ŠIAULIŲ UNIVERSITETAS

Informacinių technologijų katedra

Mindaugas Jadenkus

Žiniatinklio įvedimo laukų saugumo testavimo sistema

Bakalauro baigiamasis darbas

Vadovė lekt. S. Ramanauskaitė

Šiauliai, 2011

ŠIAULIŲ UNIVERSITETAS

Informacinių technologijų katedra

TVIRTINU

IT katedros vedėjas doc. dr. M. Bernotas
2011-06-01

Žiniatinklio įvedimo laukų saugumo testavimo sistema

Informatikos inžinerijos bakalauro baigiamasis darbas

Vadovė
IT katedros lektorė S. Ramanauskaitė
2011 m. birželio d.

Recenzentė
IT katedros docentė dr. A. Slotkienė
2011 m. birželio d.

Atliko
VI-6 gr. studentas M. Jadenkus
2011 m. birželio 1 d.

Šiauliai, 2011

DARBO SANTRAUKA

Tikslas	Sukurti sistemą, testuojančią žiniatinklio duomenų įvedimo laukus dėl populiariausių pažeidžiamumų ir galimų įvesti netinkamų duomenų.
Kuriamo produkto prototipai	XSS Me – Firefox naršyklės priedas, skirtas testuoti pažeidžiamumą XSS atakoms. SQL Me – Firefox naršyklės priedas, skirtas testuoti pažeidžiamumą SQL įterpimo atakoms. Zero day scan – sistema skirta įvairiems saugumo pažeidžiamumams tikrinti.
Technologinis sprendimas	PHP – programavimo kalba; MySQL – reliacinė duomenų bazė; xHTML 1.1 – hiperteksto žymėjimo kalba; CSS – hiperteksto vaizdavimo kalba.
Panaudota programinė įranga	XAMPP 1.7.3 – sistemos kūrimui ir testavimui; NetBeans 7.0 – kodo rašymui; Notepad++ 5.9 – kodo rašymui; Apache 2.2.18 – sistemos talpinimui; PHP 5.2.17 – programavimo kalba; MySQL 5.1.57 – duomenų bazė; PHPMyAdmin 3.4.0 – duomenų bazės valdymui.
Naudotos UML diagramos	Panaudos atvejų diagrama – aprašo ką sistema gali atlikti ir kartu aprašo išorinius sistemos veikėjus. Veiklos diagrama – parodo objektų sąveiką sistemos veikloje laiko atžvilgiu; Sekų diagrama – parodo testuotojo ir sistemos atliekamus veiksmus ir jų seką Būsenų diagrama – parodo objekto kitimą laike; Komponentų diagrama – parodo sistemos komponentus ir jų tarpusavio sąveiką.
Testavimo apimtis	Funkcinis, našumo, suderinamumo, saugumo testavimai
Vartotojo dokumentacijos sudėtinės dalys	Įdiegimo vadovas; Vartotojo vadovas; Administravimo vadovas.

SUMMARY

Website Input Control Testing System

Every day we hear more and more reports about the use of the Web security cracking and stolen consumer data, or exploit these vulnerabilities for other purposes. There are created many tools designed for testing Websites, but many them can be used for testing a particular vulnerability and do not test the correctness of input. Also there are no such a tools in the Lithuanian language.

The aim of this work is to create a system for data entry testing for Websites most popular of vulnerabilities and possible adoption of data accuracy.

This work represents information about the most common Website security threads and ways to explore these vulnerabilities using insufficient input control in website. The requirements for such a system are gathered and represented as well as possible system architecture.

According to all these specifications the website input control testing system was created. It can be used to test the websites for data entry forms based on selected criteria and make report of vulnerability. It is fully functioning and for better understanding the work with this system, the user documentation is supplied too.

TURINYS

ĮVADAS

Kiekvieną dieną pasigirsta vis daugiau pranešimų apie tai jog išnaudojant žiniatinklio spragas yra įsilaužiama į sistemas ir pavagiami vartotojų duomenys arba šios spragos išnaudojamos kitiems tikslams. Didelėse sistemose tai greičiau pastebima, o mažose turinčiose keliasdešimt vartotojų per dieną, galima išnaudoti pažeidžiamumą ilgą laiką ir taip niekams nežinant kenkti tinklapio naudotojams. Yra sukurta ne vienas įrankis žiniatinklio testavimui, tačiau daugelis jų testuoja tik po vieną pažeidžiamumą, netestuoja įvedamų duomenų teisingumo ir nėra nei vieno įrankio lietuvių kalba.

Darbo tikslas – sukurti sistemą, testuojančią žiniatinklio duomenų įvedimo laukus dėl populiariausių pažeidžiamumų ir galimų įvesti netinkamų duomenų.

Darbui keliami uždaviniai:

1. Susipažinti su žiniatinklio saugumo spragomis ir jų išnaudojimo galimybėmis;
2. Išskirti žiniatinklio įvedimo laukų saugumo testavimui keliamus reikalavimus ir jais remiantis suprojektuoti žiniatinklio įvedimo laukų saugumo testavimo sistemą;
3. Realizuoti suprojektuotą sistemą;
4. Atlikti sukurtos sistemos testavimą;
5. Parengti darbo vadovą, supažindinantį su darbu sistemoje.

Atlikus darbą turėtų būti sukurta sistema, kuri vartotojui leistų paprastu būdu įvertinti savo žiniatinklio įvedimo laukų saugumą ir suvokti jos atsparumą atitinkamoms šio tipo atakoms.

1. ŽINIATINKLIŲ SAUGUMAS IR JO TESTAVIMO PRIEMONĖS

Kiekvieną dieną sukuriama vis daugiau žiniatinklių, taip pat daugėja ir asmenų kurie bando išnaudoti jų saugumo spragas. Žiniatinklių saugumui užtikrinti yra išleidžiami milijonai, nes įsilaužus į svetainę galima perimti įvarius duomenis ar kitaip pakenkti jos savininkui ar vartotojams, todėl kuriant naują žiniatinklį prieš jį patalpinant į internetą reikia patikrinti ar žiniatinklis yra saugus ir negalima į jį įsilaužti. Tai galima padaryti naudojant įvairias sistemas ar programinę įrangą.

Dažniausiai pasigirsta pranešimai apie dviejų tipų įsilaužimus į žiniatinklius tai *SQL* įterpimo ir *XSS* atakos. Nesenai pasirodė straipsnis jog išnaudojant *SQL* įterpimo ataką buvo įsilaužta ir mysql.com žiniatinklį [5]. Žiniasklaidoje neretai pastebimi pranešimai apie tai jog socialiniuose žiniatinkliuose tokiuose kaip *twiter.com* ar *facebook.com* atrasta vis nauja XSS išnaudojimo spraga [12]. Ne taip dažnai pasitaikantys žiniatinklio pažeidžiamumo atvejis UTF-7 koduoto teksto įterpimas, nes nuo jo lengviau apsisaugoti.

1. 1 Dažniausiai pasitaikančio žiniatinklio saugumo spragos

1. 1. 1 SQL įterpimas

Tai yra SQL instrukcijų įterpimas į žiniatinklį taip, kad instrukcijos būtų įvykdytos SQL serveryje.

Internete dažnai galima sutikti tokių *HTML* formų, kurios leidžia įvesti prisijungimo vardą ir slaptažodį (žr. 1 pav.). Dažnai vartotojai būna saugomi *SQL* duomenų bazėse. Įvesto vardo ir slaptažodžio teisingumo vertinimui yra vykdomas *SQL SELECT* kreipinys. Įvedus prisijungimo vardą „Jonas“ ir Slaptažodį „slaptas“ duomenų bazėje būtų įvykdytas *SELECT* kreipinys: „*SELECT * FROM tblUsers WHERE Username=‘Jonas' and Password=‘slaptas’*“.


```
<form method="post">
    Vartotojo vardas<br />
    <input type="text" name="login" style="width:200px;" /><br />
    Slaptažodis<br />
    <input type="password" name="passwd" style="width:200px;" /><br />
    <input type="submit" value="Prisijunti" />
</form><br />
```

1 pav. *Prisijungimo forma ir jos kodas*

Tokį kodo veikimą galima pakeisti įvedus specialiai parinktas parametrų reikšmes. Pavyzdžiui, panaudojus viengubas kabutes ir įvedus ‘*or*’ instrukcijas gali būti suformuotas toks *SELECT* sakinys: „*SELECT * FROM tblUsers WHERE Username=‘‘ or ‘a’=‘a’ and Password=‘‘ or 1=1 --’*“. Šio sakinio sąlyga *WHERE* yra teisinga visada ir tokio *SELECT* sakinio rezultatas yra visa vartotojų lentelė. Gale įvedamas komentaro ženklas – eliminuoja pasiliekančią kabutę ‘ Tokiu būdu prie sistemos prisijungiama pirmojo vartotojo, rasto lentelėje, teisėmis.

Pasinaudojant SQL įterpimo spragomis, galima atlikti ir kitokius veiksmus:

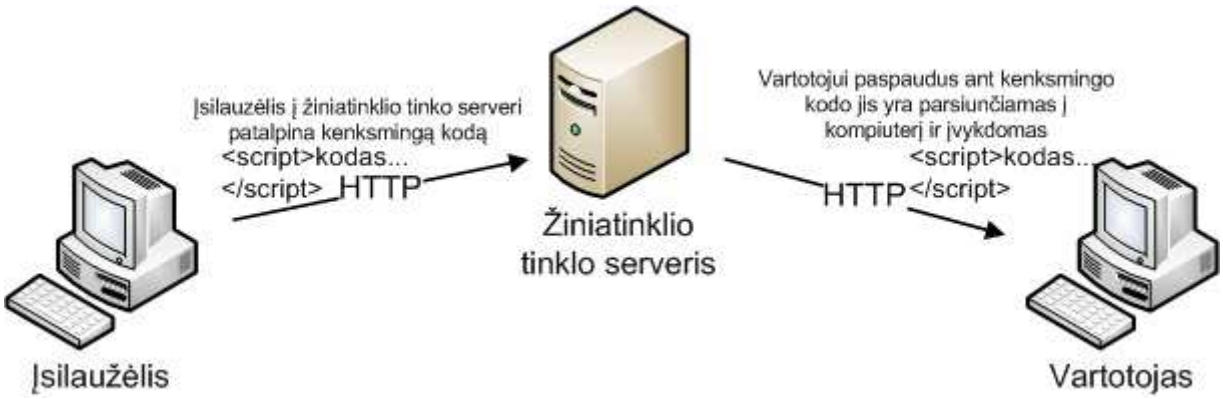
- Pakeisti esamų lentelės laukų reikšmes;
- Įterpti naujus įrašus;
- Sunaikinti lentelę;
- Ir kita.

Apsisaugojant nuo SQL įterpimo, svarbiausia tinkamai filtruoti formos parametrus ir kitą informaciją, kurią gauna žiniatinklis, tai yra neleisti įvesti simbolių: – - " , / \ * & ( ) $ % ^ @ ~ ´ ? ; NULL \n \r. Kitos galimos priemonės – tikrinti parametrų logiką naudoti funkcijas ISNUMERIC ir panašias, riboti parametrų eilutės ilgį, minimizuoti SQL serviso vartotojo privilegijas prisijungiant ne administratoriaus teisėmis [1].

1. 1. 2 Cross Site Scripting

Dažnai pasitaikantis pažeidžiamumas – *Cross Site Scripting* (*XSS*).

Jo esmė – tinklo serverio pagalba įterpti į žiniatinklį *JavaScript*, *VBScript* instrukcijas, kurias vėliau įvykdys kito vartotojo naršyklė (žr. 2 pav.).



2 pav. *XSS atakos veikimo schema*

Paprastai tokių atakų aukos būna internetinių skelbimų lentų skaitytojai, pokalbių dalyviai, el. pašto vartotojai. Pavyzdžiui, skelbimo lentoje užpuolikas palieka *JavaScript* kodą. Kodas yra išsaugojamas tinklo serveryje, ir kiekvienas vartotojas, peržiūrinėdamas šią skelbimų lentą, atsisiųs šį *JavaScript* kodą ir vartotojo naršyklė jį įvykdys [1].

Vartotojas saugotis nuo XSS atakų gali:

- Naršyklėje išjungdamas skriptų vykdymo funkcijas, tačiau tai susiaurina naršyklės funkcionalumą;
- Vengti sekti nuorodomis, gaunamomis el. paštu, *IRC*, *Skype*, *Facebook* ir kitais kanalais;
- Atsijungti iš tinklapio prieš palikdamas jį.

Pagrindinės priemonės turi būti realizuotos serveryje. Taikomosios programos turi filtruoti simbolius, kurių pagalba galima suformuoti *HTML* kodą:

- Reguliarus pažeidžiamumų tikrinimas;
- Vieno prisijungimo (*single sign-on*) eliminavimas;
- Dinaminio turinio filtravimas, paliekant tik leistinus simbolius;
- Įvedamos informacijos filtravimas, pašalinant neleistinus simbolius: – < > “ ‘ % ;) (& + -.

1. 1. 3 UTF-7

Ataka vykdoma pasinaudojant naršyklės savybe "nuspėti" naudojamą simbolių rinkinį. *UTF-7* leidžia bet kokį simbolį išreikšti *ASCII* simboliais, o naršyklė bandydama nuspėti, kokia koduotė naudojama, *UTF-7* užkoduotus simbolius gali paversti į reprezentuojamus simbolius, kurie leidžia įvykdyti ataką.

Pavyzdžiui, *UTF-7* koduotėje simbolis „<“ žymimas „+ADw“, o simbolis „>“ žymimas „+AD4“. Tokiu būdu iš simbolių „+ADw“ ir „+AD4“ galima suformuoti antraštę: *+ADw-script+AD4-alert(document.location)+ADw-/script+AD4-*, o realus gaunamas vaizdas bus: *<script>alert(document.location)</script>*. Tai suteikia galimybę įvykdyti *JavaScript* kodą.

Norint apsisaugoti reikia visada siųsti koduotės nustatymus prie *HTTP* antraštės, pvz.: *header('Content-type: text/html; charset=UTF-8')*. Prieš bet kokį dinamiškai formuojamą tekstą pvz.: *TITLE* elementą, įrašyti koduotę nustatančią eilutę, pvz.: *<meta http-equiv="content-type" content="text/html; charset=utf-8" />* [8].

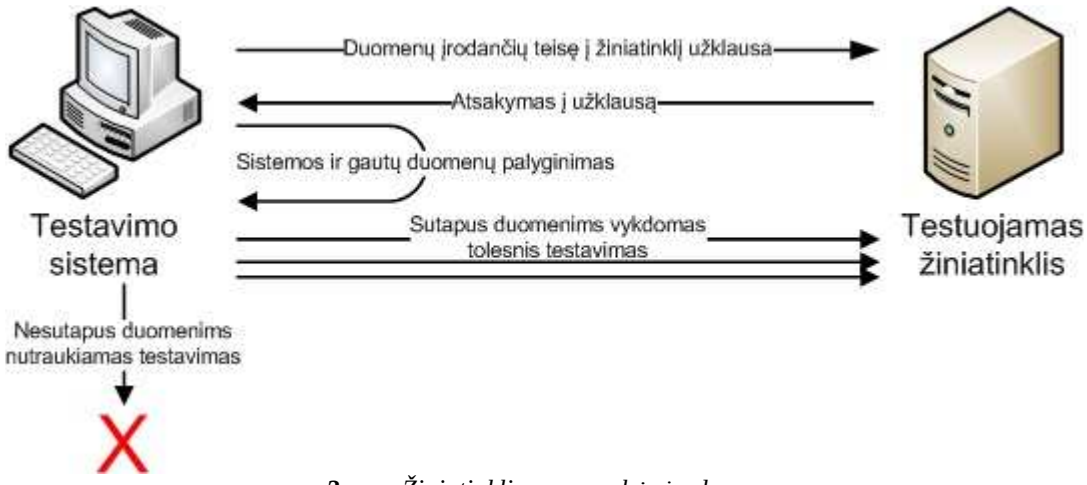
1. 2 Žiniatinklių testavimas

Kuriant testavimo sistemą susiduriama su keliomis problemomis:

- testavimo saugumas – būtina užtikrinti, kad pasinaudojant sistema nebūtų bandoma įsilaužti į svetimą žiniatinklį;
- atliekamo testavimo vientisumas – visas testavimas atliekamas kaip vienas ir trunka kuo trumpesnį laiko tarpą;
- ataskaitos formavimas – turi būti gaunami atgaliniai testavimo duomenys, kuo remiantis formuojama ataskaita.

