Security Baseline Review

findings.pdf · redacted sample · one web app + one domain

Nexora Technologies
Reference engagement
Sample data · no client name

6	2 high	3 closed	5 days
findings	fix before launch	in week one	start to readout

Findings, ranked by business impact

FINDING	SEVERITY	BUSINESS IMPACT	FIX AND OWNER
Session cookie missing `Secure` and `SameSite`	HIGH	A stolen session cookie works from any network; account takeover without a password.	Set both flags, rotate sessions. Owner: backend. 2 h.
Admin panel reachable without MFA	HIGH	One reused password on a public login page gives full admin access.	Enforce MFA for staff roles. Owner: platform. 4 h.
Password reset token valid for 72 hours	MED	A leaked reset link stays usable for three days, including after the user notices.	Reduce to 30 minutes, single use. Owner: backend. 1 h.
SPF allows unauthenticated senders	MED	Invoices and password resets can be spoofed from your domain.	Tighten SPF, add DMARC quarantine. Owner: ops. 3 h.
Nightly backup has no restore test on record	MED	The backup exists; the recovery time does not. A failed restore is discovered during an incident.	Restore to staging, record the time. Owner: ops. 4 h.
Verbose server banner discloses version	LOW	Narrows the search for known vulnerabilities in your exact stack.	Suppress the banner. Owner: ops. 30 min.

Retest and roadmap

Retest evidence

CLOSED IN WEEK ONE	RETESTED	EVIDENCE
Session cookie flags	Day 3	Response header capture, before / after
Admin MFA	Day 4	Login attempt without a second factor, rejected
Password reset token lifetime	Day 4	Expired link returned 410 after 30 minutes

90-day roadmap

- **Now (week 1):** the two high findings and the reset-token change — closed, with retest evidence above.
- **Next (days 8–30):** SPF/DMARC, backup restore test, banner suppression.
- **Later (days 31–90):** dependency policy, quarterly restore drill, logging retention review.

What is not in this report

- No exploitation, privilege escalation or denial-of-service testing.
- No source-code audit; the review covers what is deployed.
- No third-party hosted systems, payment pages or customer data.

Redacted sample. No client name, hostname, credential or customer data appears in this document. It is a reference engagement, not an audit of your systems. Findings are ranked by business impact; CVSS is included as a column, never as the conclusion. Nexora Technologies LLC · nexora.example