Lietuvos mokslo ir studijų institucijų kompiuterių tinklas LITNET

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Vilniaus Gedimino technikos universitetas

Automatinio informacijos saugumo audito paslauga

Naudotojo vadovas

Paslauga sukurta vykdant Europos socialinio fondo finansuojamą projektą „Mokslo ir studijų institucijoms LITNET teikiamų IT paslaugų plėtra“ Nr. 09.3.3-ESFA-V-711-01-0003

Kuriame Lietuvos ateitį

2014–2020 metų Europos Sąjungos fondų investicijų veiksmų programa

Turinys

Įvadas 3
Naudotojai 3
Pirmas jungimasis ir registracija prie paslaugos 3
Prisijungimas prie paslaugos 5
Automatinio saugumo audito vykdymas 6
  Naujas skenavimas 6
  Saugumo audito ataskaita 9
  Skenavimo redagavimas 12
Žurnaliniai įrašai 13
Kontaktai 14

Įvadas

Šiame dokumente pateikiama Automatinio saugos audito paslaugos naudotojo darbo instrukcija. Automatinio informacijos saugumo audito paslauga (toliau – AISAP) skirta atlikti pasirinkto serverio ar interneto svetainės informacinio pažeidžiamumo skenavimą ir gauti jo ataskaitą. Paslauga prieinama LITNET tinkle visoms mokslo ir studijų institucijoms (MSI), įsidiegusioms elektroninių tapatybių federaciją LITNET FEDI.

Naudotojai

Automatinio informacijos saugumo audito paslaugos informacinėje sistemoje (AISAP IS) yra dvi naudotojų grupės:

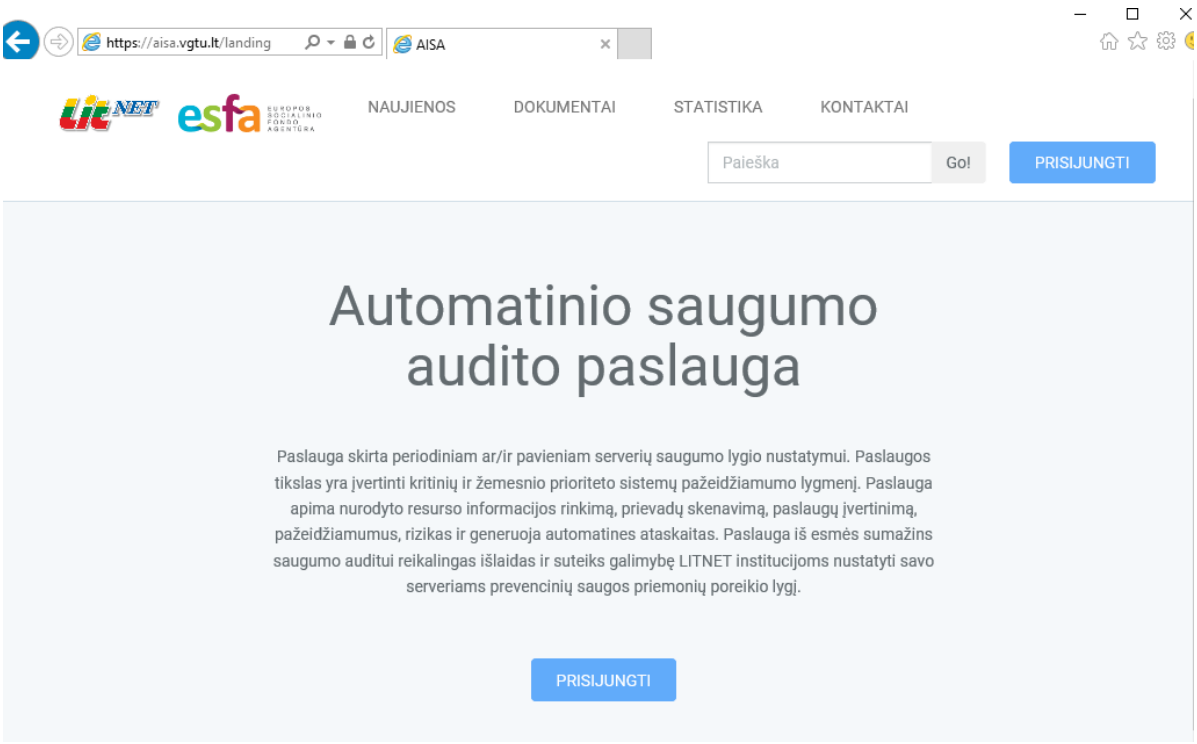
- *Naudotojai*. Ši rolė suteikiama MSI kompiuterių specialistams ar kitiems darbuotojams (mokslininkams, tyrėjams) norintiems atlikti savo naudojamų kompiuterinių resursų (serverių, interneto svetainių) saugos auditą. Naudotojai gali atlikti veiksmus, reikalingus saugos audito planavimui, vykdymui bei rezultatų valdymui savo audituojamuose serveriuose bei interneto svetainėse.
- *Administratoriai*. Ši rolė suteikiama paslaugą administruojančio ar kito Litnet techninio centro darbuotojams. Administratoriai gali atlikti saugos audito planavimo, vykdymo bei rezultatų valdymo veiksmus visame *Litnet* tinkle, taip pat atlikti paslaugos portalo bei informacinės sistemos administravimo veiksmus.

Šiame naudotojo vadove aprašoma naudotojo rolę turinčio naudotojo sąsaja, per kurią prisijungęs naudotojas gali valdyti jo sukurtus sistemų testavimus bei rezultatus. Dirbant su sistema galima naudoti visas šiuo metu plačiai naudojamas naršykles, tokias kaip *Internet Explorer, Mozilla Firefox, Google Chrome*.

Automatinio saugos audito paslauga naudotis gali tik užsiregistravę ir gavę registracijos patvirtinimą iš paslaugos administratoriaus.