1. 2. 1 Testavimo saugumo užtikrinimas

Daugelis šiuo metu egzistuojančių įrankių, gali būti panaudoti ne tik nuosavo žiniatinklio saugumo testavimui, bet svetimiems, o pasinaudojus rastomis spragomis į juos įsilaužti. Vienas iš sprendimo būdų yra nuskaitant tam tikrą informaciją iš testuojamo žiniatinklio ir ją palyginus su sistemoje saugoma. Jeigu įsitikinama, kad testuotojas turi priėjimą prie svetainės turinio tik tada atlikti testavimą (žr. 3 pav.).



3 pav. *Žiniatinklio nuosavybės įrodymas*

1. 2. 2 Testavimo vientisumas

Atliekant testavimą dažniausiai tenka vykdyti daug skirtingų testų. Jų pagalba turi būti įvertinamas visos sistemos saugumas, tačiau vartotojui šie pakartotiniai atskiri testai tūrėtų būti nejuntami, o traktuojami kaip vienas bendras testavimas. Sistema tūrėtų automatiškai generuoti skirtingų testinių duomenų srautą, o vartotoją informuoti tik įvykdžius visus testavimo atvejus.

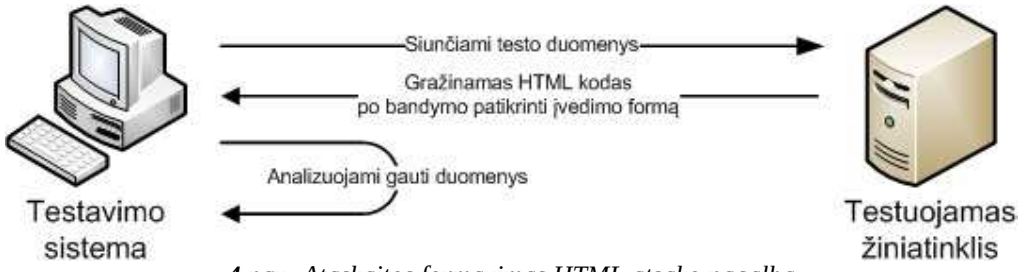
Vienas iš būdų automatizuotai vykdyti testavimą yra naudoti *Cron* – įrankį atlikti darbus tam tikru laiku. Šis įrankis veikia tik *Unix* tipo sistemose ir leistų tolygiai paskirstyti testuojančios sistemos apkrovą. Tačiau naudojant *Cron* ir esant vienu metu dideliam vartotojų skaičiui toks testavimas gali užtrukti pakankamai ilgą laiko tarpą, nes visi testiniai atvejai būtų vykdomi nuosekliai, o ne lygiagrečiai kiekvienam vartotojui.

Kitas iš būdų automatizuotai vykdyti testavimą yra panaudojant *PHP* biblioteką *cURL*. Ši biblioteka turi daug galimybių. Viena iš jų yra duomenų perdavimas į kitą žiniatinklį, kurį galima naudoti ciklo metu ir taip generuoti norimo dydžio duomenų srautą į testuojamą žiniatinklį.

1. 2. 3 Ataskaitos formavimas

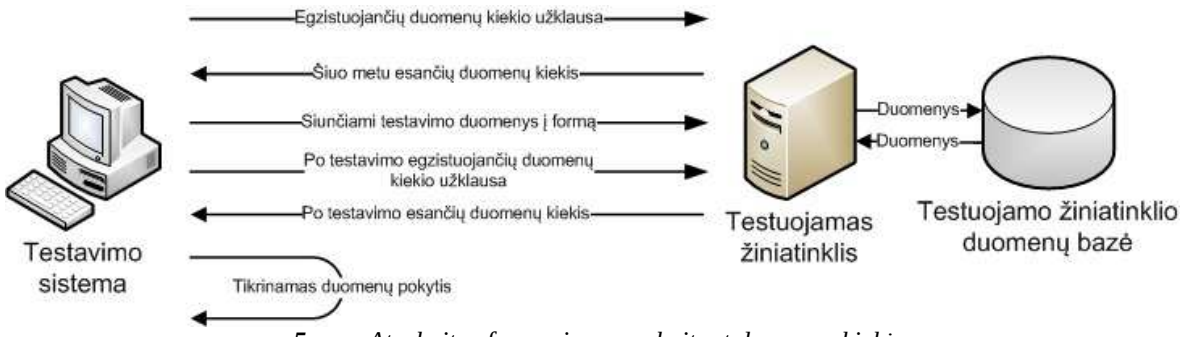
Vartotoją dažniausiai domina tik galutinis žiniatinklio įvedimo laukų saugumo testavimo rezultatas. Tad svarbu ne tik įvykdyti saugumo testavimą bet ir pateikti testavimo metu gautų rezultatų apibendrinimą.

Problema su kuria dažniausiai susiduriama generuojant testavimo ataskaita yra ta kad kiekvieno testo metu turėtų būti gražinamas testo rezultatas, tačiau praktikoje analizuoti žiniatinklio gražinamą HTML kodą nėra veiksminga, dėl iš anksto nežinomos žiniatinklio struktūros ir klaidingą jo veikimą nurodančių kodo eilučių (žr. 4 pav.).



4 pav. *Ataskaitos formavimas HTML atsako pagalba*

Kitas būdas įvertinti atskirų testinių atvejų rezultatus, analizuoti testuojamoje sistemoje kaupiamus duomenis prieš ir po testavimo. Tokiu būdu susiaurėja testavimo sistemos panaudojimo sritis, nes testuojama sistema privalo kaupti į įvedimo formą įvedamus duomenis. Tačiau leidžia tiksliau vertinti gautus rezultatus (žr. 5 pav.).



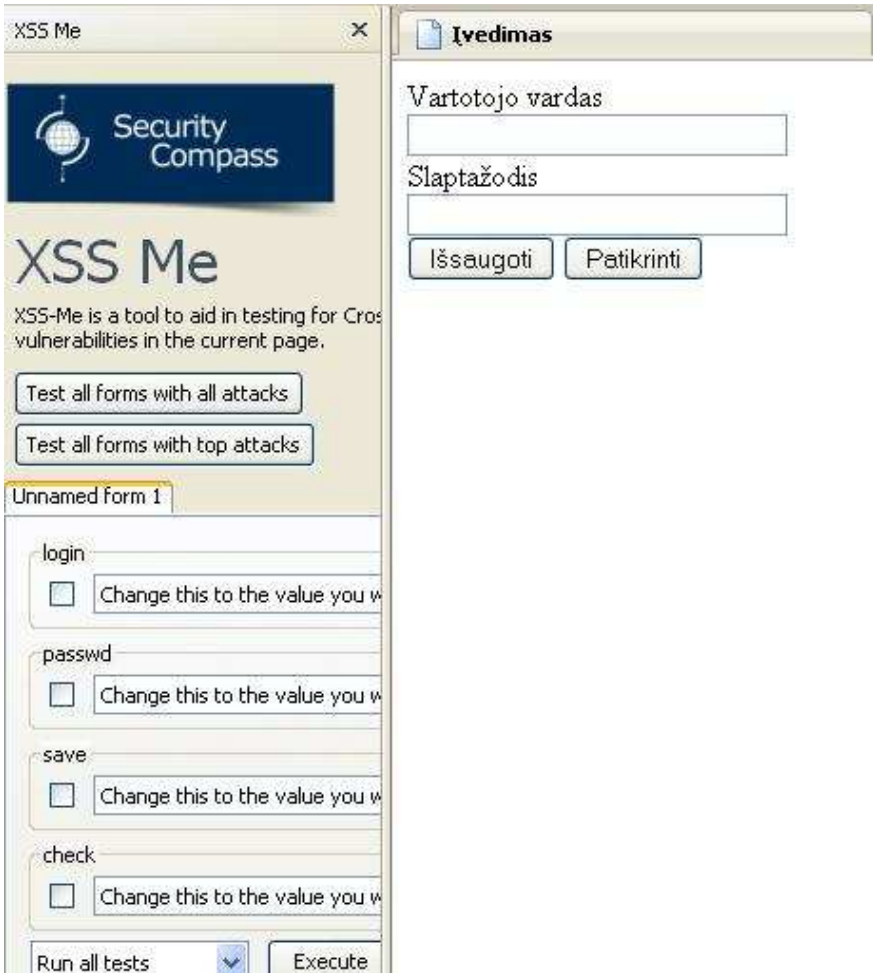
5 pav. *Ataskaitos formavimas nuskaitant duomenų kiekį*

1. 3 Egzistuojantys žiniatinklio saugumo testavimo analogai

Egzistuoja įvairių žiniatinklių saugumo testavimo sistemų, tačiau žiniatinklių įvedimo laukų teisingumo tikrinimui skirtų įrankių nėra itin daug. Neretai egzistuojantys šio tipo testavimo įrankiai yra gan specifiniai ir skirti tam tikram įvedimo laukų testavimui.

1. 3. 1 XSS Me – Firefox naršyklės priedas

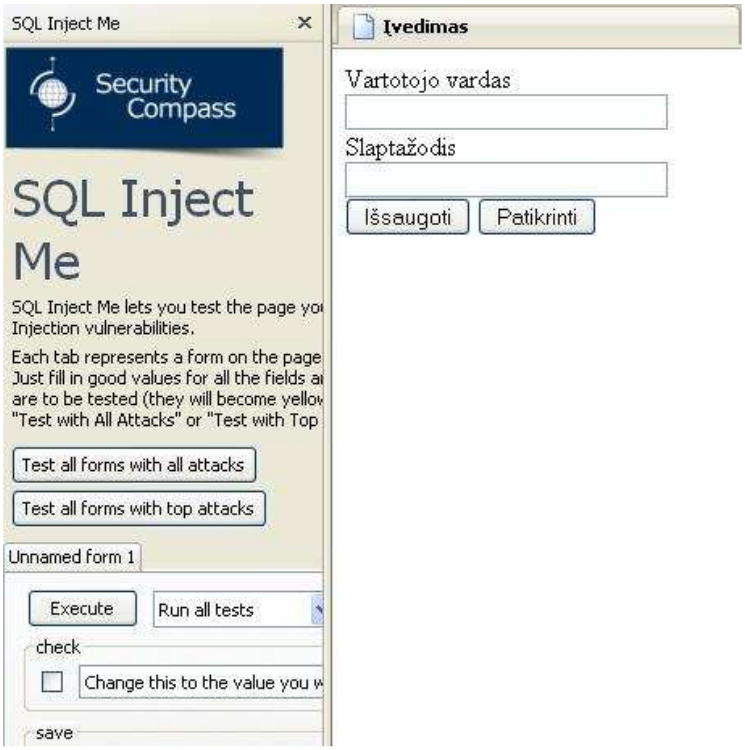
XSS-Me įrankis naudoja *XSS* atakų atmetimo mechanizmą. Į testuojamą žiniatinklį neįrašydamas testuojamų duomenų, įrankis veikia patvirtindamas parinktas *HTML* formas, į jas įrašydamas duomenis laikomus *XSS* atakomis. Rezultate *HTML* tinklapis nustato specialią *JavaScript* reikšmę (*document.vulnerable = true*) tada žiniatinklis pažymimas kaip pažeidžiamas testuotam *XSS* pažeidžiamumui. Įrankis nepažeidžia testuojamo žiniatinklio saugumo, tik ieško galimų spragų [3].



6 pav. *XSS Me – Firefox priedo vaizdas*

1. 3. 2 SQL Inject Me – Firefox naršyklės priedas

SQL Inject Me yra įrankis skirtas testuoti *SQL* įterpimo pažeidžiamumą. Veikia patvirtindamas parinktas *HTML* formas, į jas įrašydamas duomenis laikomus *SQL* injekcijų atakomis. Siunčia *SQL* atakas per formos laukus ir ieško klaidos pranešimų žiniatinklio *HTML* atsake. Įrankis nepažeidžia testuojamo žiniatinklio saugumo, tik ieško galimų spragų [2].



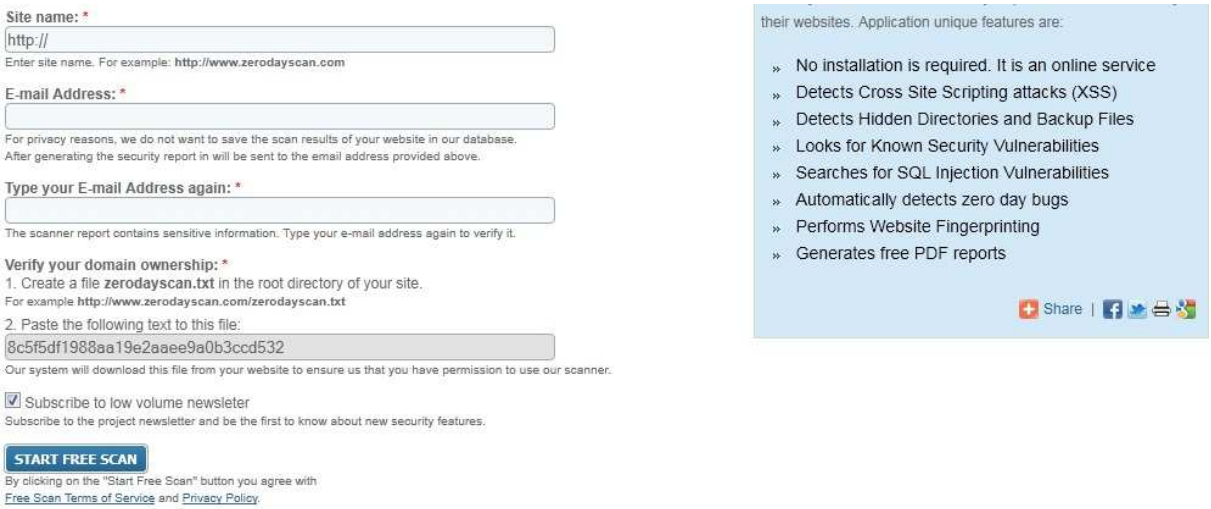
7 pav. *SQL Me – Firefox priedo vaizdas*

1. 3. 3 ZeroDayScan

ZeroDayScan yra nemokama žiniatinklių saugumą testuojanti sistema veikianti „debesyje“. Sistema naudoja serverius visame pasaulyje sujungtus i vieną tinklą, kad atliktų žiniatinklio saugumo įvertinimą.

Kiekviename žiniatinklyje, sistema atlieka tūkstančius testų. Ieško labiausiai pažeidžiamų vietų įskaitant ir netinkamą tinklo serverio konfigūravimą.

Atlikdamas saugumo įvertinimą *ZeroDayScan* naudoja sudėtingas atakas, siekdama nustatyti silpnąsias vietas. Daugeliu atvejų, kai žiniatinklyje yra rastas naujas puslapis, *ZeroDayScan* bando paleisti ataką kartu su teisingais duomenimis. Sistema tikisi gauti pranešimą, kad ataka buvo sėkminga, arba klaidos pranešimą, tada analizuojamas atsakymas, ir radus pažeidžiamumą įrašoma į ataskaitą [14].



8 pav. *ZeroDayScan sistemos vaizdas*

1. 3. 4 Analogų palyginimas

Vertinant šias sistemas pagal konkrečius kriterijus, vieni svarbiausių būtų, kokio tipo saugumo spragas analizuotas įrankis gali įvertinti, ar sudėtingas jo naudojimas ir rezultatų gavimas, ar tinkamai užtikrinamas įrankio nepanaudojimas piktavališkiems tikslams. Konkrečios įrankių vertinimo savybės bei jų reikšmės apibendrintai pateiktos 2 lentelėje.

