Hidden Vulnerability Audit Checklist

20-Point Silent Risk Discovery Audit

☐ Are all plugins/themes inventoried?
☐ Are outdated components patched?
☐ Are unused components removed?
☐ Are dormant admin users deleted?
☐ Are passwords unique and MFA enabled?
☐ Is hosting software current?
☐ Are FTP/cPanel accounts reviewed?
☐ Are file permissions checked?
☐ Are unknown scripts investigated?
☐ Are modified file dates reviewed?
☐ Are SSL warnings absent?
☐ Is mixed content resolved?
☐ Are forms tested for abuse?
☐ Are uploads restricted?
☐ Are suspicious form submissions reviewed?
☐ Are failed logins monitored?
☐ Are odd traffic patterns inspected?
☐ Are automated scans scheduled?
☐ Is monthly vulnerability review assigned?
☐ Would hidden anomalies be noticed quickly?

Scoring:

17–20 = Strong vulnerability awareness
12–16 = Moderate hidden exposure
0–11 = High silent risk probability