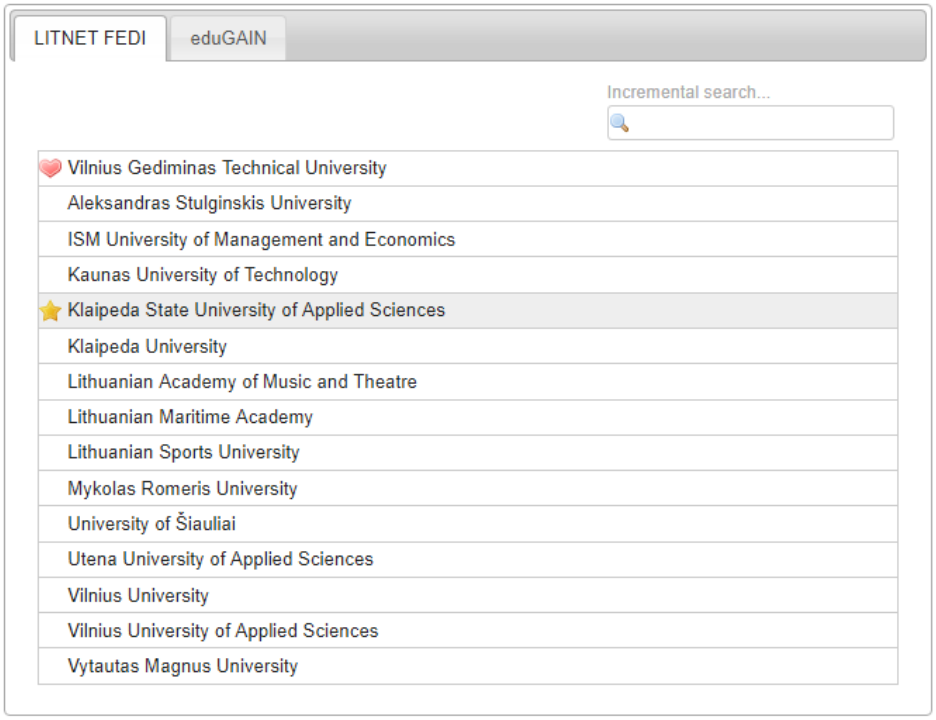
Pirmas jungimasis ir registracija prie paslaugos

Paslauga pasiekiama adresu https://aisa.vgtu.lt arba https://www.litnet.lt/lt/paslaugos. Jos pradinis langas pateiktas 1 paveiksle.



1 pav. Pradinis paslaugos langas

Prisijungimas prie paslaugos galimas tik per Litnet elektroninių tapatybių federaciją LITNET FEDI. Atitinkamas registracijos langas pasirodys paspaudus mygtuką ***Prisijungti*** (žr.2 pav.).



2 pav. LITNET FEDI prisijungimo langas

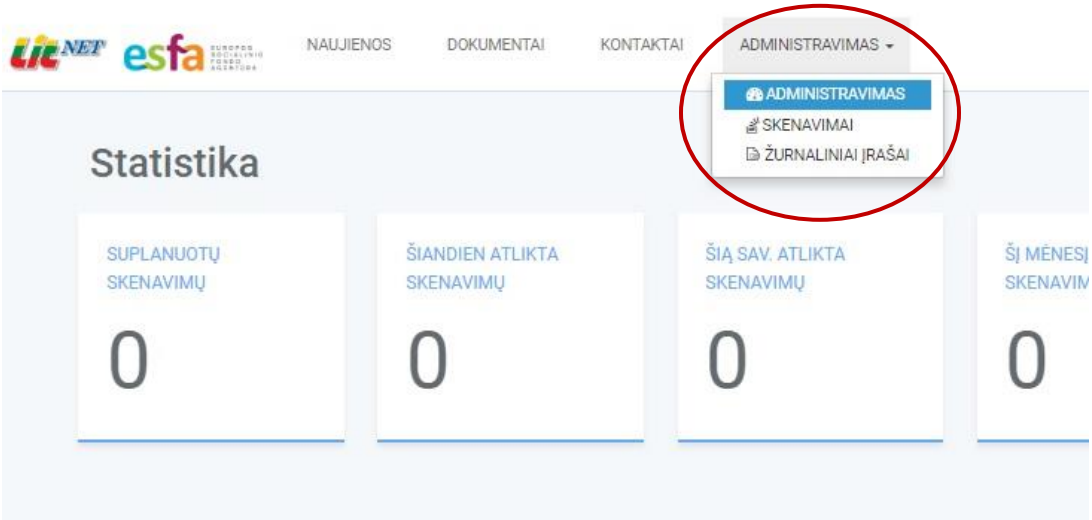
Pasirinkus savo MSI ir prisijungus pirmą kartą, naudotojui pateikiamas pranešimas apie registracijos pradžią. (žr. 3 pav.).

3 pav. Pranešimas naudotojui po pirmo prisijungimo

Naujo naudotojo registracija nėra vykdoma automatiškai. Ji atliekama ne vėliau, kaip per vieną darbo dieną. Paslaugos administratorius, gavęs iš sistemos pranešimą apie naujo naudotojo registraciją, atlieka papildomą naujo naudotojo autentifikaciją. Esant poreikiui, naudodamasis elektroninių tapatybių federacijoje LITNET FEDI esamais kontaktiniais duomenimis, susisiekia su būsimu naudotoju, aptaria bei patikslina jo poreikius vykdyti automatinį saugos auditą. Registracija užbaigiama, kai paslaugos administratorius suteikia teisę prisijungti prie paslaugos valdymo lango ir naudotis paslauga ir naudotojui apie tai pranešama el. laišku.

Prisijungimas prie paslaugos

Registruotam naudotojui prisijungus per naršyklę prie paslaugos, jos valdymo įrankiai pateikiami viršutinio meniu skiltyje ***ADMINISTRAVIMAS*** (žr. 4 pav.).