2 lentelė. Analogiškų sistemų palyginimas

Analogas / **Funkcijos**	**XSS Me 0.4.4**	**SQL Inject Me 0.4.5**	**Zero Day Scan**
Tikrinamų įvedimo laukų pasirinkimo galimybė	Yra	Yra	Nėra
Įrankio paskirtis	Testavimas	Testavimas	Testavimas
Testavimo metu padarytos žalos atitaisymas	Nedaro žalos žiniatinkliui	Nedaro žalos žiniatinkliui	Nedaro žalos žiniatinkliui
Tikrinamos spragos	*HTML* ir *JavaScript* kodo įterpimas	SQL įterpimas	*XSS*, *SQL* įterpimas ir kitos
Reikalinga papildoma programinė įranga	*Firefox* naršyklė (versija 2.0.0.8 - 3.7a1pre)	*Firefox* naršyklė (versija 2.0.0.8 - 3.7a1pre)	Nereikalinga
Ataskaitos rodymas	Naršyklėje detali ataskaita kiek ir kokių spragu buvo aptikta	Naršyklėje detali ataskaita kiek ir kokių spragu buvo aptikta	Atsiunčiama detali ataskaita į elektroninį paštą *PDF* formatu
Testo trukmė	Ne ilgiau kelių minučių	Ne ilgiau kelių minučių	Iki 72 valandų
Informacija apie aptiktų spragų ištaisymą	Nepateikiama	Nepateikiama	Pateikiama ataskaitoje po rastos spragos aprašymu
Puslapio saugumą galintys tikrinti asmenys	Visi kas nori.	Visi kas nori.	Tik asmuo turinti prieiga prie žiniatinklio šakninio katalogo
Įrankio sąsajos kalba	Anglų	Anglų	Anglų

Apibendrinant analogiškų įrankių analizės duomenis matyti, kad juntamas aiškus skirtumas tarp autonomiškai ir interneto naršyklėse įdiegtų įrankių: naršyklių priedai yra labiau specifiniai, skirti konkrečiam testavimui, bet geba rezultatus pateikti iš kart po testavimo, tuo tarpu autonominės sistemos gali būti labiau apkrautos vienu metu dėl didelio vartotojų skaičiaus, todėl naudoja išskaidytą laike testavimo metodą. Tai įtakoja, kad testavimas gali vykti palyginti ilgai. Kitas šių dviejų tipų skirtumas yra tas, kad naudojant internetinių naršyklių priedus nėra reikalaujama tinklapio nuosavybės įrodymo, tuo tarpu *Zero Day Scan* reikalauja testuojančio prieigos teisių prie šakninio katalogo.

Apibendrintai galima teigti, kad vartotojas gali pasirinkti tokio tipo testavimo įrankį, kuris jam pačiam yra labiau priimtinas, tačiau analogų, kurie palaikytų lietuvių kalbą rasti nepavyko.

2. REIKALAVIMŲ SPECIFIKACIJA

2. 1 Sistemos paskirtis

2. 1. 1 Projekto kūrimo pagrindas

Kiekvieną dieną pasigirsta vis daugiau pranešimų apie tai jog išnaudojant žiniatinklio spragas yra įsilaužiama į sistemas ir pavagiami vartotojų duomenys arba šios spragos išnaudojamos kitiems tikslams. Didelėse sistemose tai greičiau pastebima, o mažose turinčiose keliasdešimt vartotojų per dieną, galima išnaudoti pažeidžiamumą ilgą laiką ir taip niekams nežinant kenkti tinklapio lankytojams. Yra sukurta ne vienas įrankis žiniatinklio testavimui, tačiau daugelis jų testuoja tik po vieną pažeidžiamumą, netestuoja įvedamų duomenų teisingumo ir nėra nei vieno įrankio lietuvių kalba.

2. 1. 2 Sistemos tikslai (paskirtis)

Sukurti sistemą testuojančią žiniatinklio įvedimo laukelius ar per juos galima įsilaužti į žiniatinklį ir ar galima įvesti neteisingą informaciją.

2. 2 Projekto dalyviai

2. 2. 1 Užsakovas

Simona Ramanauskaitė, Informacinių technologijų katedros lektorė. Šiaulių universitetas, Technologijos fakultetas, Adresas: Vilniaus g. 141-301, LT-76353 Šiauliai.

2. 2. 2 Vykdytojas

Šiaulių Universiteto, informatikos inžinerijos, V-to kurso studentas: Mindaugas Jadenkus.

2. 3 Vartotojai

3 lentelė. Vartotojo „Testuotojas“ detalizavimas

Vartotojo kategorija	**Testuotojas**
Vartotojo sprendžiami uždaviniai	Nurodyti testuojamą žiniatinklį, parinkti testavimo kriterijus
Patirtis dalykinėje srityje	Srities specialistas
Patirtis informacinėse technologijose	Specialistas
Papildomos vartotojo charakteristikos	Nereikia
Apsimokymo poreikis	Nereikia
Amžiaus grupė	16-60

4 lentelė. Vartotojo „Administratorius“ detalizavimas

Vartotojo kategorija	**Administratorius**
Vartotojo sprendžiami uždaviniai	Naujų testavimo kriterijų suvedinėjimas, sistemos funkcionalumo tikrinimas
Patirtis dalykinėje srityje	Srities specialistas
Patirtis informacinėse technologijose	Specialistas
Papildomos vartotojo charakteristikos	Nereikia
Apsimokymo poreikis	Nereikia
Amžiaus grupė	16-60

5 lentelė. Vartotojų prioritetai.

Vartotojo kategorija	**Prioritetas**
Administratorius	Pirmaeilis vartotojas.
Testuotojas	Antraeilis vartotojas

2. 4 Įpareigojantys apribojimai

2. 4. 1 Apribojimai sprendimui

Sistema veiks kaip žiniatinklis kuriame bus galima testuoti kitus žiniatinklius.

2. 4. 2 Diegimo aplinka

Norint, kad sistema veiktų reikės:

1. Tinklo serverio: IIS (6.0 arba naujesnis), Apache (2.2.14 arba naujesnis)
2. PHP (5.2 arba naujesnis) su įjungtu cURL moduliu;
3. MySQL duomenų bazė (5.1.41 arba naujesnė).

2. 4. 3 Bendradarbiaujančios sistemos

Sistemos naudojimuisi bus reikalinga interneto naršyklė: Microsoft Internet Explorer (8.0 arba naujesnė), Mozilla Firefox (3 arba naujesnė), Google Chrome (7.0 arba naujesnė), Opera (10 arba naujesnė).

2. 4. 4 Numatoma darbo vietos aplinka

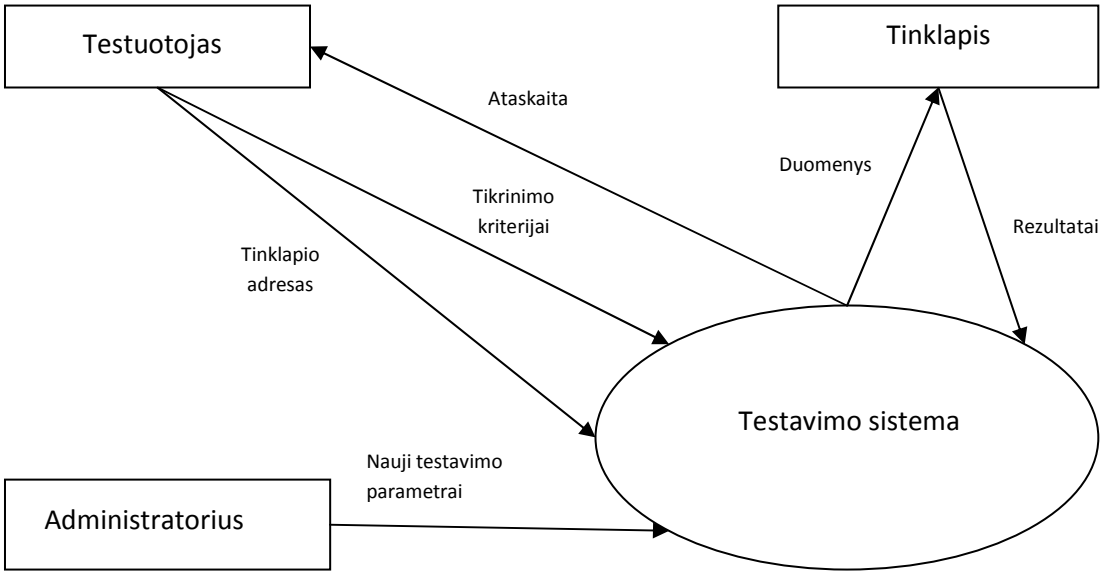
Kompiuterizuota darbo vieta su grafine interneto naršykle, jei sistema ar testuojamas tinklapis yra ne tame pačiame kompiuteryje tada reikalingas vietinio tinklo ar interneto ryšys.

2. 4. 5 Sistemos kūrimo terminai

6 lentelė. Kūrimo terminai

Eil. Nr.	Užduotis	Terminas	Pastabos
1	Reikalavimų specifikacijos rengimas	2011-03-10	Informacija derinama su užsakovu.
2	Architektūros specifikacija	2011-04-30	
3	Sistemos kūrimas	2011-05-07	
4	Sistemos testavimas	2011-05-15	Testavimas ir rastų klaidų taisymas
5	Sistemos pristatymas	2011-06-01	Galutinis pristatymas

2. 5 Veiklos kontekstas



9 pav. *Veiklos konteksto diagrama*

2. 5. 1 Veiklos padalinimas

7 lentelė. Veiklos padalinimas

Eil. Nr.	Įvykio pavadinimas	Įeinantys/išeinantys srautai
1.	Testuotojas įveda duomenis	Duomenų suvedimas (in)
2.	Testuotojas gauna ataskaitą	Ataskaita (out)
3.	Administratorius įveda naujus testavimo parametrus	Parametrų įvedimas (in)

2. 6 Produkto veiklos sfera

2. 6. 1 Sistemos ribos

10 pav. *Sistemos vartotojai ir funkcijų tarpusavio priklausomybės*

2. 6. 2 Panaudos atvejų sąrašas

8 lentelė. Panaudojimo atvejo „Nurodyti tinklapio adresą“ detalizavimas

Pavadinimas	Nurodyti tinklapio adresą	Numeris	1
Aprašymas	Testuotojas įveda testuojamo tinklapio adresą		
Aktorius	Testuotojas		
Prieš sąlyga	Atsidaryti programą		
Vykdymo sąlyga	Testuotojas patvirtina įvestą tinklapio adresą		
Po sąlyga	Ekrane parodo tinklapyje esamus įvedimo laukus		

9 lentelė. Panaudojimo atvejo „Pažymėti tikrinamus laukus ir nurodyti jų formatus“ detalizavimas

Pavadinimas	Pažymėti tikrinamus laukus ir nurodyti jų formatus	Numeris	2
Aprašymas	Testuotojas pažymi koriuos įvedimo laukus testuos ir tie kiekvienu iš testavimui pažymėtu lauku nurodo jo tipą (vartotojas, slaptažodis, elektroninis paštas, data), o mygtukams automatiškai nurodomas tipas ir jo pakeisti nebegalima		
Aktorius	Testuotojas		
Prieš sąlyga	Patvirtinamas įvestas tinklapio adresas		
Vykdymo sąlyga	Testuotojas patvirtina įvedimo laukus kuriuos testuos		
Po sąlyga	Ekrane parodo testuotojo pasirinkimą		

10 lentelė. Panaudojimo atvejo „Vartotojo vardo formato parinkimas“ detalizavimas

Pavadinimas	Vartotojo vardo formatas	Numeris	2.1
Aprašymas	Testuotojas pažymėtam laukui nurodo vartotojo vardo formatą ir pagal tai testavime bus parenkami atitinkami testiniai atvejai		
Aktorius	Testuotojas		
Prieš sąlyga	Pažymimas testuojamas laukas		
Vykdymo sąlyga	Testuotojas parenka vartotojo vardo formatą		
Po sąlyga	Ekrane rodomas testuotojo pasirinkimą		

11 lentelė. Panaudojimo atvejo „Slaptažodžio formato parinkimas“ detalizavimas

Pavadinimas	Slaptažodžio formatas	Numeris	2.2
Aprašymas	Testuotojas pažymėtam laukui nurodo slaptažodžio formatą ir pagal tai testavime bus parenkami atitinkami testiniai atvejai		
Aktorius	Testuotojas		
Prieš sąlyga	Pažymimas testuojamas laukas		
Vykdymo sąlyga	Testuotojas parenka lauko slaptažodžio formatą		
Po sąlyga	Ekrane rodomas testuotojo pasirinkimą		

12 lentelė. Panaudojimo atvejo „El. pašto formato parinkimas“ detalizavimas

Pavadinimas	El. pašto formatas	Numeris	2.3
Aprašymas	Testuotojas pažymėtam laukui nurodo el. pašto formatą ir pagal tai testavime bus parenkami atitinkami testiniai atvejai		
Aktorius	Testuotojas		
Prieš sąlyga	Pažymimas testuojamas laukas		
Vykdymo sąlyga	Testuotojas parenka lauko el. pašto formatą		
Po sąlyga	Ekrane rodomas testuotojo pasirinkimą		

13 lentelė. Panaudojimo atvejo „Netikrinamo formato aprinkimas“ detalizavimas

Pavadinimas	Netikrinamas formatas	Numeris	2.4
Aprašymas	Testuotojas pažymėtam laukui nurodo, kad netikrinti formato		
Aktorius	Testuotojas		
Prieš sąlyga	Pažymimas testuojamas laukas		
Vykdymo sąlyga	Testuotojas parenka, kad nereikia netikrinti formato		
Po sąlyga	Ekrane rodomas testuotojo pasirinkimą		

14 lentelė. Panaudojimo atvejo „Parinkti saugumo tikrinimo kriterijus“ detalizavimas

Pavadinimas	Parinkti saugumo tikrinimo kriterijus	Numeris	3
Aprašymas	Testuotojas pažymi kokiems laukams kokios saugumo spragos bus testuojamos		
Aktorius	Testuotojas		
Prieš sąlyga	Patvirtinamas įvestas tinklapio adresas		
Vykdymo sąlyga	Testuotojas parenka kokias saugumo spragas testuos		
Po sąlyga	Ekrane rodomas testuotojo pasirinkimas		

15 lentelė. Panaudojimo atvejo „SQL įterpimas“ detalizavimas

Pavadinimas	SQL įterpimas	Numeris	3.1
Aprašymas	Pažymėjus lauką testo metu bus bandoma galimybė įterpti SQL užklausą, o kokios būtent SQL užklausos bus bandomos įterpti turi būti aprašyta administratoriaus		
Aktorius	Testuotojas		
Prieš sąlyga	Patvirtinti kokie laukai bus testuojami ir kokie jų formatai		
Vykdymo sąlyga	Testuotojas turi pažymėti SQL injekcija		
Po sąlyga	Ekrane rodomas testuotojo pasirinkimą		

16 lentelė. Panaudojimo atvejo „HTML įterpimas“ detalizavimas

Pavadinimas	HTML įterpimas	Numeris	3.2
Aprašymas	Pažymėjus lauką testo metu bus bandoma galimybė įterpti HTML kodą, o kokį būtent HTLM kodą bus bandomos įterpti turi būti aprašyta administratoriaus		
Aktorius	Testuotojas		
Prieš sąlyga	Patvirtinti kokie laukai bus testuojami ir kokie jų formatai		
Vykdymo sąlyga	Testuotojas turi pažymėti HTML kodo įterpimą		
Po sąlyga	Ekrane rodomas testuotojo pasirinkimą		

17 lentelė. Panaudojimo atvejo „JavaScript įterpimas“ detalizavimas

Pavadinimas	*JavaScript* įterpimas	Numeris	3.3
Aprašymas	Pažymėjus lauką testo metu bus bandoma galimybė įterpti *JavaScript,* , o kokį būtent *JavaScript* kodą bus bandomos įterpti turi būti aprašyta administratoriaus		
Aktorius	Testuotojas		
Prieš sąlyga	Patvirtinti kokie laukai bus testuojami ir kokie jų formatai		
Vykdymo sąlyga	Testuotojas turi pažymėti *JavaScript* įterpimą		
Po sąlyga	Ekrane rodomas testuotojo pasirinkimą		

