

Security Assessment

<https://torontomu.ca>

Prepared for Sample Customer · 2026-10-11T14:47:28Z

Reviewed by GopiKrishna, Cybersecurity Consultant

Overall

F 57/100

Website & TLS

F 55/100

Email security

C 73/100

Domain & DNS

F 40/100

Executive summary. Overall, torontomu.ca scores F (57/100) — an exposed public security posture. The weakest area is domain & DNS (F). Email spoofing verdict: Partially protected — Some enforcement exists, but gaps remain — determined spoofers can still get through Deep checks found no exposed sensitive files; 80 subdomains in public records, 5 answering live; mail servers clean on major blocklists.

Email spoofing verdict: Partially protected — Some enforcement exists, but gaps remain — determined spoofers can still get through.

Priority fix planThe order I'd tackle these in.

No Content-Security-Policy — Start with a report-only policy, then enforce default-src 'self'.

2

HSTS missing includeSubDomains — Add includeSubDomains (after confirming all subdomains serve HTTPS).

3

Clickjacking protection missing — Send X-Frame-Options: DENY (or SAMEORIGIN), or set frame-ancestors in CSP.

4

X-Content-Type-Options missing — Send: X-Content-Type-Options: nosniff

5

No Referrer-Policy — Send: Referrer-Policy: strict-origin-when-cross-origin (or stricter).

Website & TLS

PassCertificate valid

Issued by SSL.com TLS Issuing RSA CA R1, 167 days remaining.

PassModern TLS

Negotiated TLS 1.3.

PassStrong cipher

Negotiated: TLS_AES_128_GCM_SHA256.

WarningHSTS missing includeSubDomains

Subdomains aren't covered by the policy.

How this gets exploitedAn attacker only needs one weak subdomain — an old blog, a forgotten staging site — to ride the parent domain's trust.

FixAdd includeSubDomains (after confirming all subdomains serve HTTPS).

FailNo Content-Security-Policy

Missing the strongest mitigation against XSS and injection.

How this gets exploitedAny injected script — a vulnerable plugin, a compromised ad, a stored comment — runs with the full privileges of your page: stealing sessions, skimming payment forms, redirecting your customers.

FixStart with a report-only policy, then enforce default-src 'self'.

WarningClickjacking protection missing

No X-Frame-Options or frame-ancestors directive.

How this gets exploitedYour site can be embedded invisibly inside an attacker's page: visitors think they're clicking a video or a prize, but they're clicking your buttons — approving, sending, deleting.

FixSend X-Frame-Options: DENY (or SAMEORIGIN), or set frame-ancestors in CSP.

WarningX-Content-Type-Options missing

Without nosniff, browsers may MIME-sniff responses.

How this gets exploitedMIME-sniffing lets an attacker pass off a harmless-looking upload as a script and execute it in your site's context.

FixSend: X-Content-Type-Options: nosniff

WarningNo Referrer-Policy

Referrer leakage defaults to the browser's (often permissive) default.

How this gets exploitedFull URLs leak to third parties through the Referer header — including password-reset links and private pages your users were viewing.

FixSend: Referrer-Policy: strict-origin-when-cross-origin (or stricter).

PassPermissions-Policy set

WarningCookies missing Secure flag

1 of 1 cookie(s) can be sent over plain HTTP.

How this gets exploitedA cookie without Secure travels over plain HTTP whenever anything loads insecurely — one shared-network session is enough to steal it.

FixSet Secure on every cookie.

WarningCookies missing HttpOnly

1 of 1 cookie(s) are readable by JavaScript.

How this gets exploitedWithout HttpOnly, any cross-site scripting flaw hands the session cookie to the attacker's server — account takeover without the password.

FixSet HttpOnly on session cookies to blunt XSS theft.

WarningCookies missing SameSite

1 of 1 cookie(s) lack a SameSite attribute.

How this gets exploitedWithout SameSite, malicious sites can ride your visitors' logged-in sessions and act as them (CSRF).