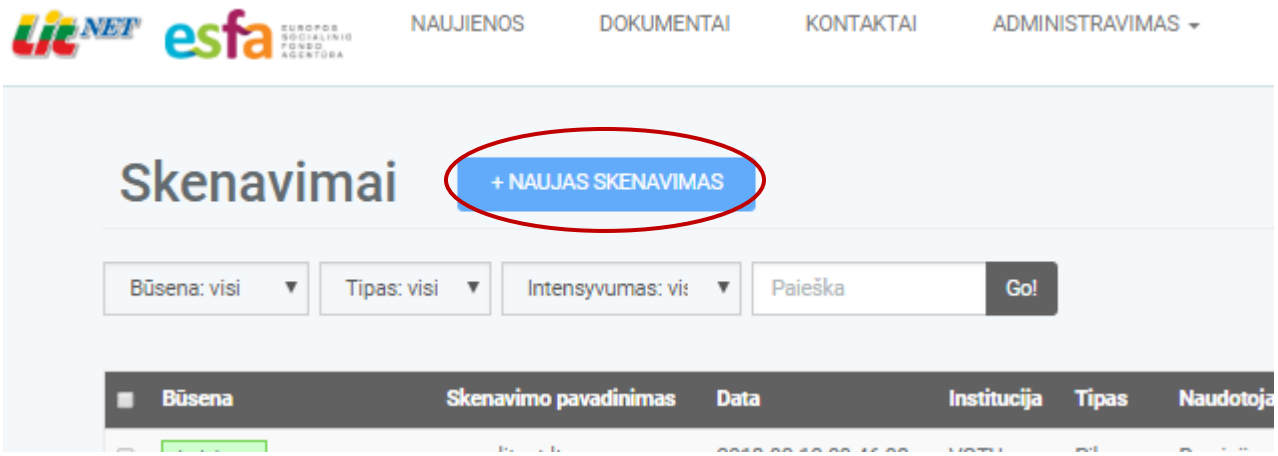


4 pav. Naudotojo paslaugos valdymo langas

Šiame lange taip pat pateikiama visa naudotojo atliktų automatinio saugumo audito skenavimų statistika.

Automatinio saugumo audito vykdymas

Automatinio saugumo auditas vykdomas skenuojant pasirinktus auditavimo objektus. Tai atliekama viršutinio meniu skiltyje ***ADMINISTRAVIMAS*** pasirinkus išsiskleidusiame sąraše punktą ***SKENAVIMAI*** ir perėjus į atsivėrusį skenavimų valdymo langą (5 pav.).



5 pav. Naudotojo skenavimų valdymo langas

Naujas skenavimas

Naujas skenavimas pradedamas pasirinkus mygtuką +NAUJAS SKENAVIMAS (5 pav.). Atsidaro naujo skenavimo langas (6 pav.), kuriame reikia sukurti skenavimo užduotį nurodant atitinkamus skenavimo parametrus.

Pavadinimas – tai naudotojo laisvai įrašomas tekstas. Rekomenduojame pavadinime užrašyti skenuojamo objekto pavadinimą ar DNS adresą. Tada skenavimų sąraše aiškiai matysis, koks objektas buvo audituojamas.

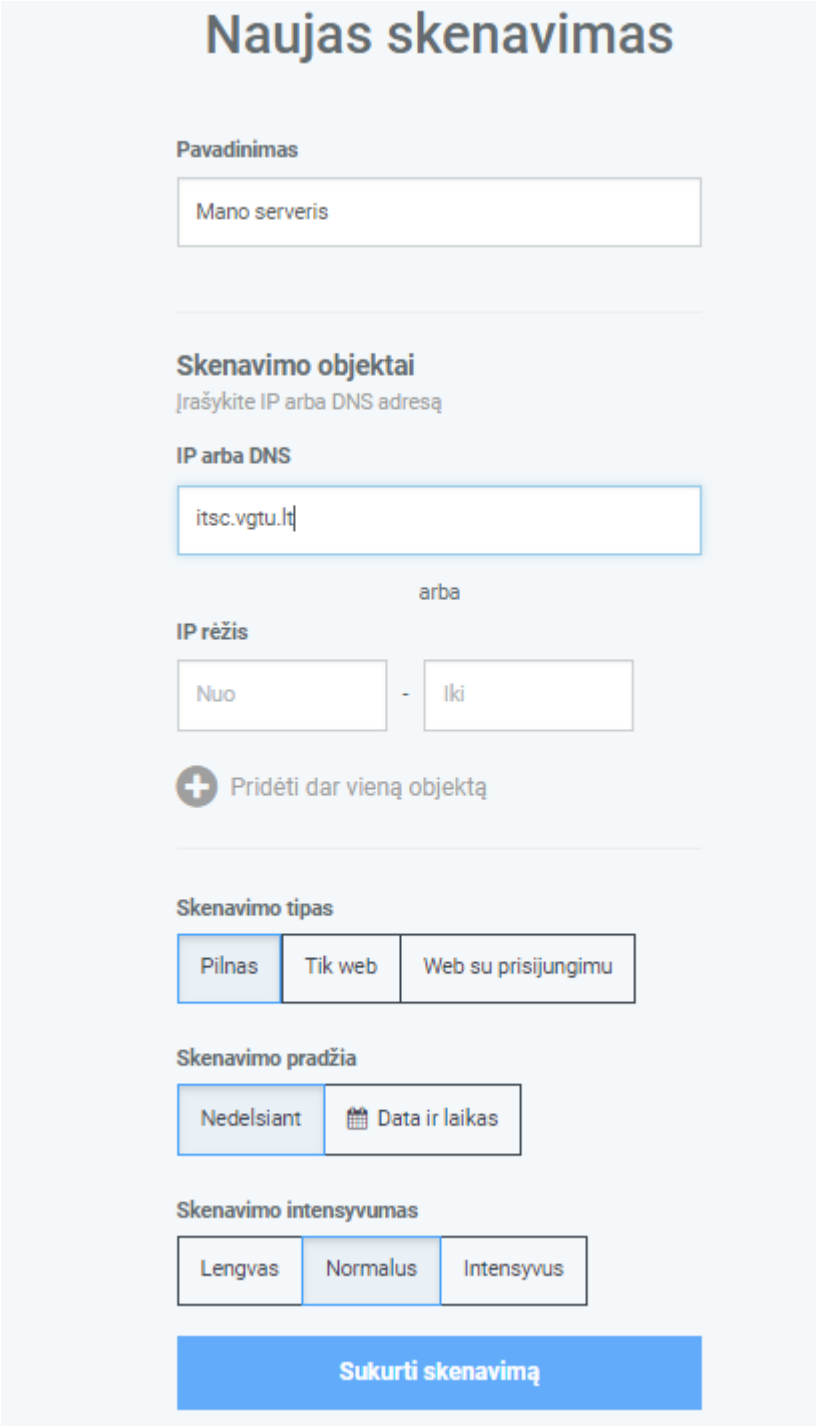
Skenavimo objektai – tai serverių ar interneto tinklalapių, kuriems norime atlikti automatinį saugumo auditą, DNS arba IP adresai. Leidžiami tiek IPv4, tiek ir IPv6 adresai CIDR notacijoje. Galima sukurti skenavimą ir keletui objektų, jei jų IP adresai kinta nuosekliai viename intervale. Šiuo atveju užpildome IP rėžį Nuo – Iki.

