KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Vitalius Radzevičius

Žiniatinklio turinio valdymo sistemų saugumo tyrimas

Magistro darbas

Darbo vadovas
dr. Audronė Janavičiūtė

Kaunas, 2012

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Vitalius Radzevičius

Žiniatinklio turinio valdymo sistemų saugumo tyrimas

Magistro darbas

Recenzentas
prof. dr. Lina Nemuraitė
2012-05-28

Vadovas
dr. Audronė Janavičiūtė
2012-05-28

Atliko
IFN-0/3 gr. stud.
Vitalius Radzevičius
2012-05-28

Kaunas, 2012

Turinys

ŽINIATINKLIO TURINIO VALDYMO SISTEMŲ SAUGUMO TYRIMAS

SANTRAUKA

Internete galima rasti nemažai svetainių, kurios yra sukurtos naudojantis viena iš daugelio šiuo metu prieinamų žiniatinklio turinio valdymo sistemų (TVS). TVS paprastai nereikalauja išsamių techninių žinių, jos ir kuriamos su idėja, kad bet kuris naudotojas galėtų nesunkiai sukurti ir paskelbti savo interneto svetainę. Deja, eiliniai TVS naudotojai dažnai turi nedaug žinių informacijos saugumo srityje.

Turinio valdymo sistemų pagrindu sukurtoms svetainėms, kaip ir nuo pagrindų suprogramuotiems tinklalapiams, kyla panašios bendrosios su saugumu susiję grėsmės. Tačiau be bendrųjų grėsmių dar egzistuoja ir specifinės, kurias įprastinės saugumo tikrinimo-vertinimo priemonės sunkiai aptinka. Šios problemos dažnai būna konfigūracijos lygmenyje, todėl iš esmės kiekvienai turinio valdymo sistemai ir jos versijai reikia individualiai pritaikyto saugumo vertinimo taisyklių rinkinio.

Šiame darbe buvo sudarytas specifinių TVS saugumo kriterijų sąrašas, pateiktas šių kriterijų atitikimą vertinančios programos modelis, suprogramuoti du kriterijų vertinimo algoritmai, įvertinantys dviejų populiarių žiniatinklio TVS (Drupal bei Joomla) reikalavimų atitikimą, bei atliktas eksperimentinis tyrimas su minėtomis žiniatinklio turinio valdymo sistemomis. Tyrimas atliktas su ką tik įdiegtomis turinio valdymo sistemomis ir pakartotas po sistemų parametrų konfigūravimo. Taip pat įvertintos dvi internetu prieinamos ir lankomos Drupal TVS pagrindu sukurtos svetainės.

Raktiniai žodžiai: žiniatinklio TVS, saugumo reikalavimai, saugumo tikrinimo programa

WEB CONTENT MANAGEMENT SYSTEMS SECURITY RESEARCH

SUMMARY

There are quite a few websites online that use one of many currently available web content management systems (CMS). CMS usually do not require in-depth technological knowledge. In fact, they are designed with an idea that any user can create and publish their website. Unfortunately, ordinary CMS users often lack knowledge in security area.

CMS-based websites, same as those that are created from scratch, experience similar common security threats. In addition to common security threats, there are some CMS-specific ones that are hardly discovered by standard security assessment programs, generally called web vulnerability scanners. Security problems often lie in configuration level and, in order to discover them, CMS-specific security checking rules are required.

In this paper, CMS-specific security requirements list was compiled and model of the programs that checks if CMS complies with requirements was provided. Then two algorithms were programmed that helped assess how Joomla and Drupal web content management systems comply with security requirements. Experimental study was carried out with two aforementioned content management systems. The study was carried out with the freshly installed content management systems, and then repeated after system configuration parameters adjustment. Finally, two Drupal CMS-based and online-accessible websites were assessed.

Key words: web CMS, security requirements, vulnerability scanner, security assessment program

ĮVADAS

Jau kurį laiką internetas yra neatsiejama daugybės žmonių gyvenimo dalis. Internete galima rasti ne tik dominančios informacijos, tačiau ir apsipirkti, bendrauti, rengti nuotolines konferencijas ir kt. Ne visi paslaugų ar informacijos tiekėjai visą sistemą kuria nuo pat pradžių. Informacijos talpinimui ir valdymui neretai yra pasitelkiamos žiniatinklio turinio sistemos (TVS), palengvinančios administratorių darbą. Nemažai vartotojų naudoja nemokamas TVS [1].

Turinio valdymo sistemos yra naudojamos siekiant supaprastinti žiniatinklio turinio kūrimo, skelbimo ir priežiūros procesus [14][21]. Paprastai jos iš naudotojo nereikalauja išsamių techninių operacinių sistemų ar programavimo kalbų žinių. Kiekvienas svetainės puslapis generuojamas dinamiškai, taip galima tuos pačius duomenis atvaizduoti skirtingais formatais, skirtinguose puslapiuose ir pan. [24]. Rinkoje yra ir komercinių, ir atvirojo kodo žiniatinklio turinio valdymo sistemų, pvz., Joomla, Drupal, Wordpress, CMS Made Simple. Turinio valdymo sistemos pasitelkiamos kuriant tiek paprastas [20], tiek sudėtingas [26] svetaines.

Deja, turinio valdymo sistemos, kaip ir dauguma informacinių sistemų, gali turėti saugumo spragų. Menką patirtį turintiems naudotojams apskritai gali būti sunku susigaudyti žiniatinklio TVS nustatymuose ir valdyme, nekalbant apie saugumo parametrų nagrinėjimą. Piktavaliai apie tai žino, todėl turinio valdymo sistemos gali tapti dažnu taikiniu, siekiant pažeisti informacijos saugumą.

Daugelis žiniatinklio svetainių naudoja turinio valdymo sistemas su numatytaisiais parametrais, įskaitant ir saugumo parametrus. Kitaip sakant, sauga yra vienas iš aspektų, kurį nemaža TVS naudotojų dalis priima kaip garantą [16]. Jei apie saugą apskritai svarstoma, paprastai norima, kad pavyktų išvengti neautorizuotos prieigos prie turinio, jo atsitiktinio redagavimo arba ištrynimo [23]. Tačiau reikia tinkamai apsvarstyti ir kitas sritis.

Žiniatinklio turinio valdymo sistemų pagrindu sukurtiems tinklalapiams iš esmės kyla tos pačios bendrosios saugumo grėsmės ir keliami panašūs saugumo reikalavimai kaip ir tinklalapiams, kurie buvo sukurti nenaudojant TVS. Šiems reikalavimams patikrinti ir galimiems pažeidžiamumams aptikti yra sukurta nemažai tikrinimo programų, apie kurias plačiau rašoma 1-oje darbo dalyje „Žiniatinklio TVS galimų saugumo grėsmių bei jų aptikimo

galimybių analizė“. Tačiau turinio valdymo sistemoms egzistuoja ir specifiniai saugumo reikalavimai, kurių atitikimą esamomis priemonės patikrinti sunku ar iš viso neįmanoma.

Taigi šiame darbe keliamas tikslas yra sudaryti metodiką, įvertinančią TVS specifinių saugumo reikalavimų atitikimą. Darbą galima išskaidyti į tokius uždavinius:

- turinio valdymo sistemų reikalavimų saugai sudarymas;
- saugos vertinimo metodikos sudarymas;
- turinio valdymo sistemų tyrimas pagal sudarytą metodiką.

Turinio valdymo sistemos pirmiausia tiriamos iš karto po diegimo, joms dar veikiant su numatytaisiais parametrais. Po to su saugumu susiję parametrai yra pakoreguojami ir tyrimas atliekamas dar kartą.

Pažeidžiamumų paieškos programų analizės metu išsiaiškinta, kad jos gerai atlieka užduotis, kurioms buvo sukurtos, tačiau negali įvertinti žiniatinklio turinio valdymo sistemų specifinių saugumo reikalavimų, kurie aprašomi 2-oje šio darbo dalyje. Iš esmės taip yra dėl to, kad standartinės pažeidžiamumų tikrinimo priemonės žiniatinklio svetainės saugumo patikrinimą atlieka svetainę skenuodamos per tinklą, o minėtų specifinių saugumo reikalavimų įvertinimas tokiu būdu sunkiai pasiekiamas.

Dėl ką tik paminėtų priežasčių šiame darbe pasiūlytas modelis programos, kuri TVS pagrindu sukurtos svetainės skenavimą atlieka jungdamasi tiesiai prie duomenų bazės ir konfigūracijos failų. Programa užkrauna tikrinimo taisyklių rinkinį nurodytai turinio valdymo sistemai bei jos versijai ir atlieka reikalavimų atitikimo vertinimą.

Eksperimentas atliktas ir metodas patikrintas su dviem populiariomis atvirojo kodo žiniatinklio turinio valdymo sistemomis: Joomla 2.5.x bei Drupal 7.x. Gautų tyrimo rezultatų analizė parodė, jog šios TVS, veikdamos su numatytaisiais parametrais, netenkina didžiosios daugumos specifinių saugumo reikalavimų. Tačiau, atsižvelgus į rekomendacijas ir pakeitus su saugumu susijusių parametrų nustatymus, rezultatai pagerėjo kelis kartus. Eksperimento pabaigoje tyrimą atlikus su dviem Drupal TVS pagrindu sukurtomis žiniatinklio svetainėmis, gauti rezultatai buvo geresni nei visiškai nekonfigūruotų sistemų atveju, tačiau iki idealaus varianto dar gerokai trūko.

Darbo struktūra:

- Pirmojoje darbo dalyje analizuojamos galimos grėsmės TVS saugumui, įvertinant bendrąsias grėsmes bei specifinius galimus pažeidžiamumus. Taip pat

analizuojamos esamos grėsmių aptikimo priemonės, jų naudojimo galimybės, privalumai bei trūkumai.

- Antrojoje dalyje iškeltas darbo tikslas ir uždaviniai, sudarytas TVS specifinių saugumo reikalavimų sąrašas. Pateikiamas saugumo reikalavimų programos veikimo modelis bei panaudojimo atvejų diagrama. Taip pat iškeliami reikalavimai programinei realizacijai.

- Trečiojoje dalyje aprašyta saugumo reikalavimų vertinimo programos realizacija. Nurodyta, kokie reikalingi pradiniai duomenys bei kokie laukiami rezultatai, pateiktas kontrolinis tikrinimo rezultatų pavyzdys. Skyriaus pabaigoje aptartos programos tobulinimo galimybės.

- Ketvirtojoje dalyje pateikiami eksperimento metu gauti rezultatai. Eksperimento metu tikrintos dvi turinio valdymo sistemos iš karto po diegimo bei po papildomos konfigūracijos. Pabaigoje įvertintas dviejų internete veikiančių ir lankomų žiniatinklio svetainių saugumo reikalavimų atitikimas.

1. ŽINIATINKLIO TVS GALIMŲ SAUGUMO GRĖSMIŲ BEI JŲ APTIKIMO GALIMYBIŲ ANALIZĖ

Šiais laikais, kai vis daugiau paslaugų perkeliama į internetą (el. parduotuvės, žemėlapiai, el. bankininkystė, duomenų apsikeitimas tarp skirtingų kompanijų ir kt.), stacionariuose, nešiojamuose ir planšetiniuose kompiuteriuose bei išmaniuosiuose telefonuose esanti naršyklė yra dažnai naudojama programa. Ji pasitelkiama plono kliento architektūroje[1], kai naudojamasi paieškos varikliais, organizacijos tinklalapiais, el. paštu per naršyklę, internetine bankininkyste, tam tikromis verslo programomis ir t. t. Šios programos gali būti prieinamos iš privataus tinklo arba iš interneto, taip pat jos gali reikalauti autorizacijos arba būti viešos. Tačiau bet kuriuo atveju prie jų galima prieiti per naršyklę, naudojančią standartinius protokolus.

Deja, kuriant kai kuriuos esminius standartinius protokolus (TCP/IP, HTTP, FTP), į saugumą nebuvo kreipiamas didelis dėmesys [34]. Todėl, kuriant interneto programas, saugumu turi pasirūpinti programuotojai, tinklalapių talpinimo paslaugų (angl. *hosting*) tiekėjai, tinklalapių administratoriai ir kt. Tačiau dėl prasto programavimo ar netinkamo duomenų išvalymo, taip pat dėl informacijos nutekėjimo ar netinkamai sukonfigūruoto serverio interneto tinklalapiams kyla įvairios grėsmės. Turinio valdymo sistemų atveju grėsmes galima skirstyti į bendrąsias, kurios kyla praktiškai visiems tinklalapiams, bei į specifines, kurios labiau susiję su turinio valdymo sistemomis. Apie tai plačiau aptariama smulkesniuose šio skyriaus poskyriuose.

Informacijos sauga yra kritinis aspektas bet kuriai internetu prieinamai sistemai. Pažeidžiamumai gali sukelti daug įvairių problemų: nuo svetainės turinio sugadinimo iki pavogtų kreditinių kortelių duomenų. Dėl to turinio valdymo sistemose, kaip ir kitose informacinėse sistemose, turėtų būti užtikrinami šie pagrindiniai su saugumu susiję veiksniai: konfidencialumas, vientisumas, autentiškumas, prieinamumas ir neišsiginamumas [13].

Konfidencialumas yra skirtas užtikrinti, kad prie informacijos galės prieiti tik autorizuoti (atitinkamas teises turintys) asmenys.

Vientisumas turi užtikrinti, kad duomenų nemodifikuoja neautorizuoti asmenys.

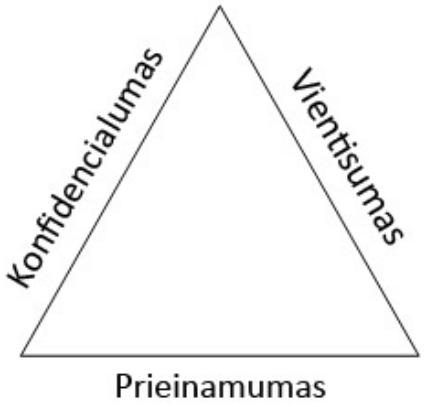
Autentiškumas turi patvirtinti turinio kilmę ir tapatybės tikrumą.

[1] Plonas klientas (angl. *thin client*) - kompiuteris ar kompiuterinė programa, kuri stipriai priklauso nuo kito kompiuterio (serverio), kai norima per klientą atlikti kokias nors operacijas

Prieinamumas skirtas užtikrinti, kad informacija visada bus prieinama autorizuotiems naudotojams.

Neišsiginamumo faktorius turi užtikrinti, kad atlikto veiksmo autorius to veiksmo nebegalės paneigti.

Konfidencialumas, vientisumas ir prieinamumas sudaro informacijos saugumo trikampį (1 pav.).



1 pav. Informacijos saugumo trikampis

Jei į sistemos saugumą neatsižvelgiama viso jos kūrimo metu, tai vėliau sistema paprastai turės daugiau saugumo spragų, jai nuolat reikės leisti pataisymus naujai atrastoms klaidoms ištaisyti.

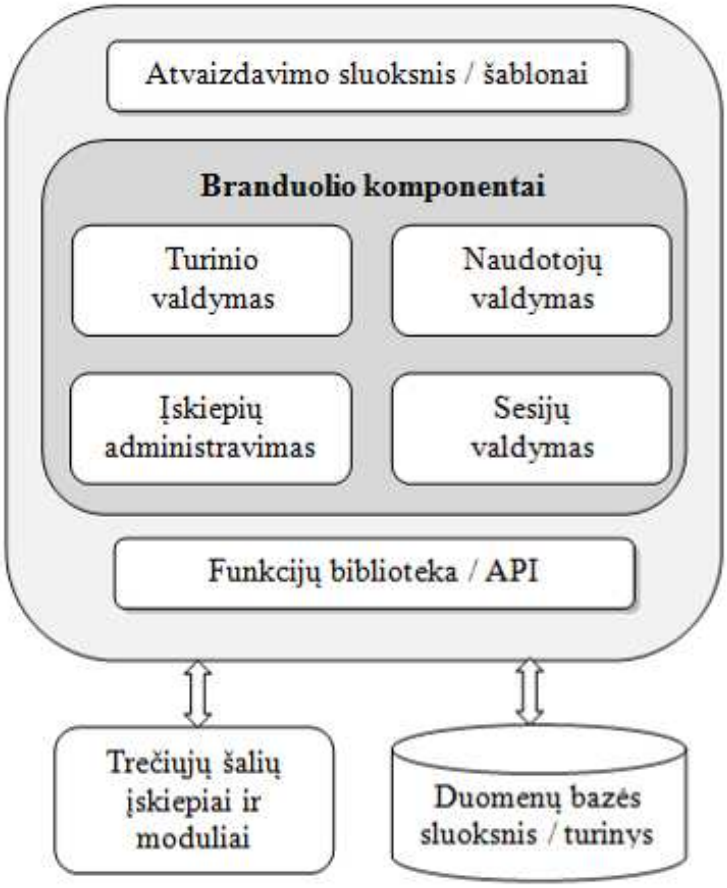
Programinės įrangos saugumo pažeidžiamumai yra vienoje ar kitoje projekto gyvavimo stadijoje palikti trūkumai. Pvz., tai gali būti klaidų apdorojimo problemos arba neteisingas teisių ir prieigos valdymas. Klaidos ir trūkumai sukelia rizikas, kurias galima apibūdinti kaip tikimybę, kad klaida ar trūkumas turės neigiamo poveikio programinės įrangos veikimui: rizika = tikimybė x poveikis. Programinės įrangos trūkumai gali egzistuoti ilgą laiką, kol juos aptiks įsilaužėliai.

1.1. Pagrindiniai TVS komponentai

TVS iš esmės sudaro svetainės lankytojams matoma dalis bei administravimo dalis.

Eiliniai svetainės lankytojais paprastai negali redaguoti turinio. Žinoma, jie gali atlikti tam tikrus paprastus veiksmus, pvz., prie straipsnių rašyti komentarus (jei šie įjungti be būtinybės registruotis), tačiau pagrindinio turinio keitimui reikia turėti aukštesnes teises.

TVS struktūrą panagrinėjus atidžiau, paprastai galima pastebėti, jog ji sudaryta iš keturių pagrindinių komponentų: atvaizdavimo sluoksnio, branduolio komponentų rinkinio, funkcijų bibliotekos ir duomenų bazės sluoksnio (2 pav.).



2 pav. Pagrindiniai TVS komponentai [14]

Atvaizdavimo sluoksnis. Kaip galima spręsti iš pavadinimo, šis sluoksnis lankytojui pateikia svetainės išvaizdą ir turinį. Paprastai turinio valdymo sistemose yra naudojami šablonai, palengvinantys dizaino procesą. Be to, pakeitus šabloną, galima nesunkiai atnaujinti svetainės išvaizdą, nepakeičiant pačios veikimo logikos.

*Branduolio komponentai***.** Šie komponentai yra atsakingi už tokias bazines TVS funkcijas kaip turinio, naudotojų ar sesijų valdymas.

*Funkcijų biblioteka / API***.** Šioje bibliotekoje esančios funkcijos atlieka įvairias užduotis, pvz., kreipiasi į duomenų bazę. Tuo tarpu programavimo sąsaja (angl. *Application Programming Interface*) leidžia TVS bendrauti su trečiųjų šalių programomis ar įskiepiais.

*Duomenų bazės sluoksnis***.** Duomenų bazėje paprastai saugomas visas turinys (išskyrus, paveikslėlius ar kitus failus, nors ir juos galima saugoti duomenų bazėje): informacija apie naudotojus, straipsniai, komentarai ir t.t. Konfigūracija arba dalis jos taip pat gali būti saugoma duomenų bazėje.

