MP

Marius Pareščius

KIBERNETINIS SAUGUMAS

Extended security scan report · generated 2026-08-14 19:34

Report date/time: **2026-08-14 19:34 (+02:00)** · GMT / UTC: **2026-08-14 17:34** · Template version: **1.1** · App version: **2.99.3** · Scan type: **extended**

F

29/100

zero.webappsecurity.com

Critical security gaps — action required.

This is the **paid extended report** — a deeper analysis than the free online test: detected components with versions, outdated software, matched known vulnerabilities (CVE) and a technical inventory (DNS, TLS, HTTP headers). For a full manual audit or ongoing monitoring: **pagalba@parescius.lt**.

Summary

We ran an external security scan of **zero.webappsecurity.com** — assessing 11 technical areas. Overall security level: **29/100 (F)**.

Found **19** items to fix (1 critical, 1 high, 8 medium, 9 low priority); 7 checks passed successfully.

Critical vulnerabilities found — immediate action is required.

What the score means: **90–100 (A)** excellent · **80–89 (B)** good · **70–79 (C)** average · **50–69 (D)** weak · **below 50 (E/F)** risky — action needed. Scored from 100, deducting for each issue (up to 10 per issue).

Priority actions

Where to start — the most important issues and what to do about them.

1 **Could not verify the SSL/TLS certificate**
Where: Hosting / server (TLS certificate)
Install a valid TLS certificate (e.g. free Let’s Encrypt via your hosting panel) and enable HTTPS for the whole domain.

2 **Domenas NEAPSAUGOTAS nuo klastojimo — bet kas gali siųsti laiškus jūsų vardu (nėra SPF/DMARC). Didelė sukčiavimo (BEC/phishing) rizika.**
Where: Domain DNS + mail provider
Fix three things: 1) SPF ending in “-all”; 2) DKIM (via your mail provider); 3) DMARC (start p=quarantine, later p=reject). Handled by whoever manages the domain DNS + your mail provider.

3 **Missing HSTS (Strict-Transport-Security)**
Where: Web server (nginx / Apache config or hosting provider)
On the web server add the response header: Strict-Transport-Security: max-age=31536000; includeSubDomains; preload.

Overview

Key technical parameters of the site at scan time.

IP address	**54.82.22.214**
SSL issuer	
Server	**Apache-Coyote/1.1**
HSTS	**no**
CSP	**no**

Reputation	**clean**

Email security (SPF / DKIM / DMARC)

This check is designed for classic mail servers at moderate sending volume (ordinary business correspondence) — **not for bulk newsletter/marketing senders**. Bulk-sender requirements (Gmail/Yahoo >5,000 msgs/day rules, spam-rate monitoring via Postmaster Tools, one-click unsubscribe) are out of scope here — those need dedicated ESP/monitoring tools.

MX (mail server)	**none**
SPF	**none**
DKIM	**not found**
DMARC	**none**

Detected technologies and versions

Components with a version link to a CVE (vulnerability) search. Click to see known issues.

Programming languages	**Java**
UI frameworks	**Bootstrap**
Web servers	**Apache Tomcat**
JavaScript libraries	**jQuery 1.8.2 ↗ · OUTDATED — update (known vulnerabilities)** **Known: CVE-2012-6708, CVE-2019-11358, CVE-2020-11023, CVE-2020-7656, CVE-2015-9251**
Font scripts	**Font Awesome**

Technical inventory

Raw DNS, TLS and HTTP response headers observed at scan time.

DNS

A	**54.82.22.214**

Issues found (19)

Issues are sorted by severity — most critical first. Each one: what it means and the concrete fix.

× Could not verify the SSL/TLS certificate -10

A secure (encrypted) connection to your site could not be established, or the certificate is invalid. Data between visitors and the site may travel unprotected (technically — no valid HTTPS/SSL).

Where to look / who is responsible: Hosting / server (TLS certificate)

How to fix: Install a valid TLS certificate (e.g. free Let’s Encrypt via your hosting panel) and enable HTTPS for the whole domain.