FixSet SameSite=Lax (or Strict) unless cross-site use is required.

InfoServer header disclosed

Server: Apache/2.4.37 (Red Hat Enterprise Linux)

How this gets exploitedThis banner is free reconnaissance: it names the exact software so an attacker skips probing and goes straight to known exploits for it.

FixStrip or genericize the Server header.

PassHTTP redirects to HTTPS

Plain HTTP correctly redirects (status 301).

Email security

InfoMail handled by escan.torontomu.ca

MX: escan.torontomu.ca

WarningSPF ends in softfail (~all)

Receivers are told forged mail 'probably isn't us — deliver anyway'.

How this gets exploitedSoftfail is a suggestion, not a block: spoofed mail lands in inboxes with at most a warning flag most users never see.

FixMove to -all once your sender list (including marketing tools) is complete.

WarningDMARC at quarantine, not reject

Spoofed mail goes to spam instead of being refused.

How this gets exploitedSpam-folder delivery still reaches some inboxes, and plenty of users fish mail out of spam. Reject is the end state that actually protects.

FixRaise the policy to p=reject once reporting shows no legitimate senders failing.

PassDKIM publishing confirmed

Selector(s): google, selector1.

WarningNo MTA-STS

Other mail servers aren't told to require TLS when delivering to this domain.

How this gets exploitedWithout MTA-STS, a network attacker can downgrade mail delivery to plain text (STARTTLS stripping) and read your incoming email in transit — silently.

FixPublish an MTA-STS TXT record + hosted policy file with mode: enforce.

InfoNo TLS-RPT

No reporting for failed encrypted mail delivery.

How this gets exploitedIf encrypted delivery to this domain is failing — or being attacked — nobody is notified. The failures stay silent.

FixAdd a _smtp._tls TXT record with a rua reporting address.

Domain & DNS

WarningDNSSEC not enabled

No DNSKEY records — DNS answers for this domain are unsigned.

How this gets exploitedUnsigned DNS can be forged in transit: visitors and email get silently redirected to attacker servers without anyone touching your actual infrastructure.

FixEnable DNSSEC at your DNS provider/registrar and publish the DS record.

WarningNo CAA records

Nothing restricts which certificate authorities may issue for this domain.

How this gets exploitedAny of the world's CAs can issue a certificate for this domain — one mis-issuance (by error or compromise) enables a pixel-perfect look-alike site with a valid padlock.

FixPublish CAA records naming only the CAs you actually use.

PassDomain registration healthy

Expires 2027-01-29 (110 days).

Deep assessment checksPaid-tier checks the free scan does not run: exposed files, subdomain surface, live-host analysis, mail blocklists, dangling CNAMEs.

PassNo exposed sensitive files found

We probed /.env, /.git/config, /.git/HEAD and /.DS_Store (with a soft-404 baseline check) — none are publicly readable.

Info80 subdomains visible in public certificate logs

Full list below. Test/dev-looking names present: api.openshiftlab.testint.torontomu.ca, api.openshiftqa.semiproduct.torontomu.ca, apps.openshiftlab.testint.torontomu.ca, apps.openshiftqa.semiproduct.torontomu.ca, fax.testint.torontomu.ca.

How this gets exploited Every public subdomain is attack surface: forgotten test systems are a classic entry point because they miss patching and hardening.

Fix Inventory these names, retire what you don't need, and make sure test systems are access-restricted.

Info 5 of 18 probed subdomains answer live on HTTPS

Each live host was fingerprinted (status, server, page title) — see the attack-surface table in this report.

PassMail servers not on major blocklists

Checked 141.117.126.6 (escan.torontomu.ca) against Barracuda — clean.

