MP

Marius Pareščius

KIBERNETINIS SAUGUMAS

Išplėstinė saugumo patikros ataskaita · sugeneruota 2026-08-14 19:34

Ataskaitos data/laikas: **2026-08-14 19:34 (+02:00)** · GMT / UTC: **2026-08-14 17:34** · Šablono versija: **1.1** · Programos versija: **2.99.3** · Patikros tipas: **išplėstinė**

F

29/100

zero.webappsecurity.com

Kritinės saugumo spragos — būtina imtis veiksmų.

Tai **mokama išplėstinė ataskaita** — gilesnė analizė nei nemokamas online testas: aptikti komponentai su versijomis, pasenusi programinė įranga, susietos žinomos spragos (CVE) ir techninis inventorius (DNS, TLS, HTTP antraštės). Dėl pilno rankinio audito ar nuolatinio stebėjimo: **pagalba@parescius.lt**.

Santrauka

Atlikome išorinę **zero.webappsecurity.com** saugumo patikrą — įvertinome 11 techninių sričių. Bendras saugumo lygis: **29/100 (F)**.

Rasta **19** taisytinų dalykų (1 kritinių, 1 aukšto, 8 vidutinio, 9 žemo prioriteto); 7 patikrinimų praėjo sėkmingai.

Rasta kritinių spragų — būtina nedelsiant imtis veiksmų.

Ką reiškia įvertis: **90–100 (A)** puikus · **80–89 (B)** geras · **70–79 (C)** vidutinis · **50–69 (D)** silpnas · **žemiau 50 (E/F)** rizikingas — reikia veiksmų. Vertinama nuo 100, atimant už kiekvieną trūkumą (iki 10 už vieną).

Prioritetiniai veiksmai

Nuo ko pradėti — svarbiausi trūkumai ir ką su jais daryti.

1 **Svetainė neturi HTTPS (SSL/TLS) — duomenys keliauja nešifruoti**

Kur: Hostingas / serveris (TLS sertifikatas)

Įdiekite galiojantį TLS sertifikatą (pvz., nemokamą Let’s Encrypt per hostingo valdymo skydelį) ir įjunkite HTTPS visam domenui.

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

Kur: Domeno DNS + el. pašto tiekėjas

Sutvarkykite tris dalykus: 1) SPF su „-all"; 2) DKIM (per pašto tiekėją); 3) DMARC (pradžiai p=quarantine, vėliau p=reject). Tvarko kas valdo domeno DNS + pašto tiekėjas.

3 **Trūksta HSTS (Strict-Transport-Security)**

Kur: Web serveris (nginx / Apache konfigūracija arba hostingo tiekėjas)

Web serveryje pridėkite atsako antraštę: Strict-Transport-Security: max-age=31536000; includeSubDomains; preload.

Apžvalga

Pagrindiniai techniniai svetainės parametrai patikros metu.

IP adresas	**54.82.22.214**
SSL išdavėjas	
Serveris	**Apache-Coyote/1.1**
HSTS	**ne**

CSP	**ne**
Reputacija	**švari**

El. pašto sauga (SPF / DKIM / DMARC)

Ši patikra skirta klasikiniams pašto serveriams su vidutiniu siuntimo intensyvumu (įprastas verslo susirašinėjimas) — **ne masinių naujienlaiškių/rinkodaros siuntimams**. Bulk-sender reikalavimai (Gmail/Yahoo >5000 laiškų/d. taisyklės, spam rate stebėjimas per Postmaster Tools, one-click unsubscribe) čia netikrinami — jiems reikalingi specializuoti ESP/monitoringo įrankiai.

MX (pašto serveris)	**nėra**
SPF	**nėra**
DKIM	**nerasta**
DMARC	**nėra**

Aptiktos technologijos ir versijos

Komponentai su versija yra nuorodos į CVE (pažeidžiamumų) paiešką. Spauskite, kad pamatytumėte žinomas spragas.

Programming languages	**Java**
UI frameworks	**Bootstrap**
Web servers	**Apache Tomcat**
JavaScript libraries	**jQuery 1.8.2 ↗** · **PASENUSI — atnaujinti (žinomos spragos)** **Žinomos spragos: CVE-2012-6708, CVE-2019-11358, CVE-2020-11023, CVE-2020-7656, CVE-2015-9251**
Font scripts	**Font Awesome**

Techninis inventorius

DNS įrašai, TLS ir HTTP atsako antraštės, užfiksuoti patikros metu.