Vienas iš pagrindinių TVS privalumų ir tai, kad jų funkcionalumą galima lengvai praplėsti: TVS kūrėjai paskelbia jų API, o trečiųjų šalių programinės įrangos plėtotojai turinio valdymo sistemoms kuria įskiepius, modulius ar kitus priedus.

Trečiųjų šalių moduliai ir įskiepiai dažnai gali turėti ir turi pilną administratoriaus lygio priėjimą prie svetainės turinio ir duomenų, tokių kaip svetainės konfigūracija, naudotojų duomenys, slaptažodžiai ir pan. Turinio valdymo sistemos administratoriams leidžia lengvai įdiegti trečiųjų šalių plėtinius, tačiau daugelio TVS kūrėjai pataria apsaugoti duomenų bazės ir serverio konfigūracijas bei pakeisti slaptažodžius po naujos programinės įrangos įdiegimo.

1.2. Tiriamų turinio valdymo sistemų apžvalga

Norint patikrinti šiame darbe iškeliamus saugumo reikalavimus, eksperimento dalyje tiriamos dvi populiarios [1] žiniatinklio turinio valdymo sistemos Joomla ir Drupal. Toliau pateikiama šiek tiek informacijos apie šias TVS.

1.2.1. Joomla

Joomla pradėta kurti kaip Mambo turinio valdymo sistemos atšaka. TVS didelį dėmesį skiria naudojimo paprastumui, todėl net techninių žinių neturintys naudotojai gali kurti ir redaguoti turinį bei administruoti svetainę. Joomla taip pat pateikia daug papildomų modulių: forumų, pokalbių, kalendorių bei tinklaraščių rašymo įskiepių. Ši TVS lengvai pritaikoma individualiems poreikiams, o jos naudojimas paplitęs nuo smulkių įmonių svetainių iki didelių organizacijų portalų [23].

Be pagrindinės Joomla kūrėjų grupės, kuri atsakinga už bendrą projekto valdymą, dar yra suburtos žmonių komandos, atsakingos už sistemos vertimus į kitas kalbas, dokumentaciją ar saugą.

Joomla forume yra saugai skirta kategorija, kurioje naudotojai diskutuoja apie saugumą bei aprašo atrastus pažeidžiamumus. Šioje kategorijoje taip pat pateikiami patarimai bei aprašymai, kaip padidinti Joomla TVS pagrindu sukurtų svetainių saugumą ir sumažinti rizikas. Saugumo problemos skirstomos į mažo, vidutinio bei aukšto lygio. Saugumo spragos užtaisomos išleidžiant pataisymus (angl. *patches*) arba smulkius TVS leidimus. Didesniuose leidimuose paprastai būna sudėti visi anksčiau išleisti pataisymai.

Joomla pagrindu yra sukurtos JAV Harvardo universiteto ir Jungtinių tautų regioninio informacijos centro svetainės [32].

1.2.2. Drupal

Drupal pradines versijas sukūrė olandų studentai. Iš pradžių jis buvo kuriamas kaip bendradarbiavimo platforma. Šiuo metu Drupal naudoja daugybė privačių kompanijų svetainių bei universitetų portalų. Tai yra populiariausia turinio valdymo sistema po WordPress [1]. Be to, reikėtų pastebėti, jog kylant svetainės sudėtingumui (atsirandant daugiau skirtingų turinio tipų, detalesnio naudotojų valdymo poreikiui), Drupal santykinis naudojimas didėja.

Drupal, kaip ir Joomla, pateikia daug papildomų modulių. Drupal kūrėjai turi atskirą saugumu besirūpinančią komandą. Šios komandos nariai įvertina saugumo pažeidžiamumus, ieško galimų klaidų branduolio komponentuose bei pataria saugumo klausimais trečiųjų šalių modulių kūrėjams. Drupal svetainėje taip pat yra saugumui skirtas skyrius, kuriame kūrėjai pateikia informaciją apie pažeidžiamumus ir jų pataisymus.

Iš žymesnių tinklalapių, naudojančių Drupal, galima paminėti šias: JAV Baltųjų rūmų svetainė, „Popular Science Magazine“ žurnalo bei „New York Observer“ svetainės [33]. Naujoji (2011 m.) ktu.lt interneto svetainė taip pat naudoja Drupal.

1.3. Turinio valdymo sistemų palaikymas saugumo atžvilgiu

Turinio valdymo sistemos traukia įsilaužėlius, nes yra plačiai naudojamos. Be to, žinios apie naujai atrastus pažeidžiamumus greitai sklinda, todėl TVS kūrėjams svarbu greitai sureaguoti į atrastus pažeidžiamumus ir sukurti bei paskelbti jų pataisymus. Kūrėjai turi suteikti TVS naudotojams žinių apie atrastus pažeidžiamumus ir pasiūlyti atsisiųsti ir įdiegti atnaujinimus. Pvz., Drupal TVS yra tam skirtas modulis: jis tikrina įdiegtų modulių versijas bei kreipiasi į išorinį serverį, gaudamas informaciją, ar nėra įdiegtiems moduliams skirtų atnaujinimų. Jei atnaujinimas susijęs su saugumu, administratoriams ir kitiems modulių diegimo teises turintiems nariams kiekviename svetainės lange rodomas pranešimas, kad yra su saugumu susijęs atnaujinimas, kurį būtina įdiegti.

TVS kūrėjai žino apie TVS saugumo problemas, todėl yra subūrę saugumu besirūpinančias komandas, sukūrę interneto forumus bei pateikia saugumo patarimus naudotojams.

Saugumu besirūpinančios bendruomenės taip pat turėtų turėti tinklapius, kuriuose pateikiama informacija apie atrastas klaidas, jų rimtumą bei esamą statusą: atrasta, ištaisyta, neteisingas pranešimas ir pan. Ir Joomla, ir Drupal bendruomenės stengiasi įgyvendinti šiuos reikalavimus:

- *Saugumo pataisymai*. Joomla turi specialus tinklapius ir naujienų grupes, kuriose pateikiama su saugumu susijusi informacija. Kūrėjų komanda kartas nuo karto pertvarko Joomla struktūrą bei kviečia kitais TVS aspektais besirūpinančias komandas padėti pagerinti sistemos saugumą. Drupal turi atskirą saugumu besirūpinančią komandą. Abiejų TVS kūrėjai periodiškai leidžia naujas versijas ir skatina naudotojus visada naudoti naujausią versiją. Atnaujinimai yra svarbūs, nes įsilaužėliai, panaršę pažeidžiamumų istoriją, gali ieškoti pažeidžiamų žiniatinklio svetainių ir sėkmingai prieš jas vykdyti atakas.
- *Pranešimai apie pažeidžiamumus*. Naudotojai gali pranešti apie aptiktus pažeidžiamumus turinio valdymo sistemų svetainėse. Joomla saugumo klausimai aptariami oficialiame forume, o Drupal turi svetainės skyrių, kuriame pateikiami detalūs su saugumu susiję pranešimai bei informacija, kaip pašalinti pažeidžiamumus.
- *Patarimai, kaip padidinti saugumą*. Joomla naudotojai apie saugumą diskutuoja forume, o Drupal komandos nariai pateikia patarimus svetainės saugumo skyriuje.

Galima teigti, kad abiejų šiame darbe tiriamų turinio valdymo sistemų kūrėjai įgyvendina gerąsias saugumo stiprinimo praktikas ir jam skiria adekvatų dėmesį.

1.4. Bendrosios saugumo grėsmės

Kaip minėta, turinio valdymo sistemoms ir jų pagrindu sukurtiems tinklalapiams bei žiniatinklio programoms iš esmės gresia tie patys pavojai kaip ir tinklalapiams, kurie yra sukurti nesinaudojant pagalbinėmis priemonėmis.

Pagrindinės grėsmės yra šios:

- Programavimas tarp tinklalapių (angl. *cross-site scripting* - *XSS*);
- Užklausų klastojimas tarp tinklalapių (angl. *cross-site request forgery* - *CSRF*);
- SQL injekcijos (angl. *SQL injection*);
- HTTP atsakymų skaidymas (angl. *HTTP response splitting*) arba CRLF injekcijos;
- Neautorizuota katalogų peržiūra (angl. *directory traversal*).

Šios grėsmės kyla praktiškai visuose dinaminiuose tinklalapiuose. Pasinaudojant vienu ar keliais aukščiau išvardintais pažeidžiamumais įgyvendinami tokie neteisėti veiksmai:

- HTTP užklausų klastojimas (angl. *spoofed HTTP requests*);
- Sesijos užgrobimas (angl. *session hijacking*);
- Sesijos fiksavimas (angl. *session fixation*);
- Slapukų vogimas;
- Neteisėtas priėjimas prie autorizacijos duomenų ir t. t.

Vieni atakų metodai yra lengviau įgyvendinami, taip pat nuo jų sąlyginai lengviau ir apsiginti (nors tuo ne visada pasinaudoja tinklalapių kūrėjai). Iš tokių paminėtini XSS atakos metodas arba SQL injekcijos. Kiti gali būti palyginti nesunkiai įgyvendinami, tačiau nuo jų apsiginti sudėtingiau. Iš tokių atakų metodų galima paminėti CSRF.

Reikėtų atkreipti dėmesį, kad populiarios TVS yra nuolat tobulinamos, ištaisomos jų žinomos klaidos ir pažeidžiamumai. Tai yra viena iš priežasčių, dėl kurių reikia sekti naudojamos TVS naujienas, parsisiųsti pataisymus ar naujas versijas.

Kartais TVS kūrėjai iš esmės atnaujina turininio valdymo sistemos pagrindą, kas lemia tai, jog kai kurie naudotojai nenori ar negali atnaujinti tuo metu naudojamos TVS versijos. Pvz., jei TVS programinis kodas rašomas PHP programavimo kalba ir pritaikomas naujesnei jos versijai, tačiau svetainės talpinimo paslaugų tiekėjas neatnaujina PHP programinės įrangos savo serveryje, naudotojas negali atnaujinti naudojamos TVS, taip palikdamas galimus pažeidžiamumus.

Panašiai gali būti ir su duomenų bazės, pvz., MySQL, atnaujinimais. Tokiu atveju reikėtų raginti tiekėją atnaujinti programinę įrangą serveryje arba perkelti svetainę kitur. Tai vėlgi sukelia papildomus nepatogumus, dėl kurių naudotojai neretai susitaiko su esama situacija ir palieka savo interneto svetainę pažeidžiamą.

Neseniai sukurtų arba trumpą laiką plėtojamų TVS naudojimas taip pat kelia papildomą riziką. Tikėtina, kad tokios sistemos gali turėti daugiau klaidų ir pažeidžiamumų nei daugelį metų kuriamos sistemos.

Toliau kai kurie galimi pažeidžiamumai aptariami plačiau.

1.4.1. Programavimas tarp tinklalapių

Naudodamas programavimo tarp tinklalapių (angl. *cross-site scripting – XSS*) metodiką, įsilaužėlis išnaudoja naršyklės pasitikėjimą serveriu, naršyklėje įterpdamas kenksmingą

programinį kodą serverio teisėmis [4]. Kad XSS būtų įvykdyta kliento naršyklėje, pakanka, jog veiktų JavaScript, kuris naršyklių nustatymuose paprastai būna įjungtas pagal nutylėjimą. Tokie apsaugos metodai kaip duomenų šifravimas su SSL (angl. *Secure Socket Layer*) neapsaugo nuo XSS atakų. SSL tiesiog užšifruoja kenksmingą kodą kartu su gerąja informacija, kol duomenys keliauja kompiuterių tinklais [5]. Laikoma, kad nuo XSS geriausiai apsaugo geras vartotojo įvedamų duomenų patikrinimas ir išvalymas, tačiau kruopščiai redaguodamas kodą, įsilaužėlis gali sudėlioti jį taip, kad kodas atrodys tinkamas, tačiau iš tikrųjų turės XSS turinį [6][8].

Egzistuoja trys pagrindinai XSS tipai:

1. atkurtasis (angl. *reflected*) arba neišliekantis (angl. *non-persistent*);
2. išsaugotasis (angl. *stored*) arba išliekantis (angl. *persistent*);
3. paremtas dokumento objekto modeliu (angl. *Document Object Model*) [5].

Atkurtojo XSS atveju įsilaužėlis nusiunčia aukai nuorodą į pažeidžiamą tinklalapį, kuriuo vartotojas pasitiki, tačiau nuorodoje būna ir kenksmingo kodo dalis, skirta vartotojo asmeninei informacijai pavogti per slapukus ar atlikti kitokius neteisėtus veiksmus. Vartotojui paspaudus ant nuorodos, naršyklė įvykdo kenksmingą kodą. Šis metodas dažniausiai sėkmingai įvykdomas dėl prasto įvedamų duomenų (tame tarpe, ir URL adresų) apdorojimo.

Išsaugoto XSS atveju serveris įrašo kenksmingą kodą į duomenų bazę ar failą ir vėliau jį atvaizduoja – įvykdo. Šis atakos metodas taip pat dažniausiai įmanomas dėl prasto naudotojo įvedamų duomenų patikrinimo ir išvalymo. Šis atakos tipas laikomas pavojingesniu, nes yra išsaugomas duomenų bazėje ar faile ir vėliau atvaizduojamas kiekvieną kartą vos tik lankytojo naršyklėje užkraunama tinklalapio dalis su kenksmingu kodu.

Skirtingai nei du pirmieji, dokumento objekto modelio XSS atveju į ekraną neišvedama jokios informacijos – ji tiesiog nuskaitoma iš DOM. Šio tipo XSS išnaudoja ryšius tarp hierarchinių DOM elementų. Dar viena problema kyla iš to, kad kenksmingą kodą įterpus į DOM viename tinklalapyje, jis gali būti panaudojamas daugiau nei vienoje svetainėje, nes į DOM galima kreiptis tarp skirtingų adresų (domenų) [9]. Pvz., 2010 m. gegužę buvo atrastas XSS pažeidžiamumas dviem socialiniams interneto portalams (yelp.com, kuriame buvo saugumo spraga, ir facebook.com, iš kurio per minėtą pažeidžiamumą buvo galima nuskaityti asmeninius vartotojų duomenis) komunikuojant tarpusavyje [10].

Tiriamose turinio valdymo sistemose per visą jų gyvavimo istoriją taip pat pasitaikę XSS pažeidžiamumų [19][22]. Jei XSS pažeidžiamumas pasitaiko srityje, kurios naudotojas negali konfigūruoti, svetainės administratorius nedaug ką gali padaryti, keisdamas prieinamus TVS konfigūracijos parametrus. Tokiu atveju paprastai belieka laukti, kol TVS kūrėjai išleis pataisymą, ir jį nedelsiant parsisiųsti.

1.4.2. Užklausų klastojimas tarp tinklalapių

Kuriant interneto tinklalapius ar programas, dažnai pamirštama, kad į juos iš naršyklių ateinančias HTTP užklausas gali suklastoti kitas toje pačioje naršyklėje atvertas interneto puslapis. Naudotojui nežinant, kenksmingas tinklalapis gali perimti jo duomenis bei, apsimesdamas naudotoju, siųsti užklausas į kitus tinklalapius [13]. Tokia ataka yra vadinama užklausų klastojimu tarp tinklalapių (angl. *cross-site request forgery – CSRF*).

Nors pavadinimas gali skambėti panašiai kaip XSS (programavimas tarp tinklalapių) atakų atveju, tačiau CSRF veikimo principas iš esmės yra priešingas: XSS atakos išnaudoja vartotojo pasitikėjimą interneto svetaine, tuo tarpu CSRF atakos išnaudoja svetainės pasitikėjimą vartotoju. Daugiausiai į pavojų patenka aukštesnes priėjimo teises prie svetainės turintys naudotojai (administratoriai, svetainės turinio talpintojai bei koreguotojai ir kt.). Atakos metu iš nieko neįtariančio naudotojo naršyklės yra siunčiamos neautorizuotos užklausos į svetainę, kurioje naudotojas turi aukštesnes teises, t.y., svetainė pasitiki naudotoju [12]. CSRF atakos yra pavojingesnės nei XSS, mažiau populiarios (tai reiškia, kad yra mažiau kūrėjams prieinamų resursų), nuo jų sunkiau apsiginti.

1.4.3. SQL injekcijos

SQL injekcijos yra dar viena iš plačiausiai paplitusių tinklalapių ir interneto programų pažeidžiamumų rūšių. Nuo pat žiniatinklio atsiradimo pradžios programuotojai duomenis talpina duomenų bazėse. SQL injekcijos ataka yra nukreipta prieš tokias žiniatinklio programas, kuriose naudojamasi duomenų bazėmis. Iš naudotojo įvestų duomenų suformuojamos užklausos, pagal kurias atrenkami reikalingi duomenys. SQL injekcijos atakos metu, pažeidėjas per įvesties laukelius gali pateikti kenksmingus SQL užklausos segmentus, taip suformuodamas tokią užklausą, kuri leistų jam gauti ir/ar keisti konfidencialią informaciją [16].

1.4.4. Neautorizuota katalogų peržiūra

Kai kuriuos failus ir katalogus, kurių neturėtų matyti eiliniai naudotojai, galima peržiūrėti tiesiog pasinaudojus naršyklės adreso laukeliu. Tai daroma siekiant išsiaiškinti svetainės katalogų struktūrą, norint rasti paslėptus kelius bei prieiti prie tinklalapio vietų, kurios reikalauja autentifikacijos ar pan. Tai yra neautorizuotos katalogų peržiūros ataka.

Paprastai tinklalapių talpinimo paslaugų tiekėjai turėtų sukonfigūruoti serverį taip, kad būtų parodomas klaidos pranešimas, jei kataloge nėra *index* failo. Deja, taip būna ne visada. Tokiu atveju tinklalapio ar programos programuotojams derėtų patiems pasirūpinti saugumu, į svetainės katalogus, kuriuose laikomi paveikslėliai ar kitokie failai, įdedant *index* failus, kurie parodytų klaidos pranešimą ar tiesiog nukreiptų į pagrindinį svetainės puslapį.

Neautorizuota katalogų peržiūra kartais galima pasinaudojus kokiu nors svetainėje naudojamu įskiepiu. Pvz., turinio valdymo sistemose neretai naudojami WYSIWYG (angl. *What You See Is What You Get*) redaktoriai, kad klientai patys galėtų sumaketuoti keliamą informaciją. Vienas iš tokių redaktorių yra „FCK Editor“ (dabar pervadintas į „CK Editor“). Iki pat 2.6.4 redaktoriaus versijos, kuri yra palyginti nesena, redaktorius buvo pažeidžiamas neautorizuotos katalogų peržiūros atakos – žinant fizinį kelią, per redaktoriaus failų įkėlimo modulį buvo galima įkelti laisvai pasirinktą failą [18]. Šiuo atveju sistemos administratorius, prieš įdiegdamas įskiepį į TVS, turėtų pasidomėti, ar toks veiksmas nepažeis sistemos saugumo.

1.5. Specifinės TVS saugumo grėsmės

Specifinės turinio valdymo sistemų grėsmės taip pat gali būti aptinkamos ir ne TVS pagrindu sukurtuose tinklalapiuose, tačiau turinio valdymo sistemose jos gali būti aptinkamos gan dažnai.

