Your Business
August 14, 2026 · 10:30 AM

SECURITY REPORT

2
/10
LOW

SCAN TARGET

rapidvuln.com

Open ports detected: **1** · Public IP: **75.2.60.5**

A risk score of 2/10 (LOW) indicates your business has security issues that need attention. The higher the score, the greater the chance of a breach, ransomware, or data theft.

EXECUTIVE SUMMARY

The security scan of rapidvuln.com found 2 medium and low severity issues. No critical vulnerabilities were detected, but 2 issues should be addressed this week to harden your security posture. Detailed fix instructions are included for each finding.

✓ No high-risk open ports were detected from the internet — your firewall appears to be blocking dangerous services.

TOP RECOMMENDATIONS

1. No HTTPS / SSL Not Available: Install an SSL certificate to enable HTTPS.
2. Weak DKIM Key — 1024-bit RSA (selector: resend): Upgrade the DKIM key for selector 'resend' to 2048 bits.

DETAILED FINDINGS

No HTTPS / SSL Not Available

Port 443 · HTTPS

MEDIUM

WHAT IT IS	No HTTPS detected on port 443 — web traffic is sent in plain text, visible to anyone on the network
BUSINESS RISK	Customer passwords, contact details, and any form submissions can be read by anyone on the same network (public wifi, ISPs, etc.), and modern browsers will actively warn visitors that your site is 'Not Secure' — which drives people away and can hurt your search rankings.
REAL-WORLD EXAMPLE	Example: A visitor fills out a contact or login form on this site from a coffee-shop wifi network. Because the connection isn't encrypted, anyone else on that same network can read the form data — including a password — as it's sent.
HOW TO FIX	Install an SSL certificate to enable HTTPS. If you use a web host (GoDaddy, Bluehost, Cloudflare, etc.), go to their control panel and enable 'Free SSL' or 'Let's Encrypt'. If you manage your own server, run: sudo certbot --nginx (or --apache) and follow the prompts. It's free.
URGENCY	**Fix within 1 week**
REFERENCE	CWE-319 — Cleartext Transmission of Sensitive Information Sensitive data is sent over the network unencrypted, so anyone monitoring the connection can read it.

Weak DKIM Key — 1024-bit RSA (selector: resend)

Port DNS · DKIM Key Strength — MEDIUM

WHAT IT IS	DKIM key for selector 'resend' appears to be approximately 1024 bits — 1024-bit RSA keys are considered weak by modern standards and NIST has deprecated them. A well-resourced attacker could factor this key, breaking your email authentication.
BUSINESS RISK	A forged DKIM signature lets an attacker send phishing or fraud emails that cryptographically appear to come from your domain — bypassing email filters that rely on DKIM as a trust signal, and making impersonation emails indistinguishable from your real ones.
REAL-WORLD EXAMPLE	Example: A security researcher demonstrated in a published study that 512-bit DKIM keys could be factored in under 72 hours using cloud computing resources costing less than $100 — allowing anyone with that capability to forge valid email signatures for the affected domain.
HOW TO FIX	Upgrade the DKIM key for selector 'resend' to 2048 bits. Generate a new key through your email provider, update the DNS TXT record to the new public key, and retire the old 1024-bit key.
URGENCY	**Fix within 1 week**
REFERENCE	CWE-326

PORT REFERENCE TABLE

PORT	SERVICE	RISK	DESCRIPTION
443	HTTPS	**MEDIUM**	No HTTPS detected on port 443 — web traffic is sent in plain text, visible to anyone on the network
DNS	DKIM Key Strength	**MEDIUM**	DKIM key for selector 'resend' appears to be approximately 1024 bits — 1024-bit RSA keys are conside

NEXT STEPS

→ Address the 2 MEDIUM risk finding(s) this week. Start with 'No HTTPS / SSL Not Available': Install an SSL certificate to enable HTTPS.