Taip pat galima nustatyti norimą skenavimo tipą, skenavimo laiką ir intensyvumą (žr. 5 pav.).

Skenavimo tipas – galima pasirinkti vieną iš trijų tipų:

- ***Pilnas*** – skenuojamos visos nurodyto skenuojamo objekto kompiuterių tinklo tarnybos ir paslaugos;

- ***Tik web*** – skenuojamatik žiniatinklio tarnyba be prisijungimo duomenų;
- ***Web su prisijungimu*** – skenuojama žiniatinklio tarnyba su pateiktais prisijungimo duomenimis.



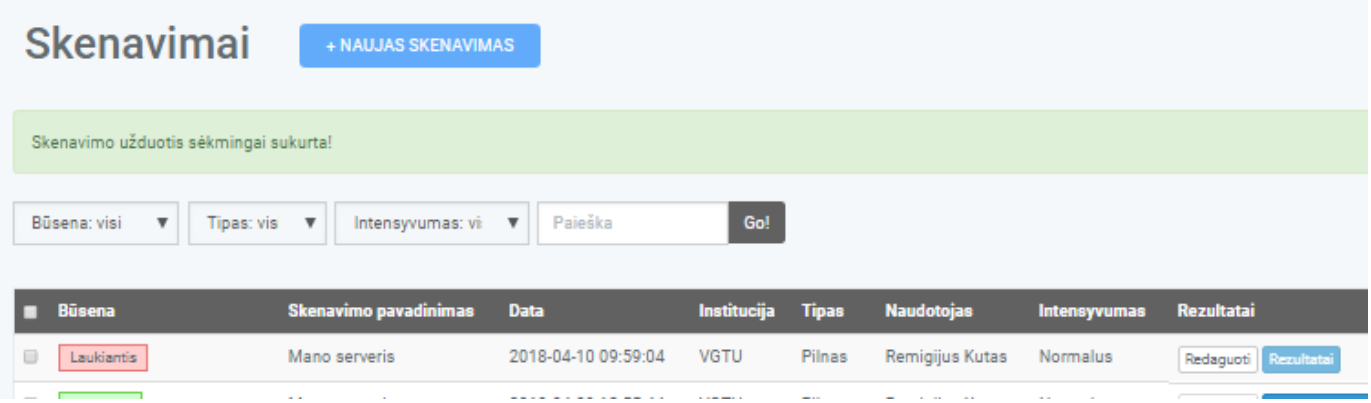
6 pav. Naujo skenavimo sukūrimo langas

Skenavimo pradžia – galima pasirinkti pradėti skenavimą nedelsiant arba nurodyti skenavimo pradžios konkrečią datą ir laiką.

Skenavimo intensyvumas – galim trys skenavimo intensyvumo lygiai:

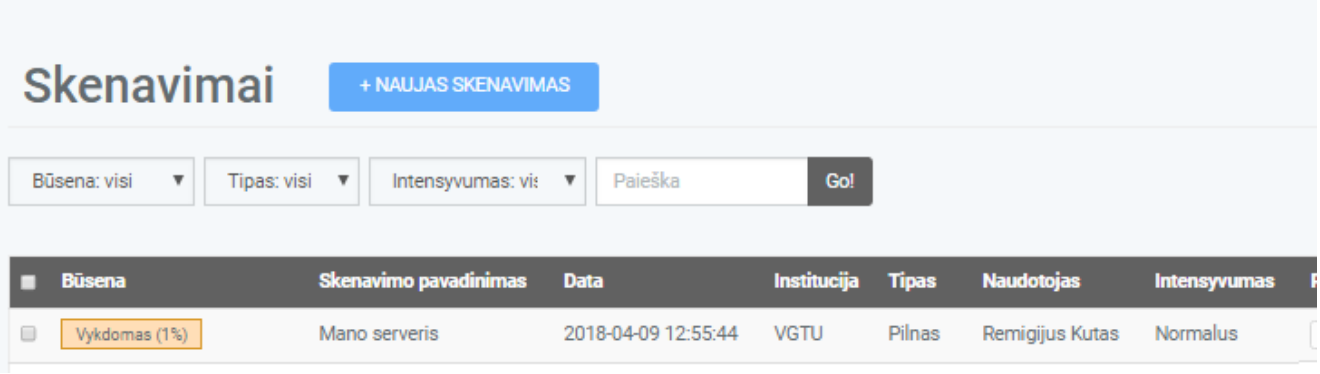
- ***Lengvas*** – bus atliktas standartinių pažeidžiamumų pagal anksčiau surinktą informaciją skenavimas, nevykdant veiksmų, galinčių kenkti skenuojamos sistemos darbui;
- ***Normalus*** – tai lėtesnis skenavimas. Jo metu bus skenuojami ir prievadai bei tikrinama daugiau kitų galimų pažeidžiamumų, kurie gali būti ir ne tokie reikšmingi. Skenavimai, galintys kenkti skenuojamos sistemos darbui nebus vykdomi;
- ***Intensyvus*** – bus atliekami visi skenavimai kaip ir ***Lengvas*** ir ***Normalus*** atvejais, bei papildomai atliekami pavojingesni pažeidžiamumų testavimai, imituojantys paslaugos nutraukimo atakas. Šis skenavimas gali užtrukti gana ilgai, jie reikėtų vykdyti tik suderinus su skenuojamo objekto administratoriumi.

Užpildžius ir pažymėjus visus skenavimo parametrų laukus, spaudžiame mygtuką ***Sukurti skenavimą*** ir grįžtame į ankstesnį skenavimo valdymo langą. Jo skenavimų sąraše atsiranda sukurtas naujas skenavimas, kurio būsena yra ***Laukiantis*** (žr. 7 pav.).



