

SECURITY REPORT



SCAN TARGET

rapidvuln.com

Open ports detected: 0 · Public IP: **75.2.60.5**

A risk score of 1/10 (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 6 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 Weak DKIM Key — 1024-bit RSA (selector: resend): Upgrade the DKIM key for selector 'resend' to 2048 bits.
- 2 CSP script-src Too Permissive: Tighten script-src to an explicit allowlist of trusted domains and drop 'unsafe-inline'/'unsafe-eval'/wildcards.

DETAILED FINDINGS

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

CSP script-src Too Permissive

Port HTTPS · Content Security Policy

MEDIUM

WHAT IT IS	CSP script-src allows 'unsafe-inline' — an injected or hijacked script can still run freely
BUSINESS RISK	This setting defeats most of the protection CSP is meant to provide. If a third-party script you rely on is ever compromised — the exact mechanism behind most 'watering hole' attacks — it will execute without restriction and with no warning.
REAL-WORLD EXAMPLE	Example: A vendor's analytics or chat-widget script gets compromised at the source; because the policy still allows it (or allows inline/eval scripts generally), the malicious code runs exactly as if it belonged on the site, with no warning to anyone.
HOW TO FIX	Tighten script-src to an explicit allowlist of trusted domains and drop 'unsafe-inline'/'unsafe-eval'/wildcards. Move inline scripts to external files or use a nonce/hash. Test changes with https://csp-evaluator.withgoogle.com before deploying.
URGENCY	Fix within 1 week
REFERENCE	CWE-693 — Protection Mechanism Failure A security safeguard that should be protecting the system is missing, disabled, or not strong enough.

Login/Admin Path Discovered — /login/

Port PATH · Content Discovery

LOW

WHAT IT IS	/login/ returned HTTP 200 with no authentication challenge. This confirms a login or admin entry point exists at this path.
BUSINESS RISK	/login/ returned HTTP 200 with no authentication challenge. This confirms a login or admin entry point exists at this path.
HOW TO FIX	Confirm this login is protected by a strong password and, ideally, multi-factor authentication. Consider IP-restricting it if it's only used by internal staff.
URGENCY	Fix within 1 month
REFERENCE	CWE-284

Login/Admin Path Discovered — /dashboard/

Port PATH · Content Discovery

LOW

WHAT IT IS	/dashboard/ returned HTTP 200 with no authentication challenge. This confirms a login or admin entry point exists at this path.
BUSINESS RISK	/dashboard/ returned HTTP 200 with no authentication challenge. This confirms a login or admin entry point exists at this path.
HOW TO FIX	Confirm this login is protected by a strong password and, ideally, multi-factor authentication. Consider IP-restricting it if it's only used by internal staff.
URGENCY	Fix within 1 month
REFERENCE	CWE-284

robots.txt Present

Port PATH · Content Discovery

INFO

WHAT IT IS	/robots.txt is present and was used to seed additional path checks.
BUSINESS RISK	/robots.txt is present and was used to seed additional path checks.
HOW TO FIX	No action needed — robots.txt is meant to be public.
URGENCY	Fix within 1 month

sitemap.xml Present

Port PATH · Content Discovery

INFO

WHAT IT IS /sitemap.xml is present and was used to seed additional path checks.

BUSINESS RISK /sitemap.xml is present and was used to seed additional path checks.

HOW TO FIX No action needed — sitemap.xml is meant to be public.

URGENCY Fix within 1 month

PORT REFERENCE TABLE

PORT	SERVICE	RISK	DESCRIPTION
DNS	DKIM Key Strength	MEDIUM	DKIM key for selector 'resend' appears to be approximately 1024 bits — 1024-bit RSA keys are consider
HTTPS	Content Security Policy	MEDIUM	CSP script-src allows 'unsafe-inline' — an injected or hijacked script can still run freely
PATH	Content Discovery	LOW	/login/ returned HTTP 200 with no authentication challenge. This confirms a login or admin entry poi
PATH	Content Discovery	LOW	/dashboard/ returned HTTP 200 with no authentication challenge. This confirms a login or admin entry
PATH	Content Discovery	INFO	/robots.txt is present and was used to seed additional path checks.
PATH	Content Discovery	INFO	/sitemap.xml is present and was used to seed additional path checks.

NEXT STEPS

→ Address the 2 MEDIUM risk finding(s) this week. Start with 'Weak DKIM Key — 1024-bit RSA (selector: resend)': Upgrade the DKIM key for selector 'resend' to 2048 bits.

This report is for informational purposes only and represents a point-in-time automated scan. It is not a substitute for a professional penetration test.