



TechSprint



Leveraging the power of AI



Team Details

- a. **Team name:** The Build Guild
- b. **Team leader name:** Sandipan Singh
- c. **Problem Statement:** Preventing Security Misconfigurations in Rapid AI-Generated MVP Deployments

Problem and Solution

The Problem

Modern AI/vibe-coded websites ship fast, but security is often skipped.

- Missing security headers (CSP, HSTS)
- Unsafe cookies and open CORS
- Exposed admin/debug endpoints
- No fast scanner for MVP workflows

VibeSecure

Owner-authorized security scanning for modern web apps.

- Domain verification before any scan
- Automated vulnerability detection
- AI-powered remediation guidance
- Optional active scanning with consent

Impact: Helps teams launch prototypes safely and confidently.

Opportunities and Differentiation

Market Fit

- AI/Vibe-coded MVPs needing fast security hardening
- Indie developers shipping projects without security teams
- Agencies auditing client sites with ownership proof
- API-first design enables future CI/CD automation

Why VibeSecure is Different

- Mandatory domain verification prevents misuse
- Consent-gated active scanning ensures compliance
- Developer-first outputs: fixes, not just findings

Key Features

Security & Authorization

- Domain ownership verification (file/meta/header)
- Two-stage consent model for active scanning

Scanning Capabilities

- Headers, TLS, CORS, endpoints, reflections, libraries
- Playwright rendering for modern SPAs
- OWASP ZAP integration for active testing

Developer Experience

- AI-powered remediation summaries (Gemini)
- PDF/JSON reports + email notifications
- Platform-specific fix configs (Vercel, Nginx, Apache)

