

SECURITY REPORT



SCAN TARGET

http://157.66.2.53/

Open ports detected: 1 · Public IP: **157.66.2.53**

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 157.66.2.53 found 10 medium and low severity issues. No critical vulnerabilities were detected, but 4 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 HTTP Not Redirecting to HTTPS: Add a permanent redirect from HTTP to HTTPS.
- 3 Missing HSTS Header: Add the HSTS header to your web server.

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: <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.

HTTP Not Redirecting to HTTPS

Port HTTP · HTTPS Redirect

MEDIUM

WHAT IT IS	Visiting <code>http://</code> doesn't redirect to <code>https://</code> — some visitors may use an unencrypted connection without knowing
BUSINESS RISK	Anyone who types or clicks an <code>http://</code> link is sending their activity on your site — potentially including form data or passwords — unencrypted, where it can be read by anyone on the same public wifi or compromised network.
REAL-WORLD EXAMPLE	Example: A customer types the domain into their browser without <code>'https://'</code> , lands on the unencrypted version of the site, and submits a form before ever reaching the secure page — sending that data in plain text the whole time.
HOW TO FIX	Add a permanent redirect from HTTP to HTTPS. Nginx: add <code>'return 301 https://\$host\$request_uri;'</code> in your port 80 server block. Apache: add <code>'RewriteRule ^https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]'</code> in your <code>.htaccess</code> . Cloudflare users: go to <code>SSL/TLS > Edge Certificates > enable 'Always Use HTTPS'</code> .
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.

Missing HSTS Header

Port HTTPS · HSTS Header

MEDIUM

WHAT IT IS	Missing Strict-Transport-Security (HSTS) — browsers aren't forced to always use HTTPS, leaving visitors open to downgrade attacks
BUSINESS RISK	An attacker on the same network as a visitor (public wifi, a compromised router, etc.) can trick their browser into using the insecure version of your site and intercept what they type — raising the odds of stolen logins or payment details.
REAL-WORLD EXAMPLE	Example: An attacker on a shared network intercepts a visitor's first request (which defaults to HTTP) before the redirect happens, and silently serves them a fake version of the page instead of the real site.
HOW TO FIX	Add the HSTS header to your web server. Nginx: add 'add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;' in your server block. Apache: add 'Header always set Strict-Transport-Security "max-age=31536000"' in your config. Cloudflare: SSL/TLS > Edge Certificates > enable HTTP Strict Transport Security.
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.

Missing Content-Security-Policy (CSP)

Port HTTPS · Content Security
Policy

MEDIUM

WHAT IT IS	Missing Content-Security-Policy (CSP) — this site has no CSP defense-in-depth layer, so if any cross-site scripting weakness exists elsewhere it's easier to exploit; this finding on its own doesn't mean an XSS vulnerability exists on this site
BUSINESS RISK	CSP is a defense-in-depth browser control, not evidence of an active vulnerability by itself — but if an attacker ever manages to slip malicious script onto your site through some other weakness (e.g. a vulnerable plugin or a comment field), a good CSP is often what stops that script from running and stealing customer data such as login sessions or payment details. Without it, that second layer of protection isn't there.
REAL-WORLD EXAMPLE	Example: A vulnerable comment form or compromised ad widget lets an attacker inject a script tag; with a properly scoped CSP in place, the browser would refuse to run it — without CSP, that same injected script runs freely and can forward a visitor's session cookie to the attacker.
HOW TO FIX	Add a Content-Security-Policy header, but roll it out carefully — a misconfigured CSP can break legitimate scripts/styles on the site. Start by deploying it in Report-Only mode first, which reports violations without blocking anything: <code>'add_header Content-Security-Policy-Report-Only "default-src \'self\'; script-src \'self\'; object-src \'none\'; report-uri /csp-report";'</code> Review the reports for a while to catch anything the policy would break, adjust the policy, then switch the header name to 'Content-Security-Policy' (without '-Report-Only') to start enforcing it. For WordPress or complex sites, use https://csp-evaluator.withgoogle.com to help build the policy.
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.

