PartyShaarty

Pre-Launch Review Report

Security · Privacy · Legal · Scaling · Content Safety

Generated: February 2026 | Codebase: Next.js 14 + Supabase | Branch: main

Executive Summary

This report covers everything you must address before launching PartyShaarty to the public. It is based on a full review of your API routes, authentication flows, database schema, file upload handling, email sending, and overall architecture. Items are prioritized by risk.

Category	Current Status	Priority
Authentication (Host)	✓ Good — Supabase OAuth + session cookies	—
Guest Auth (Gallery OTP)	⚠ Partial — weak secret fallback	Critical
File Upload Security	✕ No file size limits; no content validation	Critical
Email Template Security	✕ XSS via unescaped user content	Critical
Rate Limiting	✕ OTP only; no global throttling	Critical
Input Validation	⚠ Minimal; no sanitization	High
CSRF Protection	⚠ Relies only on SameSite=Lax	High

Privacy Policy / ToS	✕ Completely missing	Legal blocker
Email Compliance (Unsubscribe)	✕ No unsubscribe links	Legal blocker
Right to Erasure / Export	✕ No account deletion or data export	Legal blocker
Image Content Moderation	✕ No scanning for illegal content	High (Legal)
Email Sending (Gmail SMTP)	✕ 500/day limit — will fail at scale	Scaling blocker
Database / Storage Quotas	✕ No per-host limits enforced	High
Content Moderation (Text)	✕ No filtering on user-generated text	Medium
Database RLS	✓ Enabled on all tables	—
Pagination	✕ Hard 500-photo cap; no cursor pagination	Medium

1. Critical Security Issues

Fix all of these before any public traffic hits your app.

CRITICAL

#1 — No File Size Limits on Uploads

Affected files: `app/api/gallery/albums/[albumId]/photos/route.js`, `app/api/host/events/[eventId]/route.js`, `app/api/host/profile/route.js`

All upload endpoints accept files of unlimited size. A single user can upload a 10 GB video file disguised as a JPEG, exhausting your Supabase storage quota in minutes. There is also no batch-size limit, so a guest could upload thousands of tiny files simultaneously.

FIX

Add a `MAX_FILE_SIZE` env variable (suggest 10 MB per photo). Reject oversized files server-side before streaming to Supabase. Also add a max batch count (e.g., 20 photos per upload request).

CRITICAL

#2 — XSS in Outbound Email Templates

Affected files: `app/api/reminders/send/route.js`, `app/api/thankyou/send/route.js`, `app/api/gallery/verify/route.js`

User-supplied content (event names, guest names, RSVP messages, custom email body text) is embedded directly into HTML email templates using `.replace(/\n/g, "<br>")` without any HTML escaping. The `linkify()` function converts URLs to `<a>` tags with unescaped href attributes. A guest named `<script>...</script>` or a message containing `<img src=x onerror=...>` will be injected into emails sent to every recipient.

FIX

Install the `he` or `escape-html` npm package. Escape all user-provided strings before embedding in HTML: `he.escape(userInput)`. Sanitize URLs in `linkify()` to only allow `http://` and `https://` schemes.

CRITICAL

#3 — Weak Guest Session Secret Fallback

Affected file: `lib/guest-auth.js`

The HMAC secret used to sign guest gallery session cookies falls back to `HOST_SESSION_SECRET` and then to the hardcoded string `"change-me"` if `GUEST_SESSION_SECRET` is not set. Anyone who knows this default can forge valid guest session cookies and gain access to any shared gallery without going through OTP verification.

FIX

Throw a startup error if `GUEST_SESSION_SECRET` is not set in the environment. Generate a cryptographically random 32-byte value (`openssl rand -base64 32`) and set it in all deployment environments.

CRITICAL

#4 — No Rate Limiting on Public Endpoints

Affected files: `app/api/rsvp/route.js`, `app/api/gallery/verify/route.js` (partial — OTP has 5-attempt limit but no IP throttling)

The public RSVP submission endpoint (`POST /api/rsvp`) has zero throttling. A bot can submit thousands of fake RSVPs in seconds, polluting guest lists and triggering thousands of outbound emails. There is no IP-level rate limiting anywhere in the app.

FIX

Use `@upstash/ratelimit` with Upstash Redis (free tier available, works on Vercel Edge). Apply limits: 10 RSVPs/IP/minute on public RSVP, 5 OTP requests/IP/hour on gallery verify. Add rate limit headers to all public responses.

