Kaip patikrinti dirbtinio intelekto įrankiais sukurtą programėlę

Dirbtinio intelekto (DI) įrankiais sukurta programėlė gali rodyti vieno kliento duomenis kitam: kokius dešimt dalykų patikrinti ir kam tai pavesti.



Marijus Plančiūnas, Aegis Brightsmark įkūrėjas ir buvęs Paysera LT generalinis direktorius
Atnaujinta 2026 m. spalio 26 d.

Ką patikrinti prieš atveriant programėlę klientams

Patikrai verta remtis OWASP programų saugumo tikrinimo standartu ASVS (angl. Application Security Verification Standard). Lentelėje (1 pav.) surinkti 1 lygio reikalavimai, kuriuos verta patikrinti pirmiausia, papildyti įrankių kūrėjų patarimais apie raktus, duomenų bazę ir atsargines kopijas. Patikros, kurios priklauso 2 ar 3 lygiui arba kurių ASVS visai neapima, pažymėtos.

Ką patikrinti		Kas turi būti
1.	Prieiga prie įrašų	Kiekvienoje duomenų bazės lentelėje, kurią galima pasiekti iš naršyklės, įjungta eilučių lygio apsauga (RLS), o jos taisyklės leidžia naudotojui matyti ir keisti tik savo įrašus. Jei nenurodyta kitaip, Supabase rodiniai (angl. views) šią apsaugą apeina, todėl juos reikia patikrinti atskirai. Kuo remtis: ASVS `V8.2.2` (1 lygis); Supabase.
2.	Leidimai tikrinami serveryje	Ar naudotojas gali atlikti veiksmą ir matyti įrašą, tikrina serveris arba duomenų bazė. Naršyklėje paslėptas mygtukas ar prisijungimo langas duomenų neapsaugo. Kuo remtis: ASVS `V8.2.1`, `V8.3.1` (1 lygis).
3.	Slapti raktai lieka serveryje	Supabase `service_role` ar `secret` raktas nepatenka nei į naršyklei siunčiamą kodą, nei į kodo saugyklą. Naršyklėje gali būti tik `anon` ar `publishable` raktas, ir tik kai lenteles saugo RLS. Kintamieji su `VITE_` ar `NEXT_PUBLIC_` priešdėliu patenka į naršyklės kodą. Kuo remtis: Supabase; Vite; Next.js; ASVS `V13.3.1` (2 lygis).
4.	API grąžina tik reikalingus laukus	Atsakyme nėra laukų, kurių naudotojui matyti nereikia, pavyzdžiui, kitų klientų kontaktų. Kuo remtis: ASVS `V15.3.1` (1 lygis).
5.	Įvestis tikrinama serveryje	Serveris tikrina įvestį pagal leidžiamų reikšmių taisykles, net jei tą patį tikrina naršyklė. Užklausos duomenų bazei parametrizuotos, o naudotojo įvestas tekstas rodomas kaip tekstas, ne kaip HTML. Kuo remtis: ASVS `V2.2.1`, `V2.2.2`, `V1.2.4`, `V3.2.2` (1 lygis).
6.	Prisijungimas ir sesijos	Nėra numatytųjų administratoriaus paskyrų, slaptažodžio spėjimo bandymų skaičius ribojamas, slaptažodį sudaro bent 8 simboliai (ASVS primygtinai rekomenduoja 15) ir jis lyginamas su bent 3 000 dažniausių slaptažodžių sąrašu. Kai darbuotojas išeina iš įmonės, jo paskyra išjungiama ir jis iš karto atjungiamas visuose įrenginiuose. Kuo remtis: ASVS `V6.2.1`, `V6.2.4`, `V6.3.1`, `V6.3.2`, `V7.4.2` (1 lygis); OWASP Top 10:2025, A07.