18 lentelė. Panaudojimo atvejo „UTF-7 koduotė“ detalizavimas

Pavadinimas	*UTF-7* koduotė	Numeris	3.4
Aprašymas	Pažymėjus lauką testo metu bus bandoma galimybė įterpti UTF-7 kodą , o kokį būtent *UTF-7* kodą bus bandomos įterpti turi būti aprašyta administratoriaus		
Aktorius	Testuotojas		
Prieš sąlyga	Patvirtinti kokie laukai bus testuojami ir kokie jų formatai		
Vykdymo sąlyga	Testuotojas turi pažymėti *UTF-7* koduotės įterpimą		
Po sąlyga	Ekrane rodomas testuotojo pasirinkimą		

19 lentelė. Panaudojimo atvejo „Vykdyti tinklapio tikrinimą“ detalizavimas

Pavadinimas	Vykdyti tinklapio tikrinimą	Numeris	4
Aprašymas	Testuotojas paspaudžia tikrinimo mygtuką		
Aktorius	Testuotojas		
Prieš sąlyga	Turi būti patvirtinti įvedimo laukai, jų formatai ir saugumo kriterijai.		
Vykdymo sąlyga	Testuotojas patvirtina vykdymą		
Po sąlyga	Ekrane parodo testavimo ataskaitą		

20 lentelė. Panaudojimo atvejo „Peržiūrėti ataskaitą“ detalizavimas

Pavadinimas	Peržiūrėti ataskaitą	Numeris	5
Aprašymas	Testuotojui pateikiama ataskaita apie rastas tinklapio spragas		
Aktorius	Testuotojas		
Prieš sąlyga	Atliekamas tinklapio testavimas		
Vykdymo sąlyga	Turi būti atliktas testavimas		
Po sąlyga	Galima išsaugoti į failą		

21 lentelė. Panaudojimo atvejo „Peržiūrėti naršyklėje“ detalizavimas

Pavadinimas	Peržiūrėti naršyklėje	Numeris	5.1
Aprašymas	Testuotojas peržiūri ataskaita naršyklėje		
Aktorius	Testuotojas		
Prieš sąlyga	Suformuota ataskaita		
Vykdymo sąlyga	Turi būti atliktas testavimas		
Po sąlyga	Testuotojas peržiūri ataskaita naršyklėje		

22 lentelė. Panaudojimo atvejo „Išsaugoti į failą“ detalizavimas

Pavadinimas	Išsaugoti į failą	Numeris	5.2
Aprašymas	Testuotojas išsaugo ataskaitą į failą		
Aktorius	Testuotojas		
Prieš sąlyga	Suformuota ataskaita		
Vykdymo sąlyga	Testuotojas parenka kur išsaugoti ataskaita		
Po sąlyga	Kompiuteryje išsaugoma ataskaita		

23 lentelė. Panaudojimo atvejo „Naujų duomenų teisingumo testų įvedimas“ detalizavimas

Pavadinimas	Naujų duomenų teisingumo testų įvedimas	Numeris	6
Aprašymas	Administratorius įveda naujus duomenų teisingumo testus		
Aktorius	Administratorius		
Prieš sąlyga	Prisijungti administratoriaus vartotoju		
Vykdymo sąlyga	Administratorius suveda testavimo duomenis		
Po sąlyga	Nauji testai išsaugomi duomenų bazėje		

24 lentelė. Panaudojimo atvejo „Naujų saugumo testų įvedimas“ detalizavimas

Pavadinimas	Naujų saugumo testų įvedimas	Numeris	7
Aprašymas	Administratorius įveda naujus saugumo testus		
Aktorius	Administratorius		
Prieš sąlyga	Prisijungti administratoriaus vartotoju		
Vykdymo sąlyga	Administratorius įveda naujus saugumo testavimo duomenis		
Po sąlyga	Nauji testai išsaugomi duomenų bazėje		

2. 7 Funkciniai reikalavimai

25 lentelė. Funkcinio reikalavimo „Žiniatinklio nuskaitymas“ detalizavimas

Reikalavimas #:	**1**	**Reikalavimo tipas:**	**9**	**Panaudojimo atvejis #:**	**1**
Aprašymas:	Nuskaitomi žiniatinklio įvedimo laukai				
Pagrindimas:	Norint parinkti testavimo kriterijus reikia nuskaityti įvedimo laukus				
Šaltinis:	Užsakovas				
Tikimo kriterijus:	Testuotojui parodomi rasti įvedimo laukai				
Užsakovo tenkinimas:	5	**Užsakovo netenkinimas:**			5
Priklausomybės:		**Konfliktai:**	Nėra		

26 lentelė. Funkcinio reikalavimo „Testavimo kriterijų parinkimas“ detalizavimas

Reikalavimas #:	**2**	**Reikalavimo tipas:**	**9**	**Panaudojimo atvejis #:**	**2**
Aprašymas:	Galimybė parinkti testavimo kriterijus				
Pagrindimas:	Atlikti testavimui reikalingi testavimo parametrai				
Šaltinis:	Užsakovas				
Tikimo kriterijus:	Galima pasirinkti testuojamus laukus ir nurodyti kokius duomenis į jį galima įvest.				
Užsakovo tenkinimas:	5	**Užsakovo netenkinimas:**			5
Priklausomybės:	1	**Konfliktai:**	Nėra		

27 lentelė. Funkcinio reikalavimo „Saugumo testavimo kriterijų parinkimas“ detalizavimas

Reikalavimas #:	**3**	**Reikalavimo tipas:**	**9**	**Panaudojimo atvejis #:**	**3**
Aprašymas:	Galimybė parinkti įvedimo laukų saugumo tikrinimo kriterijus				
Pagrindimas:	Testuotojui turi būti galimybė patikrinti tinklapį nuo dažniausiai aptinkamų spragų				
Šaltinis:	Užsakovas				
Tikimo kriterijus:	Testuotojas pasirenka norimus kriterijus atitinkamiems laukams, ir pagal tai testavimo metu yra parenkami etatiniai atvejai				
Užsakovo tenkinimas:	5	**Užsakovo netenkinimas:**			5
Priklausomybės:	1	**Konfliktai:**		Nėra	

28 lentelė. Funkcinio reikalavimo „Žiniatinklio testavimas“ detalizavimas

Reikalavimas #:	**4**	**Reikalavimo tipas:**	**9**	**Panaudojimo atvejis #:**	**4**
Aprašymas:	Pagal parinktus kriterijus atliekamas žiniatinklio testavimas				
Pagrindimas:	Testavimas turi vykti be pertraukų				
Šaltinis:	Užsakovas				
Tikimo kriterijus:	Atliekamas vientisas testavimas, be pertraukų. Testavimo metu kiekvienam pažymėtam laukui vykdomi atitinkami testiniai atvejai, o tuo tarpu likę laukai užpildomi vartotojo nurodytais teisingais duomenimis				
Užsakovo tenkinimas:	3	**Užsakovo netenkinimas:**			3
Priklausomybės:	2, 3	**Konfliktai:**		Nėra	

29 lentelė. Funkcinio reikalavimo „Ataskaitos pateikimas“ detalizavimas

Reikalavimas #:	**5**	**Reikalavimo tipas:**	**9**	**Panaudojimo atvejis #:**	**5**
Aprašymas:	Testavimo ataskaitos pateikimas				
Pagrindimas:	Kad vartotojas žinotų, ką reikia pataisyti tinklapyje jam turi būti pateikta ataskaita				
Šaltinis:	Užsakovas				
Tikimo kriterijus:	Testuotojui baigus tinklapio testavimą parodoma ataskaita, o esant poreikiui ją atsisiųsti el. paštu				
Užsakovo tenkinimas:	4	**Užsakovo netenkinimas:**			4
Priklausomybės:	4	**Konfliktai:**		Nėra	

30 lentelė. Funkcinio reikalavimo „Duomenų teisingumo testų įvedimas“ detalizavimas

Reikalavimas #:	**6**	**Reikalavimo tipas:**	**9**	**Panaudojimo atvejis #:**	**6**
Aprašymas:	Naujų duomenų teisingumo testų įvedimas				
Pagrindimas:	Norint plėsti testavimo sistemą turi būti galimybė ją papildyti naujais testavimo duomenimis				
Šaltinis:	Užsakovas				
Tikimo kriterijus:	Administratorius gali papildyti sistema naujais testavimo duomenimis, kurie vėliau bus naudojami vykdant testavimą				
Užsakovo tenkinimas:	4	**Užsakovo netenkinimas:**			3
Priklausomybės:		**Konfliktai:**		Nėra	

31 lentelė. Funkcinio reikalavimo „Naujų saugumo testų įvedimas“ detalizavimas

Reikalavimas #:	**7**	**Reikalavimo tipas:**	**9**	**Panaudojimo atvejis #:**	**7**
Aprašymas:	Naujų saugumo testų įvedimas				
Pagrindimas:	Norint plėsti testavimo sistemą turi būti galimybė ją papildyti naujais testavimo duomenimis				
Šaltinis:	Užsakovas				
Tikimo kriterijus:	Administratorius gali papildyti sistema naujais testavimo duomenimis, kurie vėliau bus naudojami vykdant testavimą				
Užsakovo tenkinimas:	4	**Užsakovo netenkinimas:**			3
Priklausomybės:		**Konfliktai:**		Nėra	

2. 8 Nefunkciniai reikalavimai

2. 8. 1 Reikalavimai sistemos išvaizdai

32 lentelė. Nefunkcinio reikalavimo „Vartotojo sąsaja“ detalizavimas

Reikalavimas #:	**5**	**Reikalavimo tipas:**	**10**	**Panaudojimo atvejis #:**	
Aprašymas:	Lengvai skaitoma sąsaja				
Pagrindimas:	Patogus mygtukų išdėstymas, lengva suvokti kokie veiksmai bus vykdomi				
Šaltinis:	Užsakovas				
Tikimo kriterijus:	Mygtukų pavadinimai aiškūs, ir naudojama kuo mažiau trumpinių				
Užsakovo tenkinimas:	4	**Užsakovo netenkinimas:**			2
Priklausomybės:			**Konfliktai:**	Nėra	

33 lentelė. Nefunkcinio reikalavimo „Sistemos prieinamumas“ detalizavimas

Reikalavimas #:	**6**	**Reikalavimo tipas:**	**10**	**Panaudojimo atvejis #:**	
Aprašymas:	Prieinamumas, bet kas galima pasinaudoti sistema				
Pagrindimas:	Sistema bus kuriama kaip interneto tinklapis, todėl esant galimybėm galima patalpinti į norimą tinklapį arba kaip tinklapį				
Šaltinis:	Užsakovas				
Tikimo kriterijus:	Sistema pasiekiama *HTTP* protokolu				
Užsakovo tenkinimas:	4	**Užsakovo netenkinimas:**			2
Priklausomybės:			**Konfliktai:**	Nėra	

2. 8. 2 Reikalavimai panaudojamumui

34 lentelė. Nefunkcinio reikalavimo „Sistemos kalba“ detalizavimas

Reikalavimas #:	**7**	**Reikalavimo tipas:**	**11**	**Panaudojimo atvejis #:**	
Aprašymas:	Nacionalinės kalbos panaudojimas				
Pagrindimas:	Panašių sistemų lietuvių kalba sunku rast				
Šaltinis:	Užsakovas				
Tikimo kriterijus:	Sistemoje naudojama tik lietuvių kalba				
Užsakovo tenkinimas:	4	**Užsakovo netenkinimas:**			2
Priklausomybės:			**Konfliktai:**	Nėra	

2. 8. 3 Reikalavimai vykdymo charakteristikoms

35 lentelė. Nefunkcinio reikalavimo „Testavimo trukmė“ detalizavimas

Reikalavimas #:	**8**	**Reikalavimo tipas:**	**12**	**Panaudojimo atvejis #:**	
Aprašymas:	Testavimas turi trukti ne ilgiau 30 minučių				
Pagrindimas:	Panašių sistemų lietuvių kalba sunku rast				
Šaltinis:	Užsakovas				
Tikimo kriterijus:	Testavimas atliekamas greičiau nei per 30 minučių				
Užsakovo tenkinimas:	4	**Užsakovo netenkinimas:**			2
Priklausomybės:			**Konfliktai:**	Nėra	

2. 8. 4 Reikalavimai saugumui

36 lentelė. Nefunkcinio reikalavimo „Konfidencialumas“ detalizavimas

Reikalavimas #:	**8**	**Reikalavimo tipas:**	**15**	**Panaudojimo atvejis #:**	
Aprašymas:	Konfidencialumas – tik testuotojas gali matyti testavimo ataskaitą				
Pagrindimas:	Kad rastomis spragomis nepasinaudotų piktavaliai jos neturi matyti treti asmenys				
Šaltinis:	Užsakovas				
Tikimo kriterijus:	Sistema nesaugo ataskaitų				
Užsakovo tenkinimas:	4	**Užsakovo netenkinimas:**			2
Priklausomybės:			**Konfliktai:**	Nėra	

37 lentelė. Nefunkcinio reikalavimo „Patikimumas“ detalizavimas

Reikalavimas #:	**8**	**Reikalavimo tipas:**	**15**	**Panaudojimo atvejis #:**	
Aprašymas:	Patikimumas – sistema nepakenkia puslapio veiklai				
Pagrindimas:	Testavimo metu neturi būti sugadinti jokie duomenys esantys puslapyje				
Šaltinis:	Užsakovas				
Tikimo kriterijus:	Sistema nesugadina duomenų				
Užsakovo tenkinimas:	4	**Užsakovo netenkinimas:**			2
Priklausomybės:			**Konfliktai:**	Nėra	

38 lentelė. Funkcinio reikalavimo „Pasiekiamumas“ detalizavimas

Reikalavimas #:	**8**	**Reikalavimo tipas:**	**11**	**Panaudojimo atvejis #:**	
Aprašymas:	Pasiekiamumas – galimybė pasinaudoti sistema kam tik reikia				
Pagrindimas:	Sistema kuriama kaip tinklapis, todėl ją galima pateikti internete kaip puslapį arba integruoti į esamą tinklapį				
Šaltinis:	Užsakovas				
Tikimo kriterijus:	Sistema veikia kaip tinklapis				
Užsakovo tenkinimas:	3	**Užsakovo netenkinimas:**			3
Priklausomybės:			**Konfliktai:**	Nėra	

2. 9 Atviri klausimai

Kaip realizuoti kad sistema galėtų atlikti pilną testavimą su „*PRIMARY*“ ir „*UNIQUE*“ laukais duomenų bazėje.

Kaip po testavimo iš duomenų bazės išvalyti įrašytus duomenis.

2. 10 Galimos sistemos kūrimo rizikos

39 lentelė. Sistemos kūrimo rizikos

Rizikos faktorius	Tikimybinis įvertinimas
Reikalavimų specifikacijos pasikeitimai realizavimo fazėje	10
Papildomu testų atsiradimas sistemoje	9
Papildomu laukelių formatų atsiradimas sistemoje	8

2. 11 Vartotojo dokumentacija ir apmokymas

Administratorius ir testuotojui reikia žinoti kokios yra saugumo spragos, kaip jos veikia ir perskaityti vartotojo vadovą, kad paprasčiau ir greičiau būtų galima naudotis sistema.

2. 12 Perspektyviniai reikalavimai

Ataskaitos formavimas su *PostgreSQL*, *MsSQL* ir kitomis duomenų bazėmis.

3. SISTEMOS ARCHITEKTŪROS SPECIFIKACIJA

3. 1 Architektūros specifikacijos paskirtis

Supažindinti su kuriamos sistemos veikimu. Pateikti sistemos veikimo principus, bei galimybes. Parengti išsamų architektūrinį aprašymą vartotojui ir veikimo specifikaciją programuotojui. Informuoti apie architektūros tikslus ir apribojimus.

3. 2 Architektūros pateikimas

Architektūra pateikiama penkių tipų diagramomis: veiklos, būsenų, sekų, klasių ir komponentų. Diagramomis siekiame iliustruoti sistemos veikimą, atliekamas funkcijas ir veikimo etapus.

