Section 7 — Risk & Remediation

7.1 Combined Risk Register (Comprehensive Risk Table)

The following table consolidates all risks identified across both the web application penetration test and the wireless/hardware assessment. It provides a unified view of the project's attack surface with impact, likelihood, descriptions, and high-level mitigation strategies.

Risk	Impact	Likelihood	Description	Mitigation Summary
SQL Injection (SQLi)	High	High	Injection flaws allow attackers to manipulate backend SQL queries, bypass authentication, or extract database records.	Use parameterized queries, enforce validation, restrict DB privileges.
Cross-Site Scripting (XSS)	Medium–High	Medium	Poor sanitization enables malicious script injection that can steal cookies or redirect users.	Output encoding, strict CSP, sanitization.
Broken Authentication	High	High	Default admin credentials allowed unauthorized administrative access.	Strong passwords, MFA, disable defaults.
Open Redirect	Medium	Medium	Unvalidated redirect parameters enable phishing and malicious redirection.	Allowlists, redirect validation, interstitial warnings.
Security Misconfiguration	Medium	Medium	Sensitive APIs and debug endpoints exposed without	Restrict endpoints, disable debug, harden configs.

			authentication.	
Weak WPA2 Passphrase	High	High	Captured WPA2 handshake was cracked due to weak PSK, enabling unauthorized access.	Use strong PSK, rotate keys, adopt WPA3.
Rogue Access Point (Evil Twin)	Medium	Medium	Attackers can impersonate legitimate SSIDs and trick clients into connecting.	802.1X authentication, WIDS/WIPS monitoring.
RFID/NFC/IR Replay	Low–Medium	Medium	Unencrypted tags and IR signals can be cloned and replayed.	Encrypted RFID, challenge-response protocols, IR restrictions.

7.2 Remediation Playbook

This section outlines step-by-step remediation guidance, structured similarly to professional security consultancy deliverables. Each subsection corresponds to a risk category from the combined table.

7.2.1 SQL Injection (SQLi) — Remediation Steps

Root Cause - Insufficient input validation and unsafe string concatenation in SQL statements.

Recommended Remediation –

1. Implement Parameterized Queries / Prepared Statements
    - Ensure all database interactions use bound parameters.
2. Server-Side Validation & Sanitization
    - Reject unsafe characters and enforce strict schemas.
3. Least-Privilege DB Accounts
    - Disable high-privilege accounts for routine queries.
4. WAF Rules / Input Filters

- Deploy virtual patching to block known SQLi payload signatures.

Expected Outcome - Prevents database manipulation, authentication bypass, and unauthorized data exposure.

7.2.2 Cross-Site Scripting (XSS) — Remediation Steps

Root Cause - Unsanitized user-controlled data rendered directly to the DOM.

Recommended Remediation -

1. Output Encoding by Context
   - HTML encoding, JS encoding, URL encoding as needed.
2. Strict Content Security Policy (CSP)
   - Disallow inline scripts; permit only trusted sources.
3. Input Validation & Sanitization
   - Block tags, event handlers, and special characters.
4. Use Secure UI Rendering Frameworks
   - Frameworks like React/Angular auto-encode dynamic content.

Expected Outcome - Eliminates script injections, session theft, and malicious redirections.

7.2.3 Broken Authentication / Weak Default Credentials

Root Cause - Default admin credentials were never changed; no password policy enforcement.

Recommended Remediation -

1. Enforce Strong Password Policies
2. Mandatory Password Reset for Default Credentials
3. Implement MFA (Multi-Factor Authentication)
4. Rate Limiting on Login Endpoints

Expected Outcome - Prevents unauthorized administrative access and reduces compromise risk.

7.2.4 Open Redirect — Remediation Steps

Root Cause - Application accepts arbitrary redirect targets from user-controlled parameters.

Recommended Remediation -

1. Implement Allowlisted Redirect Destinations

2. Add Interstitial Warning Screens for External Domains
3. Reject User-Supplied URLs Containing http:// or External Domains

Expected Outcome - Eliminates malicious redirections used in phishing or social engineering attacks.

7.2.5 API Misconfiguration / Information Disclosure

Root Cause - Debug endpoints and sensitive APIs exposed without authentication.

Recommended Remediation -

1. Disable Debug/Developer Endpoints in Production
2. Implement Authentication & Authorization for All APIs
3. Limit Verbose Error Messages
4. Regular Configuration Audits

Expected Outcome - Reduces the attack surface and prevents leakage of sensitive information.

7.2.6 Weak WPA2 Passphrase (Wireless)

Root Cause - Short numeric PSK cracked through offline dictionary attack.

Recommended Remediation -

1. Use Complex PSK (16+ characters, mixed-case, symbols)
2. Rotate Wireless Passwords Regularly
3. Upgrade to WPA3 (SAE) for modern devices
4. Segment Wireless Networks
    - Separate guest, user, admin APs.

Expected Outcome - Prevents unauthorized wireless access and internal network pivoting.

7.2.7 Rogue Access Point (Evil Twin) Prevention

Root Cause - Unauthenticated Wi-Fi networks allow impersonation of SSID.

Recommended Remediation -

1. Implement WPA2-Enterprise (802.1X)
    - Device identity validation prevents rogue AP association.
2. Deploy Wireless Intrusion Detection Systems (WIDS/WIPS)

3. Enable AP Certificate Validation
4. Educate Users to Avoid “Open” or Duplicate Networks

Expected Outcome - Significantly reduces risk of credential theft, traffic interception, and session hijacking.

7.2.8 RFID/NFC/IR Replay Attack Mitigation

Root Cause - Legacy unencrypted tags and IR protocols lack authentication.

Recommended Remediation -

1. Migrate to Encrypted, Challenge-Response RFID Tags
2. Disable IR Ports on Devices Where Not Needed
3. Use Time-Limited or Rolling Codes for Remote Controls
4. Implement Access Control Logging and Anomaly Detection

Expected Outcome - Prevents unauthorized physical access and replay-driven device control.

7.3 Budget Allocation for Risk Mitigation

Risk Category	Estimated Cost	Notes
Web Application Fixes	$0–$200	Developer hours, CSP setup, validation fixes.
Wireless Hardening	$50–$300	WPA3-capable AP, segmentation work.
Rogue AP Monitoring	$100–$600	Optional WIDS/WIPS tools.
Hardware Security Upgrades	$20–$100	Secure RFID tags, rolling code devices.
Documentation & Verification	$0–$150	Staff time for writing & testing.

Estimated Cost Range - $200 – $2,000, depending on whether enterprise-grade wireless security tools are adopted.

7.4 Success Criteria -

The remediation effort will be considered successful when -

1. All high-severity vulnerabilities (SQLi, Broken Auth, weak WPA2) are fully remediated
2. Medium-severity issues show measurable risk reduction
3. Re-testing demonstrates no reappearance of previously confirmed vulnerabilities
4. Wireless security posture improves (new PSK, WPA3, segmentation)
5. AP monitoring detects rogue networks or suspicious associations
6. Clear documentation is produced for -
    - New secure configurations
    - Password policies
    - API hardening steps
7. Wi-Fi credential rotation procedures