Sistemos saugumo parametrai nemaža dalimi priklauso ir nuo jos konfigūravimo galimybių. Vienose TVS daugelis saugumo priemonių gali būti įgyvendinta pagal plačiai paplitusias gerąsias praktikas ir konfigūravimo aspektų palikta mažai. Tuo tarpu kitos TVS gali turėti nemažai konfigūruojamų parametrų, tokiu būdu suteikiant daugiau laisvės, tačiau ir paliekant potencialius saugumo pažeidžiamumus. Pvz., „Drupal“ TVS leidžia sukurti turinio tipus, kuriuose galima vykdyti PHP programinį kodą. Taip galima praplėsti puslapių galimybes (elementarus to pavyzdys būtų dinaminio datos spausdinimo panaudojimas), tačiau

įvėlus klaidą arba suteikus teises tokiu turinio tipu naudotis pakenkti norintiems naudotojams, galima palikti saugumo spragų.

1.5.1. Mažiausios teisės principo pažeidimas

Turinio valdymo sistemos paprastai naudotojams suteikia leidimus, remdamosi mažiausios teisės principu. Šis principas apskritai turėtų būti naudojamas visose situacijose, kur naudotojams leidžiama ką nors atlikti su sistema. Remiantis šiuo principu, naudotojas gauna tik tiek teisių, kiek reikia jo darbui atlikti. Pvz., administratorius paprastai turi visas teises valdyti sistemą, tuo tarpu straipsnių redaktoriui visiškai nebūtina suteikti teisės keisti sistemos konfigūraciją. Tačiau trečiųjų šalių plėtiniams prieigos teisių panašiu būdu suteikti negalima.

Nors trečiųjų šalių plėtiniams dažnai prieigos reikia tik prie keleto duomenų bazės lentelių, jie dažniausiai gali prieiti prie visų lentelių. Pvz., Cheek ir kiti [14] atliko eksperimentą su populiaria sistema Drupal. Jie išanalizavo 412 plėtinių kreipinius į duomenų bazę. Buvo nustatyta, kad plėtiniai kreipiasi į savo pačių sukurtas DB lenteles bei į pagrindines Drupal lenteles. Taip pat paaiškėjo, kad trečiųjų šalių plėtiniai turi žymiai didesnę prieigą prie pagrindinių duomenų bazės lentelių nei jiems reikia. Pvz., tik 2% plėtinių reikėjo priėjimo prie *sessions* lentelės. Vadinasi, ši prieiga buvo nereikalinga likusiems 98% plėtinių, tačiau jie vis tiek ją turėjo, taip palikdami galimą sesijos užgrobimo pažeidžiamumą. Tik 7% plėtinių reikėjo prieigos prie *node_revisions* (joje saugomos turinio koregavimų versijos) ir *permissions* (saugomi rolėms suteikiami leidimai), tačiau ir kiti plėtiniai turėjo prieigą prie minėtų lentelių, taip palikdami galimus privilegijų padidinimo ir turinio sugadinimo pažeidžiamumus. 1-oje lentelėje pateikiamas trečiųjų šalių įskiepių priėjimo prie Drupal TVS lentelių palyginimas.

1. lentelė. Trečiųjų šalių įskiepių priėjimas prie Drupal TVS duomenų bazės lentelių [14]

Lentelės pavadinimas	*Lentelės aprašas*	*Potencialus pažeidžiamumas*	*Moduliai, kuriems reikėjo prieigos prie lentelės, %*
sessions	Saugo sesijos informaciją, pvz., naudotojo ID, sesijos ID, IP adresą	Sesijos užgrobimas	2%
user_roles	Saugo informaciją apie naudotojų roles sistemoje	Privilegijų padidinimas	5%
node_revisions	Saugo turinio mazgų versijas	Turinio sugadinimas	7%
permissions	Saugo kiekvienai rolei suteiktus leidimus	Privilegijų padidinimas	7%
users	Saugo naudotojų prisijungimo vardus, slaptažodžius ir pan.	Paskyros sugadinimas	23%

1.5.2. Įdiegimo katalogo nepašalinimas

Turinio valdymo sistemos paprastai turi katalogą, iš kurio vyksta pradinis sistemos įdiegimas (platformos patikrinimas, duomenų bazės struktūros paruošimas ir t. t.). Per šį katalogą galima prieiti prie duomenų bazės, gauti įvairios informacijos apie sistemą ir t. t., todėl po įdiegimo šis katalogas turi būti pašalintas.

Pvz., Joomla naujausiose versijose negalima naudotis svetainės viešai prieinama ar administracine dalimi, kol diegimo katalogas neištrinamas.

1.5.3. Silpnų slaptažodžių naudojimas

Ši problema yra sena ir nuolatinė. Žmonės dažnai parenka lengvai įsimenamus trumpus slaptažodžius patogumo dėlei, taip sukeldami riziką, kad slaptažodis bus atspėtas atsitiktinio perrinkimo atakos (angl. *brute force attack*) metu. Dar blogiau – kartais parenkami slaptažodžiai susiję su asmens duomenimis, todėl pilnas perrinkimas net nereikalingas, nes slaptažodį galima atspėti žinant naudotojo artimųjų vardus ar gimimo datas.

Šiuo atveju tikslinga sudaryti įvairius ypač paprastų slaptažodžių sąrašus ir drausti naudotojams juos pasirinkti. Dar vienas pastaruoju metu prigyjantis būdas yra įvairių slaptažodžio stiprumo skalių rodymas, kad vartotojas, įvesdamas slaptažodį galėtų matyti, kokio jis stiprumo. Tokia funkcija naudojama naujausioje Drupal versijoje. Slaptažodžiai tampa atsparesni atsitiktiniam perrinkimui ar atspėjimui, jei juose kombinuotai naudojamos didžiosios ir mažosios raidės, skaitmenys bei specialūs simboliai.

1.5.4. Sudėtinga diegimo procedūra

Daugelis TVS naudotojų neturi gausių techninių žinių, todėl svarbu, kad diegimo procesas būtų kiek įmanoma labiau automatizuotas. TVS paprastai turi daug konfigūruojamų parametrų, kurių vienoks ar kitoks nustatymas gali sudaryti sąlygas pažeidžiamumui atsirasti arba jį panaikinti. Naudotojai dažnai palieka numatytuosius parametrų nustatymus, todėl jie turėtų būti saugūs pagal nutylėjimą (angl. *by default*). Leidžiant naudotojams keisti parametrus, turėtų būti paaiškinama, kokį poveikį vienoks ar kitoks jų nustatymas gali turėti saugumui.

Pvz., Joomla prieš diegimą patikrina sistemos konfigūraciją ir pateikia pranešimus, ar visi nustatymai yra optimalūs. Kai kurių reikalavimų atitikimas yra būtinas, ir be jų diegimo tęsti negalima, tuo tarpu kiti pateikiami kaip įspėjimai, tačiau diegimą galima tęsti toliau.

1.6. Grėsmių atsiradimo pavojus pagal TVS gyvavimo etapus

Per visą TVS gyvavimo ciklą nuo jos įdiegimo iki pakeitimo (pašalinimo) turinio valdymo sistemai kylančios grėsmės šiek tiek kinta.

Gyvavimo ciklą galima suskirstyti į tokius persidengiančius etapus ir periodus:

- Įdiegimas.
- Pradinis konfigūravimas.
- Tobulinimas ir papildymas (naujų modulių diegimas ir pan.).
- Konfigūravimas naudojimo eigoje.
- Atnaujinimas.
- Pašalinimas.

TVS naudojimas prasideda jos įdiegimu. Jo metu galima nustatyti kai kuriuos TVS parametrus, pvz., duomenų bazės naudotojo prisijungimus ir pavadinimą bei DB lentelių priešdėlius. Čia yra viena iš saugumo grėsmių, nes įsilaužėlis, žinodamas naudojamos TVS pavadinimą, gali žinoti ir numatytuosius nustatymus. Tarkim, jei koks nors TVS komponentas yra pažeidžiamas SQL injekcijos, įsilaužėliui tampa žymiai lengviau modifikuoti ar gauti informaciją iš duomenų bazės.

Kaip jau minėta, paliktas įdiegimo katalogas taip pat kelia didelę grėsmę, todėl jį būtina pašalinti. Kai kurios turinio valdymo sistemos, pvz., Joomla netgi neleidžia pradėti naudotis sistema, kol instaliacijos katalogas nėra pašalintas.

Dar viena problema yra silpni slaptažodžiai arba paliekami pagal nutylėjimą sukurti prisijungimo duomenys, pvz., prisijungimo vardas ir slaptažodis „test“ arba „admin“.

Pildant sistemą, pvz., diegiant naujus modulius, sukuriama potenciali grėsmė, nes kiekvienas modulis gali turėti saugumo spragų. Pvz., įdiegtas komentarų modulis gali sukelti grėsmę, kad bus įvykdyta XSS ar CSRF ataka. Todėl, prieš diegiant naujus elementus, reikėtų pasidomėti jų patikimumu. Jei modulis turi kokių nors konfigūravimo galimybių, tuomet taip pat iškyla papildomas pavojus.

Sistemos atnaujinimas paprastai reiškia naujas funkcijas ir esamų saugumo spragų užtaisymą. Tačiau praktikoje pasitaiko nemažai atvejų, kai betaisant vienus pažeidžiamumus, atsiranda kitų. Sistemos administratorius turėtų nuolat sekti TVS naujienas ir imtis atitinkamų priemonių.

1.7. Žiniatinklio svetainių saugumo tikrinimo programos

Žiniatinklio svetainių apsauga yra sudėtinga užduotis, nes svetainės paprastai yra atviros plačiajai visuomenei, įskaitant ir piktavališkus naudotojus. Be to, įvestis į svetaines ateina per HTTP užklausas. Tinkamas šių užklausų apdorojimas taip pat nėra paprastas. Iš atvirojo kodo programų saugumo projekto (angl. *Open web application security project – OWASP*) aptinkamų pažeidžiamumų dažniausiai pasitaikantis yra netinkamas arba iš viso nesamas įvesties apdorojimas [2].

Nors susirūpinimas saugumu nuolat auga – tai dažnai reglamentuoja šalių vyriausybės ir korporacijos, – tačiau egzistuoja keletas svarbių veiksnių, nulemiančių tai, kad žiniatinklio svetaines yra sunku apsaugoti:

- Žiniatinklio programų rinka sparčiai plečiasi, nuolat atsiranda naujų programų, kurias iš pažiūros paprasta sukurti ir prižiūrėti.
- Žiniatinklio programos yra lengvai prieinamos. Prieinamumas yra naudingas, norint pasiekti programą gerais tikslais, tačiau lygiai taip pat lengvai pasiekiamas ir pakenkti siekiantiems asmenims.
- Žiniatinklio programų kūrėjai ir administratoriai dažnai stokoja žinių bei patirties saugumo srityje [6].

Siekiant aptikti bent dalį žiniatinklio programose esančių pažeidžiamumų, naudojamos priemonės, vadinamos žiniatinklio svetainių ar programų saugos tikrintuvais (angl. *web application security scanner*). Paprastai tariant, šis tikrintuvas yra automatizuota programa, kuri keliauja per svetainės puslapius ir, imituodama atakas, ieško galimų pažeidžiamumų. Atakų imitavimas paprastai atliekamas generuojant kenksmingas užklausas ir tikrinant svetainės atsakymus į jas. Tikrintuvas atlieka įvairias atakas, pvz., vienos iš jų metu jis generuoja įvairaus dydžio duomenų eilutes ir bando jas pasiųsti į serverį per svetainėje esančių formų įvesties laukus [13].

1.7.1. Pažeidžiamumų paieškos programų naudojimo rekomendacijos ir apribojimai

Žiniatinklio svetainių saugos tikrintuvus verta naudoti prieš samdant saugumo ekspertus, nes taip galima sumažinti išlaidas, kurios skirtos naujiems pažeidžiamumams aptikti. Tikrintuvai gali padėti sumažinti interneto programose aptinkamas rizikas 50% arba daugiau.

Vienas iš esamų interneto svetainių saugos tikrintuvų apribojimų yra tas, kad jie tinka aptikti tik bendruosius arba plačiai žinomus pažeidžiamumus. Be to, tikrintuvai paprastai naudojami vėlyvosiose programinės įrangos kūrimo stadijose, todėl saugumu turi būti rūpinamasi projekto ruošimo ir įgyvendinimo etapuose. Nėra konkrečioms interneto programoms sukurtų tikrintuvų, kadangi kiekvienas iš jų tikrina tik tam tikras konkrečias sritis. Siekiant pagerinti rezultatus, rekomenduojama naudoti bent du arba daugiau komercinių ir/arba atvirojo kodo tikrintuvų.

Siekiant užtikrinti maksimalų saugumą, žiniatinklio svetainių saugos tikrintuvai turi būti naudojami kartu su kitomis priemonėmis, pvz., samdant saugumo ekspertus. Taip yra todėl, kad netgi geriausi komerciniai tikrintuvai negali aptikti visų galimų programoje esančių loginių klaidų ir pakeisti saugumo profesionalų, nes šios priemonės pažeidžiamumų ieško šabloniškai [10][13].

1.7.2. Esamų pažeidžiamumų paieškos programų apžvalga

Tinklalapių saugumui tikrinti yra sukurta nemažai programų. Galima rinktis tarp komercinės bei nemokamos ar atvirojo kodo programinės įrangos.

Standartinės interneto tinklalapių tikrinimo priemonės paprastai turi vieną bendrą bruožą: jos visos skenavimą atlieka tinkle, nurodžius skenuojamo kompiuterio adresą ar adresų diapazoną. Šiuo būdu gana keblu patikrinti saugumo aspektus, kurie daugiausia būdingi tik turinio valdymo sistemoms. Pvz., Drupal TVS vos įdiegus yra prieinamas modulis, skirtas atsiųsti kitus modulius bei jų atnaujinimus. Jis taip pat automatiškai ieško įdiegtų modulių versijų pasikeitimų ir apie tai informuoja administratorių. Tačiau bent jau Drupal 7.x versijoje šį modulį aktyvuojantis pasirinkimas diegimo metu nebūna pažymėtas, todėl ši savybė gali likti neįjungta. Šiame darbe kuriama programa aptinka, ar modulis yra įdiegtas ir įjungtas, bei praneša apie būseną.

Toliau pateikiama informacija apie keletą pažeidžiamumų paieškos programų.

Acunetix. Acunetix yra komercinė programa, kurią plėtoja kompanija tokiu pat pavadinimu. Pirmoji programos versija išleista 2005 m. Iš išskirtinesnių savybių galima paminėti makro komandų įrašymą, norint patikrinti duomenų įvedimo formas ir slaptažodžiais apsaugotas sritis. Taip pat yra galimybė testuoti puslapius, kuriuose naudojama CAPTCHA (testas, kuriuo siekiama nustatyti, ar naudotojas yra žmogus) bei vieno arba dviejų žingsnių autentifikacija. Tarp kompanijos klientų yra tokios kompanijos ir agentūros kaip Cisco, NASA, Sony, Vodafone [27].

w3af. w3af (trumpinys pavadinimo *Web application attack and audit framework*) yra Python programavimo kalba parašytas atvirojo kodo saugos tikrintuvas. Pirmoji versija pasirodė 2007 m. Programą galima įdiegti Windows, Linux ir Mac OS X operacinėse sistemose. Programa, atlikdama įsilaužimų testus, prie užklausų gali pridėti modifikuotas antraštes, palaiko SSL sertifikatus, leidžia įkelti failus, naudojant *multipart POST* užklausas. Yra galimybė kurti tikrinimo profilius, pasirenkant pažeidžiamumus iš galimų kategorijų [28].

Skipfish. Skipfish yra atvirojo kodo programa, kurią plėtoja Google kompanija. Kūrėjai teigia, kad C kalba parašytas įrankis atitinkamos konfigūracijos serveryje gali pasiekti iki 2000 užklausų per sekundę. Programą galima įdiegti Linux, MacOS X ir Windows OS (per emuliatorių *Cygwin*). Prieš atlikdamas paiešką, tikrintuvas sukuria interaktyvų svetainės medį ir rekursyviai atlieka pažeidžiamumų paiešką [29].

Nikto. Nikto yra atvirojo kodo (nors naudojami duomenų failai tokie nėra) pažeidžiamumų paieškos programa, plėtojama nuo 2008 m. ir yra parašyta Perl programavimo kalba. Skirtingai nuo kitų, Nikto pažeidžiamumų ieško ne pačioje žiniatinklio svetainėje, bet serveryje. Programa testus atlieka ieškodama atitikmenų tarp 6400 potencialiai pavojingų CGI scenarijų, 1200 pasenusių serverio komponentų ir specifinių problemų tarp 270 serverių. Tikrintuvas leidžia skenuoti kelis serverio prievadus vienu metu, o siekiant sumažinti neteisingai aptiktų pažeidžiamumų skaičių, tikrinimas atliekamas keliais metodais: tikrinant antraštes, puslapio turinį ir naudojant turinio maišos funkcijas [30].

NTO Spider. NTO spider yra komercinė žiniatinklio pažeidžiamumų paieškos programa. Tikrintuvas gali skenuoti tuo metu veikiančią svetainę, nepakenkiant našumui. NTO Spider naudoja trijų žingsnių JavaScript analizę, vykdo parametrų analizę, tikrina sesijos saugumą, bando vykdyti OS komandas. Programa pateikia detalias grafines ataskaitas [31].

2-oje lentelėje pateikiamas apžvelgtų pažeidžiamumų paieškos programų palyginimas.

2. lentelė. Žiniatinklio svetainių tikrinimo programų palyginimas

	Programavimo kalba	*Savybės*	*Platforma*	*Sparta (Užklausos per sekundę)*	*Licencija*
Acunetix	n/d	- Populiarių pažeidžiamumų (XSS, SQL injekcija, CSRF) paieška - Daugiagijis (*multi-threaded*) tikrinimas - Serverio tipo ir programavimo kalbos nustatymas - Serverio prievadų skenavimas - Puslapių tikrinimas, kuriuose naudojama CAPTCHA	Windows	n/d	Komercinis
w3af	Python	- Kelių tipų autetifikavimasis svetainėje - UserAgent klastojimas - Slapukų tikrinimas - Vietinis DNS podėlis, siekiant paspartinti tikrinimą - Skenavimo profiliai	Tarp-platforminis		GPL v2
Skipfish	C	- Minimalus CPU naudojimas tikrinimo metu - Automatinis formų užpildymas - Euristiniai tikrinimo metodai - Automatinio mokymosi galimybės	Tarp-platforminis	Iki 2000	Apache licence 2.0
Nikto	Perl	- SSL palaikymas - Pasenusių serverio komponentų tikrinimas - Ataskaitos XML, HTML, NBE ar CSV formatu - Populiarių prisijungimo kombinacijų bandymai - Tikrinimas keliais būdais: antraštės, puslapio turinys	Tarp-platforminis	Iki 2000	GPL
NTO Spider	n/d	- SQL / akla SQL injekcija - XSS (visos rūšys) - Parametrų analizė - OS komandos - HTTP atsako skaidymas - CSRF - Nuotolinio failo įkėlimas - Katalogų naršymas - Išsamios ataskaitos	Windows (neaišku, dėl kitų OS)	10	Komercinis

1.8. Išvados

Pirmajame darbo skyriuje išanalizuotos turinio valdymo sistemų saugumo problemos.

Nustatyta, jog TVS pagrindu paruoštų svetainių, kaip ir kitų internetu pasiekiamų tinklalapių, saugumui kyla nemažai pavojų. Nuo paprasto XSS, nukreipiančio lankytojus į kitą tinklalapį, iki komandinės eilutės panaudojimo, leidžiančio iš aukos kompiuterio ištrinti sisteminus failus ar registro informaciją. Šiuo metu egzistuoja daugybė potencialių saugumo spragų ir vis atrandama naujų. Nustatyta, kad be bendrųjų grėsmių dar egzistuoja specifiniai TVS saugumo pavojai.