3. 3 Architektūros tikslai ir apribojimai

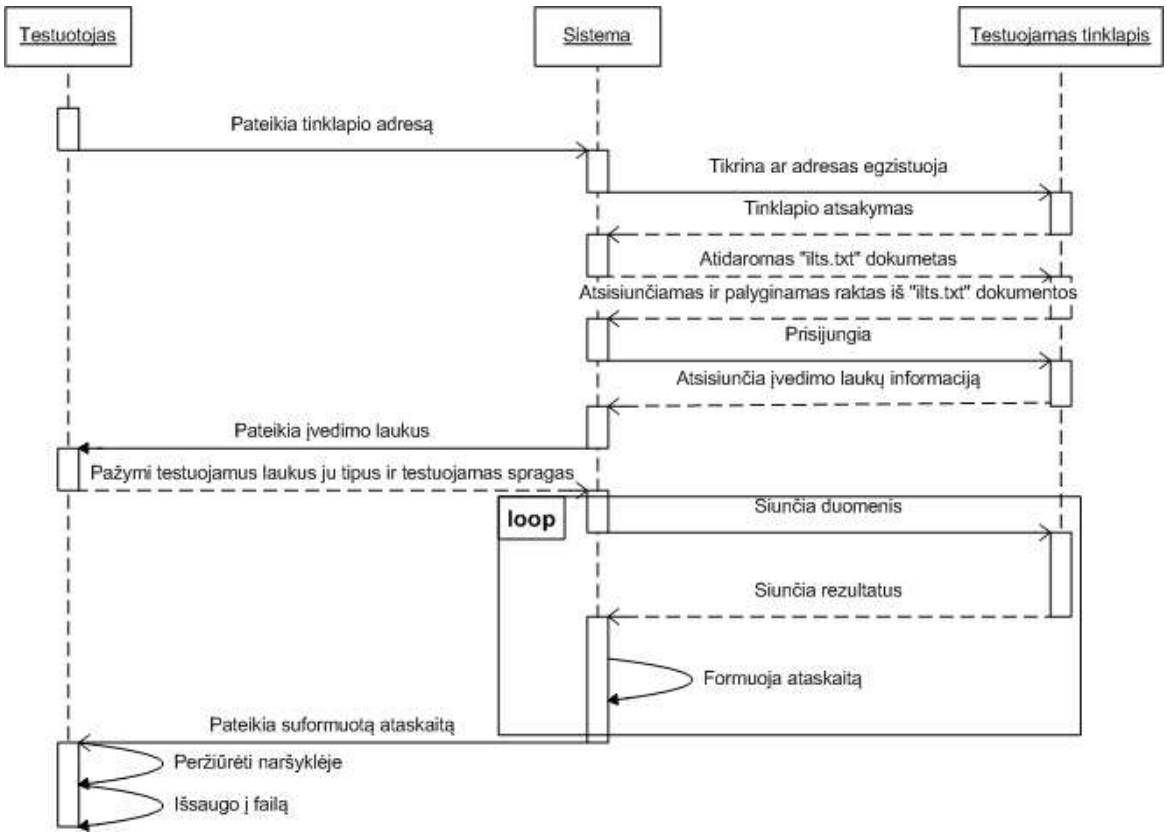
Kuriamo produkto programiniai apribojimai:

- Tinklo serveris (IIS 6.0 arba naujesnis, Apache 2.2.14 arba naujesnis);
- PHP5 su įjungtu cURL moduliu, versija (5.1 arba naujesnė);
- MYSQL duomenų bazė (5.1.41 arba naujesnė);
- Interneto naršyklė (Internet Explorer 8.0 arba naujesnė, Mozilla Firefox 3.6 arba naujesnė, Google Chrome 7.0 arba naujesnė, Opera 10 arba naujesnė).

3. 4 Sistemos dinaminis vaizdas

3. 4. 1 Sistemos pagrindinių komponentų sąveika

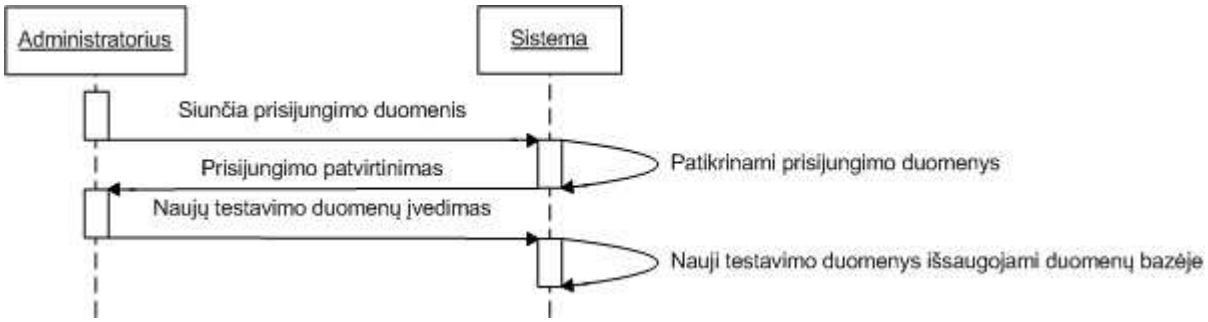
Klientas norinti testuoti tam tikrą tinklapį bendrauja tik su testavimo sistema kuri ir vykdo nurodyto tinklapio testavimą bei testų sėkmės vertinimą (žr. 11 pav.).



11 pav. *Testuotojo sekų diagrama*

11 pav. diagramoje matyti, kad testuotojas pirmiausia nurodo testuojamo tinklapio adresą, sistema patiktina ar tinklapis egzistuoja ir palygina sistemos raktą su „ilts.txt“ dokumente esančiu, tada nuskaito formas su įvedimo laukais ir pateikia testuotojui. Testuotojas parenka tikrinimo kriterijus ir sistema pagal nurodytus kriterijus atlieka testavimą, po testavimo suformuoja ataskaitą ir pateikia testuotojui naršyklėje, ataskaita galima išsisaugoti į failą.

Administratorius norėdamas keisti sistemos parametrus pirma turi prisijungti (žr. 12 pav.)

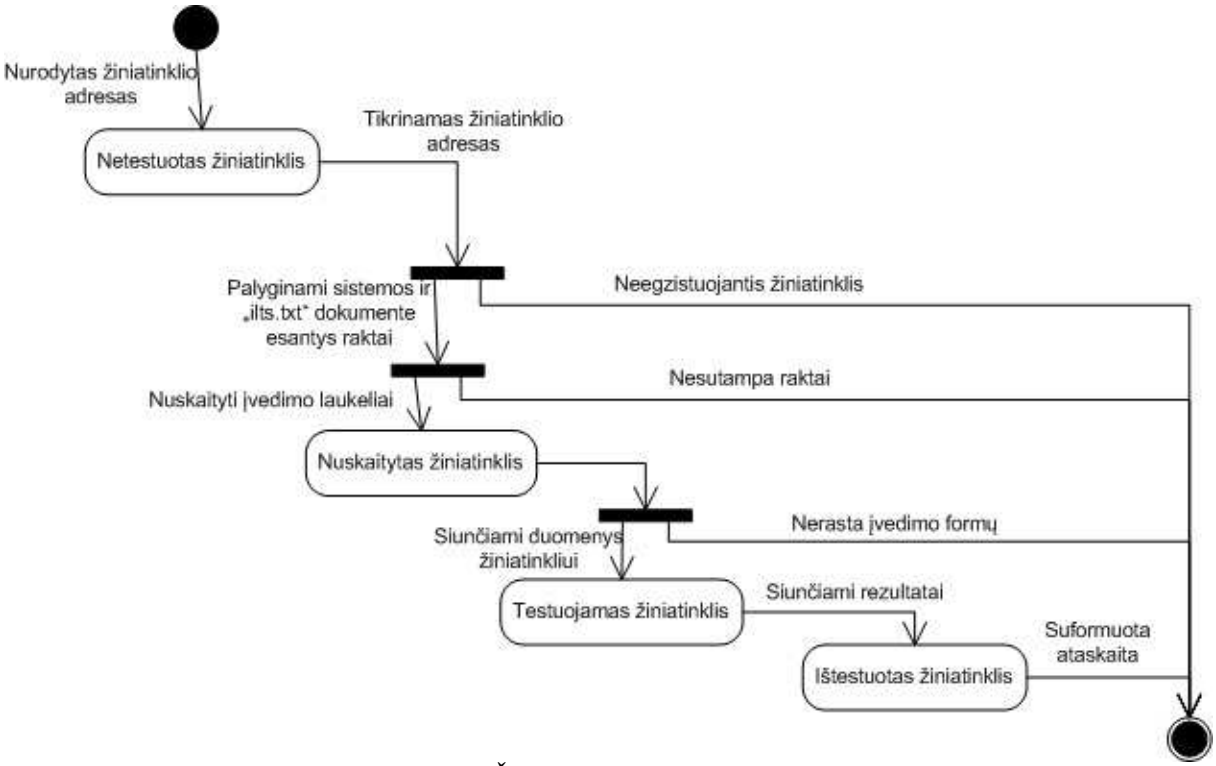


12 pav. *Administratorius sekų diagrama*

Jei sistema patvirtina prisijungimą administratorius gali keisti sistemos testavimo duomenis, o sistema pakeitimus išsaugoja duomenų bazėje.

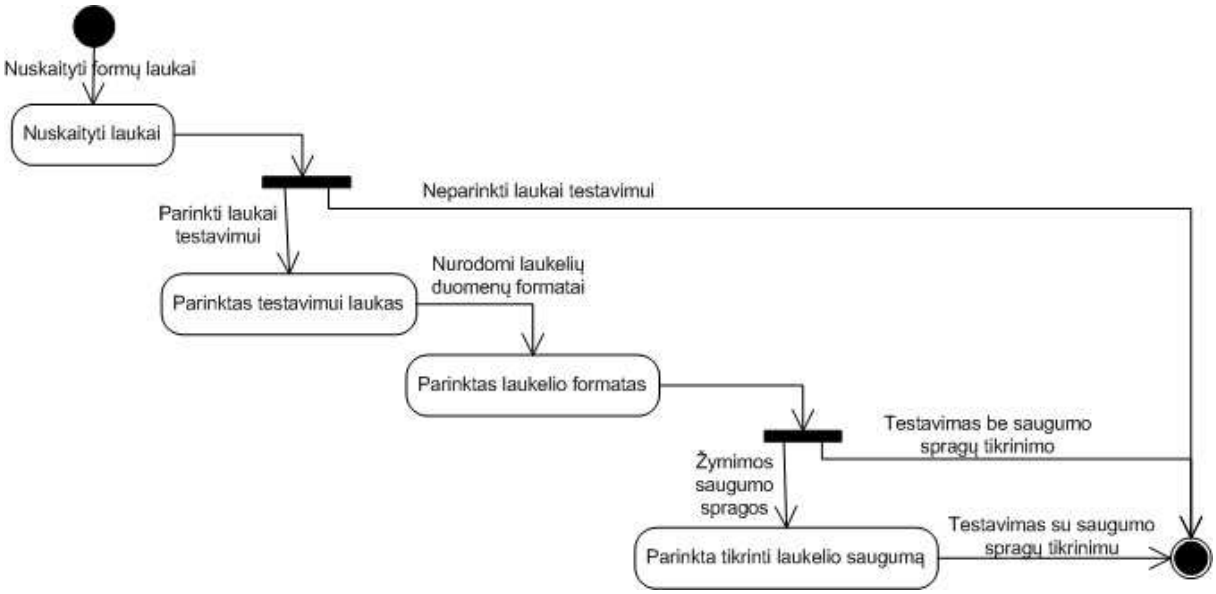
3. 4. 2 Sistemos pereinamos būsenos

Analizuojant testuojamą žiniatinklį kaip atskirą objektą Testavimo metu jis pereina keletą galimų būsenų (žr. 13 pav.). Nurodžius tinklapio adresą yra patikrinama ar svetainė egzistuoja ir ar sutampa sistemoje esantis raktas su „ilts.txt“ dokumente testuojamoje sistemoje. Nuskaičius žiniatinklį patikrinama ar rasta bent viena įvedimo forma. Jei žiniatinklis egzistuoja, sutampa raktai ir yra bent viena įvedimo forma atliekamas testavimas ir pateikiama ataskaita.



13 pav. *Žiniatinklio būsenos diagrama*

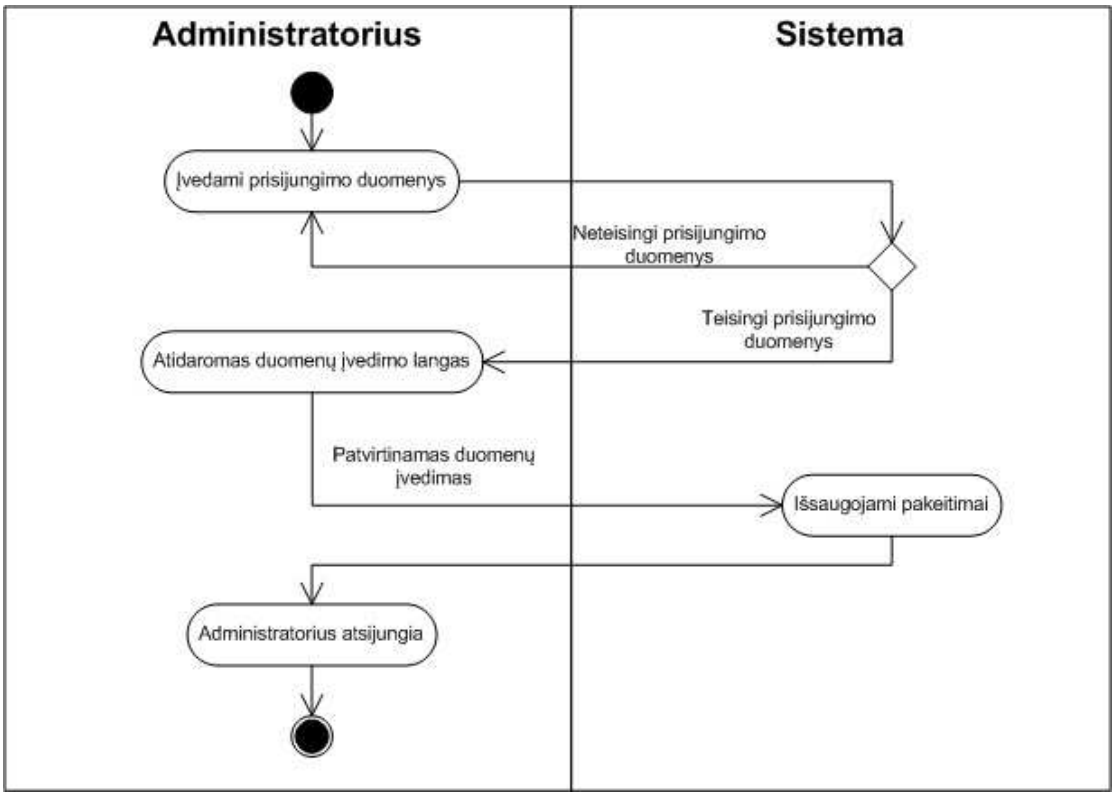
Viename žiniatinklyje gali būti keletas testuojamų įvedimo laukų. Testavimo metu pirma patikrinama ar svetainė turi įvedimo laukelių, jei turi tada reikia nurodyti laukelio formatą, ir atlikti testavimą arba dar galima nurodyti, kad testuotų saugumo spragas ir tada atlikti testavimą (žr. 14 pav.).