7 pav. Naudotojo skenavimų valdymo langas, sukūrus nauja skenavimą

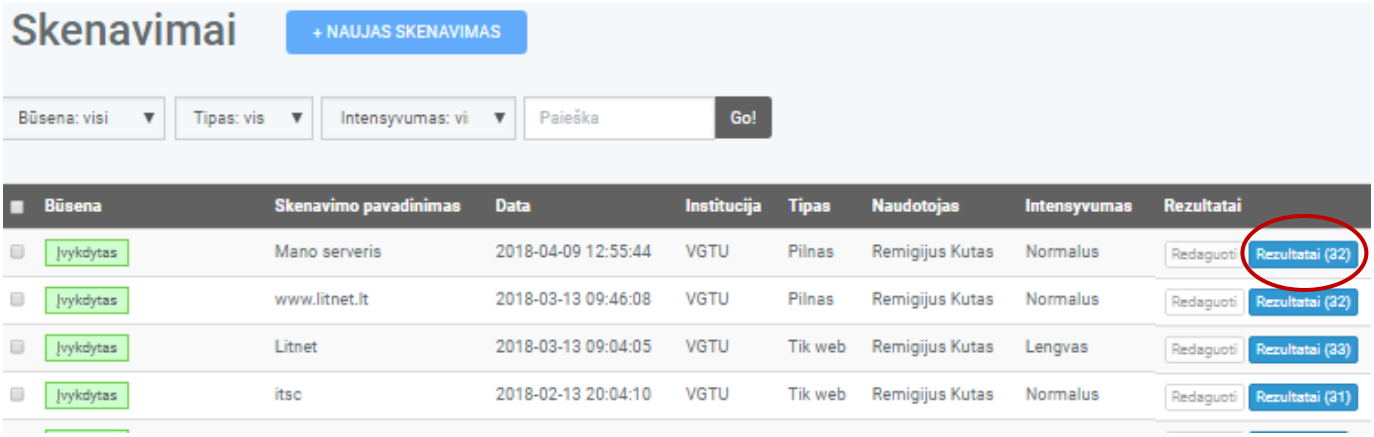
Sistema saugumo auditą (pažeidžiamumų skenavimus) vykdo eilės tvarka, todėl priklausomai nuo apkrovimo (sukurtų skenavimų skaičiaus), skenavimas gali neprasidėti iš karto ir kurį laiką būti būsenos ***Laukiantis***. Sistemai pradėjus vykdyti pažeidžiamumų skenavimą, skenavimo būsena pasikeičia į ***Vykdymas***, nurodant skliausteliuose įvykdymo procentą (žr. 8 pav.)



8 pav. Naudotojo skenavimų valdymo langas, prasidėjus pažeidžiamumų skenavimui

Saugumo audito ataskaita

Atlikto saugumo audito ataskaitą galima peržiūrėti skenavimų sąrašo (žr. 9 pav) stulpelyje ***Rezultatai*** paspaudus mygtuką ***Rezultatai***.

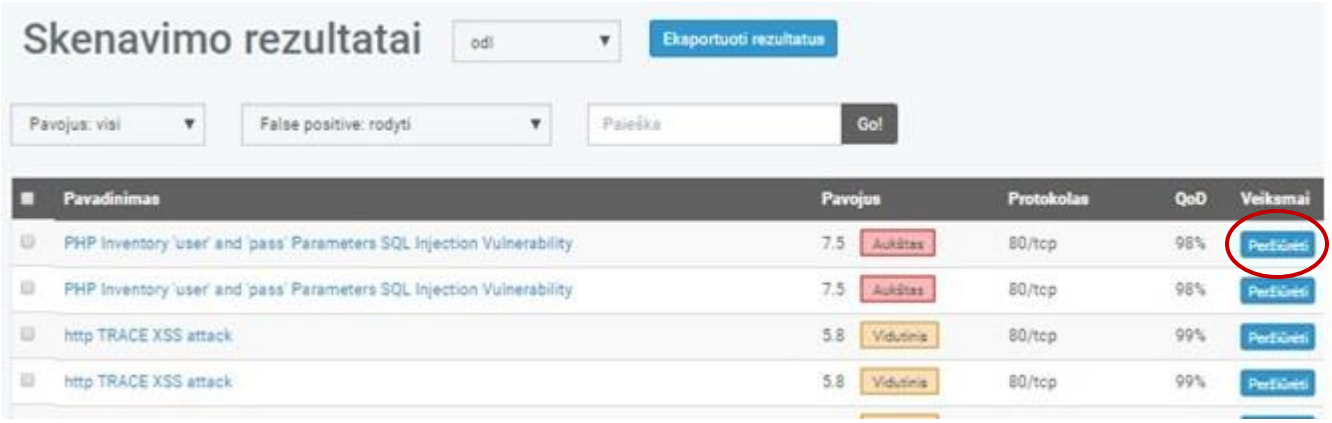


9 pav. Skenavimų sąrašas

Atsivėrusiame lange (žr. 10 pav.) pateikiamas nustatytų audituojamo objekto galimų saugumo pažeidimų sąrašas. Virš rezultatų sąrašo esančiuose laukuose pasirinkę reikiamus paieškos kriterijus ar įvedę paieškos žodį ir paspaudę *Go*, galite atlikti paiešką skenavimo rezultatų sąraše.