CRITICAL

#5 — No Image Content Validation Server-Side

Affected file: `app/api/gallery/albums/[albumId]/photos/route.js`

Photo uploads only check `file.type.startsWith("image/")` — this is a client-supplied MIME type that is trivially spoofed. A malicious actor can rename any file to `.jpg` and upload it. No server-side magic-byte or image header validation is performed.

FIX

Use the `sharp` library to attempt to decode each uploaded file. If `sharp` cannot parse it as a valid image, reject the upload. As a bonus, `sharp` can also strip EXIF metadata (location data) from photos before storing them — important for guest privacy.

2. High Priority — Fix Within First Week

HIGH

#6 — Email Injection via nodemailer

Affected file: `lib/mailer.js`, `app/api/reminders/send/route.js`

User-supplied email addresses are passed directly to nodemailer as `to:` and `replyTo:` values without format validation. An email address containing newlines or special characters can inject additional mail headers (BCC, CC, X-Mailer), potentially turning your app into a spam relay.

FIX

Validate all email addresses with `zod` (`z.string().email()`) before passing to nodemailer. Strip or reject any input containing newline characters (`\n` , `\r`).

HIGH

#7 — OTP Error Messages Leak RSVP Data

Affected file: `app/api/gallery/verify/route.js`

The OTP endpoint returns different error messages for "email not in RSVP list" vs "attending = No". This lets an attacker enumerate who was invited to a private event and whether they are attending.

FIX

Return the same generic 403 message for all access-denied cases: `"Access not available for this email."`

HIGH

#8 — No Content Security Policy (CSP)

Affected file: `middleware.js`

No `Content-Security-Policy` HTTP header is set anywhere. Without CSP, any XSS vulnerability in your dashboard allows an attacker to run arbitrary JavaScript, exfiltrate host auth cookies, or steal the entire RSVP list.

FIX

Add a CSP header in `middleware.js` on all responses. At minimum: `default-src 'self'; img-src 'self' data: https://*.supabase.co; script-src 'self' 'nonce-...'`. Use Next.js nonce-based CSP for inline scripts.

HIGH #9 — Gmail SMTP Will Fail at Scale

Affected file: `lib/mailer.js`

Gmail's SMTP limit is 500 emails per day. A single host sending reminders to 200 guests plus thank-you emails plus OTPs will hit this limit in one event. When it hits, all email sending silently fails — guests don't get OTPs and can't access galleries.

FIX

Switch to a transactional email service before launch: **Resend** (free tier: 3,000 emails/month), **Postmark**, or **AWS SES**. These also provide delivery tracking, bounce handling, and DKIM/SPF authentication automatically.

HIGH #10 — No Per-Host Storage or Event Quotas

Affected files: `lib/event-store.js`, `lib/gallery-store.js`

A single host can create unlimited events, upload unlimited photos, and store unlimited data in your Supabase account. There is no cost protection. Your storage bill is entirely at the mercy of your users.

FIX

Enforce server-side limits: max 5 events per host, max 500 RSVPs per event, max 2 GB storage per host. Check these limits at creation time and return a 403 with a clear message when exceeded.

HIGH #11 — EXIF / Location Metadata in Uploaded Photos

Affected file: `app/api/gallery/albums/[albumId]/photos/route.js`

Photos uploaded by guests may contain EXIF metadata including GPS coordinates, device model, and timestamp. These are stored and served as-is. Guests sharing photos may unknowingly expose their home location or other private device data.

FIX

Use `sharp` to strip EXIF data from all uploaded images before storing to Supabase: `sharp(buffer).rotate().toBuffer()` (the `.rotate()` call respects EXIF orientation but strips the rest of the metadata).

3. Legal Requirements — These Are Launch Blockers

⚠ **IMPORTANT**

Operating without these legal documents exposes you to regulatory fines and civil liability. GDPR fines can reach €20 million or 4% of annual global turnover. India's DPDP Act 2023 imposes fines up to ₹250 crore.

3.1 Required Legal Documents

Document	Why Required	Status
Privacy Policy	GDPR, CCPA, DPDP Act — required for any site collecting personal data. Must cover what you collect, why, how long you keep it, and user rights.	✕ Missing
Terms of Service	Defines acceptable use, your liability limits, content ownership, and grounds for account termination. Protects you from abusive users.	✕ Missing
Cookie Policy	EU ePrivacy Directive requires disclosure of all cookies used. You set auth cookies and guest session cookies.	✕ Missing
Cookie Consent Banner	Required by GDPR for EU users before setting non-essential cookies.	✕ Missing