14 pav. *Įvedimo laukelio būsenos diagrama*

3. 4. 3 Darbo sistemoje eiga

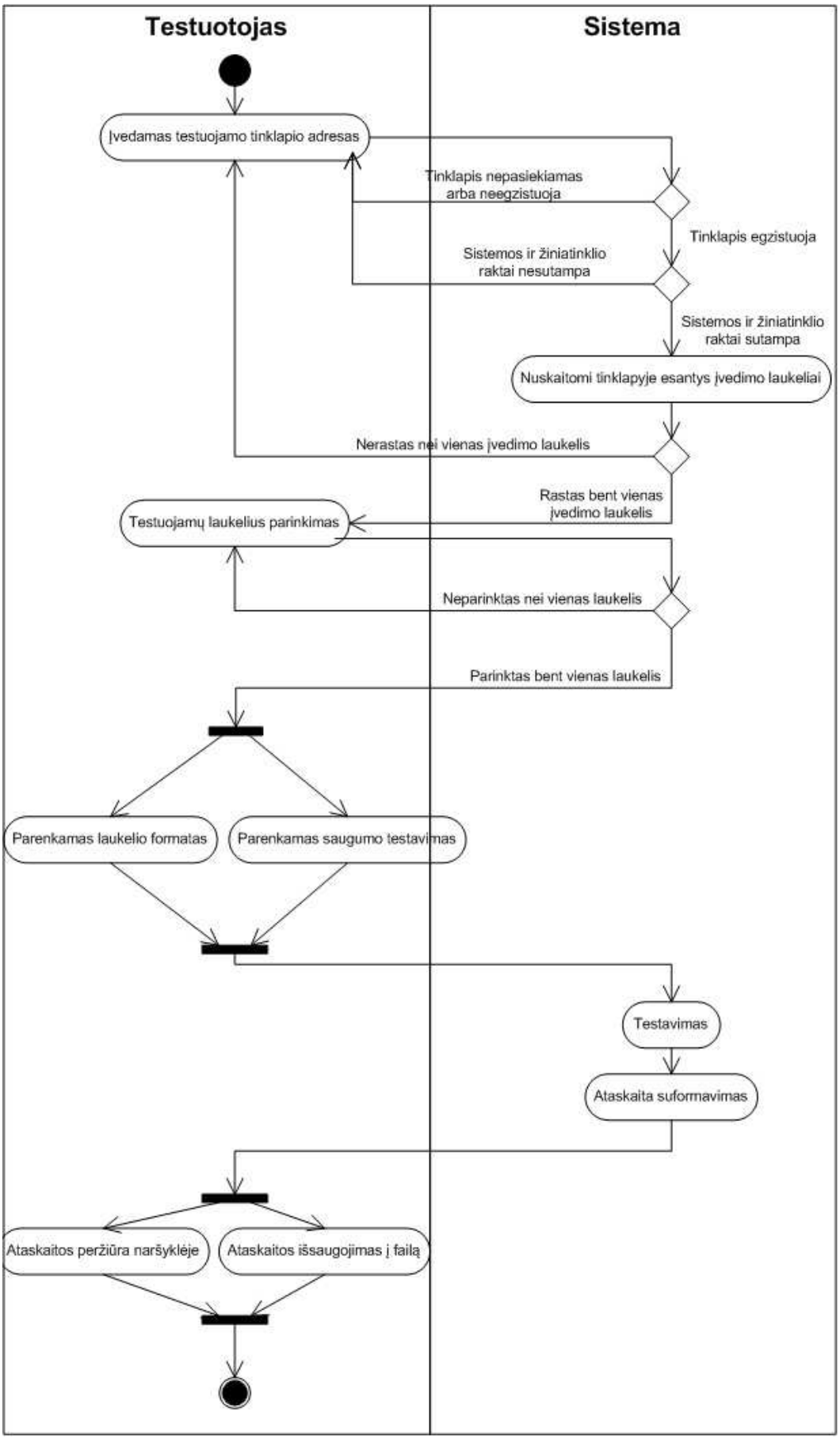
Administratorius pirmiausia turi prisijungti. Prisijungus gali keisti testavimo duomenis ir juos išsaugoti. Baigęs darbą atsijungia (žr.15 pav.).



15 pav. *Administratoriaus ir sistemos veiklos diagrama*

Apibendrinant bendrą testavimo eigą vykdoma atitinkama veiksmų seka testuotojas turi nurodyti testuojamo tinklapio adresą kuriame būtų įvedimo laukų, tada sistema patikrina ar sutampa

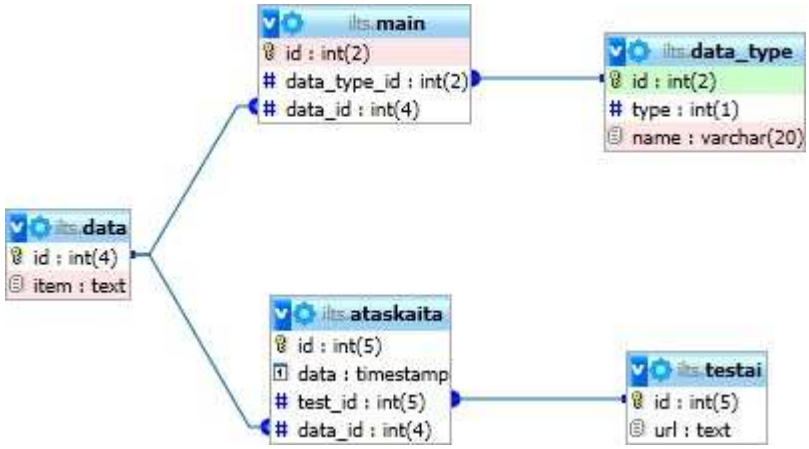
sistemos raktas su nurodytu „ilts.txt“ dokumente. Jei raktai sutampa leidžiama nurodyti testavimo kriterijus rastiems įvedimo laukams po to atliekamas testavimas ir peržiūrima ataskaitą (žr. 16 pav.).



16 pav. *Testuotojo ir sistemos veiklos diagrama*

3. 5 Duomenų vaizdas

Sistemos testiniai atvejai, ir testavo rezultatai saugojami duomenų bazėje. Joje saugomi skirtingo tipo saugumo testai ir jų testavimo atvejai ir įvykdytų testavimų rezultatai (žr. 17 pav.).



17 pav. *Duomenų bazės loginis vaizdas*

3. 5. 1 Lentelių detalizavimas

40 lentelė. Lentelės „main“ detalizavimas

Pavadinimas	main
Aprašymas	Jungia data_type ir data lenteles.
Struktūra	id – identifikatorius data_type_id – duomenų tipo identifikatorius data_id – duomenų identifikatorius
Apribojimai	id: int(2) data_type_id: int(2) data_id: int(4)
Sąsaja	data_type.id; data.id.

41 lentelė. Lentelės „data_type“ detalizavimas

Pavadinimas	data_type
Aprašymas	Saugo duomenų tipą pvz.: Vartotojas, sql injection, HTML įterpimas ir pan.
Struktūra	id – identifikatorius type – duomeny tipo kategorija name – duomenų tipo pavadinimas
Apribojimai	id: int(2) type: int(1) name: varchar(20)
Sąsaja	main.data_type_id

42 lentelė. Lentelės „data“ detalizavimas

Pavadinimas	Data
Aprašymas	Saugomi testavimo duomenys
Struktūra	id – identifikatorius item – testavimo duomenys
Apribojimai	id: int(2) item: text
Sąsaja	main.data_id ataskaita.data_id

43 lentelė. Lentelės „ataskaita“ detalizavimas

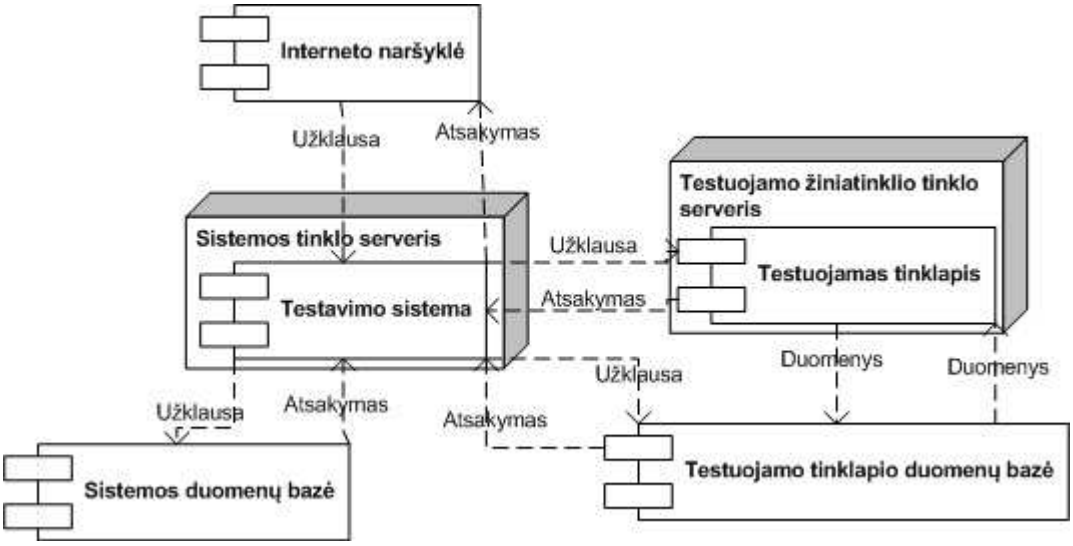
Pavadinimas	Ataskaita
Aprašymas	Jungia testai ir data lenteles.
Struktūra	id – identifikatorius data – testo atlikimo data ir laikas test_id – testo identifikatorius data_id – duomenų identifikatorius
Apribojimai	id: int(5) data: timestamp test_id: int(5) data_id: varchar(4)
Sąsaja	data.id testai.id

44 lentelė. Lentelės „testai“ detalizavimas

Pavadinimas	Testai
Aprašymas	Saugo testuojamos svetaines adresą
Struktūra	id – identifikatorius url – testuojamos svetainės adresas
Apribojimai	id: int(5) url: text
Sąsaja	data.id

3. 6 Sistemos komponentai

Sistemos komponentai ir jų tarpusavio sąveiką (žr. 18 pav.).



18 pav. *Sistemos komponentų tarpusavio sąveika*

Testuotojas interneto naršyklėje atsidaręs testavimo sistemą nurodo testuojamo tinklapio adresą. Testavimo sistema susijungia su testuojamu tinklapiu palygina sistemos rakta su testuojamo žiniatinklio ir nuskaito HTML kodą, tada pagal testuotojo parinktus kriterijus iš duomenų bazės ima duomenis ir siunčia testuojamam tinklapiui. Testuojamas tinklapis duomenis saugo savo duomenų saugykloje, sistema patikrina ar sėkmingai buvo įrašyti duomenys į duomenų bazę ir pagal tai formuoja ataskaitą.

3. 7 Sistemos kokybė

3. 7. 1 Sistemos išplečiamumas.

Administratorius naudodamas savo vartotojo sąsaja gali lengvai papildyti sistemą naujais testavimo duomenimis. Taip plėsdamas testinių atveju gausą ir testavimo išsamumą.

3. 7. 2 Sistemos pernešamumas.

Sistemą galima perkelti į, bet kokią platformą turinčią web serverį, MySQL duomenų bazę ir palaikančią PHP5 (Windows, Linux, FreeBSD ir kt.).

4. TESTAVIMAS

4. 1 Testavimo paskirtis

4. 1. 1 Testavimo tikslai

- Patikrinti ar teisingai nuskaito HTML kodą;
- Ar gerai atliekamas testavimas;
- Ar sistema veikia stabiliai.

4. 1. 2 Testavimo resursai

Klientai	**Serveriai**
Techninė įranga: CPU: Intel P8600, 2.4 GHz, RAM: DDR3, 4GB, 1066MHZ HDD: 500GB, 7200RPM 16MB cache, Interneto ryšys: 80 Mb/s Programinė įranga: OS: Windows 7, Naršyklė: Firefox 4, Internet Explorer 9, Chrome 10	Serveris (http://localhost): Techninė įranga: CPU: Intel P8600, 2.4 GHz, RAM: DDR3, 4GB, 1066MHZ HDD: 500GB, 7200RPM 16MB cache, Interneto ryšys: 80 Mb/s Programinė įranga: OS: Windows 7, Web serveris: Apache 2.2.14 Duomenų bazė: MySQL 5.1.41 PHP 5.3.1
Techninė įranga: CPU: AMD Athlon64, 2.3 GHz, RAM: DDR2, 1GB, 800MHZ HDD: 80GB, 7200RPM 16MB cache, Interneto ryšys: 8 Mb/s Programinė įranga: OS: Windows XP, Naršyklė: Firefox 3.6.17, Internet Explorer 8	Serveris (http://rude.su.lt): Programinė įranga: OS: FreeBSD 8.1, Web serveris: Apache 2.2.17 Duomenų bazė: MySQL 5.1.56 PHP 5.2.17

4. 1. 3 Pagrindiniai apribojimai

Testuojamo žiniatinklio duomenų bazės lentelėse kuriose testavimo sistema įrašo duomenis turi būti nuimti *UNIQUE* ir *PRIMARY* laukai, kitaip nebus atliekamas pilnas duomenų įrašymo testavimas.

Sistema bus naudojama naršyklės pagalba, todėl turi būti suderinama su populiariausiomis naršyklėmis: Microsoft Internet Explorer (8.0 ir naujesnėmis), Mozilla Firefox (3 ir naujesnėmis), Google Chrome (7.0 ir naujesnėmis), Opera (10 ir naujesnėmis).

4. 2 Sistemos funkcijų testavimas

45 lentelė. Žiniatinklio adreso nuskaitymo testavimas

Testo tikslas:		**Įvedimo adreso nuskaitymo testavimas**				
Testo ID	**Reikalavimai/ tikslai**	**Įvykis/įvestis**	**Laukiamas rezultatas**	**Gautas rezultatas**	**T/N**	**Pastabos**
1.	Nustatyti adreso nuskaitymo teisingumą	Adreso su“ http://“ nuskaitymas	Nuskaitomos tinklapio formos	Nuskaitomos tinklapio formos	T	
2.		Adreso be“ http://“ nuskaitymas	Nuskaitomos tinklapio formos	Nuskaitomos tinklapio formos	T	
3.		Neegzistuojančio adreso nuskaitymas	Išvedamas pranešimas apie neegzistuojanti tinklapį	Išvedamas Pranešimas apie neegzistuojanti tinklapį	T	

4.		Neteisingo adreso nuskaitymas	Išvedamas pranešimas apie neegzistuojanti tinklapį	Išvedamas pranešimas apie neegzistuojanti tinklapį	T	
5.		Adreso nuskaitymas nenurodžius formos failo	Išvedamas klaidos pranešimas apie neteisinga adresą	Išvedamas klaidos pranešimas apie neteisinga raktą	N	Funkcio-nalumui netrukdo
6.		Nurodomas teisingas adresas, tačiau skiriasi mažosios ir didžiosios raidės	Nuskaitomos tinklapio formos	Nuskaitomos tinklapio formos	T	

46 lentelė. Formos nuskaitymo testavimas

Testo tikslas:		**Patikrinti formos nuskaitymo teisingumą**				
Testo ID	**Reikalavimai/ tikslai**	**Įvykis/įvestis**	**Laukiamas rezultatas**	**Gautas rezultatas**	**T/N**	**Pastabos**
7.	Formų nuskaitymo teisingumas	Tvarkingos formos nuskaitymas	Nuskaitomos tinklapio formos	Nuskaitomos tinklapio formos	T	
8.		Neužd arytos formos žymės	Nuskaitomos tinklapio formos	Nuskaitomos tinklapio formos	T	
9.		Neuždaryti įvedimo lakų žymės	Nuskaitomos tinklapio formos	Nuskaitomos tinklapio formos	T	
10.		Nėra formos žymių	Išvedamas pranešimas apie formos nebuvimą	Nieko neparodė	N	
11.		Nėra formoje įvedimo laukų	Išveda tuščia forma	Išveda tuščia forma	T	
12.		Formoje naudojama nuo 5 iki 10 įvedimo laukų	Nuskaitomos tinklapio formos	Nuskaitomos tinklapio formos	T	
13.		Formoje naudojama 10 įvedimo laukų ir daugiau	Nuskaitomos tinklapio formos	Nuskaitomos tinklapio formos	T	
14.		Formoje nėra nei vieno patvirtinimo mygtuko	Nuskaitomos tinklapio formos	Nuskaitomos tinklapio formos	T	
15.		Formoje naudojami tik hidden tipo laukai	Nuskaitomos tinklapio formos	Nuskaitomos tinklapio formos	T	

47 lentelė. Įvairiu konfigūracijų formų testavimas

Testo tikslas:		**Testavimo teisingumas**				
Testo ID	**Reikalavimai/ tikslai**	**Įvykis/įvestis**	**Laukiamas rezultatas**	**Gautas rezultatas**	**T/N**	**Pastabos**
16.	Patikrinti testavimą su POST forma	POST formos testavimas	Testavimas matosi duomenų bazėje	Testavimas matosi duomenų bazėje	T	
17.	Patikrinti testavimą su GET forma	GET formos testavimas	Testavimas matosi duomenų bazėje	Testavimas matosi duomenų bazėje	T	

