MP

Marius Pareščius

KIBERNETINIS SAUGUMAS

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: **paprasta**

D

52/100

zero.webappsecurity.com

Silpnas saugumo lygis — rekomenduojama taisyti.

Tai **nemokamas, paprastas online testas**, skirtas svetainės savininkui — **ne IT specialistui, DevOps ar CISO**. Jis parodo tik viešai matomus, dažniausius trūkumus. **Pilnas saugumo auditas yra mokamas ir gerokai išsamesnis** (gilesnis testavimas, vidinė analizė, rankinis tikrinimas). Dėl audito: pagalba@parescius.lt

Santrauka

Atlikome išorinę **zero.webappsecurity.com** saugumo patikrą — įvertinome 11 techninių sričių. Bendras saugumo lygis: **52/100 (D)**.

Rasta **10** taisytinų dalykų (1 kritinių, 3 vidutinio, 6 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 **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.

3 **Trūksta Content-Security-Policy**
Kur: Web serveris (nginx / Apache konfigūracija arba hostingo tiekėjas)
Web serveryje apibrėžkite CSP politiką, pvz.: Content-Security-Policy: default-src 'self'; ir palaipsniui įtraukite reikalingus šaltinius.

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**

Rasti trūkumai (10)

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.

! 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.

! 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'.

• 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.).

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**.