5. OWASP Top 10 Mapping

- Injection → A1 (SQL Injection)
- Cross-Site Scripting (XSS) → A7
- CSRF / Broken Access Controls (weak token validation) → A5 / A2 depending on classification

6. Conclusion & Prioritized Remediation

1. **Fix SQL injection immediately** — parameterized queries and server-side input validation. This is highest priority (Authentication bypass).
2. **Fix output encoding / XSS** — escape user inputs in HTML contexts, implement CSP and `HttpOnly` cookies.
3. **Harden CSRF protection** — validate token authenticity (not only presence), enforce SameSite cookies and Origin checks.
4. After fixes, re-test all PoCs and run automated scans in CI. Add logging/alerting for unusual auth or token behavior.

7. Appendix — Raw Payloads & Notes

- SQLi payload used: `admin' or 1=1--`
- XSS payload used: `"><img src=x onerror=prompt(document.cookie);>` — produced popup showing cookie content.
- CSRF PoC: sample HTML provided above. Server accepted token when token was only present and not validated.
- Burp logs & recordings available in `ScreenRecordings/` folder in the repo.