Google Technologies Used

Firebase Authentication

- Secure Google OAuth login
- JWT-based API protection

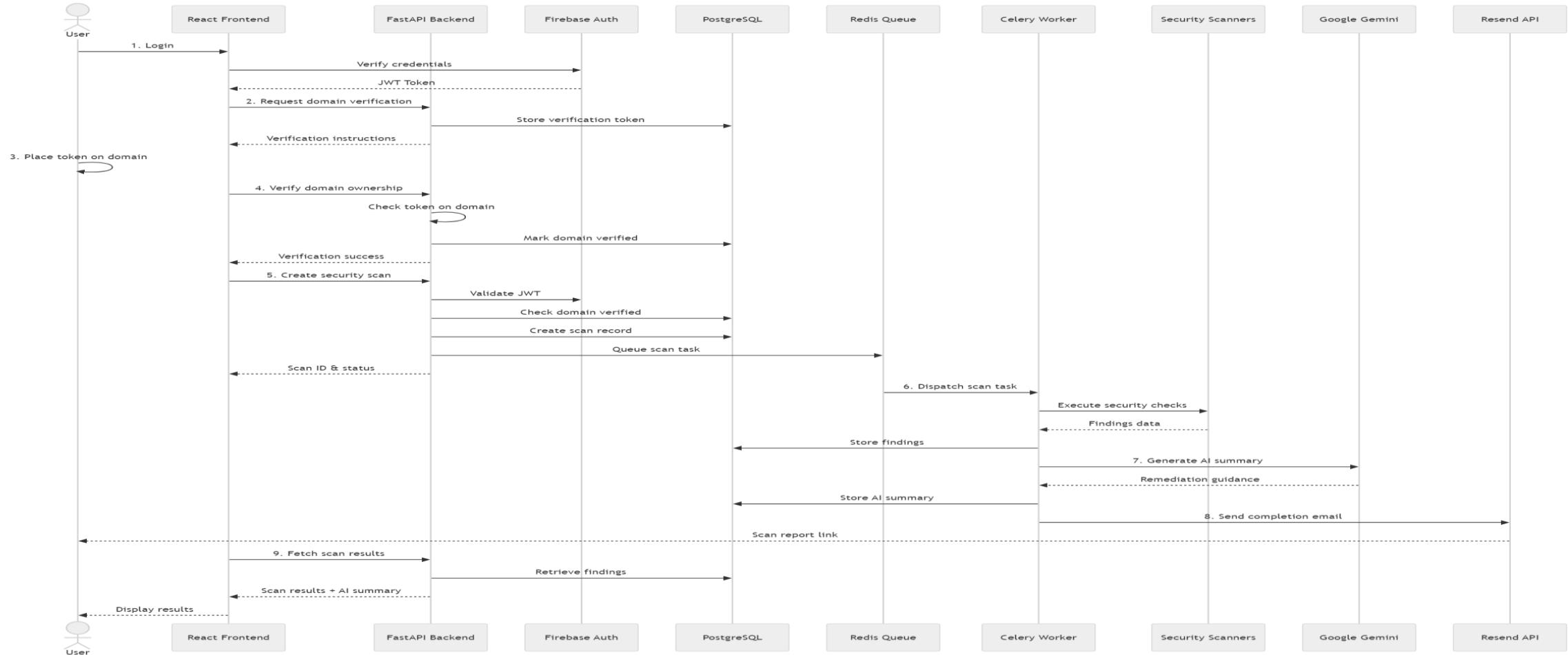
Google Gemini AI

- Converts findings into developer-friendly remediation
- Prioritizes fixes by risk and impact

