

SECURITY REPORT



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 6 issues including 1 high-risk and 2 medium-risk findings. The most critical issue is 'Admin Dashboard Exposed' which requires immediate attention. Full remediation steps are provided for each finding below.

✓ Your server is reachable, which means the web checks and SSL analysis were able to run successfully.

TOP RECOMMENDATIONS

- 1 Admin Dashboard Exposed: Restrict access to /dashboard by IP allowlist, move it to a non-standard path, or disable it if not needed.
- 2 No HTTPS / SSL Not Available: Install an SSL certificate to enable HTTPS.
- 3 Weak DKIM Key — 1024-bit RSA (selector: resend): Upgrade the DKIM key for selector 'resend' to 2048 bits.

DETAILED FINDINGS

Admin Dashboard Exposed

Port HTTPS · Admin Dashboard
Exposed

HIGH

WHAT IT IS	The path /dashboard is accessible without authentication — this exposes administration functionality to anyone on the internet
BUSINESS RISK	Publicly reachable admin panels are a primary target for automated attacks. An attacker who can reach /dashboard can attempt brute-force login, exploit known vulnerabilities in the admin software, or leverage it as a stepping stone to full server compromise — without needing any insider knowledge of the site.
REAL-WORLD EXAMPLE	Example: Automated bots constantly scan the internet for paths like /dashboard. A business that left a default admin URL accessible was compromised when a bot found it, brute-forced a weak password in minutes, and installed backdoor malware — all without any human attacker being involved.
HOW TO FIX	Restrict access to /dashboard by IP allowlist, move it to a non-standard path, or disable it if not needed. Nginx: 'location ^~ /dashboard { allow YOUR_IP; deny all; }'. Also ensure strong, unique credentials are set for any admin accounts, and enable multi-factor authentication where supported.
URGENCY	Fix immediately
REFERENCE	CWE-284

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: <code>sudo certbot --nginx</code> (or <code>--apache</code>) 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

Public IP Flagged for Abuse — 75.2.60.5

Port HTTPS · IP Reputation

LOW

WHAT IT IS	Public IP 75.2.60.5 (hosted by Amazon.com, Inc.) has an abuse confidence score of 16/100 from 26 report(s) in the last 90 days on AbuseIPDB.
BUSINESS RISK	A flagged IP usually means one of two things: this server has already been compromised and is being used to send spam or attack other systems, or this is a shared-hosting IP where a different customer on the same server is doing something malicious — either way, some mail providers and firewalls will treat traffic from this IP with extra suspicion, which can affect email deliverability and how visitors' security software treats your site.
HOW TO FIX	If this is a dedicated server, check for signs of compromise (unexpected processes, outbound traffic, unfamiliar scheduled tasks) and consider a malware scan. If this is shared hosting, contact your hosting provider — ask whether the IP is shared and whether they can move you to a clean one. You can see the specific reports at https://www.abuseipdb.com/check/75.2.60.5 .
URGENCY	Monitor

Hosting Network Identified

Port HTTPS · IP WHOIS /
Network Ownership

INFO

WHAT IT IS	Public IP 75.2.60.5 is registered to Amazon.com, Inc. — network: AMAZO-4 — block: 75.2.0.0 – 75.2.191.255.
BUSINESS RISK	This is informational — it tells you (and anyone else who looks it up) which hosting provider or network actually operates this IP. Useful for confirming you're hosted where you expect, or for context if the IP reputation check above flags anything.
HOW TO FIX	No action required — this is identifying information, not a vulnerability.
URGENCY	Informational

BIMI Opportunity — Verified Logo Not Enabled

Port DNS · BIMI Not Configured

INFO

WHAT IT IS	DMARC is already enforcing, so this domain qualifies for BIMI — a verified logo shown next to emails in Gmail, Yahoo, and Apple Mail — but no BIMI record is set up
BUSINESS RISK	This isn't a vulnerability — it's a missed brand-trust opportunity. Since DMARC is already enforcing (a prerequisite most mailbox providers require), this domain could show a verified logo next to its emails in supporting inboxes, which can measurably improve open rates and make phishing look more out of place by comparison.
REAL-WORLD EXAMPLE	Example: two otherwise-identical marketing emails land in a Gmail inbox — one from a sender with BIMI configured shows a verified brand logo next to it, the other shows a generic default icon indistinguishable from a spoofed sender.
HOW TO FIX	Add a TXT record for 'default._bimi' with a value pointing to a hosted SVG logo, e.g. 'v=BIMI1; l=https://yourdomain.com/logo.svg'. Some mailbox providers (notably Gmail) also require a Verified Mark Certificate (VMC) — a paid trademark-backed certificate — before they'll display the logo; Apple Mail and Yahoo currently do not require one. This is optional and lower-priority than any HIGH/MEDIUM finding above.
URGENCY	Fix within 1 month

PORT REFERENCE TABLE

PORT	SERVICE	RISK	DESCRIPTION
HTTPS	Admin Dashboard Exposed	HIGH	The path /dashboard is accessible without authentication — this exposes administration functionality

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 consider
HTTPS	IP Reputation	LOW	Public IP 75.2.60.5 (hosted by Amazon.com, Inc.) has an abuse confidence score of 16/100 from 26 rep
HTTPS	IP WHOIS / Network Ownership	INFO	Public IP 75.2.60.5 is registered to Amazon.com, Inc. — network: AMAZO-4 — block: 75.2.0.0 – 75.2.19
DNS	BIMI Not Configured	INFO	DMARC is already enforcing, so this domain qualifies for BIMI — a verified logo shown next to emails

NEXT STEPS

→ Start with the 1 HIGH risk finding(s) today — these are your most urgent risks. First, address 'Admin Dashboard Exposed': Restrict access to /dashboard by IP allowlist, move it to a non-standard path, or disable it if not needed. Then work through the remaining findings in order of severity.

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.