-priority follow-up focused on secret-management discipline before broader launch.