Public IP Flagged for Abuse — 157.66.2.53

Port HTTPS · IP Reputation

LOW

WHAT IT IS	Public IP 157.66.2.53 (hosted by PT Ashyla Karya Abadi) has an abuse confidence score of 13/100 from 6 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/157.66.2.53 .
URGENCY	Monitor

Missing MIME Sniffing Protection

Port HTTPS · MIME Sniffing

LOW

WHAT IT IS	Missing X-Content-Type-Options — browsers may guess file types incorrectly, which can enable content injection
BUSINESS RISK	This is a minor gap on its own, but it slightly raises the odds that a malicious file could be misread as something else by a visitor's browser, helping a separate attack succeed.
REAL-WORLD EXAMPLE	Example: A user-uploaded file intended to be harmless (like an image) is reinterpreted by the browser as executable script because the server never told it what the file actually was, letting an unrelated vulnerability turn into a working attack.
HOW TO FIX	Add: 'add_header X-Content-Type-Options "nosniff" always;' (Nginx) or 'Header always set X-Content-Type-Options nosniff' (Apache). This is a one-line fix that takes 2 minutes.
URGENCY	Fix within 1 month
REFERENCE	CWE-693 — Protection Mechanism Failure A security safeguard that should be protecting the system is missing, disabled, or not strong enough.

Missing Referrer-Policy Header

Port HTTPS · Referrer Policy

LOW

WHAT IT IS	Missing Referrer-Policy — page URLs (which may include sensitive data) are shared with third-party sites your pages link to
BUSINESS RISK	If any of your page addresses contain sensitive details (like a password-reset token or account ID), that information could leak to outside sites your pages link to — a small but easily avoidable privacy gap.
REAL-WORLD EXAMPLE	Example: A customer clicks an outbound link from a page whose URL happens to include an account ID or a password-reset token, and that full address — token included — is handed to the destination site in the Referer header.
HOW TO FIX	Add: 'add_header Referrer-Policy "strict-origin-when-cross-origin" always;' (Nginx) or 'Header always set Referrer-Policy strict-origin-when-cross-origin' (Apache).
URGENCY	Fix within 1 month
REFERENCE	CWE-16 — Configuration The weakness comes from how the software was configured, not from a flaw in its code.

Missing Permissions-Policy Header

Port HTTPS · Permissions Policy

LOW

WHAT IT IS	Missing Permissions-Policy — browser features like camera, microphone, and location aren't restricted for embedded third-party scripts
BUSINESS RISK	If you ever embed third-party ads, widgets, or analytics scripts, they could request a visitor's camera, microphone, or location without you intending to allow it — an avoidable privacy risk for your customers.
REAL-WORLD EXAMPLE	Example: An embedded ad network's script requests the visitor's location or microphone access through a permission prompt the site owner never intended to allow, simply because nothing in the page's headers restricted it.
HOW TO FIX	Add: 'add_header Permissions-Policy "camera=(), microphone=(), geolocation=()" always;' Adjust based on what your site actually uses. This limits what ad/analytics scripts can access.
URGENCY	Monitor
REFERENCE	CWE-693 — Protection Mechanism Failure A security safeguard that should be protecting the system is missing, disabled, or not strong enough.

Hosting Network Identified

Port HTTPS · IP WHOIS /
Network Ownership

INFO

WHAT IT IS	Public IP 157.66.2.53 is registered to Andri Suryadi (ID) — network: IDNIC-ASHYLANET-ID — block: 157.66.2.0 – 157.66.3.255.
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

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

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
HTTP	HTTPS Redirect	MEDIUM	Visiting http:// doesn't redirect to https:// — some visitors may use an unencrypted connection with
HTTPS	HSTS Header	MEDIUM	Missing Strict-Transport-Security (HSTS) — browsers aren't forced to always use HTTPS, leaving visit
HTTPS	Content Security Policy	MEDIUM	Missing Content-Security-Policy (CSP) — this site has no CSP defense-in-depth layer, so if any cross
HTTPS	IP Reputation	LOW	Public IP 157.66.2.53 (hosted by PT Ashyla Karya Abadi) has an abuse confidence score of 13/100 from
HTTPS	MIME Sniffing	LOW	Missing X-Content-Type-Options — browsers may guess file types incorrectly, which can enable content

HTTPS	Referrer Policy	LOW	Missing Referrer-Policy — page URLs (which may include sensitive data) are shared with third-party s
HTTPS	Permissions Policy	LOW	Missing Permissions-Policy — browser features like camera, microphone, and location aren't restricte
HTTPS	IP WHOIS / Network Ownership	INFO	Public IP 157.66.2.53 is registered to Andri Suryadi (ID) — network: IDNIC-ASHYLANET-ID — block: 157
PATH	Content Discovery	INFO	/robots.txt is present and was used to seed additional path checks.

NEXT STEPS

→ Address the 4 MEDIUM risk finding(s) this week. Start with 'No HTTPS / SSL Not Available': Install an SSL certificate to enable HTTPS.

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.