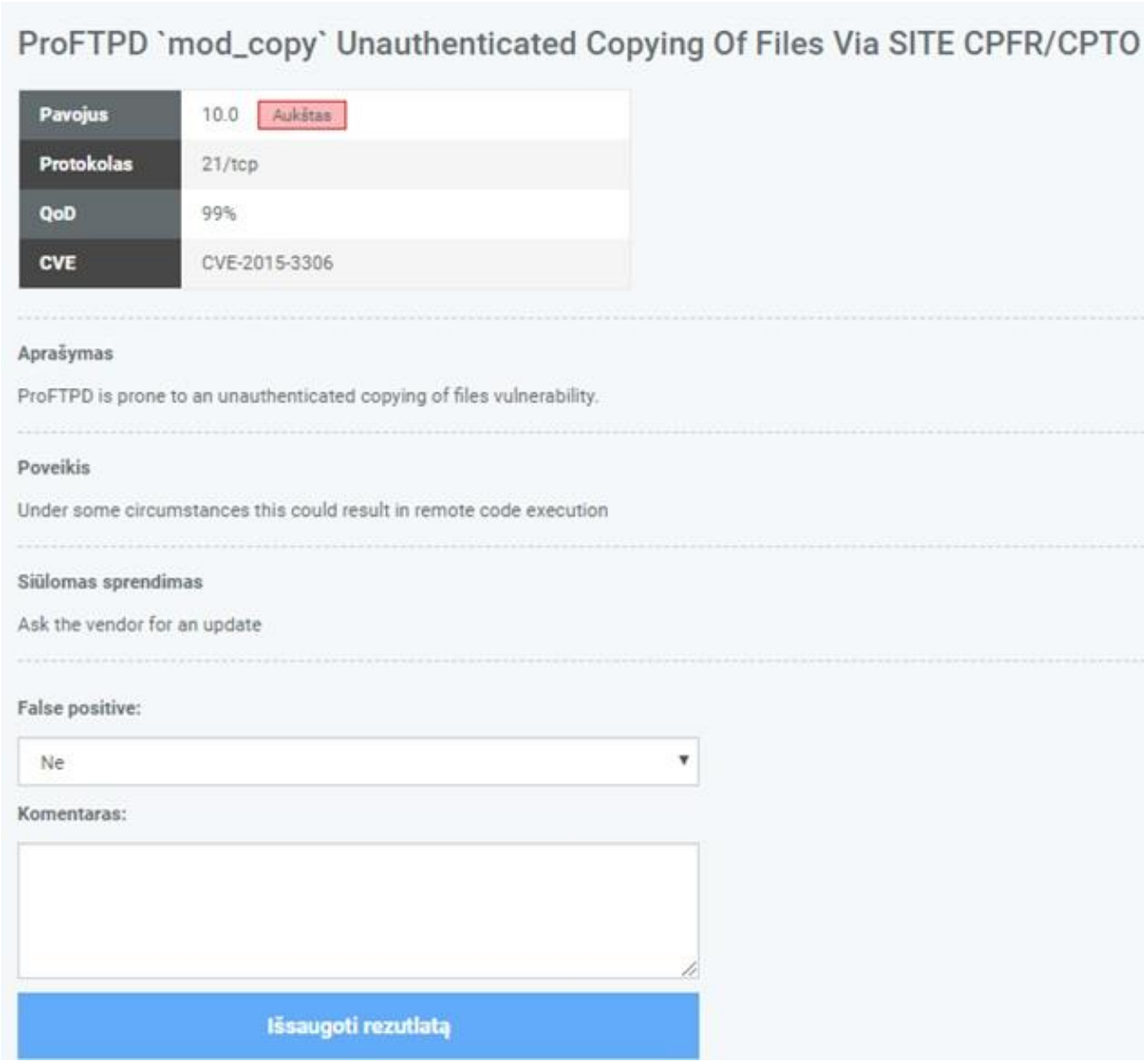
Galimi saugumo pažeidžiamumai yra surikiuojami pagal jų pavojingumo lygį. Aptikus galimą pažeidžiamumą sistema įvertina jį ir priskiria pavojingumo balą nuo 0 iki 10, pavojingiausiems skirdama 10 balų.. Priklausomai nuo pažeidžiamumui pavojaus balo reikšmės, jie suskirstomi į 4 pavojingumo lygius: Aukštas (7,1-10 balų), Vidutinis (4,1-7,0 balų), Žemas (0,1-4,0 balų), Pastaba (0,0 balų).

Pažeidžiamumų sąraše taip pat pateikiamas su pažeidžiamumu susijęs protokolas bei pažeidžiamumo aptikimo kokybės (QoD) rodiklis, kurio vertė nuo 0 % iki 100 %, parodo atlikto pažeidžiamumo aptikimo patikimumą.



10 pav. Nustatytų galimų saugumo pažeidimų sąrašas

Kiekvieno aptikto pažeidžiamumo ataskaita (11 pav.) pateikiama paspaudus mygtuką ***Peržiūrėti.***

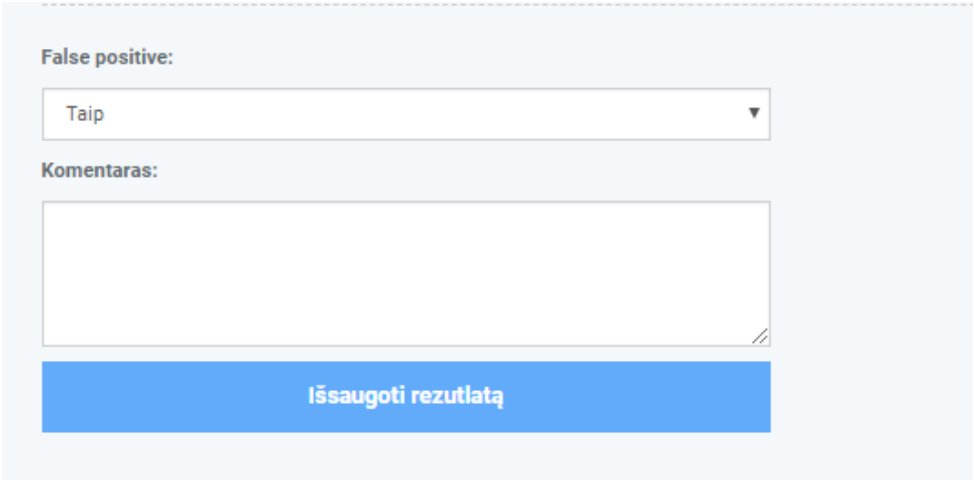


11 pav. Aptikto galimo saugumo pažeidimo ataskaita

Ataskaitoje pakartojama skenavimo rezultatų sąraše pateikta informacija – galimo pažeidžiamumo pavadinimas, nurodantis pažeidžiamumo esmę, protokolas, pažeidžiamumo aptikimo kokybės (QoD) rodiklis bei nuoroda į pažeidžiamumų žinių bazės (CVE) įrašą (daugiau apie CVE įrašus rasite https://cve.mitre.org), kuriuo remiantis nustatytas šis pažeidžiamumas. ***CVE išsamiau*** tinklalapyje adresu https://www.cvedetails.com/ naudojantis šia CVE įrašo nuoroda galima gauti detalesnę informaciją apie aptiktą pažeidžiamumą.