48 lentelė. Testavimo teisingumo įvertinimas

Testo tikslas:		**Testavimo teisingumas**				
Testo ID	**Reikalavimai/ tikslai**	**Įvykis/įvestis**	**Laukiamas rezultatas**	**Gautas rezultatas**	**T/N**	**Pastabos**
18.	Testavimo teisingumas	Testavimas su UNIQUE laukais.	Testavimas matosi duomenų bazėje	UNIUE lauke matosi tik vienas įrašas	N	
19.		Testavimas su įvedimo kaukėmis	Nieko neįrašo į duomenų bazę	Nieko neįrašo į duomenų bazę	T	Filtruojami įvedimo laukai
20.		Su kaukėmis ir vartotojų veiksmų registravimu duomenų bazėje	Testavimas atliekamas tvarkingai	Ataskaitoje pateikiama apie visas sėkmingas atakas, tačiau nebuvo įvykdyta nei viena ataka	N	
21.		Forma nesaugo formos duomenų bazėje	Nieko neįrašo į duomenų bazę	Nieko neįrašo į duomenų bazę	N	Negalima įvertinti formos duomenų įvedimo teisingumo
22.		Testuojamas tinklapis, kuriam duomenų įvedimui būtini atitinkami sesijos kintamieji	Nieko neįrašo į duomenų bazę	Nieko neįrašo į duomenų bazę	N	
23.		Pasirenkant testavimo parametrus nurodomi netinkami teisingi prisijungimo duomenys	Nieko neįrašo į duomenų bazę	Nieko neįrašo į duomenų bazę	T	
24.	Patikrinti testavimą su forma, kada patvirtinimui reikalingas mygtuko paspaudimas	Pažymėtas mygtukas	Testavimas atliekamas	Testavimas atliekamas tvarkingai	T	
25.		Nepažymėtas mygtukas	Testavimas nevykdomas	Testavimas atliekamas, bet neranda nė vienos spragos	T	
26.	Patikrinti testavimą su forma, kada patvirtinimui nereikalingas mygtuko paspaudimas	Pažymėtas mygtukas	Testavimas atliekamas	Testavimas atliekamas tvarkingai	T	
27.		Nepažymėtas mygtukas	Testavimas atliekamas	Testavimas atliekamas tvarkingai	T	

4. 3 Sistemos charakteristikų testavimas

4. 3. 1 Našumo testavimas

49 lentelė. Žiniatinklio nuskaitymo greičio testavimas

Testo tikslas:		**Sistemos sparta**				
Testo ID	**Reikalavimai/ tikslai**	**Įvykis/įvestis**	**Laukiamas rezultatas**	**Gautas rezultatas**	**T/N**	**Pastabos**
28.	Žiniatinklio nuskaitymo sparta	Nuskaitymas mažai teksto ir 4 įvedimo laukai	10s	0.74s	T	
29.		Daug testo 6 formos su 70 laukų nuskaitymas	10s	1.52s	T	
30.		Nuskaitymas mažai teksto ir 4 įvedimo laukai, kuomet testuojamame tinklapyje yra daug dizaino elementų (paveikslėlių)	10s	0.84s	T	
31.		Daug testo 6 formos su 70 laukų nuskaitymas, kuomet testuojamame tinklapyje yra daug dizaino elementų (paveikslėlių)	10s	1.59s	T	
32.		Nuskaitymas mažai teksto ir 4 įvedimo laukai, kuomet testuojamame tinklapyje yra daug papildomos informacijos (teksto)	10s	1.34s	T	
33.		Daug testo 6 formos su 70 laukų nuskaitymas, kuomet testuojamame tinklapyje yra daug papildomos informacijos	10s	2.28s	T	
34.	Testavimo sparta	Pilnas dviejų įvedimo laukų testavimas, kuomet panaudota 47 testiniai atvejai	10s	1.961s	T	Testuojama vietiniame serveryje
35.		Pilnas dešimties įvedimo laukų testavimas, kuomet naudojama 940 testinių atvejų	30s	6.245s	T	
36.		Pilnas dvidešimties įvedimo laukų testavimas, kuomet naudojami ~3000 testinių atvejų	1 min	Klaidos pranešimas	N	
37.		Pilnas dviejų įvedimo laukų testavimas, kuomet panaudoti 5 testiniai atvejai	10s	1.161s	T	
38.		Pilnas dešimties įvedimo laukų testavimas, kuomet naudojama 25 testinių atvejų	20s	3.045s	T	
39.		Pilnas dvidešimties įvedimo laukų testavimas, kuomet naudojami 100	20s	4.34s	T	

40.		Pilnas dviejų įvedimo laukų testavimas, kuomet panaudota 47 testiniai atvejai	10s	4.19s	T	Testuojama nutolusiame serveryje (interneto greitis ~50Mbps)
41.		Pilnas dešimties įvedimo laukų testavimas, kuomet naudojama 940 testinių atvejų	20s	9.25s	T	
42.		Pilnas dvidešimties įvedimo laukų testavimas, kuomet naudojami ~3000 testinių atvejų	1 min	Klaidos pranešimas	N	
43.		Pilnas dviejų įvedimo laukų testavimas, kuomet panaudoti 5 testiniai atvejai	10s	2.21s	T	
44.		Pilnas dešimties įvedimo laukų testavimas, kuomet naudojama 25 testinių atvejų	20s	7.48s	T	
45.		Pilnas dvidešimties įvedimo laukų testavimas, kuomet naudojami 100	20s	6.34s	T	

4. 3. 2 Suderinamumo testavimas

50 lentelė. Naršyklių suderinamumo testavimas

Testo tikslas:		**Tinklapio atvaizdavimas**				
Testo ID	**Reikalavimai/ tikslai**	**Įvykis/įvestis**	**Laukiamas rezultatas**	**Gautas rezultatas**	**T/N**	**Pastabos**
46.	Taisyklingas tinklapio atvaizdavimas	Firefox 4	Taisyklingai atvaizduojamas tinklapis	Taisyklingai atvaizduojamas tinklapis	T	
47.		Internet Explorer 8	Taisyklingai atvaizduojamas tinklapis	Taisyklingai atvaizduojamas tinklapis	T	
48.		Chrome 10	Taisyklingai atvaizduojamas tinklapis	Taisyklingai atvaizduojamas tinklapis	T	
49.		Internet Explorer 9	Taisyklingai atvaizduojamas tinklapis	Taisyklingai atvaizduojamas tinklapis	T	

4. 3. 3 Saugumo testavimas

51 lentelė. Atsparumo SQL įterpimo atakoms testavimas

Testo tikslas:		**Sistemos saugumas**				
Testo ID	**Reikalavimai/ tikslai**	**Įvykis/įvestis**	**Laukiamas rezultatas**	**Gautas rezultatas**	**T/N**	**Pastabos**
50.	Įsilaužimas į kitas sistemas	Testavimas	Negalima pakenkti svetimoms svetainėms	Negalima pakenkti svetimoms svetainėms	T	
51.	Galimybė, bet kam pasinaudoti sistema	Svetainės atsivėrimas	Gali, bet kas pasinaudoti sistema	Gali, bet kas pasinaudoti sistema	T	

4. 4 Testavimo išvados

Atlikus testavimą su nagrinėtomis analogiškomis programomis, buvo pastebėtas sukurtos sistemos pranašumas. Kadangi testuojamas žiniatinklis neišvedinėja tinkamų klaidų pranešimų, nei vienas analogas nerado, nei vienos spragos, nors ir yra pažeidžiamas visoms atakoms. Kadangi ši sistema įrašinėja duomenis į testuojamą sistemą testavimo rezultatai yra užtikrinti.

Sistema veikia teisingai, tačiau pastebėti keli trūkumai kurie sistemos funkcionalumui didelės įtakos neturi.

5. VARTOTOJO DOKUMENTACIJA

5. 1 Vartotojo vadovo paskirtis

Vartotojo vadovas skirtas supažindinti tinklapio testuotoją ir administratorius su sistema. Tinkamai testavimo kriterijus parinkti, kad būtų atlinktas žiniatinklio testavimas testuotojui ir sistemos testavimo duomenų pildymas administratoriui.

5. 2 Sistemos funkcinis aprašymas

Sistema turi kelias funkcijas:

- HTML kodo nuskaitymas;
- Žiniatinklio įvedimo laukų testavimą;
- Ataskaitos formavimas.

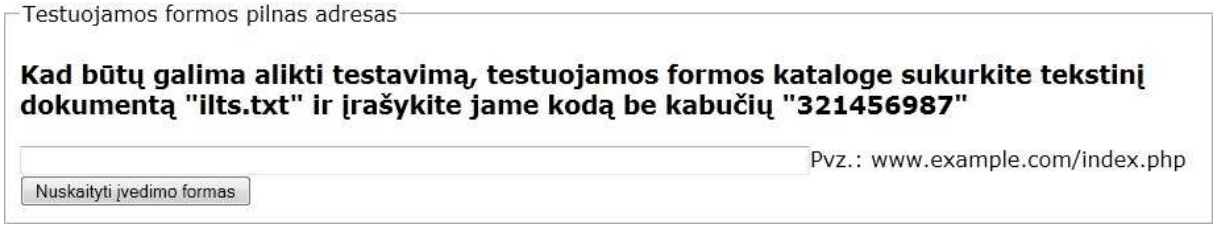
5. 3 Sistemos vartotojo vadovas

5. 3. 1 Verta žinoti

Testavimo sistema į duomenų bazę įrašo duomenis ir norint juos pašalinti tai reikia padaryt pačiam, todėl prieš testavimą geriau pasidaryti duomenų bazės kopija ir po testavimo duomenų bazę įkelti iš atsarginės kopijos, taip bus lengviau matyti kokie duomenys ir kur buvo įrašyti ir nebus sugadinti duomenys.

5. 3. 2 Adreso įvedimas

Jei įvedant adresą nėra prierašo "http://" sistema automatiškai prirašys. Būtina nurodyti pilną adresą į testuojamą formą, pavyzdžiui jeigu jūsų domenas yra „example.com“, testuojama forma yra kataloge „test“, o byla kurioje yra testuojama forma index.php, tai testavimo adresas bus „example.com/test/index.php“ (žr. 19 pav.).



19 pav. *Adreso įvedimas*

5. 3. 3 Rakto įkėlimas į svetainę

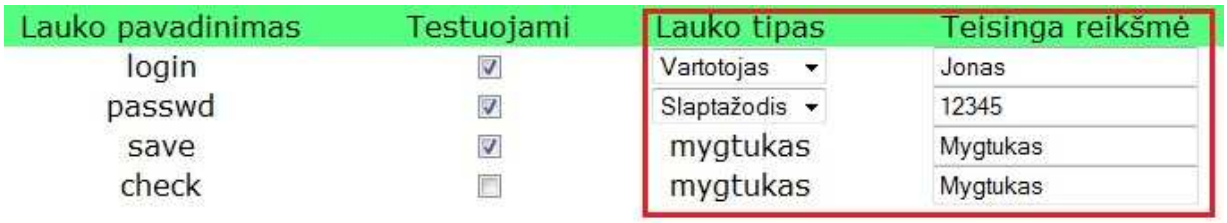
Kad įrodytumėte jog žiniatinklis priklauso būtent jums reikia į testuojamos formos katalogą įkelti tekstinį dokumentą „ilts.txt“ (be kabučių) ir jame įrašyti 9 skaitmenų raktą esanti virš adreso įvedimo laukelio (žr. 19 pav.). Pavyzdžiui jeigu jūsų domenas yra „example.com“, testuojama forma yra kataloge „test“, tai adresas iki „ilts.txt“ bus „example.com/test/ilts.txt“

5. 3. 4 Laukelių žymėjimas

20 pav. *Laukelių žymėjimas*

Žymint laukelius testavimui reikia būtinai pažymėti visus laukeliu kurie yra būtini duomenų įvedimui ir pagal poreikį nebūtinus laukelius. Pavyzdžiui jei būtina registracijai įvesti ir Vartotojo vardą ir slaptažodį, tada reikia žymėti abu laukelius kaip paveikslėlyje esančiame aukščiau. Tačiau jei duomenų įvedimui patvirtinti yra būtinas ir mygtuko paspaudimas, tada vien laukelių nepakanka (žr. 21 pav.).

5. 3. 5 Laukelių formatų ir teisingos reikšmės parinkimas



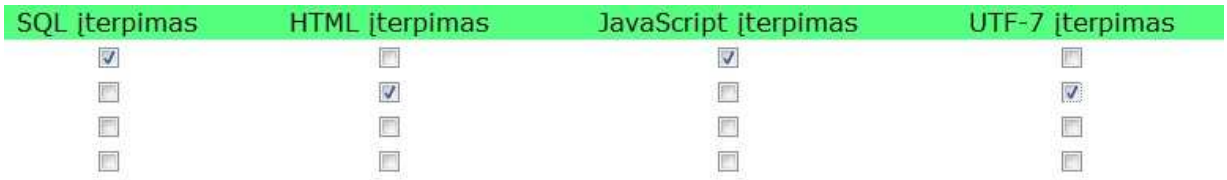
21 pav. *Formatų ir reikšmių nurodymas*

Laukelio formatą reikia parinkti pagal į tą laukelį įvedamus duomenis, jei tai vartotojo vardas tada "Vartotojas", jei data tada "Data" ir t.t. Jei nėra tokio formato kokio jums reikia, tada reikia parinkti "Netestuoti" ir tas laukelis nebus testuojamas neteisingais duomenimis

Teisinga reikšmę reikia įrašyti tokia, kad jei yra duomenų teisingumą tikrinanti funkcija pvz.: "preg_match", ji neturi blokuoti įvestos teisingos reikšmės Pavyzdžiui jei vartotojo vardas turi prasidėti didžiąja raide ir gali būti tik raidės tada, teisinga reikšme galima įrašyti "Vardenis"

5. 3. 6 Saugumo testavimo parinkimas

Jei norite patikrinti tinklapį dėl saugumo spragų, tada sužymėkite kokiam laukeliui kokias spragas norite tikrinti. Jei pas jus turi būti galimybė įvesti *JavaScript* ar *HTML* kodą tada galite nežymėti kad nereiktų po to be reikalo valyti duomenų bazės (žr. 22 pav.).



22 pav. *Saugumo spragų žymėjimas*

5. 3. 7 Ataskaitos formavimas

Jei jūsų žiniatinklis naudoja *MySQL* duomenų bazę, suvedus *MySQL* duomenų bazės prisijungimo duomenis jums bus suformuota ataskaita kokie duomenys buvo įrašyti į duomenų bazę.

Virš testavo mygtuko yra forma skirta suvesti duomenis prisijungti prie jūsų testuojamo duomenų bazės, prisijungimo duomenys nebus saugomi jie tik bus naudojami testavimo metu (žr. 23 pav.).

23 pav. *Ataskaitos formavimas su MySQL duomenų baze*

5. 3. 8 Testavimas

Pažymėjus visus testavimo kriterijus reikia paspausti mygtuką esantį po visų formų. Jei testavimas atliktas sėkmingai naršyklėje turėtų pasirodyti užrašas "Testavimas baigtas", jeigu nurodėte teisingus prisijungimo duomenis prie jūsų duomenų bazės po užrašu „Testavimas baigtas“ turi būti nuoroda į ataskaitos failą.

5. 4 Sistemos administravimo vadovas

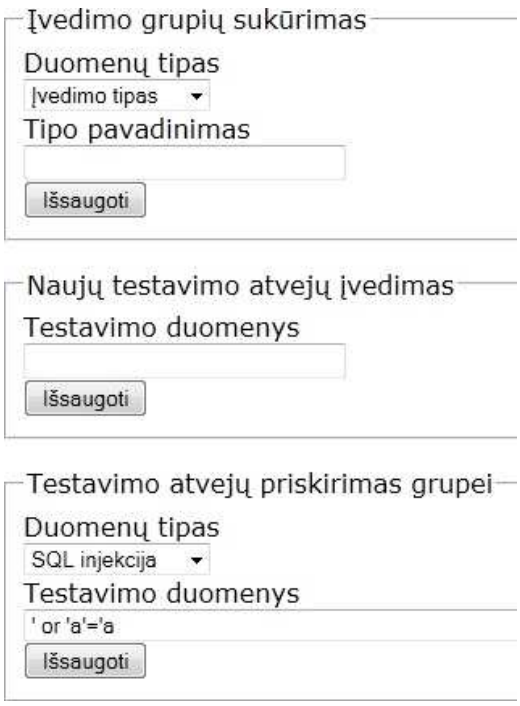
5. 4. 1 Prisijungimas

Sistemos administratorius norėdamas prisijungti turi atsidaręs sistemą paspausti viršuje esančią nuorodą „Administratoriui“ ir įvesti prisijungimo vardą „admin“ ir slaptažodį „laikinas“ (žr. 24 pav.).

