Your Business
August 23, 2026 · 07:03 AM

SECURITY REPORT

5
/10
HIGH

SCAN TARGET

akisushi.com

Open ports detected: **0** · Public IP: **15.197.225.128**

A risk score of 5/10 (HIGH) 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 akisushi.com found 14 issues including 2 high-risk and 6 medium-risk findings. The most critical issue is 'Missing SPF Record — Email Spoofing Possible' which requires immediate attention. Full remediation steps are provided for each finding below.

✓ Your server is reachable, which means the web checks and SSL analysis were able to run successfully.

TOP RECOMMENDATIONS

1. Missing SPF Record — Email Spoofing Possible: Add an SPF TXT record to your DNS listing every service that actually sends mail for this domain — leaving one out will cause its mail to fail SPF and possibly get rejected.
2. Missing DMARC Record — Email Impersonation Risk: Add a DMARC TXT record to your DNS.
3. HTTP Not Redirecting to HTTPS: Add a permanent redirect from HTTP to HTTPS.

DETAILED FINDINGS

Missing SPF Record — Email Spoofing Possible

Port DNS · SPF Record

HIGH

WHAT IT IS	No SPF record — there's no DNS-level list of which mail servers are authorized to send using this domain's envelope sender, so any server can pass an SPF check for your domain
BUSINESS RISK	Without SPF, nothing tells receiving mail servers which senders are legitimate for this domain's SMTP envelope, making it easier for forged mail to get through — and easier for your own legitimate mail to be misjudged as spam. Note that SPF on its own, even correctly configured, doesn't stop the visible 'From:' address a recipient sees from being spoofed — that requires DMARC (see below) to enforce alignment between SPF/DKIM and the From header.
REAL-WORLD EXAMPLE	Example: A customer receives an email that looks exactly like it's from the business — same display name, same domain — asking them to 'confirm' a payment or click a link, with nothing in DNS to stop the forgery or warn the recipient.
HOW TO FIX	Add an SPF TXT record to your DNS listing every service that actually sends mail for this domain — leaving one out will cause its mail to fail SPF and possibly get rejected. Log into your domain registrar, go to DNS, add a TXT record for '@' with a value matching your provider: Google Workspace: 'v=spf1 include:_spf.google.com -all' | Microsoft 365: 'v=spf1 include:spf.protection.outlook.com -all'. If you use additional senders (helpdesk, marketing platform, invoicing tool, etc.), add each as its own 'include:' entry in the same record — a domain can only have one SPF TXT record, so don't create a second one. Use https://mxtoolbox.com/spf.aspx to verify, then add a DMARC record too so the visible From address is covered as well.
URGENCY	**Fix immediately**
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.

Missing DMARC Record — Email Impersonation Risk

Port DNS · DMARC Record

HIGH

WHAT IT IS	No DMARC record — your domain has zero email authentication enforcement, making it trivial to impersonate your business
BUSINESS RISK	This makes it significantly easier for scammers to send convincing fake emails 'from' your business — a common tactic in invoice fraud and phishing — which can directly cost your customers money and damage trust in your brand.
REAL-WORLD EXAMPLE	Example: A scammer sends an invoice-fraud email that appears to come straight from the business's own domain; with no DMARC record in place, nothing tells the recipient's mail provider the message is forged, so it lands in the inbox looking completely legitimate.
HOW TO FIX	Add a DMARC TXT record to your DNS. Go to your domain registrar's DNS settings, add a TXT record for '_dmarc' (not '@') with value: 'v=DMARC1; p=none; rua=mailto:youremail@yourdomain.com' Start at p=none — this only turns on reporting, nothing is blocked yet. Review the aggregate reports for a few weeks to confirm every legitimate mail source for this domain (email provider, helpdesk, marketing tools, etc.) is passing DMARC alignment, then move to p=quarantine, and finally p=reject once you're confident nothing legitimate will be caught. Verify at https://mxtoolbox.com/dmarc.aspx
URGENCY	**Fix immediately**
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.

HTTP Not Redirecting to HTTPS

Port HTTP · HTTPS Redirect

MEDIUM

WHAT IT IS	Visiting http:// doesn't redirect to https:// — some visitors may use an unencrypted connection without knowing
BUSINESS RISK	Anyone who types or clicks an http:// 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 'https://', 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 'return 301 https://$host$request_uri;' in your port 80 server block. Apache: add 'RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]' in your .htaccess. Cloudflare users: go to SSL/TLS > Edge Certificates > enable 'Always Use HTTPS'.
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 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.

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): os.onebrandingny.com, www.opentable.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.

Protected Path — /server-status

Port PATH · Content Discovery

LOW

WHAT IT IS	/server-status returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/server-status returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
HOW TO FIX	No action needed if this is intentionally restricted. Confirm the credentials protecting it are strong and not left at a default.
URGENCY	**Fix within 1 month**
REFERENCE	CWE-284

Detected Technology Stack

Port HTTPS · Technology Fingerprint

INFO

WHAT IT IS	Detected technology stack: Jquery 1.12.4.
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**

Path Discovered — /phpmyadmin/

Port PATH · Content Discovery

INFO

WHAT IT IS	/phpmyadmin/ 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	/phpmyadmin/ 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

PORT REFERENCE TABLE

PORT	SERVICE	RISK	DESCRIPTION
DNS	SPF Record	HIGH	No SPF record — there's no DNS-level list of which mail servers are authorized to send using this do
DNS	DMARC Record	HIGH	No DMARC record — your domain has zero email authentication enforcement, making it trivial to impers
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	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
HTTPS	Third-Party Script Loading	MEDIUM	2 third-party script source(s) loaded without Subresource Integrity (SRI): os.onebrandingny.com, www
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
PATH	Content Discovery	**LOW**	/server-status returned HTTP 403. This confirms the path exists, but access control prevented access
HTTPS	Technology Fingerprint	**INFO**	Detected technology stack: Jquery 1.12.4.
PATH	Content Discovery	**INFO**	/phpmyadmin/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This

NEXT STEPS

→ Start with the 2 HIGH risk finding(s) today — these are your most urgent risks. First, address 'Missing SPF Record — Email Spoofing Possible': Add an SPF TXT record to your DNS listing every service that actually sends mail for this domain — leaving one out will cause its mail to fail SPF and possibly get rejected. Then work through the remaining findings in order of severity.