DNS

A	**54.82.22.214**

Rasti trūkumai (19)

Trūkumai surūšiuoti pagal svarbą — nuo kritiškiausių. Prie kiekvieno: ką tai reiškia ir konkretus taisymo žingsnis.

× Svetainė neturi HTTPS (SSL/TLS) — duomenys keliauja nešifruoti -10

> Nepavyko užmegzti saugaus HTTPS ryšio arba sertifikatas netinkamas. Tai reiškia, kad duomenys tarp lankytojo ir svetainės gali keliauti neužšifruoti.
>
> **Kur ieškoti / kas atsakingas:** Hostingas / serveris (TLS sertifikatas)
>
> **Kaip taisyti:** Įdiekite galiojantį TLS sertifikatą (pvz., nemokamą Let’s Encrypt per hostingo valdymo skydelį) ir įjunkite HTTPS visam domenui.

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

> Jūsų domenas visiškai neapsaugotas nuo apsimetinėjimo — bet kas gali siųsti laiškus tarsi jūsų vardu (nėra veikiančio SPF/DMARC). Didelė sukčiavimo (BEC / phishing) rizika jums ir jūsų klientams.
>
> **Kur ieškoti / kas atsakingas:** Domeno DNS + el. pašto tiekėjas

Kaip taisyti: Sutvarkykite tris dalykus: 1) SPF su „-all"; 2) DKIM (per pašto tiekėją); 3) DMARC (pradžiai p=quarantine, vėliau p=reject). Tvarko kas valdo domeno DNS + pašto tiekėjas.

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

Naršyklė neįpareigota visada jungtis prie jūsų svetainės saugiu (užšifruotu) ryšiu, todėl pirmą apsilankymą galima perimti ir lankytoją nukreipti į netikrą svetainę (techniškai — trūksta HSTS antraštės).

Kur ieškoti / kas atsakingas: Web serveris (nginx / Apache konfigūracija arba hostingo tiekėjas)

Kaip taisyti: Web serveryje pridėkite atsako antraštę: Strict-Transport-Security: max-age=31536000; includeSubDomains; preload.

! Trūksta Content-Security-Policy -8

Svetainė neriboja, iš kur gali būti įkeliamas kodas, todėl į ją lengviau įterpti kenkėjišką skriptą, vagiantį lankytojų duomenis (techniškai — nėra Content-Security-Policy, apsaugos nuo XSS).

Kur ieškoti / kas atsakingas: Web serveris (nginx / Apache konfigūracija arba hostingo tiekėjas)

Kaip taisyti: Web serveryje apibrėžkite CSP politiką, pvz.: Content-Security-Policy: default-src 'self'; ir palaipsniui įtraukite reikalingus šaltinius.

! Nėra SPF įrašo — laiškai jūsų vardu nefiltruojami, dažnai patenka į spam -8

Nenurodyta, kurie serveriai turi teisę siųsti laiškus jūsų domeno vardu (tai vadinama SPF įrašu). Be jo bet kas gali apsimesti jūsų adresu, o jūsų pačių siunčiami laiškai dažniau patenka į šlamštą arba atmetami.

Kur ieškoti / kas atsakingas: Domeno DNS nustatymai (tvarko hostingas / registratorius / administratorius)

Kaip taisyti: Domeno DNS nustatymuose pridėkite SPF įrašą (TXT), nurodantį jūsų pašto serverį, pvz.: v=spf1 a mx ip4:JŪSŲ-IP -all. Tai padaro jūsų el. pašto tiekėjas arba kas tvarko domeno DNS.

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

Jūsų svetainę galima nematomai įdėti į svetimą puslapį ir apgauti lankytojus, kad paspaustų ne ten, kur galvoja (techniškai — nėra apsaugos nuo „clickjacking").

Kur ieškoti / kas atsakingas: Web serveris (nginx / Apache konfigūracija arba hostingo tiekėjas)

Kaip taisyti: Web serveryje pridėkite X-Frame-Options: SAMEORIGIN arba CSP direktyvą frame-ancestors 'self'.

! Nėra DMARC įrašo — laiškų klastojimas jūsų vardu neblokuojamas -6

Jūsų domenui nenustatyta taisyklė, ką daryti su laiškais, kurie tik apsimeta esą nuo jūsų (tai vadinama DMARC politika). Be jos sukčiai gali siųsti laiškus tarsi jūsų vardu (pvz. „iš" jūsų įmonės klientams), o gavėjo paštas nežino, ar juos blokuoti. Tai kenkia reputacijai ir didina sukčiavimo riziką.

