**Detailed Feature List**

1. **URL Scan Submission**  
   1.1. Input field with URL validation  
   1.2. “Start Scan” button to call /scan API  
   1.3. Disable button & show loader during scan
2. **Real‑Time Scan Monitoring**  
   2.1. Display progress bar or spinner  
   2.2. Poll backend for scan status  
   2.3. Option to cancel an in‑progress scan
3. **Data Persistence & Retrieval**  
   3.1. Store scan metadata (ID, timestamp, URL)  
   3.2. Save each vulnerability record (name, severity, description)  
   3.3. Endpoint /results to fetch history and details
4. **Summary Dashboard**  
   4.1. Cards showing: Total Scans, Critical, High, Medium, Low counts  
   4.2. Time‑series chart (vuln count over days/weeks)  
   4.3. Top 5 recurring vulnerabilities
5. **Vulnerability Table**  
   5.1. Columns: Name, Severity, Description, Recommendation  
   5.2. Sort & filter by severity, date, name  
   5.3. Pagination for large result sets
6. **Risk Scoring & Remediation**  
   6.1. Calculate weighted risk score (e.g. CVSS‑lite)  
   6.2. Color‑code rows/cards (Red=Critical, Yellow=High, etc.)  
   6.3. Tooltip or modal with step‑by‑step fix guidance
7. **Report Export** (MVP stretch)  
   7.1. Generate PDF/TXT of summary + detailed list  
   7.2. Download link in UI
8. **Authentication & Roles** (Post‑MVP)  
   8.1. Login/logout flows  
   8.2. Admin vs. Read‑only user roles  
   8.3. Secure API endpoints
9. **Automated Scanning** (Post‑MVP)  
   9.1. CRON‑based scheduled scans  
   9.2. Email/webhook alerts for new critical issues