



Security Assessment Report

Infrastructure Risk Analysis & Remediation Roadmap

Executive Summary

Prepared For	Sample Plumbing Co. (sample report, fictional business)
Domain	sample-plumbing.example
Scan Date	October 05, 2026
Scan ID	a1b2c3d4
Scan Type	Passive Public Assessment (SSL, headers, email DNS)
Total Checks Run	3
Risk Level	Needs Attention
Overall Security Score	45/100

Findings Distribution

Severity	Count	Status
CRITICAL	0	None detected
HIGH	2	Requires immediate remediation
MEDIUM	1	Should remediate within 30 days
LOW	1	Best-practice recommendations
INFO	2	Informational observations

ALERT: 2 high-priority issues found. Fix the HIGH items first; most are configuration changes, not rebuilds.

Findings — In Priority Order

HIGH SEVERITY (2)

HIGH #1: Missing: Strict-Transport-Security Header

Issue: No HSTS header is configured, so browsers do not enforce HTTPS-only connections.

Risk Impact: Visitors on public Wi-Fi can be downgraded to unencrypted HTTP and have form data intercepted.

Remediation: Add the response header: Strict-Transport-Security: max-age=31536000; includeSubDomains

NIST 800-53: SC-8, SC-23

HIGH #2: No DMARC Record Found

Issue: No DMARC record exists at _dmarc.sample-plumbing.example.

Risk Impact: Anyone can send email that appears to come from this domain, which enables invoice and phishing scams.

Remediation: Add a TXT record at _dmarc.sample-plumbing.example: v=DMARC1; p=quarantine; adkim=r; aspf=r

NIST 800-53: SI-8, IA-8

MEDIUM SEVERITY (1)

MEDIUM #3: Missing: X-Frame-Options

Risk Impact: The site can be embedded inside another page (clickjacking).

Remediation: Add X-Frame-Options: SAMEORIGIN

NIST 800-53: SI-10

LOW SEVERITY (1)

- Missing: Referrer-Policy — Add Referrer-Policy: strict-origin-when-cross-origin

Security Strengths

- SSL certificate valid
- SPF record present

NIST 800-53 Control Mapping

6 NIST SP 800-53 Rev. 5 controls relate to the findings above. NIST 800-53 is a widely used security baseline (and the basis of CMMC).

Control	Requirement	Gap Found In	Severity
CM-6	Configuration Settings	Missing: Referrer-Policy	LOW
IA-8	Identification & Authentication (Non-Org Users)	No DMARC Record Found	HIGH
SC-23	Session Authenticity	Missing: Strict-Transport-Security Header	HIGH

Control	Requirement	Gap Found In	Severity
SC-8	Transmission Confidentiality & Integrity	Missing: Strict-Transport-Security Header	HIGH
SI-10	Information Input Validation	Missing: X-Frame-Options	MEDIUM
SI-8	Spam Protection	No DMARC Record Found	HIGH

Remediation Roadmap

Phase 1: Urgent (Days 1-7)

- Missing: Strict-Transport-Security Header: Add the response header: Strict-Transport-Security: max-age=31536000; includeSubDomains
- No DMARC Record Found: Add a TXT record at _dmarc.sample-plumbing.example: v=DMARC1; p=quarantine; adkim=r; aspf=r

Phase 2: Important (Days 8-30)

- Missing: X-Frame-Options: Add X-Frame-Options: SAMEORIGIN

Phase 3: Hardening (Days 31-60)

- Missing: Referrer-Policy: Add Referrer-Policy: strict-origin-when-cross-origin

Next Steps

- This week: review the HIGH severity items with whoever manages your website and domain.
- Next: complete the Phase 1 fixes, then work through the medium and low items.
- Then: re-scan to confirm every fix took effect.

Questions? Talk to your Connect Helm contact: Connect Helm · (732)-554-0055 · connecthelm.com

About this assessment: this report reflects the public security posture of sample-plumbing.example at the time of the scan. Only information any visitor can see was examined (SSL certificate, security headers, email DNS records); no login, port scan or exploitation was attempted. It is not a penetration test or a guarantee of security.