Prie minėtų problemų prisideda ir tai, jog eilinis TVS naudotojas dažnai neturi plačių žinių saugumo srityje.

Analizės dalyje aptartos ir saugumo problemų aptikimo priemonės. Išsiaiškinta, jog nors jos ir yra naudingos, šios priemonės negali aptikti visų egzistuojančių pažeidžiamumų bei negali pakeisti saugumo ekspertų.

Dalies pabaigoje apžvelgtos kelios konkrečios pažeidžiamumų paieškos programos.

2. TVS REIKALAVIMŲ SAUGAI SUDARYMAS IR JŲ ATITIKIMO ĮVERTINIMO PROGRAMOS MODELIO PARENGIMAS

Ar specifinis pažeidžiamumas egzistuos turinio valdymo sistemoje, dažnai priklauso ir nuo sistemos konfigūracijos parametrų reikšmių. Kiekvienos TVS konfigūracija skiriasi, gali skirtis ir tos pačios TVS skirtingų versijų konfigūracija. Pvz., vienoje TVS visa konfigūracija gali būti saugoma faile, kitoje – faile ir duomenų bazėje. Taigi, norint patikrinti šiame skyriuje apibūdinamus, su TVS specifiniais saugumo reikalavimais susijusius konfigūracijos nustatymus, reikia jungtis tiesiogiai prie duomenų bazės ar tikrinti konfigūracijos failą. Standartiniai žiniatinklio svetainių ir programų saugumo tikrintuvai šiuo atveju netinka, nes jie skenavimą atlieka per tinklą. Be to, kaip minėta analizės dalyje, jie sukurti aptikti tik tam tikros srities pažeidžiamumus, todėl TVS specifinių saugumo kriterijų įvertinimas gali būti netgi nenumatytas jų tikrinimo taisyklėse.

Taigi šiame darbe modeliuojama ir kuriama saugumo kriterijų vertinimo programa tikrinimą atlieka jungdamasi tiesiai prie TVS duomenų bazės ar konfigūracijos failo. Kadangi kiekvienos TVS konfigūracija skiriasi (skiriasi duomenų bazės lentelių, konfigūracijos failų ir parametrų pavadinimai), kiekvienai turinio valdymo sistemai ir jos versijoms reikalingas specialiai pritaikytas saugumo kriterijų vertinimo algoritmas.

Šiame skyriuje iškeliamas darbo tikslas ir uždaviniai, apibūdinami specifiniai TVS saugumo kriterijai, pateikiamas kriterijų atitikimą vertinančios programos modelis, panaudos atvejų bei veiklos diagramos. Skyriaus pabaigoje išvardijami realizacijos reikalavimai.

2.1. Darbo tikslas ir uždaviniai

Žemiau pateikiamas šio darbo tikslas ir išsikelti uždaviniai.

2.1.1. Darbo tikslas

Sudaryti metodiką, įvertinančią TVS specifinių saugumo kriterijų atitikimą.

2.1.2. Uždaviniai

- Aprašyti specifinius TVS saugumo vertinimo kriterijus;
- Sudaryti kriterijų vertinimo programos modelį;
- Nurodyti, kokius reikalavimus turi tenkinti programinė realizacija;

- Realizuoti programos dalį, kuri įvertina dviejų tiriamų turinio valdymo sistemų saugumo reikalavimų atitikimą;
- Eksperimento metu ištirti dvi turinio valdymo sistemas prieš saugumo parametrų keitimą bei po jo;
- Pabaigoje pagal gautus darbo rezultatus parašyti išvadas.

2.2. TVS saugumo įvertinimo kriterijų sudarymas

Siekiant išspręsti vieną iš įvade iškeltų uždavinių, toliau aprašomi specifiniai TVS saugumo vertinimo kriterijai.

1. Naudotojams suteikiamų teisių ir rolių sistema

Kiekvienoje sistemoje (ne tik TVS) paprastai galima atlikti nemažai veiksmų, tačiau toli gražu ne visiems naudotojams turi būti leidžiama atlikti visus veiksmus. Dėl šios priežasties paprastai pasitelkiama teisių ir rolių sistema.

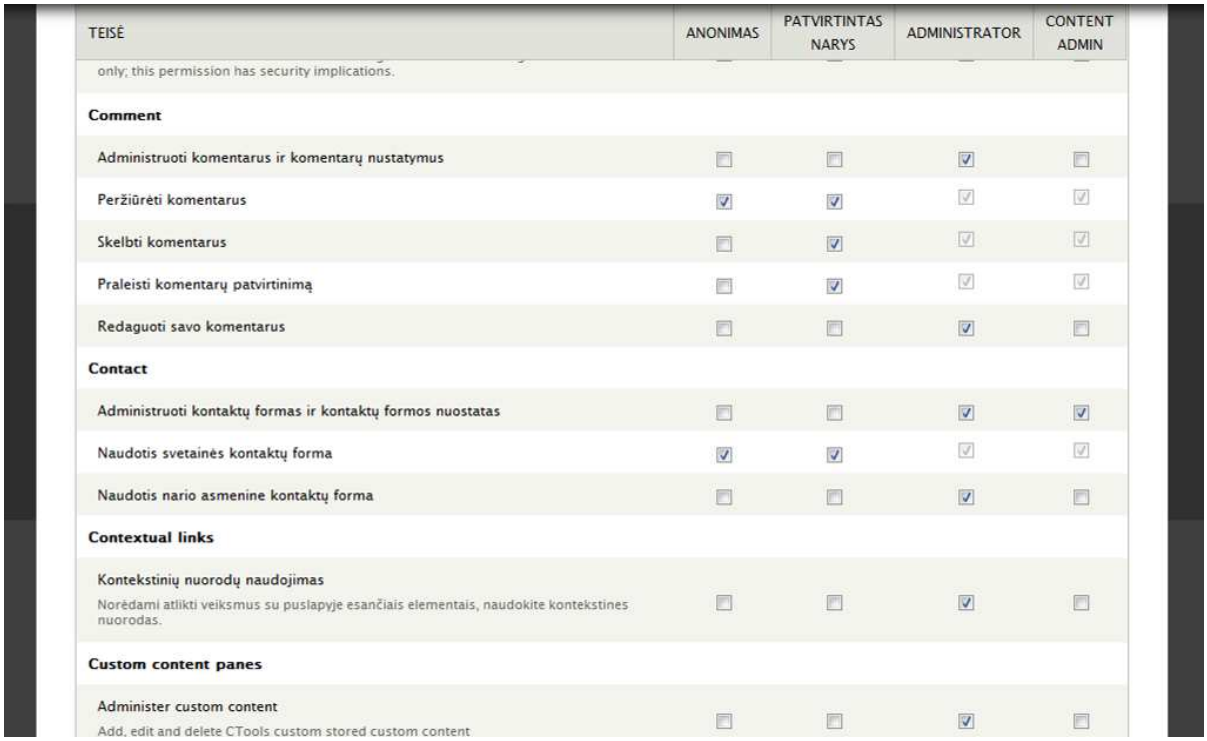
Prieigos teisių pavyzdžiai:

- Turinio peržiūra. Papildomas leidimas gali būti įvestas nepublikuoto turinio peržiūrai.
- Turinio pridėjimas ir koregavimas. Kadangi turinio tipų paprastai būna daugiau nei vienas, kiekvienam iš jų taip pat gali būti suteikiama teisė.
- Failų įkėlimas. Failų tipų taip pat yra įvairių, todėl turėtų būti galimybė leisti įkelti tik tam tikrus failus. Tipas turėtų būti nustatomas ne pagal plėtinį, kurį galima lengvai pakeisti, o pagal failo antraštėje esančią MIME žymę.
- HTML, JavaScript, PHP ar kitų scenarijų kalbų naudojimas turinyje. Kadangi scenarijų (angl. *scripts*) naudojimas yra potencialiai pavojingas, ši teisė turėtų būti suteikiama tik patikimiems naudotojams.

Atskiras teises galima suteikti vartotojui tiesiogiai, tačiau tai priimtina tik esant pakankamai mažam skaičiui naudotojų ir pačių teisių. Didėjant kuriam nors iš šių skaičių, prieigos valdymas gali tapti labai sudėtingas. Dėl šios priežasties yra taikomas rolių principas. Rolė – tai tam tikrų teisių rinkinys. Taigi teisės yra priskiriamos rolėms, o rolės yra priskiriamos naudotojams. 3 ir 4 pav. pavaizduotos rolės ir teisės Drupal TVS.

	NARIO VARDAS	BŪSENA	ROLĖS	NARYS JAU	NAUDOJOSI	VEIKSMAI
☐	tn	aktyvus	• content admin	1 savaitė 1 diena	prieš 2 dienos 17 valandų	redaguoti
☐	admin	aktyvus	• administrator	1 savaitė 6 dienos	prieš 3 minutės 51 sek	redaguoti

3 pav. Naudotojams suteiktos rolės Drupal TVS



TEISĖ	ANONIMAS	PATVIRTINTAS NARYS	ADMINISTRATOR	CONTENT ADMIN
only; this permission has security implications.				
Comment				
Administruoti komentarus ir komentarų nustatymus	☐	☐	☑	☐
Peržiūrėti komentarus	☑	☑	☑	☑
Skelbti komentarus	☐	☑	☑	☑
Praleisti komentarų patvirtinimą	☐	☑	☑	☑
Redaguoti savo komentarus	☐	☐	☑	☐
Contact				
Administruoti kontaktų formas ir kontaktų formos nuostatas	☐	☐	☑	☑
Naudotis svetainės kontaktų forma	☑	☑	☑	☑
Naudotis nario asmenine kontaktų forma	☐	☐	☑	☐
Contextual links				
Kontekstinių nuorodų naudojimas Norėdami atlikti veiksmus su puslapyje esančiais elementais, naudokite kontekstines nuorodas.	☐	☐	☑	☐
Custom content panes				
Administer custom content Add, edit and delete CTools custom stored custom content	☐	☐	☑	☐

4 pav. Rolėms suteikiamos teisės Drupal TVS

Turinio valdymo sistemose gali būti išskiriamos šios naudotojų rolės:

TVS administratorius

Tai yra centrinė rolė, turinti pilną priėjimą prie visų TVS funkcijų. Jis gali keisti sistemos parametrus, kurti kitas roles bei priskirti jas naudotojams.

Publikuotojas

Šią rolę turintis naudotojas patvirtina arba atšaukia turinio pakeitimus bei yra atsakingas už tai, koks turinys matomas svetainės lankytojams.

Redaktorius

Šios rolės naudotojai gali redaguoti arba trinti turinį, kurį sukuria „autoriaus“ rolę turintys naudotojai. Po redagavimo darbų, turinį turi patvirtinti „publikuotojo“ rolę turintis naudotojas.

Autorius

Autoriai gali kurti puslapius, bei koreguoti arba ištrinti savo sukurtą turinį. Autoriai gali turėti turinio talpinimo ir koregavimo teises tik tam tikroje svetainės dalyje.

Lankytojas

Klientas, siunčiantis užklausas į žiniatinklio serverį ir peržiūrintis turinį tam tikru momentu.

Taigi naudojant rolių bei teisių metodą, gaunama lanksti priėjimo valdymo sistema.

2. Sesijų gyvavimo laikas

Sesijos gyvavimo laikas nurodo, kiek tarp kliento kompiuterio ir serverio užmegzta sesija bus aktyvi po paskutinio veiksmo, kurį atlieka naudotojas. Patogumo dėlei (kad naudotojams nereikėtų vis prisijungti iš naujo) sesijos gyvavimo laikas kartais nustatomas gana ilgas. Tačiau tai turi poveikį saugumui. Kuo sesijos gyvavimo laikas trumpesnis, tuo sunkiau turėtų būti atlikti tokį piktavališką veiksmą kaip sesijos užgrobimas.

Be to, jei naudotojas netyčia pamiršta atsijungti nuo sistemos, trumpas sesijos gyvavimo laikas apsaugos nuo veiksmų, kuriuos gali atlikti kiti tuo pačiu kompiuteriu besinaudojantys asmenys.

3. Atsarginių kopijų kūrimas

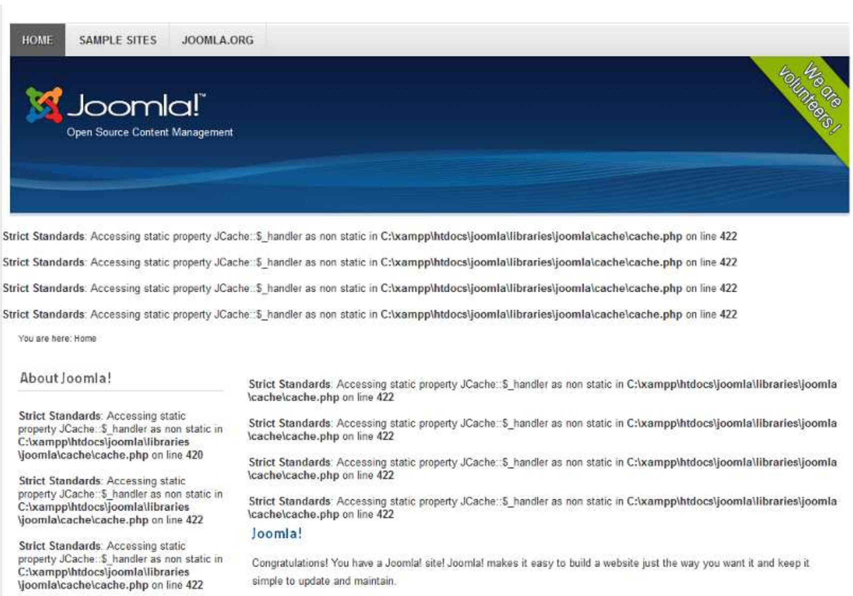
Bet kurioje informacinėje sistemoje ar ją saugančioje techninėje įrangoje gali kilti nesklandumų, susijusių su duomenų praradimu. Tai gali būti techninės įrangos (informacijos saugojimo įrenginių) gedimas, įsilaužimas į sistemą iš išorės, siekiant sunaikinti duomenis, arba tiesiog žmogiškasis faktorius, kai informacija ištrinama netyčia. Dėl visų šių priežasčių atsarginės kopijos yra vienas iš būtinų aspektų.

Paprastai atsarginės kopijos gali būti daromos serveryje, kuriame saugoma TVS, tačiau ne visada galima greitai ir lengvai prie jų prieiti. Dėl to atsarginių duomenų kopijų įjungimas ir nustatymai galėtų būti atliekami pačioje TVS.

Atsarginių duomenų kopijų laikymas tame pačiame serveryje yra pavojingas, nes gedimo atveju gali dingti visi jame esantys duomenys. Dėl šios priežasties atsarginės kopijos turėtų būti perkeliamos į kitą vietą. Idealiu atveju jos turėtų būti laikomos kitoje geografinėje vietovėje.

4. Klaidų rodymo išjungimas

Informacija apie klaidas įsilaužėliui gali atskleisti labai daug naudingos informacijos: paprastai klaidų pranešimuose nurodomas kodo eilutės numeris ir failas, kuriame įvyko klaida. Jei klaida susijusi su duomenų baze, nurodomas duomenų bazės lentelės pavadinimas ir, pvz., lentelės stulpelio pavadinimas. Visos šios priežastys skatina tai, kad produkcinėje (galutiniams lankytojams) svetainės versijoje klaidų rodymas būtų išjungtas. Tuo tarpu, TVS pradinio administravimo metu klaidų rodymas yra gali būti naudingas.



5 pav. Rodomos klaidos iš karto po Joomla 1.7 diegimo

Žinoma, klaidų rodymą galima išjungti serverio lygmenyje bei svetainės lygmenyje per failus, tačiau rodymo išjungimas turėtų būti prieinamas ir pačios turinio valdymo sistemos administravimo lygmenyje. 5 pav. matoma, kad Joomla 1.7 versijoje klaidos būdavo rodomos iš karto po diegimo. Paaiškėjo, jog taip atsitiko dėl to, jog numatytoji serverio reikšmė buvo „visų klaidų rodymas įjungtas“. Joomla 2.5 versijoje ši problema pašalinta.

5. TVS versijos rodymo išjungimas

Jei TVS gali rodyti savo versiją lankytojams, rekomenduojama, kad ši funkcija būtų išjungta. Tai atrodo daug problemų nekeliantis dalykas, tačiau, atradus pažeidžiamumą vienoje sistemoje ir atlikus sėkmingą ataką, ją galima pakartoti ir kitose analogiškose sistemose. Programinės įrangos versijos žinojimas šiuo atveju įsilaužėlį atlaisvina nuo bereikalingo spėliojimo, kokius įrankius reikia panaudoti, norint įsilaužti į sistemą.

6. Failų katalogo apsauga

Žiniatinklio serveryje turėtų būti numatyta galimybė išjungti katalogo turinio rodymą, ir serverių administratoriai paprastai ja naudojasi. Pvz., katalogo turinys gali būti parodomas, jei jame nėra „index“ failo. Šiaip ar taip ši funkcija ne visada gali būti įjungta serverio lygmenyje, o duomenų katalogas gali turėt daug pakatalogių, pvz., po vieną kiekvienam turinio tipui, kiekvienam vartotojui ir pan. Tokiu atveju reikėtų kiekviename kataloge patalpinti po „index“ failą, o tai nėra patogu.

Pvz., paveiksliuką galima atsidaryti atskirame naršyklės lange ir matyti, kokiu adresu jis prieinamas. Tarkim kelias yra www.pavyzdys.com/paveiksliukai/vaizdas.jpg. Iš adreso galima spręsti, kad failas yra kataloge „paveiksliukai“, o nutrynus „vaizdas.jpg“ galima tikėtis kitų failų parodymo, kurie svetainės turinyje nenaudojami arba prienami tik tam tikro turinio kontekste, reikalaujančiame papildomų teisių. Nesant serverio apsaugos ir „index“ failo, taip ir atsitiktų. Dėl to TVS galėtų apdoroti URL užklausas ir neparodyti katalogo turinio, jei nesikreipiama į konkretų failą.

Reikia pastebėti, kad ši funkcija paprastai veikia tik tuo atveju, jei įjungtas URL adresų perrašymas, pvz., pasinaudojant „Apache“ žiniatinklio serverio moduliu „mod_rewrite“. Jei modulio serveryje nėra (nors tai pasitaiko gana retai), o reikalingas ribojimas prie failų, gali praversti privatus failų katalogas.

7. Privatus failų katalogas

Kartais reikia dar aukštesnės saugos, norint apsaugoti failų katalogą. Tai gali būti pasiekiama, kai naudotojų įkelti failai talpinami ne tame pačiame šakniniame kataloge, kur ir

pati svetainė. Tokiu atveju, juos reikia iškelti vienu ar keliais lygiais aukščiau serverio katalogų, o priėjimas prie jų galimas tik per TVS scenarijų funkcionalumą.

