SECURITY REPORT

Your Business
August 30, 2026 · 12:50 PM

1
/10
LOW

SCAN TARGET

103.127.56.35

Open ports detected: **1** · Public IP: **103.127.56.35**

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 103.127.56.35 found 3 medium and low severity issues. No critical vulnerabilities were detected, but 1 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.

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.

Public IP Flagged for Abuse — 103.127.56.35

Port HTTPS · IP Reputation

LOW

WHAT IT IS	Public IP 103.127.56.35 (hosted by Unified Core Limited) has an abuse confidence score of 0/100 from 2 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/103.127.56.35.
URGENCY	**Monitor**

Hosting Network Identified

Port HTTPS · IP WHOIS / Network Ownership — INFO

WHAT IT IS	Public IP 103.127.56.35 is registered to Unified Core Limited (BD) — network: UNIFIED-BD — block: 103.127.56.0 – 103.127.59.255.
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

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
HTTPS	IP Reputation	**LOW**	Public IP 103.127.56.35 (hosted by Unified Core Limited) has an abuse confidence score of 0/100 from
HTTPS	IP WHOIS / Network Ownership	**INFO**	Public IP 103.127.56.35 is registered to Unified Core Limited (BD) — network: UNIFIED-BD — block: 10

NEXT STEPS

→ Address the 1 MEDIUM risk finding(s) this week. Start with 'No HTTPS / SSL Not Available': Install an SSL certificate to enable HTTPS.