Security Gap Analysis & Remediation Plan

Scope: kiranregmi.com
Assessment Type: Internal Security Review

1. Assessment Overview

This internal assessment evaluates implemented controls against common security best practices. Gaps are documented to support risk-based remediation.

2. Identified Gaps

- Authentication rate limiting not enforced
- Bot and CAPTCHA protections missing
- Security headers not fully implemented
- Limited alerting on authentication anomalies
- Backup and recovery procedures not formally tested

3. Risk Rating & Impact

Gaps were evaluated based on likelihood and impact. Authentication weaknesses present the highest risk due to potential account compromise.

4. Remediation Strategy

- Phase 1: Authentication hardening and rate limiting
- Phase 2: Monitoring, alerting, and backup validation
- Phase 3: Automation, dependency scanning, and WAF rules

5. Risk Acceptance

Low-impact risks may be temporarily accepted where mitigation would negatively affect usability or provide minimal risk reduction.

6. Continuous Review

This assessment will be reviewed after remediation milestones or significant platform changes.