8. El. pašto adresų apsauga

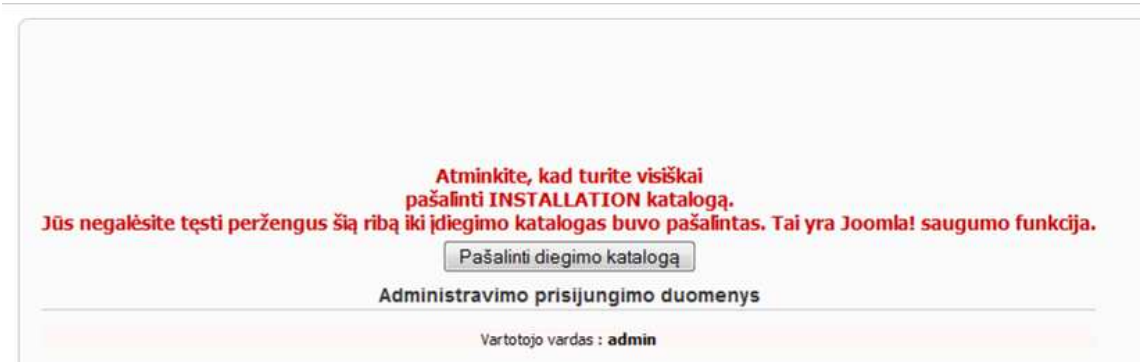
Žiniatinklio svetainės ir el. pašto adresų savininkai jau seniai kenčia nuo automatinio el. pašto adresų surinkimo iš svetainių. Automatizuotos piktavališkos programos keliauja per tinklalapius ir surenka el. pašto adresus, į kuriuos vėliau gali būti siunčiami nepageidaujami laiškai – brukalai (angl. *spam*). Vieną kartą surinktas adresas gali būti perparduotas kelis kartus, ir, jei el. pašto serveris neturi pakankamų apsaugų nuo brukalų, adreso savininkas gali gauti daug nepageidaujamo el. pašto.

Dėl aukščiau paminėtų priežasčių svarbu, kad turinio valdymo sistemose būtų įdiegta apsauga nuo automatinio el. pašto adresų surinkimo.

9. Diegimo failo bei papildomą informaciją suteikiančių failų pašalinimas po diegimo

Po pradinio TVS įdiegimo, diegimo failas ar katalogas turėtų būti pašalintas, o rašymas į konfigūracijos failą uždraustas.

Joomla TVS netgi negalima pradėti naudotis vieša ar administracine svetainės dalimi, kol katalogas nepašalintas (6 pav.).



6 pav. Joomla TVS instaliacinį katalogą reikia pašalinti iš karto po diegimo

Turinio valdymo sistemų šakniniame kataloge dažnai pasitaiko papildomų informacinių failų populiariais pavadinimais:

- *readme.txt*, kuriame pateikiama bendra informacija apie sistemą.
- *changelog.txt*, kuriame galima rasti informacijos apie naujausius sistemos pataisymus ir papildymus. Jame taip pat galima rasti ir dabartinį esamos sistemos versijos numerį.
- *install.txt* ir *upgrade.txt*, kuriuose aprašoma sistemos diegimo ir atnaujinimo procedūros.

Priklausomai nuo TVS ir jos versijos, gali pasitaikyti ir kitokių informacinių failų, kuriuose rekomenduojama pašalinti.

10. Vartotojo įvedamų duomenų tikrinimas, skirtingi teksto formatai

Vartotojo įvedamų duomenų tikrinimas turinio valdymo sistemoje yra viena iš svarbiausių priemonių, siekiant apsisaugoti nuo tokių atakų kaip XSS, CSRF, SQL injekcijos ir pan.

Turinio valdymo sistemoje turėtų būti numatyta skirtingų teksto įvesties tipų galimybė. Turėtų būti bent 3 teksto įvesties tipai:

- Pilnas HTML. Šis teksto tipas turėtų būti prieinamas tik patikimiems registruotiems naudotojams (straipsnių autoriams, publikuotojams).
- Filtruotas HTML. Tai „apkarpytas“ auščiau minėto turinio tipo variantas. Šis tipas tam tikrais atvejais gali būti naudojamas atsiliepimų formose, komentaruose ir pan.
- Paprastas tekstas. Šis tipas galėtų būti naudojamas tose srityse, kur HTML kodas nereikalingas. Jis taip pat gali būti naudojamas atsiliepimų formose, komentaruose ir apskritai tose srityse, kur reikalingas maksimalus saugumas.

Be HTML dar gali būti sukuriami specialūs teksto įvesties formatai, kur leidžiama naudoti JavaScript ir PHP scenarijus. Tačiau teisė naudoti šiuos turinio tipus turi būti suteikiami tik visiškai patikimiems vartotojams.

11. Slaptažodžių ir prisijungimo bandymų politika

Turinio valdymo sistemoje gali būti įgyvendinama slaptažodžių politika. Pvz., gali būti reikalaujama, kad slaptažodžiuose būtų bent po vieną didžiąją bei mažąją raidę ir skaitmenį, o pats slaptažodis būtų bent 8 simbolių ilgio. Tačiau nereikėtų taikyti pernelyg griežtos

slaptažodžių politikos, nes naudotojai, nesugebėdami jų prisiminti, gali slaptažodžius užsirašyti.

Nors slaptažodžių politika yra geras dalykas, ne mažiau svarbus aspektas yra leidžiamų nesėkmingų bandymų prisijungi skaičius. Neretai sėkmingas slaptažodžio atspėjimas „grubios jėgos“ (angl. *brute force*) būdu galimas dėl to, kad svetainė leidžia neribotą bandymų jungtis skaičių. Panaudojant slaptažodžio spėjimą pagal žodyną, kai paeiliui bandomi visi realūs žodžiai, perrinkimas ilgai neužtrunka, o naudotojai savo prieigos slaptažodžiui neretai pasirenka kokį nors realų žodį.

Viso to galima išvengti, naudojant nesėkmingų bandymų prisijungti ribojimą. Pvz., leidžiami penki bandymai, o po to naudotojo paskyra blokuojama penkioms minutėms. Po dar kelių nesėkmingų bandymų, paskyros blokavimo laikas gali būti pailginimas. Taip pat po kelių nesėkmingų bandymų galima įjungti CAPTCHA lauką, kur vartotojas turi patvirtinti, jog slaptažodį bando įvesti žmogus („Google“ prisijungimo pavyzdys).

12. Saugi vienkryptės maišos funkcija

Slaptažodžiai duomenų bazėje niekada neturi būti saugomi atviru tekstu, o turi būti užkoduoti, panaudojant vienkryptės maišos (angl. *hash*) funkciją. Naudotojui jungiantis prie sistemos, jo įvesto slaptažodžio vienkryptės maišos funkcijos reikšmė palyginama su esančia duomenų bazėje. Jei reikšmės sutampa, prisijungimas leidžiamas.

Nors, kaip teigia pats pavadinimas, pradinės slaptažodžio reikšmės iš maišos reikšmės turi būti neįmanoma rasti, tačiau yra aptikta tam tikrų vienkryptės maišos algoritmų pažeidžiamumų. Pvz., anksčiau vienu iš populiaresnių buvusio MD5 maišos algoritmo naudoti nerekomenduojama. Taip pat populiarų SHA-1 maišos algoritmą siūloma pakeisti naujesniais ir saugesniais SHA-256 arba SHA-512 algoritmais.

13. Papildoma slaptažodžių apsauga

Prie papildomos slaptažodžių apsaugos gali būti priskiriamas slaptažodžio „druskos“ (angl. *salt*) naudojimas. Jei naudotojas pasirenka silpną slaptažodį, o įsilaužėlis gauna slaptažodžių vienkryptės maišos vertes, jas perrinkinėdamas jis gali nustatyti, kokį slaptažodį naudotojas pasirinko. Nuo šios grėsmės galima bent dalinai apsisaugoti naudojant slaptažodžio „druską“ – papildomą simbolių rinkinį, pridedamą pradinio slaptažodžio

pradžioje arba pabaigoje prieš jį apdorojant vienkryptės maišos funkcija. „Druskos“ reikšmė paprastai saugoma programiniame kode, o įsilaužėlis, pavogęs slaptažodžio maišos vertę, „druskos“ matyti negali.

14. Pakeisto turinio versijos

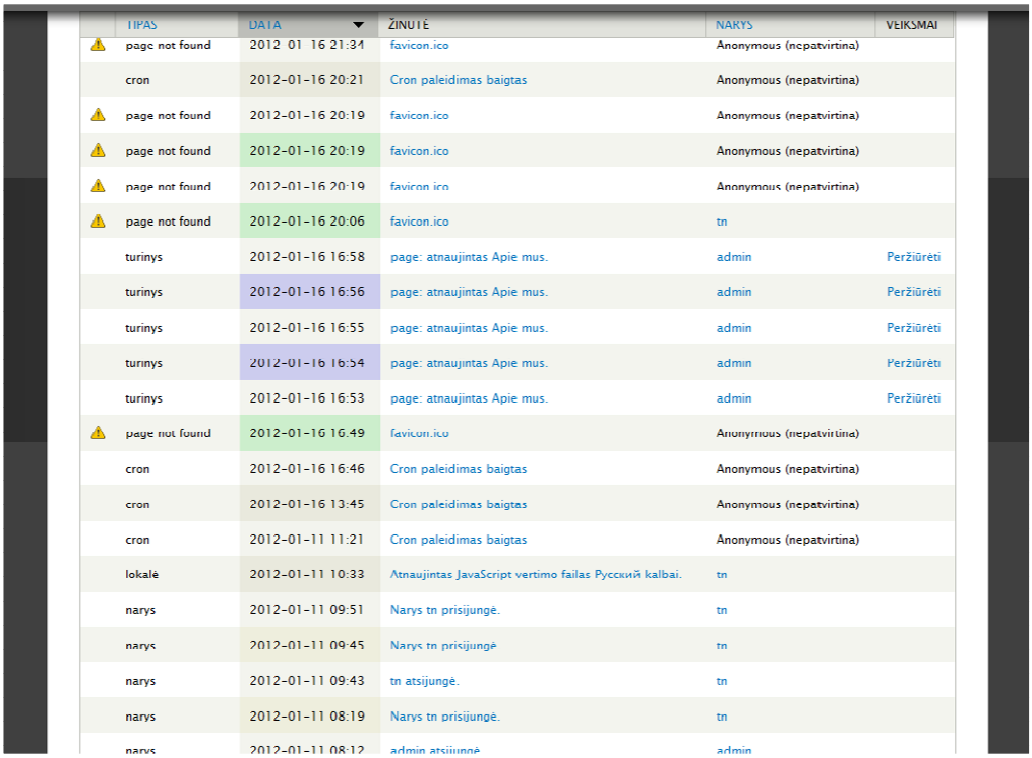
Kaip minėta, TVS turėtų būti numatytos bent kelios naudotojų rolės. Tarkim, straipsnių autoriui pakeitus straipsnio tekstą, jį turi patvirtinti aukštesnes teises turintis naudotojas. Tačiau, nesaugant ankstesnių turinio versijų, netgi nelabai galima palyginti, kokie pakeitimai buvo atlikti. Be to, net ir tuo atveju, kai naudotojas, kurio veiksmams nereikia patvirtinimo, atlieka pakeitimus, gali prireikti turinio atstatymo į ankstesnę versiją.

15. Žurnalizavimas

Sistema turėtų turėti žurnalizavimo (angl. *logging*) funkcijas. Žurnalizavimas yra svarbus, norint žinoti, kokie veiksmai sistemoje buvo atlikti vienu ar kitu metu bei kas juos atliko. Žurnalizuojant turėtų būti registruojami šie aspektai:

- Sėkmingas vartotojo prisijungimas prie sistemos.
- Vartotojo atsijungimas nuo sistemos.
- Nesėkmingi prisijungimo bandymai ir su jais susijusi informacija: paskyros vardas, laikas, IP adresas. Tačiau reikia nepamiršti, kad niekada negalima įrašyti net ir neteisingai įrašyto slaptažodžio – tik naudotojo vardą. Slaptažodžiai duomenų bazėje turi būti saugomi užšifruoti, todėl ir čia jų, net ir neteisingų, negalima rodyti atviru tekstu.
- Nerasti puslapiai (404 klaidos).
- Turinio redagavimo veiksmai: kas redagavo, kada, koks turinys.
- Modulių įjungimai / išjungimai.
- Programinio kodo klaidos. Jos turi būti nerodomos svetainės lankytojams, tačiau vis tiek registruojamos įvykių žurnale.

7 pav. matoma Drupal žurnalizavimo ataskaita.



7 pav. Skirtingi žurnalizavimo įrašai Drupal TVS

Kadangi didesnio lankytojų srauto sulaukiančioje ir daug informacijos turinčioje sistemoje gali būti nemažai žurnalizavimo įrašų, turėtų būti numatytas jų filtravimas pagal tam tikrus parametrus, pvz., data ir laikas, naudotojo vardas, sistemos sritis.

16. Nestandartiniai naudotojų prisijungimo vardai

Naudotojai dažnai mėgsta pasirinkti paprastus ir populiarius prisijungimo vardus, tarp kurių populiariausi yra *admin* arba *administrator*. Įsilaužėliui bandant neteisėtai prisijungti prie sistemos, neužtenka žinoti vien slaptažodį, reikalingas ir prisijungimo vardas, o populiarūs naudotojų vardai tai palengvina (8 pav.).

8 pav. Pagal nutylėjimą siūlomas prisijungimo vardas „admin“ Joomla TVS

Dėl šių priežasčių rekomenduojama naudoti nestandartinius naudotojų prisijungimo vardus, tai ypač taikoma paskyroms, kurios sistemoje turi aukšto lygio teises. Deja, būtent šios paskyros dažniausiai ir yra *admin, root* ir pan.

17. DB lentelių priešdėlių konfigūravimas

Įdiegiant turinio valdymo sistemą, paprastai leidžiama pasirinkti duomenų bazės lentelių pavadinimų priešdėlį. Tai patogu tuo atveju, jei TVS DB lentelės laikomos duomenų bazėje, kuria dalijasi kitas projektas. Tai nėra labai gerai, bet pasitaiko atvejų, kai svetainės talpinimo paslaugų tiekėjas leidžia susikurti tik vieną duomenų bazę ir pan.

Be aukščiau minėtos priežasties, duomenų bazės lentelių pavadinimų priešdėliai prisideda prie saugumo. Pvz., norint atlikti sėkmingą SQL injekcijos ataką, dažnai reikia žinoti konkrečios DB lentelės pavadinimą. Naudojant standartinius DB lentelių pavadinimų priešdėlius arba nenaudojant jų visai, tai padaryti yra lengviau.

9 pav. Atsitiktinai automatiškai sugeneruotas DB lentelės priešdėlis

Pvz., ankstesnėse Joomla TVS versijose standartinis siūlomas priešdėlis būdavo „jos_“, o dabar generuojamas automatiškai (9 pav.). Nustatyti, kad svetainė naudoja Joomla TVS nėra sudėtinga. Internete yra ir įrankių, kurie tai gali atlikti, užtenka tik nurodyti svetainės adresą. Žinant pačią turinio valdymo sistemą, nesunku išsiaiškinti ir kokia jos DB lentelių struktūra.

18. TVS ir jos modulių atnaujinimai TVS administravimo aplinkoje

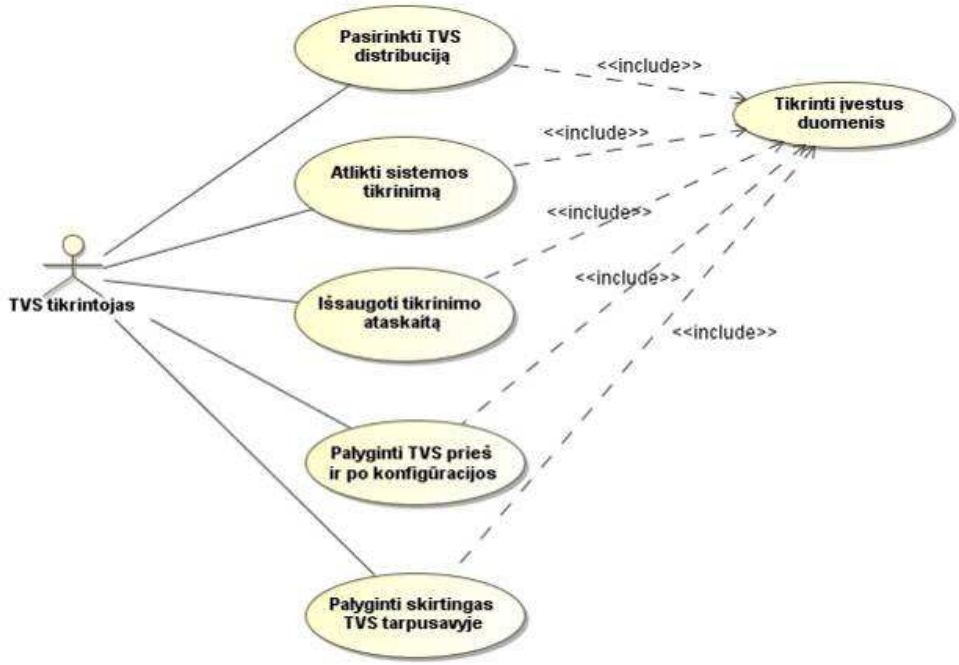
Turinio valdymo sistema paprastai yra praplečiama, pasinaudojant jai skirtų modulių funkcionalumu. Pvz., tai gali būti nuotraukų galerijų moduliai, už turinio daugiakalbiškumo palaikymą atsakingi moduliai, RSS srautų moduliai ir pan.

10 pav. Drupal TVS siūlo automatiškai parsisiųsti atnaujinimus

Moduliai bei pats TVS branduolys neretai yra nuolat papildomi, taisomos jų klaidos, gerinamas saugumas, todėl juos būtina nuolat atnaujinti – ypač dėl saugumo. Vartotojai ne visada turi priėjimą prie FTP tam, kad galėtų įkelti atnaujinto modulio failus, todėl patogiau ir paprasčiau atnaujinimus parsisiųsti ir įdiegti TVS administravimo aplinkoje.

2.3. Programos panaudojimo atvejų diagrama

Panaudojimo atvejų diagramose galima aprašyti, ką vienas ar kitas naudotojas gali daryti sistemoje. Šiuo atveju bus tik vienas naudotojas – TVS tikrintojas. Kriterijų vertinimo programos panaudojimo atvejų diagrama matoma 11 pav.

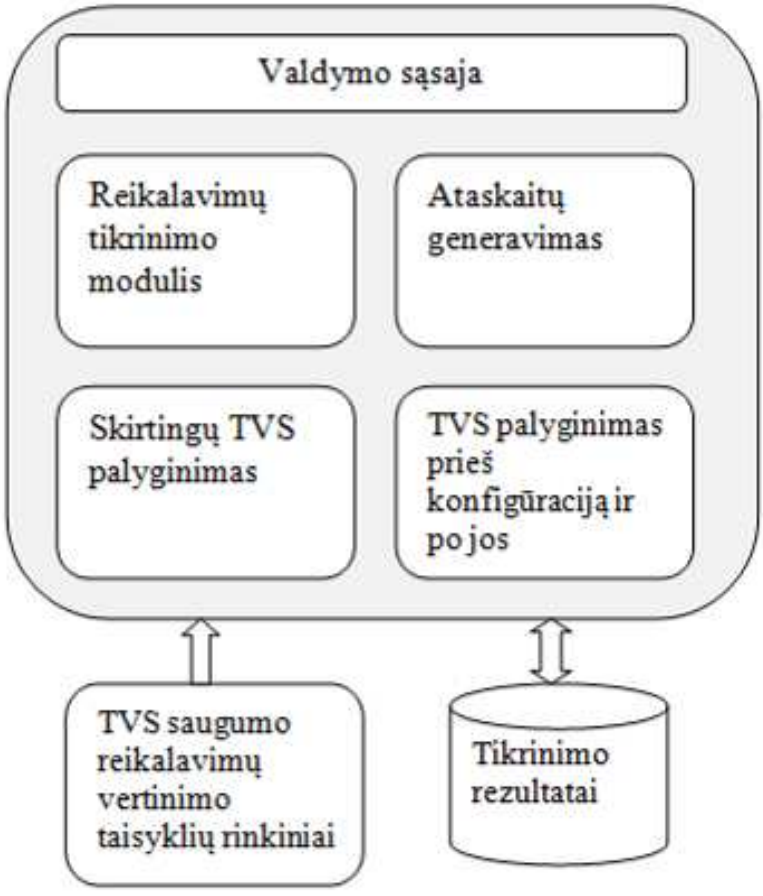


11 pav. Kriterijų vertinimo programos panaudojimo atvejų diagrama

Kaip matoma, tikrintojas gali nurodyti skirtingas TVS distribucijas (versijas), atlikti tikrinimą, išsaugoti ataskaitą, kuri gali būti naudinga vėlesniam rezultatui palyginimui. Taip pat numatyta galimybė palyginti skirtingas TVS tarpusavyje.

