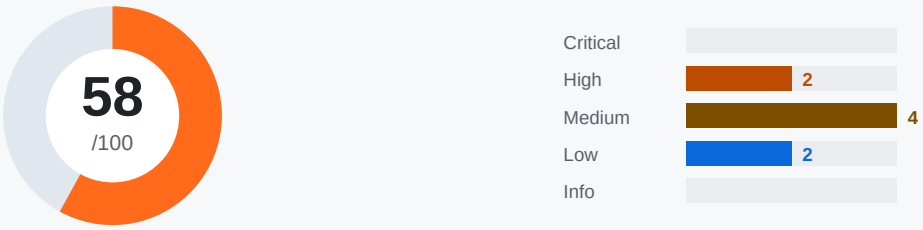
SECURITY AUDIT REPORT

SURFACE SCAN

Target	[domain-redacted].com
Client	[Client Confidential]
Auditor	Exposurix Platform
Date	2026-04-18
Report ID	EXP-2026-0047
Scope	External attack surface — [domain-redacted].com and all subdomains

Executive Summary



TOTAL	CRITICAL	HIGH	MEDIUM	LOW
8	0	2	4	2

The surface scan of [domain-redacted].com identified 8 vulnerabilities across the external attack surface. Two high-severity findings related to email security and an outdated web server require prompt remediation. All results were manually reviewed to eliminate false positives before delivery. No active exploitation was detected during the assessment window.

Scan Details

Tool	Target	Duration	Findings	Notes
Nuclei	[domain-redacted].com	11m 04s	5	Community + Pro templates v9.9.7 — web, dns, ssl categories
Nmap	[domain-redacted].com	3m 22s	2	SYN scan — top 1000 ports, OS detection disabled
HIBP API	[domain-redacted].com	< 1s	1	Domain-level breach check — 3 employee emails exposed
DNS Analyzer	[domain-redacted].com	< 1s	3	SPF, DMARC, DKIM, MX record validation
SSL Labs (API)	[domain-redacted].com	45s	1	TLS configuration audit — cipher suite analysis

Findings Overview

#	Severity	Title	Host / URL	Status
1	HIGH	Missing DMARC Policy	[domain-redacted].com	Confirmed
2	HIGH	Outdated Nginx 1.18.0 (CVE-2021-23017)	www.[domain-redacted].com	Confirmed
3	MEDIUM	SPF Record Allows Too Many Senders (+all)	[domain-redacted].com	Confirmed

#	Severity	Title	Host / URL	Status
4	MEDIUM	Employee Email Addresses Found in Data Breach	[domain-redacted].com (3 accounts)	Confirmed
5	MEDIUM	HTTP to HTTPS Redirect Missing on Subdomains	shop.[domain-redacted].com, blog.[domain-redacted].com	Confirmed
6	MEDIUM	TLS 1.0 and 1.1 Still Enabled	[domain-redacted].com:443	Confirmed
7	LOW	Server Version Disclosed in HTTP Headers	www.[domain-redacted].com	Confirmed
8	LOW	Unused Port 8080 Open (No Service)	[domain-redacted].com:8080	Confirmed

Remediation Roadmap

Short-term (1–4 weeks)

• **Missing DMARC Policy** — Publish a DMARC TXT record at _dmarc.[domain-redacted].com with p=quarantine. Progress to p=reject after 30-day monitoring period. This prevents attackers from spoofing your domain in phishing emails targeting your customers.

• **Outdated Nginx 1.18.0 (CVE-2021-23017)** — Upgrade Nginx to the latest stable release (1.26.x or higher). The current version is affected by a 1-byte heap buffer overflow in the DNS resolver that may allow remote code execution under specific conditions.

Mid-term (1–3 months)

• **SPF Record Allows Too Many Senders (+all)** — Replace the current SPF record ending in +all with -all to hard-fail unauthorized senders. Audit all legitimate sending sources and list them explicitly in the SPF record.

• **Employee Email Addresses Found in Data Breach** — Force password resets for the affected accounts immediately. Enable MFA for all employee accounts. Brief staff on phishing risks stemming from credential exposure.

• **HTTP to HTTPS Redirect Missing on Subdomains** — Configure 301 redirects from HTTP to HTTPS on all subdomains. Add HSTS header with min-age 31536000 to enforce secure connections in browsers.

• **TLS 1.0 and 1.1 Still Enabled** — Disable TLS 1.0 and 1.1 in your Nginx/Apache SSL configuration. Only TLS 1.2 and 1.3 should be accepted. This is required for PCI-DSS compliance for e-commerce sites.

Long-term (3+ months)

• **Server Version Disclosed in HTTP Headers** — Add 'server_tokens off;' to your Nginx configuration to suppress version disclosure. This reduces reconnaissance value for attackers.

• **Unused Port 8080 Open (No Service)** — If port 8080 is not serving a required application, close it via firewall rule. Unused open ports expand the attack surface unnecessarily.

Legal Disclaimer

This report was prepared by Exposurix for the exclusive use of the named client. The findings reflect the security posture at the time of the assessment. Exposurix makes no warranties as to completeness. The client is solely responsible for remediation decisions. Unauthorized distribution of this report is prohibited.