Kur ieškoti / kas atsakingas: Domeno DNS nustatymai (hostingas / registratorius)

Kaip taisyti: Domeno DNS nustatymuose pridėkite DMARC įrašą (TXT, vardu _dmarc), pvz.: v=DMARC1; p=quarantine; rua=mailto:postmaster@jūsų-domenas. Pradėkite nuo stebėjimo, vėliau sustiprinkite. Tvarko kas valdo domeno DNS.

! Nerasta DKIM parašo (tikrinti įprasti selektoriai) — laiškai nepasirašomi, dažniau patenka į spam -6

Jūsų siunčiami laiškai nepasirašomi skaitmeniniu „antspaudu", kuris gavėjui įrodo, kad laiškas tikrai iš jūsų (tai vadinama DKIM parašu). Be jo Gmail, Outlook ir kiti dažnai meta jūsų laiškus į šlamštą arba juos atmeta.

Kur ieškoti / kas atsakingas: El. pašto tiekėjas / serveris + domeno DNS nustatymai

Kaip taisyti: Įjunkite laiškų pasirašymą (DKIM) savo el. pašto tiekėjo nustatymuose ir paskelbkite jo duodamą įrašą domeno DNS. Paprastai tai atlieka pašto tiekėjas (pvz. Google Workspace, Zoho, hostingo paštas).

! Nerasta XML svetainės schema (sitemap) — turinys sunkiau indeksuojamas; reikalinga pateikti Google Search Console -3

Svetainė neturi XML schemos (sitemap) — paieškos sistemoms sunkiau surasti ir indeksuoti visus puslapius, todėl jie gali nepatekti į Google paiešką.

Kur ieškoti / kas atsakingas: Svetainė / SEO (administratorius ar programuotojas)

Kaip taisyti: Sugeneruokite XML sitemap (WordPress automatiškai pateikia /wp-sitemap.xml; SEO įskiepiai, pvz. Rank Math ar Yoast — /sitemap_index.xml), nurodykite ją robots.txt eilutėje „Sitemap:" ir pateikite per Google Search Console.

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

El. pašto autentikacijos pagrindui trūksta pamatinių elementų (SPF / DKIM / DMARC). Tai būtina kiekvienam domenui, net jei laiškų siunčiate mažai — kitaip juo lengva apsimesti.

Kur ieškoti / kas atsakingas: Domeno DNS + el. pašto tiekėjas

Kaip taisyti: Sukonfigūruokite visus tris domeno DNS: SPF (v=spf1 ... -all), DKIM (per pašto tiekėją) ir DMARC (_dmarc, pradžiai p=quarantine). Tai standartinis higienos minimumas.

• Serveris atskleidžia programinės įrangos versijas -5

Jūsų serveris viešai rodo, kokios programinės įrangos ir kokią versiją naudoja. Tai užpuolikams palengvina rasti būtent tai versijai tinkamą spragą įsilaužti (techniškai — versijos atskleidžiamos atsako antraštėse).

Kur ieškoti / kas atsakingas: Web serveris (nginx / Apache konfigūracija)

Kaip taisyti: Web serveryje paslėpkite versijas (pvz. server_tokens off; Nginx, ServerTokens Prod Apache, pašalinkite X-Powered-By).

• Trūksta X-Content-Type-Options -4

Naršyklė gali neteisingai „atspėti" failo tipą ir įvykdyti kenkėjišką turinį (techniškai — nėra X-Content-Type-Options).

Kur ieškoti / kas atsakingas: Web serveris (nginx / Apache konfigūracija arba hostingo tiekėjas)

Kaip taisyti: Web serveryje pridėkite antraštę: X-Content-Type-Options: nosniff.

• Trūksta Referrer-Policy -3

Lankytojui pereinant iš jūsų svetainės į kitą, gali nutekėti tikslūs jūsų puslapių adresai ir parametrai (techniškai — nėra Referrer-Policy).

Kur ieškoti / kas atsakingas: Web serveris (nginx / Apache konfigūracija arba hostingo tiekėjas)

Kaip taisyti: Web serveryje pridėkite: Referrer-Policy: strict-origin-when-cross-origin.

• Nėra IPv6 (AAAA įrašo) — svetainė nepasiekiama per IPv6 -2

Domenas neturi AAAA įrašo — svetainė nepasiekiama per IPv6. IPv6 jau yra standartas; dalis vartotojų ir mobiliųjų tinklų naudoja tik IPv6, todėl jiems svetainė gali veikti lėčiau ar visai neatsidaryti.

