

SECURITY REPORT



SCAN TARGET

<https://mikrotik.com/>

Open ports detected: 0 · Public IP: 159.148.172.205

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 mikrotik.com found 10 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

CSP script-src Too Permissive: Tighten script-src to an explicit allowlist of trusted domains and drop 'unsafe-inline'/'unsafe-eval'/wildcards.

DETAILED FINDINGS

CSP script-src Too Permissive

Port HTTPS · Content Security Policy

MEDIUM

WHAT IT IS	CSP script-src allows 'unsafe-inline', 'unsafe-eval' — 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.

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.

No Abuse Reports Found for Public IP

Port HTTPS · IP Reputation

INFO

WHAT IT IS	Public IP 159.148.172.205 (hosted by MIKROTIKLS SIA) has no abuse reports on AbuseIPDB in the last 90 days.
BUSINESS RISK	A clean IP reputation is a good sign — no other indication needed here.
HOW TO FIX	No action required.
URGENCY	Informational

Hosting Network Identified

Port HTTPS · IP WHOIS /
Network Ownership

INFO

WHAT IT IS	Public IP 159.148.172.205 is registered to LATNET-MNT (LV) — network: MIKROTIKLSSIA — block: 159.148.172.128 – 159.148.172.255.
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

Path Discovered — /.well-known/security.txt

Port PATH · Content Discovery

INFO

WHAT IT IS	/.well-known/security.txt returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/.well-known/security.txt returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
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

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
HTTPS	Content Security Policy	MEDIUM	CSP script-src allows 'unsafe-inline', 'unsafe-eval' — an injected or hijacked script can still run
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 Reputation	INFO	Public IP 159.148.172.205 (hosted by MIKROTIKLS SIA) has no abuse reports on AbuseIPDB in the last 9
HTTPS	IP WHOIS / Network Ownership	INFO	Public IP 159.148.172.205 is registered to LATNET-MNT (LV) — network: MIKROTIKLSSIA — block: 159.148
DNS	BIMI Not Configured	INFO	DMARC is already enforcing, so this domain qualifies for BIMI — a verified logo shown next to emails

PATH	Content Discovery	INFO	<code>/.well-known/security.txt</code> returned HTTP 200, a real distinct response rather than the site's soft-40
PATH	Content Discovery	INFO	<code>/sitemap.xml</code> is present and was used to seed additional path checks.
PATH	Content Discovery	INFO	<code>/robots.txt</code> is present and was used to seed additional path checks.

NEXT STEPS

→ Address the 1 MEDIUM risk finding(s) this week. Start with 'CSP script-src Too Permissive': Tighten script-src to an explicit allowlist of trusted domains and drop 'unsafe-inline'/'unsafe-eval'/wildcards.

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.