2.4. TVS saugumo kriterijų vertinimą atliekančios sistemos veikimo modelis

12 pav. pavaizduotas TVS saugumo kriterijų vertinimą atliekančios sistemos veikimo modelis. Kaip galima matyti iš aukščiau esančios panaudojimo atvejų diagramos, modelyje pavaizduoti panaudojimo atvejus įgyvendinantys elementai.



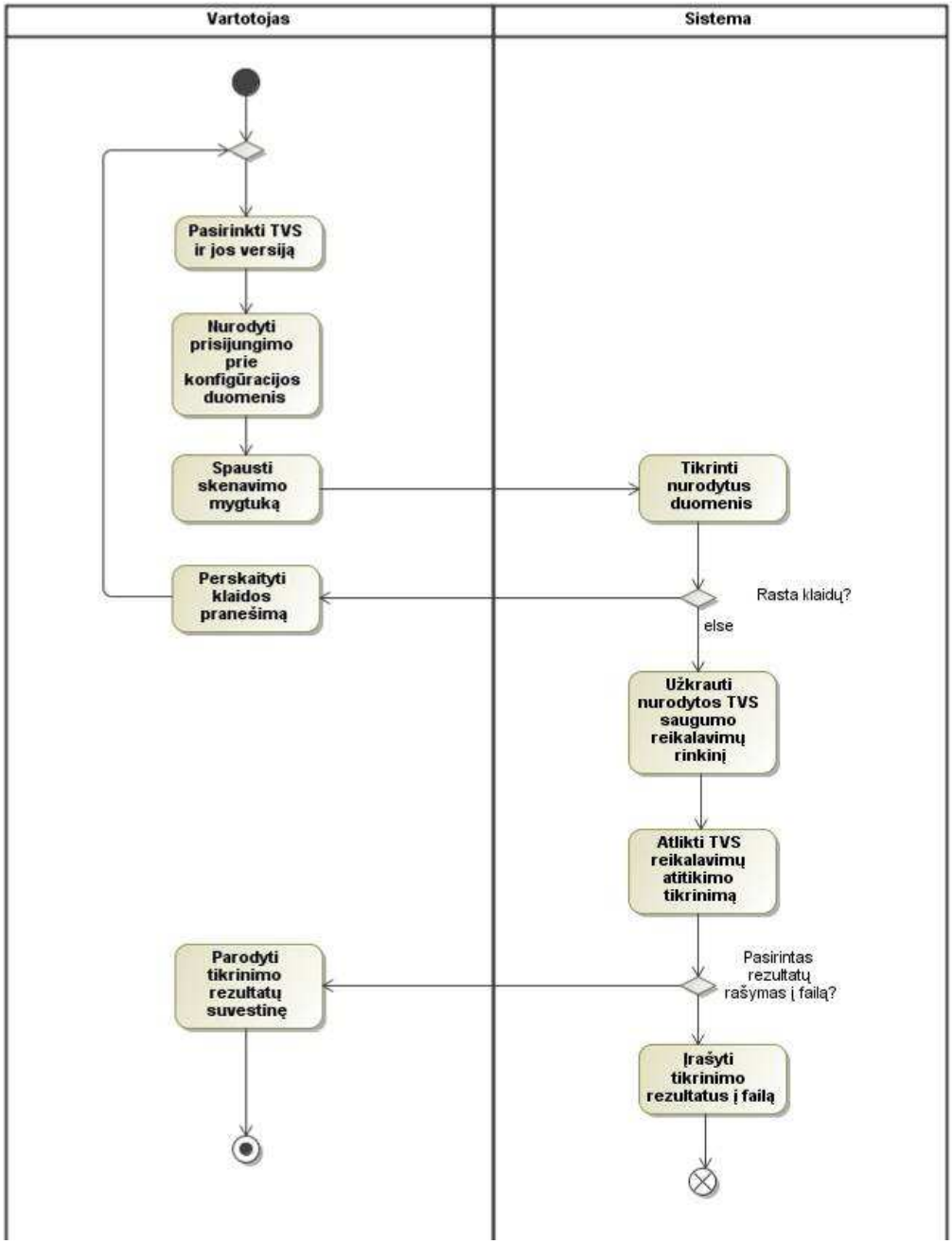
12 pav. TVS tikrinimą atliekančios sistemos veikimo modelis

Modelyje matosi, kad sistema TVS tikrinimui naudoja užkraunamus taisyklių rinkinius, kurie, kaip minėta, pritaikomi konkrečiai turinio valdymo sistemai ir jos versijai. Tikrinimo rezultatų ataskaitą galima išsaugoti, norint palyginti TVS tikrinimo rezultatus, esant vienokiai ar kitokiai TVS konfigūracijai.

2.5. TVS saugumo reikalavimų tikrinimas

Vienos turinio valdymo sistemos tikrinimo modeliui pavaizduoti pasirinkta veiklos diagrama (13 pav.). Diagramoje matomi tikrinimo priemonės naudotojo veiksmai bei sistemos atsakas į juos.

Svarbu atkreipti dėmesį, jog, norint tinkamai atlikti sistemos tikrinimą, reikia pasirinkti reikiamą turinio valdymo sistemą ir jos versiją. Kadangi tikrinimo taisyklių rinkinys pritaikomas konkrečiai TVS ir jos versijai, tik tokiu būdu skenavimo priemonė gali teisingai įvertinti tikrinimus kriterijus.



13 pav. TVS saugumo reikalavimų tikrinimo seka

Iš tiesų, jei pasirenkama vienokia tikrinimo sistema, o prisijungimo parametrai nurodomi kitokie, tikrinimas visai nepavyks, ypač tuo atveju, jei pasirenkamos visiškai skirtingos turinio valdymo sistemos: neteisingai nurodžius versiją, dalis tikrinimo gali pavykti.

2.6. Programos modelio realizuojamos dalies reikalavimai

Realizacijos skyriuje bus įgyvendinta 2.4 skyriuje pateikto modelio dalis. Modelyje ir panaudos atvejų diagramoje matoma, kad TVS saugumo kriterijų vertinimo programa turėtų palyginti turinio valdymo sistemas prieš konfigūraciją ir po jos, taip pat palyginti skirtingas TVS tarpusavyje bei įrašyti tikrinimo rezultatus. Tačiau pilnas tokios programos sukūrimas išeina už šio darbo ribų, todėl realizacijoje bus įgyvendinta siauresnė funkcionalumo dalis. Realizacijoje bus koncentruojamasi ties vertinimo taisyklių suprogramavimu dviem turinio valdymo sistemoms, jų sėkmingu užkrovimu bei tikrinimo ataskaitų ir rekomendacijų pateikimu. Taigi realizacijai galima kelti tokius reikalavimus:

- sukurti programą, įvertinančią nurodytos TVS versijos saugumą;
- suprogramuoti dviejų TVS tikrinimo taisyklių rinkinius;
- pateikti tikrinimo rezultatus, nurodant, kokie nustatymai buvo tikrinami, kurie iš jų reikalavimus tenkina, o kurie – ne;
- jei reikalavimas netenkinamas, pateikti paaiškinimą, kodėl taip yra ir ką reikia padaryti, jog rezultatas būtų teigiamas.

2.7. Išvados

Antrajame darbo skyriuje buvo iškeltas darbo tikslas ir išvardinti uždaviniai.

Buvo aprašyti specifiniai TVS saugumo vertinimo kriterijai. Pagal šiuos kriterijus sudaromos sistemų tikrinimo taisyklės.

Pateiktas turinio valdymo sistemų saugumo kriterijų atitikimą vertinančios programos modelis, panaudojimo atvejų bei veiklos diagramos.

Nustatyti realizacijoje įgyvendinamos programos dalies reikalavimai.

3. TVS SAUGUMO REIKALAVIMŲ TIKRINIMO-VERTINIMO PROGRAMOS REALIZACIJA

Sudarius TVS saugumo kriterijų vertinančios programos modelį, realizacijai pasirinkta jo dalis, kuri užkrauna nurodytos TVS ir jos versijos tikrinimo taisyklių rinkinį bei atlieka tikrinimą, pateikdama ataskaitą, kokie parametrai buvo tikrinami ir ar jie atitiko reikalavimus. Realizuojamai programai keliami reikalavimai pateikiami 2-oje šio darbo dalyje.

Įgyvendinant sistemos realizaciją, buvo sukurta turinio valdymo sistemas pagal konkrečiai TVS sukurtas taisykles tikrinanti programa bei taisyklių rinkiniai Drupal 7.x ir Joomla 2.5.x turinio valdymo sistemoms. Tikrinimo programa parašyta PHP programavimo kalba.

Kaip minėta antrame darbo skyriuje, turinio valdymo sistemos skiriasi tarpusavyje, taip pat skiriasi ir jų pagrindinės distribucijos. Pvz., Drupal 7 versijos (7.1, 7.2 ir t.t.) tarpusavyje panašios, tačiau tarp 6-os ir 7-os versijos yra daug skirtumų. Vien slaptažodžių maišos funkcijos Drupal 7 yra stipriai patobulintos [25].

3.1. Reikalingi įrankiai

Norint patikrinti, ar konkreti TVS versija tenkina specifinius saugumo reikalavimus, reikalingas kompiuteris, kuriame įdiegiama turinio valdymo sistema. Įdiegta TVS – tai praėjusi instaliacijos procesą, kurio metu parengiama turinio valdymo sistemos duomenų bazė ir konfigūracijos failai. Gali būti tikrinama ir žiniatinklio serveryje ilgą laiką veikianti TVS. Tikrinimo programa į duomenų bazę ir konfigūracijos failus kreipiasi tiesiogiai.

Tikrinimo programos valdymui reikalinga žiniatinklio naršyklė. Valdymo sąsaja ypatingų reikalavimų neturi, todėl tinka bet kuri šiuolaikinė naršyklė.

3.2. Programos veikimo aprašymas

Prieš įvertinant turinio valdymo sistemą turi būti žinomas jos pavadinimas bei versija. Tikrinimo taisyklės pritaikomos konkrečiai TVS, nes konfigūravimo parametrų saugojimo vieta gali kisti. Pirmiausia programa patikrina, ar pasirinkta kokia nors TVS ir jos versija. Tada tikrinama, ar pasirinktai versijai yra suprogramuotas taisyklių rinkinys. Jei taip, rinkinys

užkraunamas ir paruošiamas tikrinimui, jei ne – išvedamas klaidos pranešimas. Po to sistema bando prisijungti prie nurodytos duomenų bazės ir/ar nuskaityti konfigūracijos failą.

Tikrinant sistemą, saugumo kriterijai įvertinami paeiliui po vieną tokia tvarka, kokia jie suprogramuoti taisyklių rinkinyje. Priklausomai nuo su saugumu susijusio parametro saugojimo vietos, kreipiamasi į duomenų bazę arba skaitomas konfigūracijos failas.

Toliau pateikiama informacija, kokie reikalingi pradiniai duomenys ir kokie laukiami rezultatai.

3.3. Pradiniai duomenys ir laukiami rezultatai

Pradiniai duomenys yra turinio valdymo sistemos pavadinimo ir jos versijos nurodymas, bei konfigūravimo parametrų įvedimas: kelias iki konfigūracijos failo ir prisijungimo prie duomenų bazės duomenys.

Programa turi grąžinti tikrinimo ataskaitą, kurioje matoma, kas buvo tikrinta ir kokie gauti rezultatai: kurie reikalavimai tenkinami, o kurie – ne. Pastaruoju atveju pateikiama informacija, ką reikia atlikti, jog reikalavimas būtų tenkinamas.

3.4. Kontrolinis pavyzdys

Kontrolinis pavyzdys parodo, jog algoritmo realizacija veikia. Pavyzdžiui pateikti buvo pasirinkta vienos turinio valdymo sistemos versija ir atliktas tikrinimas. Žemiau esančiame pavyzdyje pateikiami ką tik įdiegtos Drupal 7.12 turinio valdymo sistemos tikrinimo rezultatai.

Atlikta kriterijų vertinimų: 18
Atitiko reikalavimus: 3 (16,67%)

Konfigūracijos failo apsauga
Rašymas uždraustas.

Klaidų rodymo režimas
Įjungtas klaidų rodymo režimas.

Sesijos laiko limitas
Nustatytas didesnis nei 30 min. sesijos laiko limitas. Rekomenduojama sesijos laiką sumažinti.

Duomenų bazės lentelių priešdėlis
Nenaudojamas joks duomenų bazės lentelių priešdėlis.

Populiarių naudotojų vardų prisijungimo paieška
Sistemoje yra naudotojas, kurio varde yra frazė "admin".

Atsarginės duomenų kopijos
Neįdiegtas arba neįjungtas "Backup and migrate" modulis. Šis modulis yra skirtas daryti duomenų bazės atsargines kopijas. Jei nenaudojate jokio kito atsarginių kopijų darymo metodo, rekomenduojama pasinaudoti šiuo moduliu.

Turinio revizijų naudojimas
Neįjungtos turinio revizijos turinio tipui "Article".
Neįjungtos turinio revizijos turinio tipui "Basic page".

El. pašto adresų apsauga
Sistemoje nenaudojama el. pašto adresų apsauga. Rekomenduojama įdiegti ir įjungti "Spamspan Filter" arba "Invisimail" modulį.

Failai, kuriuos reikia pašalinti po įdiegimo
Po įdiegimo nepašalinti šie failai: install.php, CHANGELOG.txt, INSTALL.txt, INSTALL.mysql.txt, INSTALL.pgsql.txt, LICENSE.txt, MAINTAINERS.txt, UPGRADE.txt

El. pašto siuntimas per SMTP su autorizacija
Neįdiegtas arba neįjungtas "SMTP Authentication Support" modulis. Jis reikalingas, norint suteikti papildomo saugumo, siunčiant el. paštą.

.htaccess failas ir katalogų apsauga
Options -Indexes aptiktas.

Drupal maišos druskos (hash salt) saugojimo vieta
Rekomenduojama "hash salt" saugoti išoriniame faile, neprieinamame per naršyklės adreso laukelį.

Drupal maišos druskos (hash salt) stiprumas
Naudojama saugi maišos druskos eilutė.

Prisijungimo bandymų ribojimas
Sistemoje gali būti neribojamas prisijungimo bandymų kiekis. Rekomenduojama įdiegti ir įjungti "Flood control" modulį.

Žurnalizavimas (modulis "Syslog")
Neįjungtas arba neįdiegtas "Drupal Syslog" modulis. Šis modulis reikalingas žurnalizavimui.

Žurnalizavimas (modulis "Statistics")
Neįjungtas arba neįdiegtas "Drupal Statistics" modulis. Šis modulis reikalingas žurnalizavimui.

Numatytasis failų katalogas
Pagal nutylėjimą naudojamas viešas failų katalogas. Rekomenduojama naudoti privatų.

Informacija apie galimus atnaujinimus

Neįdiegtas arba neįjungtas "Update manager" modulis. Šis modulis automatiškai tikrina, ar nėra sistemos bei modulių atnaujinimų. Naudojantis šiuo moduliu, naujus modulius galima diegti bei jų atnaujinimus atsisiųsti per administravimo sąsają.

Kaip matoma, tikrinimo priemonė pateikia bendrą informaciją, jog buvo atlikta 18 kriterijų vertinimų, iš kurių 3 atitiko keliamus reikalavimus. Taip pat pateikiama detali ataskaita apie tai, kas buvo tikrinama ir kokie gauti rezultatai. Rezultatuose pateikiami ir patarimai, ką reikia atlikti, jog reikalavimas būtų tenkinamas.

3.5. Sistemos tobulinimo galimybės

Kadangi turinio valdymo sistemų tikrinimas vyksta kreipiantis tiesiai į konfigūracijos failus ir duomenų bazę, programą galima papildyti funkcijomis, kurios aktyviai koreguoja reikiamus parametrus, jog saugumo reikalavimai taptų tenkinami. Tačiau tokiam funkcionalumui pasiekti reikia atlikti papildomų testų ir tyrimų, nes reikia žinoti, kokie tiksliai parametrai koreguojami failuose ar duomenų bazėje, keičiant atitinkamus nustatymus.

Pasyviai vertinant reikalavimo atitikimą, pakanka žinoti vieną kurį nors parametrą ir tikrinti jo reikšmę. Tačiau „iš šalies“ pakeitus jo reikšmę, nėra aišku, ar parametras neįtakoja kurių nors kitų nustatymų. Padarius klaidą, galima sutrikdyti kurio nors komponento ar visos sistemos darbą.

4. SPECIFINIŲ SAUGUMO REIKALAVIMŲ ATITIKIMĄ VERTINANČIOS PROGRAMOS EKSPERIMENTINIS TYRIMAS

Eksperimentinis sistemos tyrimas atliekamas pasinaudojant programinės realizacijos skyriuje aprašyta priemone.

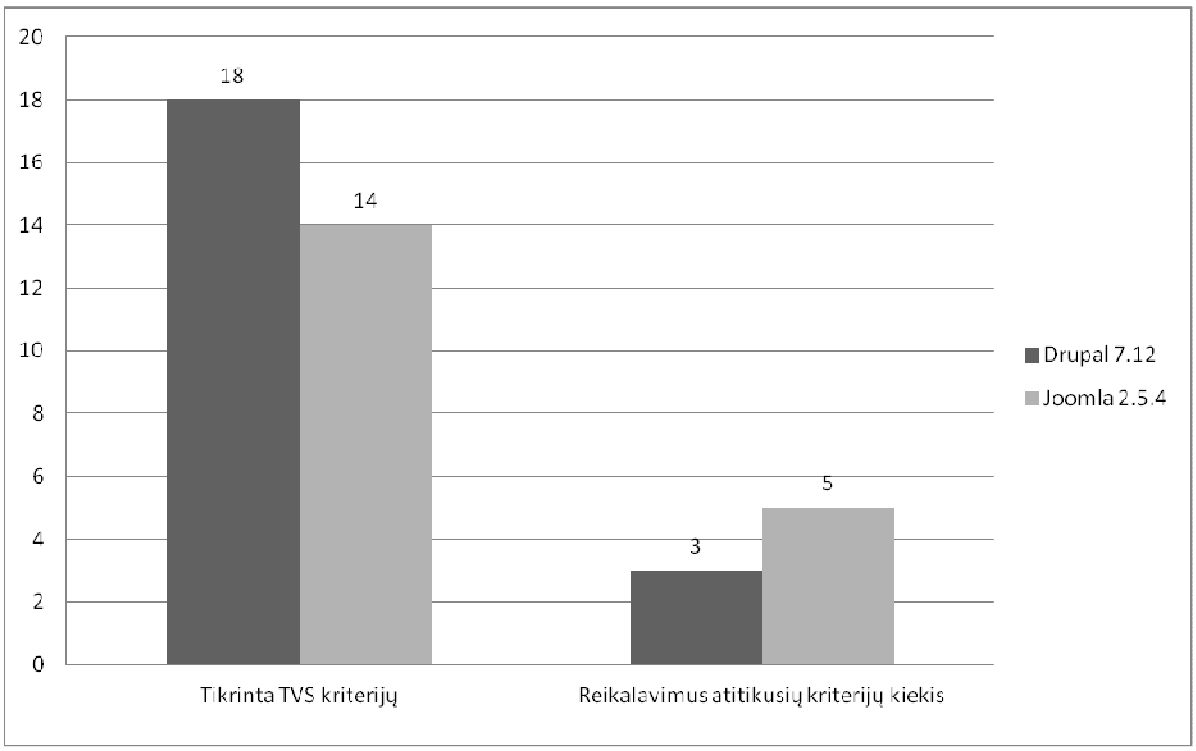
Eksperimento metu siekiama išsiaiškinti, kiek konfigūruota sistema yra saugesnė už nekonfigūruotą. Galimas ir atvirkščias variantas, kai netinkama konfigūracija gali sumažinti saugumą.