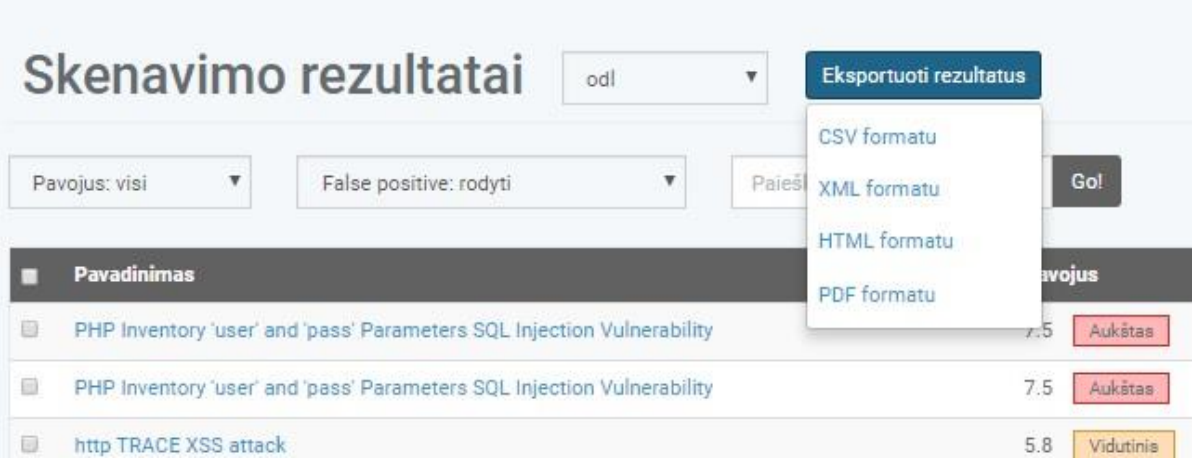
Toliau pateikiamas trumpas aptikto galimo pažeidžiamumo aprašymas, jo poveikis bei siūlomas sprendimas pažeidžiamumo panaikinimui. Pavyzdžiui, 10 pav. pateiktoje pažeidžiamumo ataskaitoje, jo aprašas sako, kad *per ProFTPD tarnybą galimas neautentifikuotas failų kopijavimas neautomatiniu būdu naudojant mod_copy*. Šio pažeidžiamumo poveikis – *gali būti pradėtas vykdyti nuotoliniu būdu įkeltas programinis kodas*. Ir siūlomas sprendimas – *reikalingas esamo kodo atnaujinimas.*

Kadangi pažeidžiamumų aptikimas vykdomas automatiniu būdu analizuojant audituojamo serverio ar web svetainės programinį kodą, nėra šimtaprocentinės garantijos, kad pateikta auditavimo išvada bus visada teisinga. Todėl sistemoje yra sukurta galimybė naudotojui pažymėti, jei pateiktas perspėjimas yra neteisingas, t.y. nustatyti ataskaitos lauko ***False positive*** reikšmę ***Taip*** bei įrašyti atitinkamą komentarą. (žr. 12 pav.)



12 pav. Neteisingo perspėjimo pažymėjimo įrankis

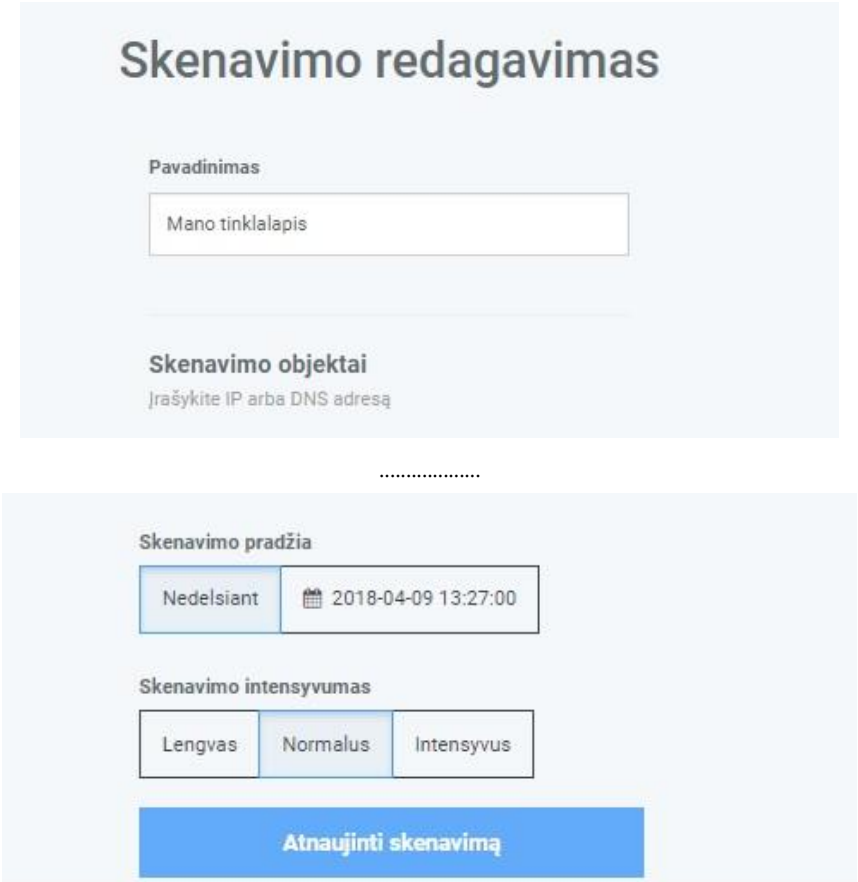
Skenavimo rezultatų ataskaitą galima suformuoti ir išsaugoti atskirame faile. Leidžiami formatai – CSV, XML, HTML ir PDF. Ataskaitos suformavimui ir atsiuntimui, pasirinkite mygtuką ***Eksportuoti rezultatus*** ir pateiktame sąraše pasirinkite reikiamą formatą (žr. 13 pav.).



13 pav. Skenavimo rezultatų atsisiuntimas pasirinktu formatu.