!! Domenas NEAPSAUGOTAS nuo klastojimo — bet kas gali siųsti laiškus jūsų vardu (nėra SPF/DMARC). Didelė sukčiavimo (BEC/phishing) rizika.

Your domain is completely unprotected against impersonation — anyone can send mail as if from you (no working SPF/DMARC). A major fraud (BEC / phishing) risk to you and your customers.

Where to look / who is responsible: Domain DNS + mail provider

How to fix: Fix three things: 1) SPF ending in “-all”; 2) DKIM (via your mail provider); 3) DMARC (start p=quarantine, later p=reject). Handled by whoever manages the domain DNS + your mail provider.

! Missing HSTS (Strict-Transport-Security) -10

The browser is not forced to always connect to your site securely (encrypted), so the first visit can be intercepted and the visitor redirected to a fake site (technically — the HSTS header is missing).

Where to look / who is responsible: Web server (nginx / Apache config or hosting provider)

How to fix: On the web server add the response header: Strict-Transport-Security: max-age=31536000; includeSubDomains; preload.

! Missing Content-Security-Policy -8

The site does not restrict where code may be loaded from, making it easier to inject a malicious script that steals visitors' data (technically — no Content-Security-Policy, the main XSS defence).

Where to look / who is responsible: Web server (nginx / Apache config or hosting provider)

How to fix: On the web server define a CSP, e.g.: Content-Security-Policy: default-src 'self'; then gradually allow the sources you need.

! No SPF record -8

It is not specified which servers may send mail in your domain's name (this is called an SPF record). Without it anyone can impersonate your address, and your own mail more often lands in spam or is rejected.

Where to look / who is responsible: Domain DNS settings (hosting / registrar / admin)

How to fix: In the domain DNS settings add an SPF record (TXT) listing your mail server, e.g.: v=spf1 a mx ip4:YOUR-IP -all. Your email provider or whoever manages the DNS does this.

! Missing X-Frame-Options / frame-ancestors -6

Your site can be invisibly embedded into someone else's page and trick visitors into clicking where they did not intend (technically — no clickjacking protection).

Where to look / who is responsible: Web server (nginx / Apache config or hosting provider)

How to fix: On the web server add X-Frame-Options: SAMEORIGIN or the CSP directive frame-ancestors 'self'.

! No DMARC record -6

Your domain has no rule for what to do with mail that merely pretends to be from you (this is called a DMARC policy). Without it scammers can send mail as if from you (e.g. "from" your company to clients), and the recipient's mail does not know whether to block it. This hurts reputation and raises fraud risk.

Where to look / who is responsible: Domain DNS settings (hosting / registrar)

How to fix: In the domain DNS settings add a DMARC record (TXT, named _dmarc), e.g.: v=DMARC1; p=quarantine; rua=mailto:postmaster@your-domain. Start in monitoring mode, then tighten. Whoever manages the DNS does this.

! No DKIM signature found (common selectors checked) -6

Your outgoing mail is not signed with a digital "seal" that proves to the recipient the message is really from you (this is called a DKIM signature). Without it Gmail, Outlook and others often drop your mail into spam or reject it.

Where to look / who is responsible: Email provider / server + domain DNS settings

How to fix: Enable message signing (DKIM) in your email provider's settings and publish the record it gives you in the domain DNS. Usually the email provider (e.g. Google Workspace, Zoho, hosting mail) does this.

! No XML sitemap (indexing / Search Console) -3

The site has no XML sitemap — search engines find it harder to discover and index all pages, so some may never make it into Google Search.

Where to look / who is responsible: Website / SEO (admin or developer)

How to fix: Generate an XML sitemap (WordPress serves /wp-sitemap.xml automatically; SEO plugins such as Rank Math or Yoast use /sitemap_index.xml), reference it in robots.txt with a "Sitemap:" line, and submit it via Google Search Console.

! El. pašto autentikacijos pagrindui trūksta: SPF, DKIM, DMARC. Tai pagrindiniai apsaugos elementai kiekvienam pašto serveriui, nepriklausomai nuo siuntimo apimties.