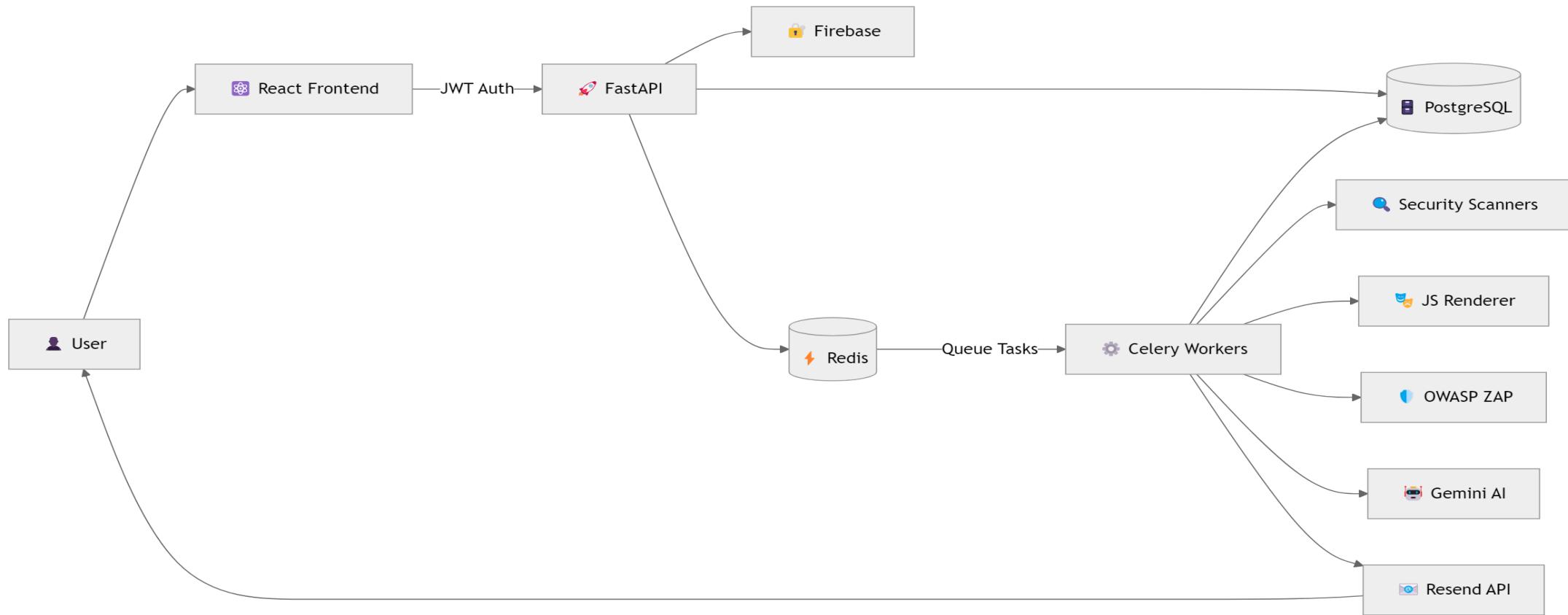
Developer Ecosystem

- Designed for scalable cloud-native security automation

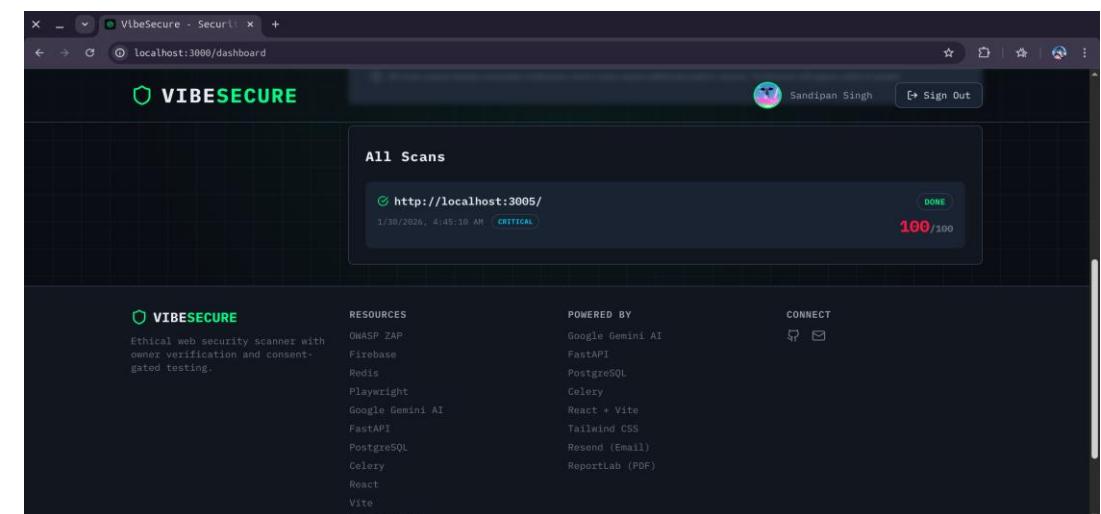
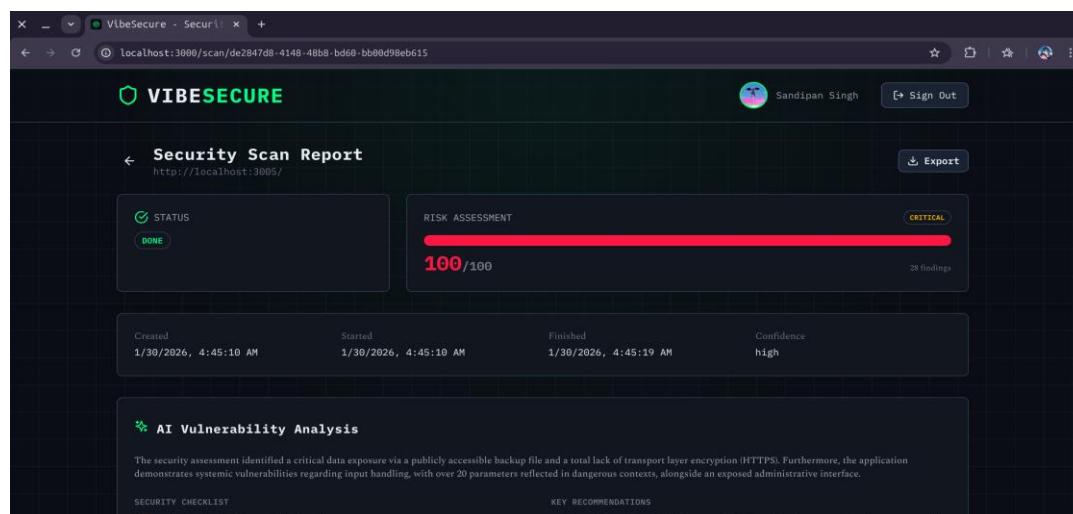
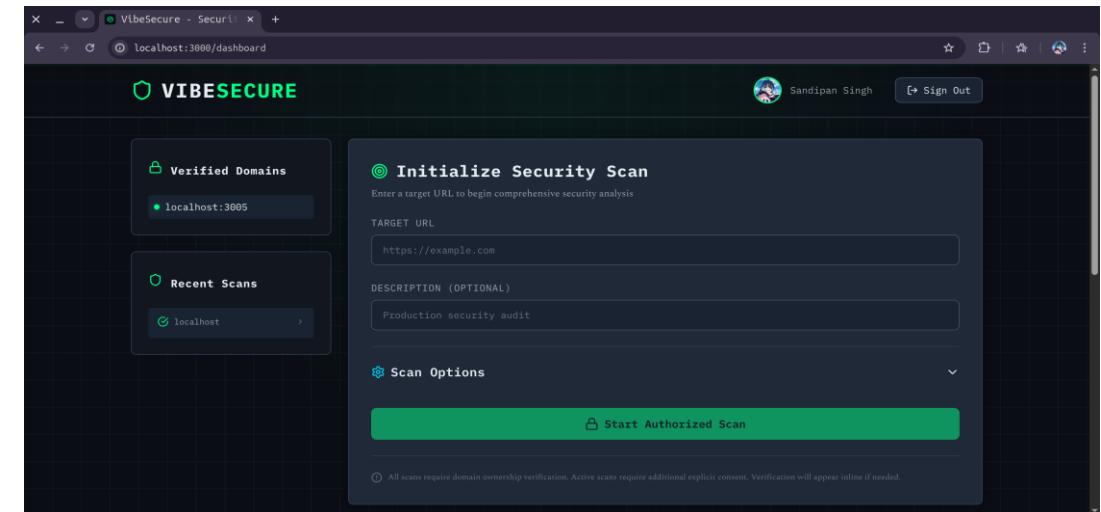
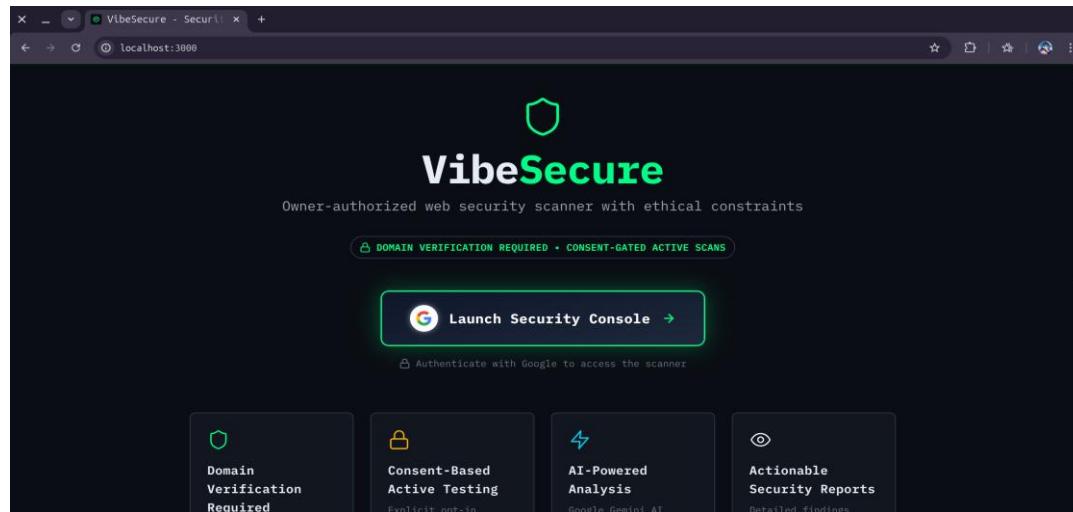
Process Flow Diagram



System Architecture Diagram



MVP Demonstration



Future Development & Roadmap

Short-term Enhancements

- CI/CD integration (GitHub Actions, GitLab CI)
- Scheduled recurring scans
- Custom security policy definitions
- Slack/Discord webhooks

Long-term Vision

- Browser extension for instant scans
- Collaborative team workspaces
- Compliance reporting (GDPR, SOC 2)
- API marketplace for custom scanners
- ML-based vulnerability prediction

Project Resources

Team: The Build Guild

Sandipan Singh • Zulekha Aalmi • Shakshi Kotwala • Kartavya Kumar

GitHub Repository

<https://github.com/thebuildguild-dev/vibesecure>

Demo Video

<https://youtu.be/5bEbh1KOYpE>

Live MVP

<https://vibesecure.thebuildguild.dev/>

Thank you for your time! Questions welcome.



TechSprint



Leveraging the power of AI



Thank you!