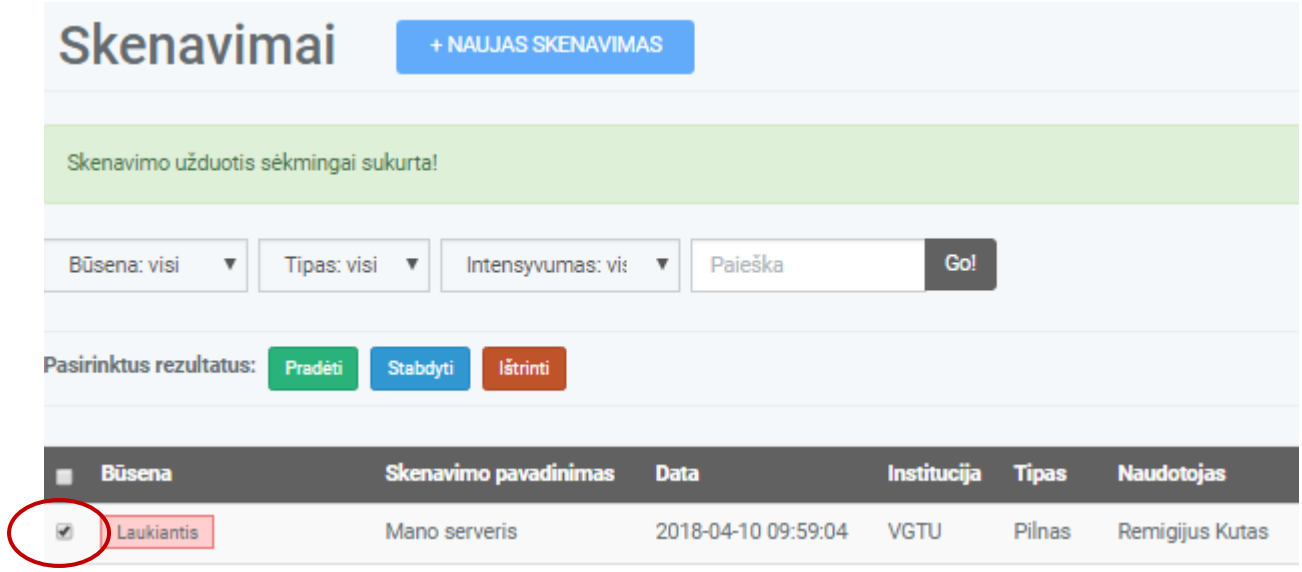
Skenavimo redagavimas

Jei skenavimas dar nėra pradėtas, t.y. jo būsena yra ***Laukiantis*** (žr. 7 pav.), skenavimą galima redaguoti. Norėdami redaguoti skenavimą, skenavimų sąrašo stulpelyje ***Rezultatai*** pasirinkite mygtuką ***Redaguoti*** (žr. 7 pav.), pateiktame Skenavimo redagavimo lange redaguokite reikiamus duomenis ir spauskite ***Atnaujinti skenavimą*** (žr. 14 pav.).



14 pav. Skenavimo parametrų redagavimo langas

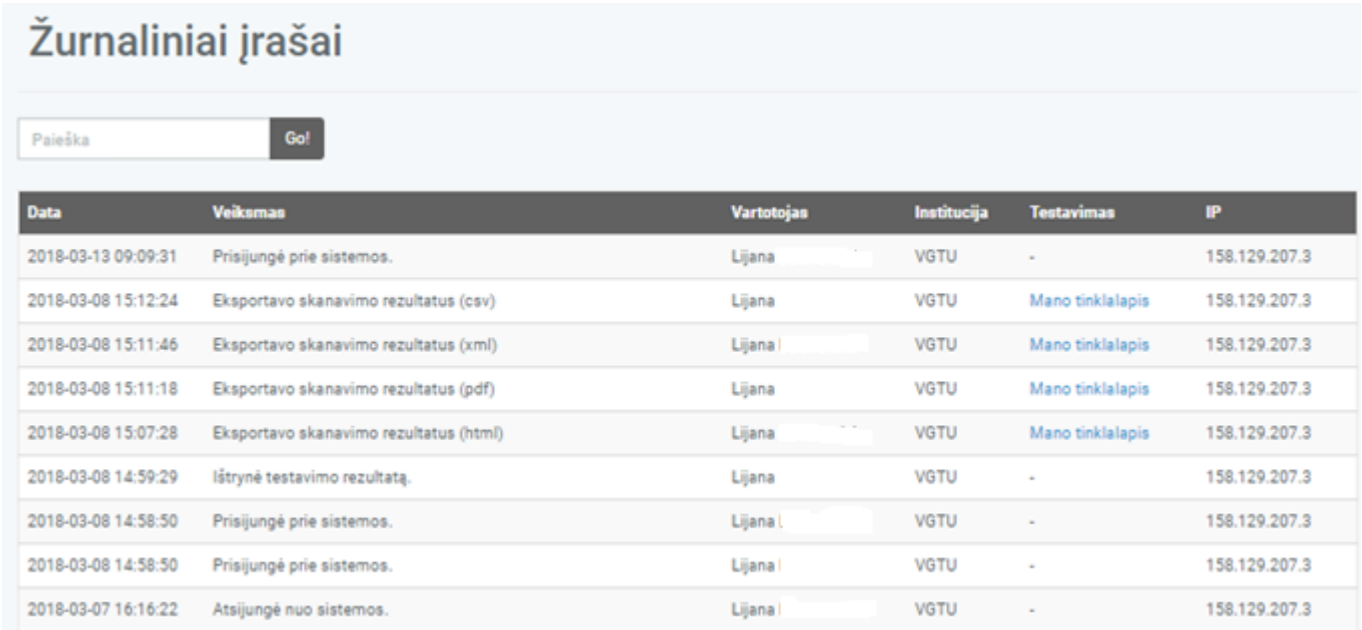
Naudotojas taip pat gali stabdyti ar ištrinti jau pradėtą ar laukiantį skenavimą bei pradėti skenavimą, kuriam buvo nurodytas vėlesnis laikas. Tai atliekama skenavimų sąraše pažymėjus pasirinktą skenavimą (- us), ir bakstelėjus vieną iš atsiradusių mygtukų – ***Pradėti, Stabdyti*** ar ***Ištrinti*** (15 pav.).



15 pav. Veiksmai su pasirinktu skenavimo sąrašo elementu

Žurnaliniai įrašai

Puslapyje *Žurnaliniai įrašai* pateikiama išsami įvykių, kuriuos naudotojas atliko sistemoje, informacija (žr. 16 pav.).



16 pav. Žurnalinių įrašų langas

Kontaktai

Iškilus klausimams ar problemoms naudojantis automatinio saugumo audito paslauga, prašome kreiptis į paslaugos administratorių el. paštu adresu aisa@vgtu.lt