3.2 User Rights You Must Support

Right	Law	What You Need	Status
Right to Erasure	GDPR Art. 17, DPDP Act	Account deletion endpoint that removes all host data, events, RSVPs, photos, and the Supabase auth user	✕ Missing
Right to Data Portability	GDPR Art. 20	Full data export (you have RSVP export; extend to cover all personal data)	⚠ Partial
Right to Access	GDPR Art. 15	Users can request a copy of all data you hold about them	✕ Missing
Right to Rectification	GDPR Art. 16	Users can correct inaccurate personal data	⚠ Partial

3.3 Email Compliance (CAN-SPAM / GDPR)

Every outbound email from your app (reminders, thank-yous, OTPs) must comply with the following:

Requirement	Status
Unsubscribe link in every marketing/reminder email	✕ Missing
Physical postal address or PO Box in email footer	✕ Missing
Honour unsubscribes within 10 business days (CAN-SPAM)	✕ No mechanism
Explicit opt-in before sending marketing emails	⚠ Implied via RSVP; clarify in Privacy Policy
DKIM/SPF/DMARC authentication on sending domain	✕ Gmail SMTP without domain auth

⚠ IMMEDIATE ACTION

Even sending 10 reminder emails without unsubscribe links violates CAN-SPAM. This law applies to any commercial email sent to US recipients, regardless of where you are based.

3.4 Image & Content Legal Obligations

HIGH (Legal) **CSAM Detection Obligation**

By hosting user-uploaded images, you are legally required in many jurisdictions (US PROTECT Our Children Act, UK Online Safety Act, India IT Act) to detect and report Child Sexual Abuse Material (CSAM). Even if accidental, failure to have detection systems is a criminal liability.

FIX

Integrate **PhotoDNA** (Microsoft — free for qualifying startups), **AWS Rekognition** content moderation, or **Google Vision SafeSearch** API for all uploaded images. Report detections to NCMEC (US) as required by law.

4. Personal Data Handling

4.1 What Personal Data You Currently Store

Data Type	Table / Location	Who Can Access	Risk
Full name	`invite_rsvps.name`	Host (via RLS)	Low
Email address	`invite_rsvps.email`, `gallery_album_shares.email`, `otp_codes.email`	Host, service-role	High — PII
Phone number	`invite_rsvps.phone`	Host (via RLS)	High — PII
Personal photos	Supabase Storage `event-photos/`	Host; guests via signed URLs	High — biometric PII
RSVP messages	`invite_rsvps.message`	Host	Medium
Event attendance	`invite_rsvps.attending`	Host	Medium — reveals plans
Auth session tokens	Supabase Auth + browser cookies	Supabase + browser	High

4.2 Recommended Data Minimization Actions

> **Phone Numbers Stored in Plaintext**
>
> Phone numbers are displayed unmasked in the host dashboard. If your database is ever exposed, all guest phone numbers are immediately readable.
>
> **FIX**
>
> Only collect phone numbers if you actively use them (e.g., for WhatsApp). Display masked in dashboard (`+91 ****-**12`). Do not include phone numbers in CSV exports unless explicitly requested by the host with a confirmation step.

No Data Retention Policy

RSVP data, photos, and guest emails are stored indefinitely. GDPR requires you to only retain personal data for as long as necessary for its original purpose.

FIX

Define retention periods in your Privacy Policy (e.g., "RSVP data retained for 90 days after event date"). Implement a scheduled Supabase function or cron job to purge data beyond the retention window. Notify hosts before deletion.

Guest Photos May Contain Location Data (EXIF)

Photos uploaded by guests contain GPS coordinates, device model, timestamp, and other metadata. Guests may not realise this data is being shared with the host and other gallery viewers.

FIX

Strip EXIF metadata from all images on upload using `sharp`. Disclose this in your Privacy Policy and mention it as a privacy feature to guests.

5. Abuse & Content Safety

5.1 Content Moderation Gaps

MEDIUM **No Text Content Filtering**

RSVP names, messages, and event names are stored as-is and displayed in the host dashboard and emailed to guests. A guest can submit derogatory names, slurs, hate speech, or spam URLs in their RSVP message field.

FIX

Add server-side profanity/content filtering before storing RSVP text. Use the `bad-words` npm package for basic filtering, or integrate the **OpenAI Moderation API** (free) for more sophisticated text analysis. Block or flag submissions that trigger the filter.

MEDIUM **No Abuse Reporting Mechanism**

There is no way for guests or hosts to report inappropriate content, harassment, or misuse of the platform. Once you go public, you will need this.

FIX

Add a "Report Content" button on gallery pages and a "Report" link in the footer. Route reports to an admin email address. Create a simple `reports` table in Supabase to track reports.