Eksperimento metu buvo testuojamos dvi turinio valdymo sistemos – Drupal 7.12 ir Joomla 2.5.4 – iš karto po diegimo. Gavus rezultatus, buvo bandoma pagerinti nurodytus TVS saugumo aspektus, ir tikrinimai atliekami iš naujo.

Paskutinėje eksperimentinio tyrimo dalyje buvo patikrintos dvi veikiančios ir lankomos Drupal TVS pagrindu sukurtos svetainės.

4.1. Nekonfigūruotų turinio valdymo sistemų tikrinimas

14 pav. pateikiami ką tik įdiegtų turinio valdymo sistemų tikrinimo rezultatai.



14 pav. Ką tik įdiegtų turinio valdymo sistemų tikrinimo rezultatai

Galima pastebėti, kad Drupal atveju reikalavimus atitiko 3 iš 18 testų arba 16,66%.

Joomla atveju reikalavimus atitiko 5 iš 14 testų arba 35,71%.

Tikrintų kriterijų kiekis skiriasi, nes, kaip minėta ankstesniuose šio darbo skyriuose, saugumo parametrų kiekis kinta iš vienos TVS į kitą. Pvz., Joomla leidžia išjungti arba įjungti TVS versijos rodymą, o Drupal toks funkcionalumas nenumatytas. Tuo tarpu Drupal turinio valdymo sistemoje galima įjungti modulį, kuris tikrina, ar kitiems įdiegtiems moduliams nėra išleista atnaujinimų. Joomla toks funkcionalumas numatytas branduolyje, todėl šio parametro tikrinti nereikia.

Pilna nekonfigūruotos Drupal sistemos tikrinimo ataskaita pateikiama 1-ame priede, o nekonfigūruotos Joomla TVS – 2-ame priede.

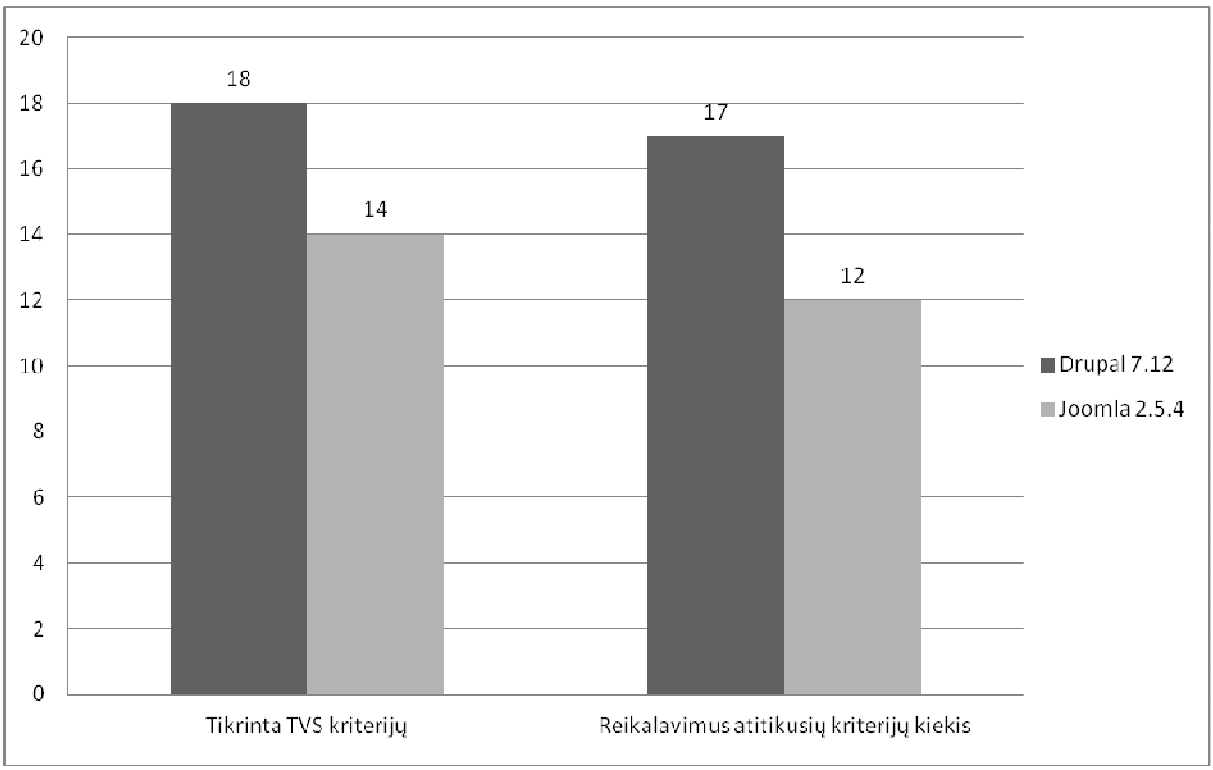
4.2. Konfigūruotų sistemų tikrinimas

Gavęs pirminio tikrinimo rezultatus, administratorius gali pakeisti tam tikrus TVS parametrus, kurie įtakoja saugumą. Po to skenavimas atliekamas dar kartą (15 pav.).

Matoma, kad Drupal atveju pavyko įgyvendinti beveik visus reikalavimus. Įgyvendintų reikalavimų skaičius pakilo nuo 3 iki 17, tai yra, 5,6 karto. Po konfigūravimo buvo tenkinama 17 iš 18 reikalavimų arba 94,44%.

Vienas neįgyvendintas reikalavimas yra duomenų bazės lentelių priešdėlių konfigūravimas, į kurį įeina programavimo arba SQL žinios, kurių paprastas TVS naudotojas gali ir neturėti.

Konfigūruojant Drupal, daugelis pakeitimų, siekiant užtikrinti papildomą saugumą, atliekama lengvai: reikia pakeisti konfigūracijos faile esančias nustatymų reikšmes arba iš administravimo sąsajos pakeisti tam tikrus parametrus ar įdiegti reikiamus modulius. Išimtis gali būti taikoma duomenų bazės lentelių priešdėlių konfigūravimui. Jei priešdėlių naudojimas nebuvo nustatytas diegimo metu, norint tai atlikti, reikia, arba jungtis tiesiai prie duomenų bazės ir pakeisti lentelių pavadinimus, kad jos būtų su priešdėliais, arba parašyti programą (pvz., PHP), kuri jungiasi prie duomenų bazės ir pakeičia kiekvienos lentelės pavadinimą.



15 pav. Konfigūruotų turinio valdymo sistemų tikrinimo rezultatai

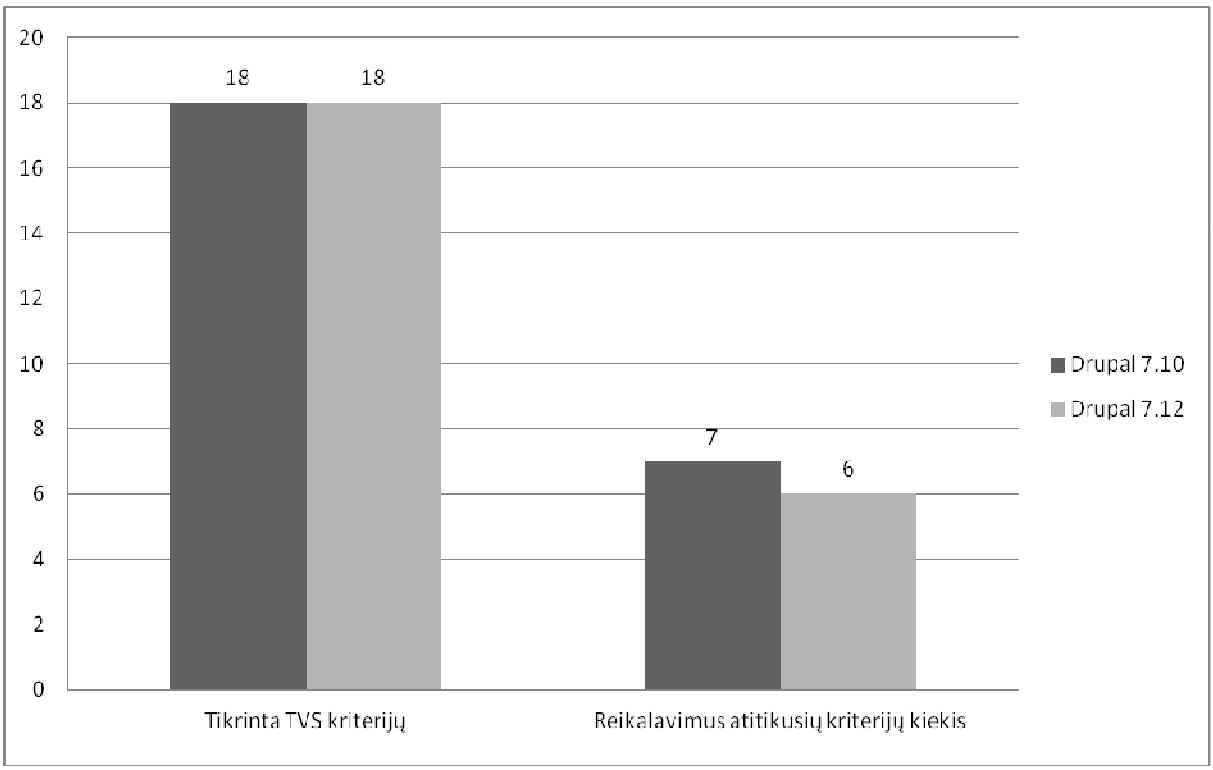
Joomla TVS taip pat buvo gan paprastai konfigūruojama, tačiau siekiant įgyvendinti kai kuriuos reikalavimus, iškilo problemų: nepavyko rasti „Joomla 2.5.x“ versijai pritaikyto turinio versijų kūrimo modulio bei atsarginių kopijų ruošimo modulio. Darbo rašymo metu neseniai buvo įvykęs perėjimas nuo 1.7 versijos į 2.5 versiją, ir trečiųjų šalių modulių programuotojai nespėjo atnaujinti savo produktų.

Po Joomla TVS konfigūravimo tenkinamų reikalavimų skaičius pakilo nuo 5 iki 12 arba 2,4 karto. Taigi tenkinamų reikalavimų buvo 12 iš 14 galimų arba 85,71%.

Pilna konfigūruotos Drupal TVS tikrinimo ataskaita pateikiama 3-iame priede, o konfigūruotos Joomla TVS – 4-ame priede.

4.3. Veikiančių ir lankomų tinklalapių tikrinimas

Šio eksperimento metu siekta išsiaiškinti dviejų internete veikiančių bei lankomų Drupal TVS pagrindu sukurtų svetainių saugumo reikalavimų tenkinimą (16 pav.).



16 pav. Veikiančių ir lankomų Drupal TVS pagrindu sukurtų svetainių tikrinimo rezultatai

Galima pastebėti, jog tenkinamų reikalavimų kiekis yra didesnis nei nekonfigūruotos sistemos atveju (14 pav., Drupal stulpeliai), tačiau iki idealaus rezultato dar gerokai trūksta. Pirmajame tinklalapyje reikalavimus atitikusių kriterijų kiekis buvo 7 iš 18 arba 38,89%, o antrajame buvo tenkinami 6 iš 18 reikalavimų arba 33,33%.

Pirmasis tinklalapis veikia „Drupal 7.12“ TVS versijos pagrindu, o antrasis – „Drupal 7.10“. Tikrinimas pavyko sėkmingai, todėl galima teigti, jog „Drupal 7.x“ algoritmą galima naudoti „Drupal 7“ tarpinėms versijoms tikrinti.

Pilnos abiejų Drupal TVS pagrindu sukurtų tinklalapių tikrinimo ataskaitos pateikiamos 5-ame priede.

4.4. Išvados

Ketvirtajame darbo skyriuje pateikiamas atlikto eksperimentinio tyrimo aprašymas. Tyrimo metu paaiškėjo, jog nekonfigūruotos turinio valdymo sistemos tenkina mažą dalį specifinių saugumo reikalavimų.

Pakeitus TVS konfigūraciją pagal tikrinimo rezultatuose pateiktas rekomendacijas, tenkinamų reikalavimų kiekis išaugo kelis kartus. Konfigūracijos parametrų keitimas nebuvo

sudėtingas, tačiau pasitaikė keletas išimčių, kai rekomendacijos įgyvendinimui reikėjo šiek tiek techninių žinių. Joomla atveju kai kurių reikalavimų nebuvo įmanoma patenkinti, nes dar nebuvo išleista tam reikalingų modulių atnaujinimų.

Eksperimento pabaigoje ištirtos dvi internete veikiančios ir lankomos svetainės. Šio tyrimo metu išsiaiškinta, kad tenkinamų reikalavimų dalis didesnė nei ką tik įdiegtose ir nekonfigūruotose turinio valdymo sistemose, tačiau vis tiek nebuvo tenkinama nė pusės tikrinamų reikalavimų.

5. IŠVADOS

Analizės metu paaiškėjo, kad turinio valdymo sistemų pagrindu sukurtoms svetainėms, kaip ir nuo pagrindų sukurtiems tinklalapiams, gresia panašūs saugumo pavojai: programavimas tarp tinklalapių, užklausų klastojimas tarp tinklalapių, SQL injekcijos, neautorizuota katalogų peržiūra ir pan. Be to, TVS kyla ir tam tikros specifinės saugumo grėsmės: įdiegimo katalogo bei svarbią informaciją atskleidžiančių failų nepašalinimas, sudėtinga diegimo procedūra, neapsaugotas naudotojų įkeltų failų katalogas ir kt.

Taip pat išsiaiškinta, jog standartinės tinklalapių saugumo tikrinimo priemonės negali padėti įvertinti kai kurių specifinių žiniatinklio valdymo sistemoms keliamų saugumo reikalavimų.

Kadangi kiekvienos turinio valdymo sistemos specifinių aspektų konfigūravimas skiriasi, norint įvertinti tam tikrus saugumo parametrus, reikia sudaryti konkrečiai turinio valdymo sistemai ir jos versijai pritaikytą tikrinimo algoritmą.

Buvo sudarytas specifinių saugos kriterijų sąrašas, pateiktas šių kriterijų atitikimą turinio valdymo sistemoje vertinančios programos modelis, o pagal modelio dalį suprogramuotas turinio valdymo sistemos tikrinimo algoritmas, jį pritaikant skirtingoms turinio valdymo sistemoms ir jų versijoms.

Eksperimento dalyje buvo tiriamos dvi populiarios žiniatinklio TVS. Kaip parodė tyrimas, ką tik įdiegtose turinio valdymo sistemose daug specifinių reikalavimų nėra tenkinama. Tačiau po sistemų konfigūravimo rezultatai pagerėja kelis kartus.

Sistemą galima plėsti, įdiegiant papildomo funkcionalumo, kai reikiamus pataisymus atlieka pati tikrinimo programa. Tai yra įmanoma, nes programa turi tiesioginį priėjimą prie duomenų bazės ir failų. Tačiau tai yra aktyvus turinio valdymo sistemos parametrų keitimas pašaline priemone, todėl reikalingi papildomi tyrimai ir testavimas.

NAUDOTA LITERATŪRA

1. **CMS Usage Statistics.** *Web and Internet Technology Usage Statistics* [interaktyvus], [žiūrėta: 2011-01-10], prieiga per internetą: <http://trends.builtwith.com/cms>
2. **Fong, E.; Gaucher R.; Okun, V.; Black, P.E.** *Building a Test Suite for Web Application Scanners,* Hawaii International Conference on System Sciences, Proceedings of the 41st Annual, 2008 m., p. 478-478
3. **Wassermann, G.; Zhendong, U.** *Static Detection of Cross-Site Scripting Vulnerabilities,* ICSE: International Conference on Software Engineering. 2008 m., p. 171-172, 177
4. **Andress, M.** C*ross-Site Scripting, Infoworld,* 2002 m., vol. 25, issue 18., p. 28
5. **Braganza, R.** *Cross-Site Scripting - An Alternative View,* Network Security, 2006 m., vol. 2006, issue 9, p. 19
6. **Fonseca, J.; Vieira, M.; Madeira, H.** *Vulnerability & Attack Injection for Web Applications,* Dependable Systems & Networks, 2009. DSN '09. IEEE/IFIP International Conference. 2009 m., p. 93-102
7. **Morgan, D.** *Web Injection Attacks,* Network Security. 2006 m., vol. 2006, issue 3, p. 8
8. **Monthie, B.** *What, Who, When, Where, Why, How of XSS,* Network World, 2008 m., vol. 25, issue 28, p. 26
9. **Vamosi, R.** *Cross-Site Scripting: An Old problem Returns,* PC World, 2010 m., vol. 28, issue 8, p. 37
10. **Baral, P.** *Web Application Scanners - A Review of Related Articles,* Potentials, IEEE, 2011 m., p. 10-14
11. **Alexenko, T.; Jenne, M.; Roy, S.D.; Wenjun, Zeng.** *Cross-Site Request Forgery: Attack and Defense,* Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE, 2010 m., p. 1
12. **Feil, R.; Nyffenegger, L.,** *Evolution of Cross Site Request Forgery Attacks,* Journal in Computer Virology, 2008 m., vol. 4, p. 61-63
13. **Fong, E.; Okun, V.,** *Web Application Scanners: Definitions and Functions,* System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference, 2007 m., p. 280b-280b
14. **Cheek, G.; Shehab, M.; Truong, Ung.; Williams, E.,** *iLayer: Toward an Application Access Control Framework for Content Management Systems,* Policies for Distributed Systems and Networks (Policy), 2011 IEEE International Symposium, 2011 m., p. 65-72
15. **Wei, K.; Muthuprasanna, M.; Suraj, K.** *Preventing SQL Injection Attacks in Stored Procedures,* Software Engineering Conference, 2006 m., p. 1

