Your Business
September 03, 2026 · 04:47 AM

SECURITY REPORT

3
/10
MEDIUM

SCAN TARGET

https://bgpengineering.com/

Open ports detected: **0** · Public IP: **3.130.60.26**

A risk score of 3/10 (MEDIUM) 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 bgpengineering.com found 13 medium and low severity issues. No critical vulnerabilities were detected, but 6 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. Missing HSTS Header: Add the HSTS header to your web server.
2. Missing Clickjacking Protection (X-Frame-Options): Add the X-Frame-Options header.
3. Missing Content-Security-Policy (CSP): Add a Content-Security-Policy header, but roll it out carefully — a misconfigured CSP can break legitimate scripts/styles on the site.

DETAILED FINDINGS

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 Clickjacking Protection (X-Frame-Options)

Port HTTPS · Clickjacking Protection

MEDIUM

WHAT IT IS	Missing X-Frame-Options — your website can be embedded in an attacker's invisible iframe to trick users into unwanted actions
BUSINESS RISK	An attacker could trick your customers into clicking hidden buttons — like 'change password' or 'confirm purchase' — without realizing it, potentially leading to account takeovers or unauthorized actions carried out under your brand's name.
REAL-WORLD EXAMPLE	Example: An attacker embeds the site's 'delete account' or 'confirm payment' button inside an invisible iframe on their own page, disguised under something like a fake 'play video' button — a visitor's real click triggers the hidden action on your site.
HOW TO FIX	Add the X-Frame-Options header. Nginx: 'add_header X-Frame-Options "SAMEORIGIN" always;' Apache: 'Header always set X-Frame-Options SAMEORIGIN' This tells browsers to only allow your site to be framed by pages on the same domain.
URGENCY	**Fix within 1 week**
REFERENCE	CWE-1021 — Improper Restriction of Rendered UI Layers (Clickjacking) The site doesn't prevent itself from being embedded inside another page, which attackers can exploit to trick users into clicking something they didn't intend to.

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: 'add_header Content-Security-Policy-Report-Only "default-src \'self\'; script-src \'self\'; object-src \'none\'; report-uri /csp-report";' 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.

DKIM Not Detected Under Common Selectors

Port DNS · DKIM Record

MEDIUM

WHAT IT IS	No DKIM record found under common selector names — this does not confirm DKIM is unconfigured, only that it wasn't found under any of the selector names checked; many providers use a custom or provider-specific selector this check can't guess
BUSINESS RISK	If DKIM genuinely isn't configured, email providers increasingly use it as a trust signal, and its absence can make legitimate emails more likely to be flagged as suspicious or land in spam. But this check only queries a fixed list of common selector names (default, google, mail, etc.) — many providers assign a random or account-specific selector, so this finding should be treated as 'couldn't confirm DKIM,' not 'DKIM is definitely missing.'
REAL-WORLD EXAMPLE	Example: A legitimate invoice email from the business gets flagged as suspicious or dropped into spam by the recipient's mail provider, simply because there's no DKIM signature to prove the message wasn't altered or forged in transit — this only actually happens if DKIM is truly unconfigured, which this check alone can't confirm.
HOW TO FIX	First confirm whether DKIM is actually configured: check your email provider's admin console (Google Workspace: Admin console > Apps > Gmail > Authenticate email; Microsoft 365: Defender > Email authentication > DKIM) for the exact selector name in use, since it's often not one of the common defaults this scan checks. If it turns out DKIM genuinely isn't enabled, turn it on there and add the resulting TXT record to DNS. If you're not sure how to check, share the selector name your provider gives you and this can be verified directly.
URGENCY	**Fix within 1 week**
REFERENCE	CWE-290 — Authentication Bypass by Spoofing The login or identity check can be tricked by faking trusted information, letting an attacker in without real credentials.