Kur ieškoti / kas atsakingas: DNS / hostingas (IPv6)

Kaip taisyti: Pridėkite AAAA DNS įrašą ir įjunkite IPv6 serveryje arba per CDN.

• Aptikta 1 komponentų su atskleista versija (tikrinti žinomus CVE)

Svetainė atskleidžia naudojamų komponentų versijas. Pagal jas užpuolikai gali ieškoti viešai žinomų pažeidžiamumų (CVE).

Kur ieškoti / kas atsakingas: Svetainė (komponentų / įskiepių versijos)

Kaip taisyti: Reguliariai atnaujinkite visus komponentus iki naujausių versijų ir, kur įmanoma, slėpkite versijų informaciją.

• HTTP/3 (QUIC) nepalaikomas — naujesnis, greitesnis protokolas

Svetainė nepalaiko HTTP/3 (QUIC) — naujesnio, greitesnio ir atsparesnio tinklo trikdžiams protokolo. Tai ne saugumo spraga, o našumo/modernumo rekomendacija.

Kur ieškoti / kas atsakingas: Web serveris / CDN (HTTP/3)

Kaip taisyti: Įjunkite HTTP/3 serveryje (pvz. nginx su QUIC) arba per CDN (Cloudflare ir kt.).

• Nerasta MX įrašų (domenas nepriima el. pašto)

Domenui nenurodytas pašto serveris (techniškai — MX įrašas), todėl jis nepriima el. laiškų arba paštas sukonfigūruotas netinkamai.

Kur ieškoti / kas atsakingas: Domeno DNS nustatymai / el. pašto tiekėjas

Kaip taisyti: Jei domenas turi gauti laiškus, domeno DNS nustatymuose nurodykite savo pašto tiekėjo serverius (MX įrašus).

• Nėra BIMI įrašo — el. laiškuose nerodomas jūsų logotipas (pasitikėjimo ženklas)

Domenas neturi BIMI įrašo — el. pašto programos nerodo jūsų prekės ženklo logotipo prie siunčiamų laiškų. Tai pasitikėjimo ir atpažįstamumo ženklas (veikia kartu su griežta DMARC politika).

Kur ieškoti / kas atsakingas: Pašto DNS (BIMI)

Kaip taisyti: Sutvarkykite DMARC (p=quarantine arba reject), paruoškite SVG logotipą ir pridėkite BIMI TXT įrašą default._bimi.<domenas>.

• Registruoti panašūs (typosquat) domenai: zero.net, zero.org, zero.eu, zero.lt, zero.info, zero.shop — gali būti naudojami apgaulei (phishing); patikrinkite, ar jie jūsų

Rasta registruotų į jūsų domeną panašių (typosquat) domenų — pakeista ar praleista raidė, sukeistos vietomis raidės arba kitas plėtinys. Tokie domenai dažnai naudojami apgaulei: netikriems laiškams, suklastotoms svetainėms, prekės ženklo pasisavinimui.

Kur ieškoti / kas atsakingas: Domeno apsauga (panašūs domenai)

Kaip taisyti: Patikrinkite, ar šie domenai priklauso jums; jei ne — stebėkite juos, apsvarstykite svarbiausių apsauginį registravimą ir praneškite apie piktnaudžiavimą.

Tvarkingi punktai (7)

Patikrinimai, kuriuos jūsų svetainė praėjo sėkmingai.

- ✓ Slapukai naudoja Secure/HttpOnly
- ✓ DNSSEC įjungtas
- ✓ Grėsmių bazėse neaptikta
- ✓ Neįtrauktas į blokavimo sąrašus
- ✓ Svetainės IP švarus reputacijos sąrašuose (11 tikrinta)
- ✓ Domenas registruotas 2001-05-24 (prieš 25 m.)
- ✓ Google Safe Browsing: grėsmių nerasta

Tolimesni žingsniai

1. Pradėkite nuo kritinių ir aukšto prioriteto trūkumų (žr. „Prioritetiniai veiksmai“).
2. Atnaujinkite pasenusią programinę įrangą ir įjunkite reguliarią priežiūrą.
3. Po pataisymų atlikite pakartotinę patikrą, kad įsitikintumėte rezultatu.

Reikia pagalbos sutvarkant? Padarome auditą, ištaisome spragas ir prižiūrime — **pagalba@parescius.lt**.