Web Application Security Readiness Assessment Checklist

Mark each item:

- Yes
- No
- Needs Review

Application Visibility

1. We maintain an inventory of all business-critical web applications.
2. We know which applications store customer or sensitive internal data.
3. Hidden admin routes, legacy modules, and retired pages are reviewed.

Authentication Security

4. Strong password policy and MFA are enforced where applicable.
5. Password reset workflows are securely designed.
6. Session tokens expire and invalidate appropriately.

Input & Form Security

7. User inputs are validated server-side, not only browser-side.
8. Hidden form values are not trusted without verification.
9. Upload features are security reviewed.

Authorisation & Data Protection

10. Users cannot access records outside their ownership role.
11. Administrative functions are tightly permission controlled.
12. Sensitive backend responses are minimized.

API & Integration Oversight

13. API endpoints are tested for authorisation enforcement.
14. Third-party plugins and integrations are inventoried.
15. Old or deprecated backend services are decommissioned.

Information Leakage Control

16. Error messages do not reveal internal system details.
17. Sensitive data is not unnecessarily exposed in browser responses.
18. Download/export functions are permission reviewed.

Development & Governance

19. Significant app updates trigger security review.
20. Developers receive baseline security awareness.
21. Pentest findings are tracked to remediation closure.
22. Similar flaw patterns are reviewed across the application.

Continuous Resilience

23. Web applications are periodically penetration tested.
24. Customer trust impact is considered in vulnerability prioritization.
25. Leadership reviews major application security findings.

SCORING GUIDE

Strong Maturity (20–25 Yes Answers)

Your organisation demonstrates healthy application security visibility, disciplined testing habits, and customer trust awareness.

Moderate Exposure (11–19 Yes Answers)

Basic controls exist, but web application trust assumptions may still leave meaningful attacker opportunities.

High Vulnerability (0–10 Yes Answers)

Your web-facing business systems likely rely on functionality more than validated security and require structured application review urgently.