Domain Renewal Due in 31 Days

Port WHOIS · Domain Registration

MEDIUM

WHAT IT IS	Domain registration expires in 31 days (registrar: Cloudflare, Inc.)
BUSINESS RISK	Not urgent yet, but a missed renewal takes the site and all email on this domain offline — worth confirming auto-renew is on now rather than relying on remembering later.
REAL-WORLD EXAMPLE	Example: A similar business assumed auto-renew was on, it wasn't, and the domain quietly lapsed — a five-minute check now is the only thing standing between routine upkeep and that same scramble.
HOW TO FIX	Confirm auto-renew is enabled at your registrar, or renew manually in the next few weeks.
URGENCY	**Monitor**

Third-Party Scripts Missing Subresource Integrity (SRI)

Port HTTPS · Third-Party Script Loading

MEDIUM

WHAT IT IS	2 third-party script source(s) loaded without Subresource Integrity (SRI): cdnjs.cloudflare.com, pages.convertkit.com
BUSINESS RISK	If any of these third-party providers is ever compromised — a real, recurring attack pattern called a 'watering hole' or supply-chain attack, where attackers hit a widely-trusted vendor instead of you directly — the malicious code they inject would run on your site with no verification and no warning to you or your visitors.
REAL-WORLD EXAMPLE	Example: A widely-used analytics or widget provider gets compromised (a real, recurring attack pattern), and because the script loads without integrity verification, the malicious version executes on every visitor's browser with no warning to you or them.
HOW TO FIX	Add integrity and crossorigin attributes to each third-party <script> tag, e.g. <script src="..." integrity="sha384-..." crossorigin="anonymous"></script>. Most CDNs (cdnjs, jsdelivr, unpkg) publish the correct hash on their site — copy it directly.
URGENCY	**Fix within 1 week**
REFERENCE	CWE-353 — Missing Support for Integrity Check There's no way to verify that data wasn't altered in transit, so tampering would go unnoticed.

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 3.130.60.26 (hosted by Amazon Technologies Inc.) 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 3.130.60.26 is registered to Amazon Technologies Inc. — network: AT-88-Z — block: 3.128.0.0 – 3.255.255.255.
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

Detected Technology Stack

Port HTTPS · Technology Fingerprint — INFO

WHAT IT IS	Detected technology stack: Openresty 1.27.1.2.
BUSINESS RISK	Knowing your exact software versions helps attackers pick targeted exploits instead of guessing — this isn't a vulnerability by itself, but it's worth knowing what your site publicly reveals about its own software.
HOW TO FIX	No action required unless you'd prefer to hide version banners (e.g. removing WordPress's generator meta tag and readme.html, or disabling Apache/nginx's Server header version string) to make automated targeting slightly harder. Keeping the software itself patched matters far more than hiding the version number.
URGENCY	Informational

PORT REFERENCE TABLE

PORT	SERVICE	RISK	DESCRIPTION
HTTPS	HSTS Header	**MEDIUM**	Missing Strict-Transport-Security (HSTS) — browsers aren't forced to always use HTTPS, leaving visit

HTTPS	Clickjacking Protection	**MEDIUM**	Missing X-Frame-Options — your website can be embedded in an attacker's invisible iframe to trick us
HTTPS	Content Security Policy	**MEDIUM**	Missing Content-Security-Policy (CSP) — this site has no CSP defense-in-depth layer, so if any cross
DNS	DKIM Record	**MEDIUM**	No DKIM record found under common selector names — this does not confirm DKIM is unconfigured, only
WHOIS	Domain Registration	**MEDIUM**	Domain registration expires in 31 days (registrar: Cloudflare, Inc.)
HTTPS	Third-Party Script Loading	**MEDIUM**	2 third-party script source(s) loaded without Subresource Integrity (SRI): cdnjs.cloudflare.com, pag
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 3.130.60.26 (hosted by Amazon Technologies Inc.) has no abuse reports on AbuseIPDB in the
HTTPS	IP WHOIS / Network Ownership	**INFO**	Public IP 3.130.60.26 is registered to Amazon Technologies Inc. — network: AT-88-Z — block: 3.128.0.
DNS	BIMI Not Configured	**INFO**	DMARC is already enforcing, so this domain qualifies for BIMI — a verified logo shown next to emails
HTTPS	Technology Fingerprint	**INFO**	Detected technology stack: Openresty 1.27.1.2.

NEXT STEPS

→ Address the 6 MEDIUM risk finding(s) this week. Start with 'Missing HSTS Header': Add the HSTS header to your web server.