Web Attack Prevention Audit Checklist

20-Point Application Security Audit

☐ Are all forms validated strictly?
☐ Is user input sanitised before storage/use?
☐ Are database queries parameterised safely?
☐ Is XSS output encoding reviewed?
☐ Are uploads filtered aggressively?
☐ Are dangerous file types blocked?
☐ Is authentication hardened?
☐ Is MFA enabled for admins?
☐ Are session tokens handled securely?
☐ Are CSRF protections active?
☐ Are third-party plugins audited?
☐ Are abandoned components removed?
☐ Is a WAF configured?
☐ Are suspicious requests logged?
☐ Are failed logins monitored?
☐ Are vulnerability scans scheduled?
☐ Are debug tools removed?
☐ Are admin permissions reviewed?
☐ Are monthly update reviews enforced?
☐ Is security treated as ongoing development?

Scoring:

17–20 = Strong web application security maturity

12–16 = Moderate exploit exposure

0–11 = High vulnerability probability