The email authentication baseline is missing core elements (SPF / DKIM / DMARC). These are required for every domain, even if you send little mail — otherwise it's easy to impersonate.

Where to look / who is responsible: Domain DNS + mail provider

How to fix: Configure all three in the domain DNS: SPF (v=spf1 ... -all), DKIM (via your mail provider), and DMARC (_dmarc, start p=quarantine). This is the standard hygiene minimum.

• Server discloses software versions -5

Your server publicly shows which software and version it runs. This helps attackers find a vulnerability matching exactly that version (technically — versions disclosed in response headers).

Where to look / who is responsible: Web server (nginx / Apache config)

How to fix: On the web server hide versions (e.g. server_tokens off; on Nginx, ServerTokens Prod on Apache, remove X-Powered-By).

• Missing X-Content-Type-Options -4

The browser may mis-"guess" a file type and execute malicious content (technically — no X-Content-Type-Options).

Where to look / who is responsible: Web server (nginx / Apache config or hosting provider)

How to fix: On the web server add the header: X-Content-Type-Options: nosniff.

• Missing Referrer-Policy -3

When a visitor moves from your site to another, the exact addresses and parameters of your pages can leak (technically — no Referrer-Policy).

Where to look / who is responsible: Web server (nginx / Apache config or hosting provider)

How to fix: On the web server add: Referrer-Policy: strict-origin-when-cross-origin.

• No IPv6 (missing AAAA record) -2

The domain has no AAAA record — the site is not reachable over IPv6. IPv6 is now standard; some users and mobile networks are IPv6-only and may reach the site slowly or not at all.

Where to look / who is responsible: DNS / hosting (IPv6)

How to fix: Add an AAAA DNS record and enable IPv6 on your server or CDN.

• Components with a disclosed version detected (check known CVEs)

The site discloses the versions of the components it uses. Attackers can use these to look for publicly known vulnerabilities (CVEs).

Where to look / who is responsible: Website (component / plugin versions)

How to fix: Regularly update all components to the latest versions and, where possible, hide version information.

• HTTP/3 (QUIC) not supported

The site does not support HTTP/3 (QUIC) — a newer, faster protocol more resilient to network loss. This is a performance/modernity recommendation, not a security flaw.

Where to look / who is responsible: Web server / CDN (HTTP/3)

How to fix: Enable HTTP/3 on the server (e.g. nginx with QUIC) or via a CDN such as Cloudflare.

• No MX records found (domain does not receive email)

No mail server is set for the domain (technically — no MX record), so it cannot receive email or mail is misconfigured.

Where to look / who is responsible: Domain DNS settings / email provider

How to fix: If the domain should receive mail, set your provider's mail servers (MX records) in the domain DNS settings.

• No BIMI record

The domain has no BIMI record — mail clients do not show your brand logo next to the messages you send. It is a trust and recognition signal (works together with an enforced DMARC policy).

Where to look / who is responsible: Mail DNS (BIMI)

How to fix: Get DMARC right (p=quarantine or reject), prepare an SVG logo and add a BIMI TXT record at default._bimi.<domain>.

• Registered look-alike (typosquat) domains

Registered look-alike (typosquat) domains were found — a changed or dropped letter, swapped letters, or a different TLD. Such domains are often used for fraud: fake emails, spoofed sites, brand impersonation.

Where to look / who is responsible: Brand protection (look-alike domains)

How to fix: Check whether these domains are yours; if not, monitor them, consider defensively registering the most important ones, and report abuse.

Passed checks (7)

Checks your site passed successfully.

✓ Cookies use Secure/HttpOnly

✓ DNSSEC enabled

✓ Not found in threat databases

✓ Not on any blocklists

✓ Site IP is clean on reputation lists

✓ Domain registration date

✓ Google Safe Browsing: no threats found

Next steps

1. Start with the critical and high-priority issues (see "Priority actions").
2. Update outdated software and set up regular maintenance.
3. After fixing, re-run the scan to confirm the result.

Need help getting this sorted? We audit, fix the gaps and maintain it — **pagalba@parescius.lt**.