16. **Vaidyanathan, G.; Mautone, S.** *Security in Dynamic Web Content Management Systems Applications,* Communications of the ACM; 2009-12, vol. 52, issue 12, p. 121-125
17. **Walikar, R. A.** *Multiple Joomla XSS Vulnerabilities - CVE-2010-1649* [interaktyvus], [žiūrėta: 2011-01-22], prieiga per internetą: <http://riyazwalikar.blogspot.com/2010/06/multiple-joomla-xss-vulnerabilities-cve.html>
18. **FCKeditor CurrentFolder directory traversal** [interaktyvus], [žiūrėta: 2011-01-24], prieiga per internetą: <http://xforce.iss.net/xforce/xfdb/51569>
19. **Joomla 1.5.20 <= Cross Site Scripting (XSS) Vulnerability** [interaktyvus], [žiūrėta: 2011-01-22], prieiga per internetą: <http://seclists.org/fulldisclosure/2010/Oct/109>
20. **Mohorovicic, S.; Tijan, E.; Čisic, D.** *Using Web Content Management Systems in University E-Commerce Courses,* International Journal of Emerging Technologies in Learning, 2010 m., supplement 2, p. 38-42
21. **Ming-Ju Yang; Wen-Chung Chang; Win-Jet Luo; Shou-Ping Hsu; Kao-Feng Yarn; Tsung-Chan Cheng; Po-Chun Yang,** *A User-friendly Web Content Management System,* Innovative Computing Information and Control, 2008. ICICIC '08. 3rd International Conference, 2008 m.
22. **Drupal XSS** [interaktyvus], [žiūrėta: 2011-01-22], prieiga per internetą: <http://security.exabytes.com/2008/07/drupal-xss.html>
23. **Meike, M.; Sametinger, J.; Wiesauer, A.** *Security in Open Source Web Content Management Systems,* Security & Privacy, IEEE, 2009 m., vol. 7, issue 4, p. 44-51
24. **Dobecki, M.; Zabierowski, W.** *Web-based Content Management System,* Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), 2010 International Conference, 2010 m., p. 177-179
25. **Cave, J.** *Drupal 7: Secure password storage by default at last* [interaktyvus], [žiūrėta: 2012-04-29], prieiga per internetą: <http://joncave.co.uk/2011/01/password-storage-in-drupal-and-wordpress/>
26. **Black, E. L.** *Selecting a Web Content Management System for an Academic Library Website,* Information Technology & Libraries, 2011 m., vol. 30, issue 4, p185-189
27. **Acunetix web vulnerability scanner** [interaktyvus], [žiūrėta: 2012-05-02], prieiga per internetą: <http://www.acunetix.com/>
28. **w3af - Web Application Attack and Audit Framework** [interaktyvus], [žiūrėta: 2012-05-02], prieiga per internetą: <http://w3af.sourceforge.net/>
29. **skipfish – web application security scanner** [interaktyvus], [žiūrėta: 2012-05-02], prieiga per internetą: <http://code.google.com/p/skipfish/>

30. **Nikto2** [interaktyvus], [žiūrėta: 2012-05-02], prieiga per internetą: <http://cirt.net/Nikto2>
31. **NTOSpider** [interaktyvus], [žiūrėta: 2012-05-02], prieiga per internetą: <http://www.ntobjectives.com/security-software/ntospider-application-security-scanner/>
32. **What is Joomla** [interaktyvus], [žiūrėta: 2012-05-21], prieiga per internetą: <http://www.joomla.org/about-joomla.html>
33. **About Drupal** [interaktyvus], [žiūrėta: 2012-05-21], prieiga per internetą: <http://drupal.org/about>
34. **TCP/IP Vulnerabilities And Weaknesses** [interaktyvus], [žiūrėta: 2012-05-21], prieiga per internetą: <www.governmentsecurity.org/forum/topic/1753-tcpip-vulnerabilities-and-weaknesses/>

PRIEDAI

1 priedas. Nekonfigūruotos Drupal 7.12 TVS tikrinimo ataskaita

Atlikta kriterijų vertinimų: 18
Atitiko reikalavimus: 3 (16,67%)

Konfigūracijos failo apsauga
Rašymas uždraustas.

Klaidų rodymo režimas
Įjungtas klaidų rodymo režimas.

Sesijos laiko limitas
Nustatytas didesnis nei 30 min. sesijos laiko limitas. Rekomenduojama sesijos laiką sumažinti.

Duomenų bazės lentelių priešdėlis
Nenaudojamas joks duomenų bazės lentelių priešdėlis.

Populiarių naudotojų vardų prisijungimo paieška
Sistemoje yra naudotojas, kurio varde yra frazė "admin".

Atsarginės duomenų kopijos
Neįdiegtas arba neįjungtas "Backup and migrate" modulis. Šis modulis yra skirtas daryti duomenų bazės atsargines kopijas. Jei nenaudojate jokio kito atsarginių kopijų darymo metodo, rekomenduojama pasinaudoti šiuo moduliu.

Turinio revizijų naudojimas
Neįjungtos turinio revizijos turinio tipui "Article".
Neįjungtos turinio revizijos turinio tipui "Basic page".

El. pašto adresų apsauga
Sistemoje nenaudojama el. pašto adresų apsauga. Rekomenduojama įdiegti ir įjungti "Spamspan Filter" arba "Invisimail" modulį.

Failai, kuriuos reikia pašalinti po įdiegimo
Po įdiegimo nepašalinti šie failai: install.php, CHANGELOG.txt, INSTALL.txt, INSTALL.mysql.txt, INSTALL.pgsql.txt, LICENSE.txt, MAINTAINERS.txt, UPGRADE.txt

El. pašto siuntimas per SMTP su autorizacija
Neįdiegtas arba neįjungtas "SMTP Authentication Support" modulis. Jis reikalingas, norint suteikti papildomo saugumo, siunčiant el. paštą.

.htaccess failas ir katalogų apsauga
Options -Indexes aptiktas.

Drupal maišos druskos (hash salt) saugojimo vieta
Rekomenduojama "hash salt" saugoti išoriniame faile, neprieinamame per naršyklės adreso laukelį.

Drupal maišos druskos (hash salt) stiprumas
Naudojama saugi maišos druskos eilutė.

Prisijungimo bandymų ribojimas
Sistemoje gali būti neribojamas prisijungimo bandymų kiekis. Rekomenduojama įdiegti ir įjungti "Flood control" modulį.

Žurnalizavimas (modulis "Syslog")
Neįjungtas arba neįdiegtas "Drupal Syslog" modulis. Šis modulis reikalingas žurnalizavimui.

Žurnalizavimas (modulis "Statistics")
Neįjungtas arba neįdiegtas "Drupal Statistics" modulis. Šis modulis reikalingas žurnalizavimui.

Numatytasis failų katalogas
Pagal nutylėjimą naudojamas viešas failų katalogas. Rekomenduojama naudoti privatų.

Informacija apie galimus atnaujinimus
Neįdiegtas arba neįjungtas "Update manager" modulis. Šis modulis automatiškai tikrina, ar nėra sistemos bei modulių atnaujinimų. Naudojantis šiuo moduliu, naujus modulius galima diegti bei jų atnaujinimus atsisiųsti per administravimo sąsają.

---

2 priedas. Nekonfigūruotos Joomla 2.6.4 TVS tikrinimo ataskaita

Atlikta kriterijų vertinimų: 14
Atitiko reikalavimus: 5 (35,71%)

Konfigūracijos failo apsauga
Neuždraustas rašymas į konfigūracijos failą.

Klaidų rodymo režimas
Įjungtas klaidų rodymo režimas.

Sesijos laiko limitas
Sesijos laikas 30 min arba trumpesnis.

Duomenų bazės lentelių priešdėlis
Naudojamas nestandartinis duomenų bazės lentelių priešdėlis.

Populiarių naudotojų vardų prisijungimo paieška
Sistemoje yra naudotojas, kurio varde yra frazė "admin".

Atsarginės duomenų kopijos
Neaptikta jokio atsarginių kopijų ruošimo modulio. Rekomenduojama įdiegti "Backup" arba "Sypex" modulį.

Turinio revizijų naudojimas
Nenaudojamos turinio revizijos. Jei yra galimybė, rekomenduojama įjungti "Simple content versioning" modulį.

El. pašto siuntimas per SMTP su autorizacija
Nenaudojamas el. pašto siuntimas per SMTP su serverio autorizacija.

El. pašto adresų apsauga
El. pašto adresų apsauga įjungta.

Failai, kuriuos reikia pašalinti po įdiegimo
Po įdiegimo nepašalinti šie failai: README.txt, LICENSE.txt

.htaccess failas ir katalogų apsauga
Aptikta, kad nenaudojamas .htaccess failas. Šis failas gali suteikti papildomą katalogų apsaugą. Joomla! diegimo kataloge turėtų būti failas htaccess.txt, kurį reikia pervadinti į .htaccess.

Htaccess.txt failas
Aptikta, kad Joomla! diegimo kataloge yra htaccess.txt failas. Šį failą reikia pervadinti į .htaccess arba pašalinti iš viso.

TVS versijos rodymas
TVS versija nerodoma.

Prisijungimas prie FTP
Prisijungimo duomenys faile nesaugomi.

3 priedas. Konfigūruotos Drupal 7.12 TVS tikrinimo ataskaita

Atlikta kriterijų vertinimų: 18
Atitiko reikalavimus: 17 (94,44%)

Konfigūracijos failo apsauga
Rašymas uždraustas.

Klaidų rodymo režimas
Klaidų pranešimai nerodomi

Sesijos laiko limitas
Sesijos laikas 30 min arba trumpesnis.

Duomenų bazės lentelių priešdėlis
Nenaudojamas joks duomenų bazės lentelių priešdėlis.

Populiarių naudotojų prisijungimo vardų paieška
Sistemoje populiarių naudotojų prisijungimo vardų nerasta.

Atsarginės duomenų kopijos
Atsarginių kopijų ruošimo modulis įjungtas

Turinio revizijų naudojimas
Revizijos įjungtos visiems turinio tipams.

El. pašto adresų apsauga
El. pašto adresų apsauga įjungta.

Failai, kuriuos reikia pašalinti po įdiegimo
Visi failai pašalinti.

El. pašto siuntimas per SMTP su autorizacija
El. pašto siuntimo per SMTP modulis įjungtas.

.htaccess failas ir katalogų apsauga

Options -Indexes aptiktas.

Drupal maišos druskos (hash salt) stiprumas
Naudojama saugi maišos druskos eilutė.

Drupal maišos druskos (hash salt) saugojimo vieta
Aptikta, kad hash salt saugoma išoriniame faile.

Prisijungimo bandymų ribojimas
Įdiegtas prisijungimo bandymų ribojimo modulis.

Žurnalizavimas (modulis "Syslog")
Modulis "Syslog" įjungtas.

Žurnalizavimas (modulis "Statistics")
Modulis "Statistics" įjungtas.

Numatytasis failų katalogas
Pagal nutylėjimą naudojamas privatus failų katalogas.

Informacija apie galimus atnaujinimus
Automatiniam atnaujinimų tikrinimui reikalingas modulis įjungtas.

4 priedas. Konfigūruotos Joomla 2.6.4 TVS tikrinimo ataskaita

Atlikta kriterijų vertinimų: 14
Atitiko reikalavimus: 12 (85,71%)

Konfigūracijos failo apsauga
Rašymas uždraustas.

Klaidų rodymo režimas
Klaidų pranešimai nerodomi.

Sesijos laiko limitas
Sesijos laikas 30 min arba trumpesnis.

Duomenų bazės lentelių priešdėlis
Naudojamas nestandartinis duomenų bazės lentelių priešdėlis.

Populiarių naudotojų prisijungimo vardų paieška
Sistemoje populiarių naudotojų prisijungimo vardų nerasta.

Atsarginės duomenų kopijos
Neaptikta jokio atsarginių kopijų ruošimo modulio. Jei yra galimybė, rekomenduojama įdiegti "Backup" arba "Sypex" modulį.

Turinio revizijų naudojimas
Nenaudojamos turinio revizijos. Jei yra galimybė, rekomenduojama įjungti "Simple content versioning" modulį.

El. pašto siuntimas per SMTP su autorizacija

El. pašto siuntimo per SMTP modulis įjungtas.

El. pašto adresų apsauga
El. pašto adresų apsauga įjungta.

Failai, kuriuos reikia pašalinti po įdiegimo
Visi failai pašalinti.

.htaccess failas ir katalogų apsauga
.htaccess failas naudojamas, ir "Options -Indexes" taisyklė aptikta.

Htaccess.txt failas
htaccess.txt failo nerasta.

TVS versijos rodymas
TVS versija nerodoma.

Prisijungimas prie FTP
Prisijungimo duomenys faile nesaugomi.

5 priedas. Veikiančių ir lankomų tinklapių tikrinimo ataskaita

1-as tinklapis	2-as tinklapis
Atlikta kriterijų vertinimų: 18 **Atitiko reikalavimus: 7 (38,89%)**	**Atlikta kriterijų vertinimų: 18** **Atitiko reikalavimus: 6 (33,33%)**
Konfigūracijos failo apsauga Rašymas uždraustas.	**Konfigūracijos failo apsauga** Rašymas uždraustas.
Klaidų rodymo režimas Klaidų pranešimai nerodomi	**Klaidų rodymo režimas** *Įjungtas klaidų rodymo režimas. Galutinėje versijoje klaidų rodymą rekomenduojama išjungti.*
Sesijos laiko limitas *Nustatytas didesnis nei 30 min. sesijos laiko limitas. Rekomenduojama sesijos laiką sumažinti.*	**Sesijos laiko limitas** *Nustatytas didesnis nei 30 min. sesijos laiko limitas. Rekomenduojama sesijos laiką sumažinti.*
Duomenų bazės lentelių priešdėlis *Nenaudojamas joks duomenų bazės lentelių priešdėlis.*	**Duomenų bazės lentelių priešdėlis** *Nenaudojamas joks duomenų bazės lentelių priešdėlis.*
Populiarių naudotojų vardų prisijungimo paieška *Sistemoje yra naudotojas, kurio varde yra frazė "admin".*	**Populiarių naudotojų vardų prisijungimo paieška** *Sistemoje yra naudotojas, kurio varde yra frazė "admin".*
Atsarginės duomenų kopijos *Neįdiegtas arba neįjungtas "Backup and migrate" modulis. Šis modulis yra skirtas daryti duomenų bazės atsargines kopijas. Jei nenaudojate jokio kito atsarginių kopijų*	**Atsarginės duomenų kopijos** *Neįdiegtas arba neįjungtas "Backup and migrate" modulis. Šis modulis yra skirtas daryti duomenų bazės atsargines kopijas. Jei nenaudojate jokio kito atsarginių kopijų darymo metodo,*

darymo metodo, rekomenduojama pasinaudoti šiuo moduliu.

Turinio revizijų naudojimas
Neįjungtos turinio revizijos turinio tipui "Article".
Neįjungtos turinio revizijos turinio tipui "Bėganti eilutė".
Neįjungtos turinio revizijos turinio tipui "Book page".
Neįjungtos turinio revizijos turinio tipui "FAQ".
Neįjungtos turinio revizijos turinio tipui "Forum topic".
Neįjungtos turinio revizijos turinio tipui "Lankytinos vietos".
Neįjungtos turinio revizijos turinio tipui "Leidiniai".
Neįjungtos turinio revizijos turinio tipui "Naujienos".
Neįjungtos turinio revizijos turinio tipui "Panel".
Neįjungtos turinio revizijos turinio tipui "Pirmo puslapio besikeičiančios nuotraukos".
Neįjungtos turinio revizijos turinio tipui "Poll".
Neįjungtos turinio revizijos turinio tipui "Reklaminiai baneriai".
Neįjungtos turinio revizijos turinio tipui "Renginiai".
Neįjungtos turinio revizijos turinio tipui "Review".
Neįjungtos turinio revizijos turinio tipui "Šoniniai meniu punktai".
Neįjungtos turinio revizijos turinio tipui "TIC paslaugos".
Neįjungtos turinio revizijos turinio tipui "Turinys su vaizdo grotuvu".
Neįjungtos turinio revizijos turinio tipui "Vaizdų pavadinimai".

El. pašto adresų apsauga
Sistemoje nenaudojama el. pašto adresų apsauga. Rekomenduojama įdiegti ir įjungti "Spamspan Filter" arba "Invisimail" modulį.

Failai, kuriuos reikia pašalinti po įdiegimo
Po įdiegimo nepašalinti šie failai: install.php, CHANGELOG.txt, INSTALL.txt, INSTALL.mysql.txt, INSTALL.pgsql.txt, LICENSE.txt, MAINTAINERS.txt, UPGRADE.txt

El. pašto siuntimas per SMTP su autorizacija
Neįdiegtas arba neįjungtas "SMTP Authentication Support" modulis. Jis rekomenduojama pasinaudoti šiuo moduliu.

Turinio revizijų naudojimas
Neįjungtos turinio revizijos turinio tipui "Article".
Neįjungtos turinio revizijos turinio tipui "Book page".
Neįjungtos turinio revizijos turinio tipui "Contacts".
Neįjungtos turinio revizijos turinio tipui "FAQ".
Neįjungtos turinio revizijos turinio tipui "Forum topic".
Neįjungtos turinio revizijos turinio tipui "Front page image slider".
Neįjungtos turinio revizijos turinio tipui "News".
Neįjungtos turinio revizijos turinio tipui "Panel".
Neįjungtos turinio revizijos turinio tipui "Poll".
Neįjungtos turinio revizijos turinio tipui "Review".

El. pašto adresų apsauga
Sistemoje nenaudojama el. pašto adresų apsauga. Rekomenduojama įdiegti ir įjungti "Spamspan Filter" arba "Invisimail" modulį.

Failai, kuriuos reikia pašalinti po įdiegimo
Po įdiegimo nepašalinti šie failai: install.php, CHANGELOG.txt, INSTALL.txt, INSTALL.mysql.txt, INSTALL.pgsql.txt, LICENSE.txt, MAINTAINERS.txt, UPGRADE.txt

El. pašto siuntimas per SMTP su autorizacija
Neįdiegtas arba neįjungtas "SMTP Authentication Support" modulis. Jis reikalingas, norint suteikti papildomo saugumo, siunčiant el. paštą.

.htaccess failas ir katalogų apsauga
Options -Indexes aptiktas.

Drupal maišos druskos (hash salt) saugojimo vieta
Rekomenduojama "hash salt" saugoti išoriniame faile, neprieinamame per naršyklės adreso laukelį.

Drupal maišos druskos (hash salt) stiprumas
Naudojama saugi maišos druskos eilutė.

Prisijungimo bandymų ribojimas
Sistemoje gali būti neribojamas prisijungimo bandymų kiekis. Rekomenduojama įdiegti ir įjungti "Flood control" modulį.

Žurnalizavimas (modulis "Syslog")
Modulis "Syslog" įjungtas.

Žurnalizavimas (modulis "Statistics")
Modulis "Statistics" įjungtas.

Numatytasis failų katalogas

reikalingas, norint suteikti papildomo saugumo, siunčiant el. paštą. **.htaccess failas ir katalogų apsauga** Options -Indexes aptiktas. **Drupal maišos druskos (hash salt) saugojimo vieta** *Rekomenduojama "hash salt" saugoti išoriniame faile, neprieinamame per naršyklės adreso laukelį.* **Drupal maišos druskos (hash salt) stiprumas** Naudojama saugi maišos druskos eilutė. **Prisijungimo bandymų ribojimas** *Sistemoje gali būti neribojamas prisijungimo bandymų kiekis. Rekomenduojama įdiegti ir įjungti "Flood control" modulį.* **Žurnalizavimas (modulis "Syslog")** Modulis "Syslog" įjungtas. **Žurnalizavimas (modulis "Statistics")** Modulis "Statistics" įjungtas. **Numatytasis failų katalogas** *Pagal nutylėjimą naudojamas viešas failų katalogas. Rekomenduojama naudoti privatų.* **Informacija apie galimus atnaujinimus** Automatiniam atnaujinimų tikrinimui reikalingas modulis įjungtas.	*Pagal nutylėjimą naudojamas viešas failų katalogas. Rekomenduojama naudoti privatų.* **Informacija apie galimus atnaujinimus** Automatiniam atnaujinimų tikrinimui reikalingas modulis įjungtas.