24 pav. *Kairėje prisijungimo nuoroda, dešinėje prisijungimo forma*

5. 4. 2 Duomenų pildymas

Prisijungus yra rodomos trys formos. Pirma „Įvedimo grupių sukūrimas“ yra skirta sukurti naujoms duomenų grupės skirtoms testuoti ar galima neteisingiems įvedamiems duomenims testuoti. Įvedus naują saugumo testavimo grupę testavimo sistemoje jokių naujovių neatsiras. Antra forma „Naujų testavimo atvejų įvedimas“ čia galima įrašyti bet koki naują testavimo atvejį, o trečiojoje „Testavimo atvejų priskirimas grupei“ lentelėje reikia susieti įvestą duomenų tipą su įvestais testavimo duomenimis (žr. 25 pav.).



25 pav. *Duomenų pildymo formos*

5. 4. 3 Duomenų šalinimas

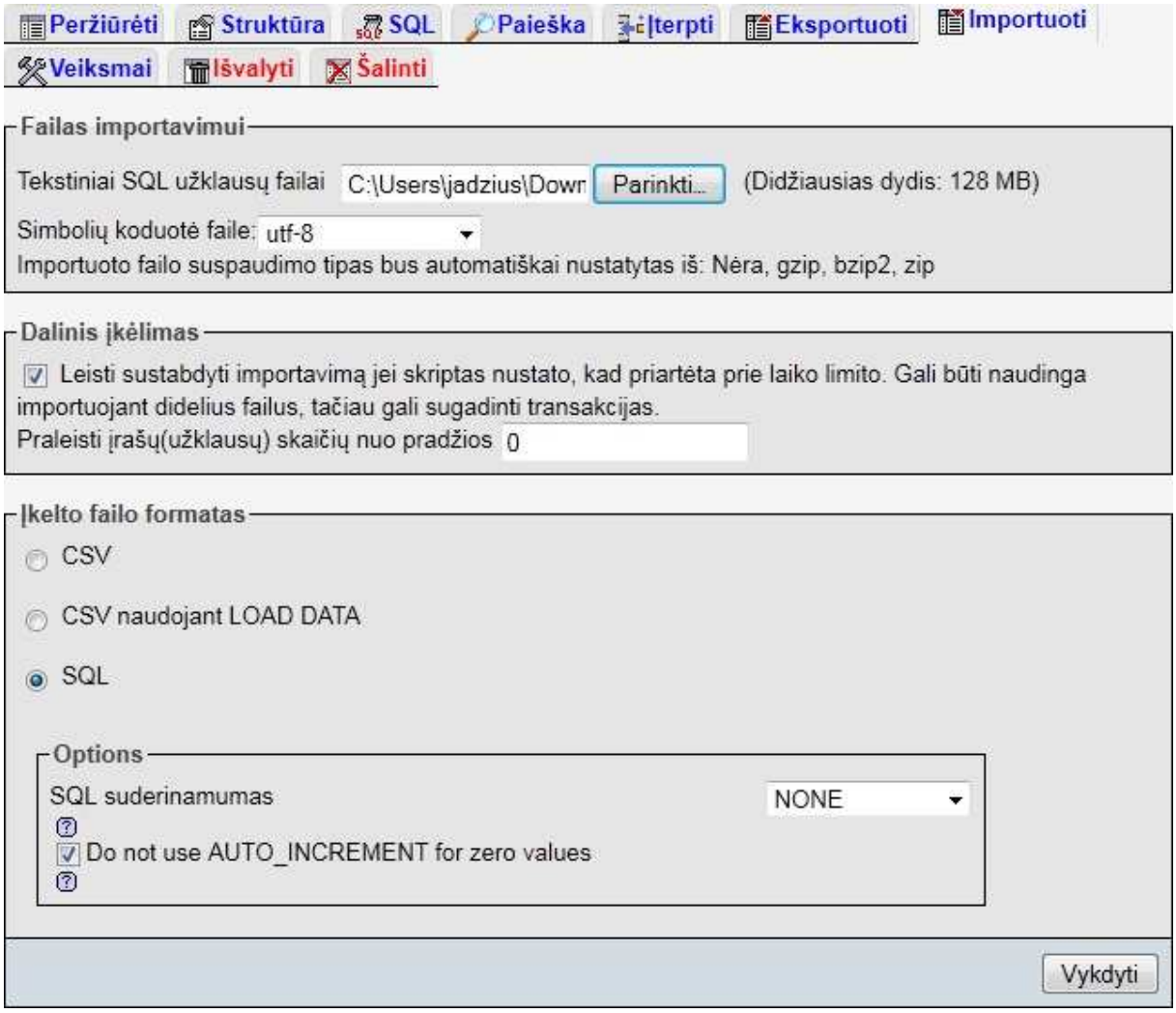
Norint pašalinti duomenis iš testavimo reikia šalia norimų pašalinti testavimo duomenų paspausti nuorodą „Šalinti“ (žr. 26 pav.)

Nr.	Tipas	Įrašas	
1	SQL injekcija	' or 'a'='a	Šalinti
2	SQL injekcija	1 OR 1=1	Šalinti
3	SQL injekcija	1=1	Šalinti
4	SQL injekcija	1 UNI/**/ON SELECT ALL FROM WHERE	Šalinti
5	SQL injekcija	1 AND 1=1	Šalinti

26 pav. *Duomenų šalinimas*

5. 5 Sistemos diegimo vadovas naudojant XAMPP 1.7.3 programą

1. Iš svetainės http://www.apachefriends.org/en/xampp.html parsisiunčiame reikiamai operacinei sistemai XAMPP programą.
2. Įsidiegiame XAMPP programą į kompiuterį arba USB atmintuką pagal programos kūrėjų instrukcijas ir paleidžiame Apache ir MySQL modulius.
3. Jei XAMPP įsidiegėte į savo kompiuterį tada naršyklėje įrašykite http://localhost/phpmyadmin, prisijungus sukurkite naują duomenų bazę, atsivėrus importuoti kortelę paspauskite „Parinkti...“ nurodykite „ilts.sql“ bylą ir paspauskite „Vykdyti“ (žr. 27 pav.) duomenų bazės įkėlimas baigtas.



27 pav. *„Ilts.sql“ bylos įkėlimas*

4. Nueikite į XAMPP programos kataloge esantį htdocs katalogą čia suskurkite katalogą norimu pavadinimu ir įkelkite sistemos failus. Atsidarykite mysql_conf.php byla ir reikiamose eilutėse surašykite prisijungimo duomenis prie MySQL duomenų bazės, išsaugokite pakeitimus ir uždarykite bylą.
5. Grįžkite į XAMPP programos katalogą ir eikite į PHP katalogą, čia atsidarykite „php.ini“ bylą ir raskite eilutę kurioje butu parašyta „extension=php_curl.dll“ jeigu prieš šia eilutę yra kabliataškis jį nutrinkite ir tada išsaugoję pakeitimus uždarykite „php.ini“ bylą ir iš naujo paleiskite Apache servisą.
6. Dabar galite atsidaryti naršyklėje sistemą adresu http://localhost/JUSU_KATALOGO_PAVADINMAS. Prisijungti prie administratoriaus adresu http://localhost/JUSU_KATALOGO_PAVADINMAS/admin.php, vartotojo vardas: „admin“, slaptažodis „laikinas“

IŠVADOS

Išanalizavus žiniatinklių saugumui galimas grėsmes ir jų vykdymo būdus pastebima, kad jų įvykdymas nereikalauja ypatingo pasiruošimo ir resursų, tačiau sukeliama žala sistemoms gali būti pakankamai didelė. Kadangi šiuo metu ši problema gan aktuali, o egzistuojantys įrankiai neatitinka Lietuvos rinkos poreikių, galime teigti, kad lietuviškos ir paprastai valdomos žiniatinklio įvedimo formų saugumo tikrinimo sistemos poreikis yra, ir jos atsiradimas galėtų paskatinti labiau susirūpinti saugumu asmenis, kuriančius net ir paprastas žiniatinklio tipo sistemas.

Reikalavimų specifikacija buvo paruošta remiantis tokio tipo sistemoms būtinomis funkcijomis ir vartotojo darbą galinčiais palengvinti veiksniais, o pagal surinktus ir aprašytus reikalavimus paruošta išsami architektūros specifikacija. Kadangi šios specifikacijos naudoja *UML* diagramas ir detalius jų aprašymus, tad norint suvokti sistemos veikimą ar jos realizavimo principus, parengtos specifikacijos turėtų būti suprantamos tiek informatikos inžinerijos specialistui, tiek ir mažai su tuo susipažinusiems.

Sukurta sistema kuria galima testuoti žiniatinklio duomenų įvedimo saugumą ir teisingumą. Sistema veikia taip pat kaip ir įsilaužimo atveju bandoma į žiniatinklio įvedimo laukus užpildyti testavimo duomenimis. Po testavimo galima peržiūrėti ataskaitą apie duomenis kurie buvo įrašyti duomenų bazėje ir matyti reikiamus svetainės patobulinimus. Sistema galima tobulinti naujais testavimo duomenimis. Sistema atitinka visus jai keltus reikalavimus, tad gali būti naudojama praktikoje kaip papildomas įrankis teik kuriantiems, tiek ir testuojantiems sistemų saugumą asmenims.

Parengti įdiegimo, vartotojo ir administratoriaus vadovai skirti palengvinti sistemos diegimą ir naudojimą.

LITERATŪRA

1. Litnet. HTTP atakos. 2004 m. gruodis. – [žiūrėta 2011-04-20]. Prieiga per internetą: <http://cert.litnet.lt/dokumentai/http_atakos.pdf>.
2. Seccom Labs. SQL Inject Me FAQ. – [žiūrėta 2011-04-20]. Prieiga per internetą: <http://labs.securitycompass.com/index.php/exploit-me/sql-inject-me/sql-inject-me-faq/>.
3. Seccom Labs. XSS ME FAQ. – [žiūrėta 2011-04-20]. Prieiga per internetą: <http://labs.securitycompass.com/index.php/exploit-me/xss-me/xss-me-faq/>.
4. Seccom Labs [interaktyvus]. XSS ME FAQ. – [žiūrėta 2011-04-20]. Prieiga per internetą: <http://labs.securitycompass.com/index.php/exploit-me/xss-me/xss-me-faq/>.
5. MySQL.com compromised. – [žiūrėta 2011-04-20]. Prieiga per internetą: <http://blog.sucuri.net/2011/03/mysql-com-compromised.html>.
6. SQL Injection Attacks by Example. – [žiūrėta 2011-04-20]. Prieiga per internetą: <http://unixwiz.net/techtips/sql-injection.html>.
7. KING. SQL injekcija (išsamiai). – [žiūrėta 2011-04-20]. Prieiga per internetą: <http://www.cyberlords.lt/biblioteka/7693-sql-injekcija-issamiai.html>.
8. Tinklalapių saugumas. – [žiūrėta 2011-04-20]. Prieiga per internetą: <http://www.lescinskas.lt/lt/blog/tag/xss>.
9. „Twitter“ pragraužė interneto kirminas. – [žiūrėta 2011-04-20]. Prieiga per internetą: <http://www.technologijos.lt/n/technologijos/it/S-15000/straipsnis?name=S-15000&l=2&p=1>.
10. Critical Security. Italijoje sukurtas pirmasis CSS/XSS kirminas internetiniam paštui – [žiūrėta 2011-04-20]. Prieiga per internetą: <http://www.technologijos.lt/n/technologijos/it/S-15000/straipsnis?name=S-15000&l=2&p=1>.
11. Exploiting a cross-site scripting vulnerability on Facebook. – [žiūrėta 2011-04-20]. Prieiga per internetą: <http://www.acunetix.com/websitesecurity/xss-facebook.htm>.
12. New highly critical Facebook XSS vulnerabilities pose serious privacy risks – [žiūrėta 2011-04-20]. Prieiga per internetą: <http://www.xssed.com/news/80/New_highly_critical_Facebook_XSS_vulnerabilities_pose_serious_privacy_risks/>.
13. SQL Injection (howto) – [žiūrėta 2011-04-20]. Prieiga per internetą: <http://scripterz.linija.net/v3/index.php?id=katalogas&f=59/>.
14. ZeroDayScan - [žiūrėta 2011-04-20]. Prieiga per internetą: <http://www.zerodayscan.com/>

TERMINŲ IR SANTRUMPŲ ŽODYNĖLIS

Cron Sistemos darbų planavimo įrankis *Unix* tipo operacinėse sistemose.

CSS kalba skirta nusakyti kita struktūrine kalba aprašyto dokumento vaizdavimą, pvz.: *HTML, SVG, XUL*

cURL Biblioteka kuri leidžia prisijungti ir bendrauti tarp skirtingu tipų serverių naudojant daug įvairių protokolų.

Duomenų bazė Organizuotas (susistemintas, metodiškai sutvarkytas) duomenų rinkinys, kuriuo galima individualiai naudotis elektroniniu ar kitu būdu.

Hipertekstas Dokumentas, sudarytas iš tekstų ir piešinių, turi nuorodas arba hipersaitus į kitus dokumentus ar kitas sritis tame pačiame dokumente.

HTML (angl. *Hyper text Markup Language* „Hiperteksto žymėjimo kalba“) – tai kompiuterinė žymėjimo kalba, naudojama pateikti turinį internete.

Interneto Naršyklė (angl. *browser*) - programa, skirta sklaidyti tinklo serverių (angl. web *server*) Pateikiamą informaciją naršant žiniatinklyje, vidiniuose įmonės tinkluose ar savo kompiuteryje.

IRC (angl. *Internet Relay Chat*) arba IRC yra ryšio protokolas ir interneto paslauga, skirti gyvai bendrauti internete.

JavaScript Objektiškai orientuota skriptų programavimo kalba, besiremianti prototipų principu.

PDF (angl. *Portable Document Format*) PDF yra atviro standarto dokumentų formatas skirtas dokumentų apsikeitimui.

PHP Plačiai paplitusi dinaminė interpretuojama programavimo kalba (angl. Hypertext Preprocessor), sukurta 1997 m. ir specialiai pritaikyta interneto svetainių kūrimui.

Single sign-on Prisijungimo kontrolė kai vienu prisijungimu galima patekti į kelias nepriklausomas sistemas.

SQL (angl. *Structured Query Language* - „struktūrizuota užklausų kalba“) – populiariausia iš šiuo metu naudojamų kalbų, skirtų aprašyti duomenis ir manipuliuoti jais reliacinių duomenų bazių valdymo sistemose.

Tinklo serveris Programa naudojama statinio ir dinaminio turinio žiniatinkliams internete.publikuoti.

UML (angl. *Unified Modeling Language* - „*vieninga modeliavimo kalba*“) – modeliavimo ir specifikacijų kūrimo kalba, skirta specifikuoti, atvaizduoti ir konstruoti objektiškai orientuotų programų dokumentus.

Unix Grupė operacinių sistemų, kilusių iš 1969–1970 sukurtos UNICS sistemos, skirtos PDP kompiuteriams. Tarp jų FreeBSD, Mac OS X, Linux ir kitos.

UTF-7 (angl. 7 -bitų Unicode Transformation Format) - kintamo ilgio simbolių koduotė.

VBScript (angl. *Visual Basic Scripting Edition*) tai aktyvių skriptų kalba sukurta Microsoft Visual Basic pagrindu.

xHTML (angl. *eXtensible HyperText Markup Language* – „išplečiama hiperteksto žymėjimo kalba“) yra žymėjimo kalba, kuri turi panašias į *HTML* žymėjimo taisykles, tik jos sintaksė yra griežtesnė.

XSS (angl. *Cross Site Scripting*) - viena iš tinklapių atakų skirta žiniatinklyje įterpti kodą, kuris vėliau pateikiamas kitiems sistemos vartotojams.