Ką patikrinti	Kas turi būti
7. Ryšys ir publikavimas	Visas ryšys vyksta per HTTPS su HSTS antrašte, kartu su programėle nepublikuojamas `.git` aplankas, o raktai ir sesijų žetonai neperduodami adreso eilutėje. Kuo remtis: ASVS `V12.2.1`, `V3.4.1`, `V13.4.1`, `V14.2.1` (1 lygis).
8. Bibliotekos	Užrašyta, per kiek laiko atnaujinamos bibliotekos su žinomais pažeidžiamumais, ir to laikomasi. Apie tokias bibliotekas praneša `npm audit` ir GitHub Dependabot. Kuo remtis: ASVS `V15.1.1`, `V15.2.1` (1 lygis); npm; GitHub.
9. Atsarginės kopijos	Daromos duomenų bazės atsarginės kopijos ir bent kartą išbandyta, ar iš jų pavyksta atkurti duomenis. Supabase kasdien automatiškai daro Pro, Team ir Enterprise planų projektų atsargines kopijas, o kitų planų naudotojams pataria reguliariai eksportuoti duomenis ir kopijas laikyti kitur; Storage failai į duomenų bazės kopiją nepatenka. ASVS atsarginių kopijų neapima. Kuo remtis: Bendrojo duomenų apsaugos reglamento (BDAR) 32 straipsnio 1 dalies c punktas (EUR-Lex); Supabase.
10. Jei raktas nutekėjo	Raktas iš karto ištrinamas arba atšaukiamas ir pakeičiamas nauju. Supabase įspėja: nors naršyklėje slaptasis raktas neveikia, užpuolikas jį vis tiek gali panaudoti kitais įrankiais. Kuo remtis: ASVS `V13.3.4` (3 lygis); Supabase; OWASP.

1 pav. Patikra prieš atveriant DI sukurtą programėlę klientams. Patikros aprašytos mūsų žodžiais, o po kiekvienos nurodyti atitinkamų OWASP ASVS 5.0.0 reikalavimų numeriai ir kiti šaltiniai (cituojant nurodoma ir versija, pavyzdžiui, `v5.0.0-8.2.2`). ASVS į lietuvių kalbą neišverstas, jo originalas anglų kalba (OWASP ASVS 5.0.0).

Kas turi tikrinti ir kada

Patikrinti reikia, kol nuoroda dar nepasiekė nė vieno kliento, ir geriausia, kad tikrintų kitas žmogus nei tas, kuris programėlę sukūrė.

Taisyklės programėlėms, kurias darbuotojai susikuria patys

Kai programėlę naudodamas DI gali susikurti bet kuris darbuotojas, patikrą prieš atveriant reikėtų paversti įmonės taisykle, kurios laikosi visi. Tokias taisykles nustato DI šeimininkas, t. y. žmogus, kuris įmonėje atsako už tai, kaip naudojamas DI; ką jis daro, rašėme straipsnyje „Kodėl dirbtiniam intelektui įmonėje reikia šeimininko“. Susitarti verta dėl keturių dalykų:

- **Kas gali kurti.** Kurie darbuotojai gali naudotis DI programėlių kūrimo įrankiais ir su kokiomis įmonės paskyromis.
- **Kokie duomenys.** Kokius įmonės duomenis galima įkelti į tokią programėlę ar prie jos prijungti, o kokių negalima.
- **Kas atveria.** Kas gali programėlę atverti klientams ir kas prieš tai ją patikrina pagal 1 pav.
- **Programėlių sąrašas.** Kokios programėlės jau veikia, kas jas prižiūri ir kokius duomenis jos mato.

Visas straipsnis su šaltinių nuorodomis:
aegisbrightsmark.com/lt/zinios/kaip-patikrinti-su-di-sukurta-programele

Marijaus vadovaujama įmonė Aegis Brightsmark sujungia jūsų programas su DI ir padeda susitarti dėl taisyklių. Pirmas pokalbis trunka 45 minutes.

Aegis Brightsmark Capital MB · info@aegisbrightsmark.com · +370 621 41478