Host	Status	What it looks like	Notes
arch.torontomu.ca	HTTP 302	https://www.torontomu.ca/architectural-science/	
blog.torontomu.ca	HTTP 200	blog.torontomu.ca	
click.trsm-connect.torontomu.ca	HTTP 403	403 - Forbidden: Access is denied.	
cloud.trsm-connect.torontomu.ca	HTTP 404		
courses.torontomu.ca	HTTP 302	/d2l/login	sign-in page
api.openshiftlab.testint.torontomu.ca	no HTTPS answer		test/dev
api.openshiftqa.semiproduct.torontomu.ca	no HTTPS answer		test/dev
apps.labs.torontomu.ca	no HTTPS answer		
apps.openshiftlab.testint.torontomu.ca	no HTTPS answer		test/dev
apps.openshiftqa.semiproduct.torontomu.ca	no		test/

	HTTPS answer	dev
boomer.as.torontomu.ca	no HTTPS answer	
bsbm-app1.prodint.torontomu.ca	no HTTPS answer	
bsbm-app1.semiprodint.torontomu.ca	no HTTPS answer	
fax.testint.torontomu.ca	no HTTPS answer	test/ dev
ubs-instantid.testint.torontomu.ca	no HTTPS answer	test/ dev
www.api.openshiftlab.testint.torontomu.ca	no HTTPS answer	test/ dev
www.api.openshiftqa.semiprodint.torontomu.ca	no HTTPS answer	test/ dev
www.fax.testint.torontomu.ca	no HTTPS answer	test/ dev

Subdomains seen in certificate logs (50 of 80 shown):

api.openshiftlab.testint.torontomu.ca, api.openshiftqa.semiprodint.torontomu.ca, apps.labs.torontomu.ca, apps.openshiftlab.testint.torontomu.ca, apps.openshiftqa.semiprodint.torontomu.ca, arch.torontomu.ca, blog.torontomu.ca, boomer.as.torontomu.ca, bsbm-app1.prodint.torontomu.ca, bsbm-app1.semiprodint.torontomu.ca, click.trsm-connect.torontomu.ca, cloud.trsm-connect.torontomu.ca, courses.torontomu.ca, de.spi.torontomu.ca, de.torontomu.ca, esrs.dcmgt.torontomu.ca, ezproxy.lib.torontomu.ca, fasma.arts.torontomu.ca, fax.prodint.torontomu.ca, fax.testint.torontomu.ca, help.arch.torontomu.ca, hr.torontomu.ca, hrrpt.torontomu.ca, hrsup.torontomu.ca, image.trsm-connect.torontomu.ca, infisical.prodint.torontomu.ca, lake.itsec.torontomu.ca, lake2.itsec.torontomu.ca, math.torontomu.ca, ome.dcmgt.torontomu.ca, onguardweb.prodint.torontomu.ca, onguardweb.tmuad.torontomu.ca, onguardweb1.prodint.torontomu.ca, onguardweb1.tmuad.torontomu.ca, onguardwebt.semiprodint.torontomu.ca, onguardwebt.tmuad.torontomu.ca, print.arch.torontomu.ca, print.torontomu.ca, qrcon01.prodint.torontomu.ca, qrcon02.prodint.torontomu.ca, rnet.torontomu.ca, rshare.library.torontomu.ca, ru-bexpe01.torontomu.ca, ru-bexpe02.torontomu.ca, ru-bexpe03.torontomu.ca, ru-ccp01.torontomu.ca, ru-expe-cluster1.torontomu.ca, ru-expe01.torontomu.ca, ru-expe02.torontomu.ca, ru-expe03.torontomu.ca

I reviewed this assessment personally before sending it over.

If you fix one thing first, make it this: No Content-Security-Policy. The priority plan above orders the rest.

Nothing in this report required a login or intrusive testing — it's all public configuration, which also means anyone else can see the same gaps.

If you'd like help closing them, reply to my email and we'll talk through what's quick, what matters, and what can wait.

GopiKrishna

Cybersecurity Consultant · HeaderScope

Generated by HeaderScope and personally reviewed before delivery. This assessment covers the public configuration of the domain above — headers, TLS, DNS and email authentication, plus the paid deep checks listed. It is not a penetration test and does not test logins, passwords or internal systems.