MEDIUM **No Host Verification or Vetting**

Any email address can sign up and immediately start creating events, importing guest lists with hundreds of email addresses, and sending mass emails (reminders/thank-yous). There is no approval step, email domain verification, or identity check.

FIX

In the short term, require email verification before hosts can send mass communications (Supabase Auth handles this). Consider a daily send limit per host (e.g., 200 emails/day) until you have a review process for high-volume senders.

LOW **Guests Can Be Spammed by Malicious Hosts**

A host can import any email list (not just their actual guests) and send unlimited reminder and thank-you emails. There is no verification that imported emails actually consented to receive communications about this event.

FIX

Add a per-event daily send limit. Require confirmation before sending bulk emails. Log all bulk send events (timestamp, host, recipient count) for audit purposes.

5.2 Terms of Service Must Address

Your Terms of Service should explicitly prohibit:

- Uploading or sharing illegal content (CSAM, non-consensual intimate images)
- Harassment or threatening communications via the platform
- Importing email lists without recipient consent (spam)
- Using the platform for commercial promotions without disclosure
- Scraping or bulk data extraction
- Impersonating other people or events
- Using the platform for events promoting hate, violence, or discrimination

6. Scaling Considerations

6.1 Infrastructure Limits

Component	Current State	Problem	Recommendation
Email sending	Gmail SMTP	500 emails/day hard limit	Switch to Resend / AWS SES now
Photo storage	Single Supabase bucket, no quotas	Unbounded cost growth	Add per-host quotas; enable Supabase CDN
Photo listing	Hard cap at 500 files per album	Silent data loss for large events	Implement cursor-based pagination
Signed URLs	Regenerated per request, 1-hr expiry	API quota exhaustion with many guests	Cache URLs client-side with TTL
RSVP listing	No pagination on dashboard	Dashboard breaks with 1,000+ guests	Add server-side pagination
Event slug generation	Retry loop up to 5 attempts	Collision possible at scale	Append UUID suffix; make slug globally unique by design

6.2 Database Performance

N+1 Queries in Album Listing

`lib/gallery-store.js` — `listAlbumsByEvent()` may perform additional queries per album to fetch share counts. With 100 albums, this is 100+ sequential database queries per page load.

FIX

Use a single SQL JOIN with `GROUP BY` to fetch album share counts in one query. Consider adding a `share_count` denormalized column to `gallery_albums` for very high-traffic scenarios.

Orphaned Storage Objects

If an album or event deletion fails partway through (e.g., network error), storage files in Supabase may become orphaned — no longer referenced in the database but still consuming storage.

FIX

Create a scheduled cleanup function (Supabase Edge Function or cron) that lists all storage paths, cross-references with database records, and deletes orphaned files. Run weekly.

7. Pre-Launch Checklist

Minimum viable items before any public launch.

Security (Must-Do Before Launch)

- □ Set `GUEST_SESSION_SECRET` to a strong random value; throw startup error if missing
- □ Add file size limits — 10 MB per photo, 50 MB per upload batch, server-side enforced
- □ Add rate limiting on `POST /api/rsvp` and `POST /api/gallery/verify`
- □ HTML-escape all user content in email templates (install `he` or `escape-html`)
- □ Validate all email addresses with `zod` before passing to nodemailer
- □ Return identical error messages for all gallery access-denied cases (prevent enumeration)
- □ Add `Content-Security-Policy` header in middleware for all responses
- □ Use `sharp` to validate uploaded images server-side and strip EXIF metadata
- □ Add per-host limits: max events, max RSVPs/event, max storage

Legal (Must-Do Before Launch)

- □ Write and publish Privacy Policy at `/privacy`
- □ Write and publish Terms of Service at `/terms` (include prohibited content list)
- □ Add cookie consent banner for EU visitors
- □ Add unsubscribe link to all reminder and thank-you emails
- □ Add physical address or registered address to email footers
- □ Add account deletion endpoint in dashboard settings
- □ Integrate basic image content moderation (AWS Rekognition or Google Vision SafeSearch)

Scaling (Must-Do Before Launch)

□ Switch from Gmail SMTP to Resend, Postmark, or AWS SES

□ Enable Supabase automated database backups

□ Add pagination to photo listing and RSVP dashboard

□ Set Supabase storage quotas per host

Content Safety (Must-Do Before Launch)

□ Add basic profanity filter on RSVP message field before storing

□ Add daily email send limit per host (e.g., 200 emails/day)

□ Add an abuse reporting mechanism (button on gallery pages → admin email)

PartyShaarty — Pre-Launch Review Report | February 2026
Reviewed against: GDPR (EU), CAN-SPAM (US), DPDP Act 2023 (India), OWASP Top 10