TARTU ÜLIKOOL
LOODUS- JA TÄPPISTEADUSTE VALDKOND
Arvutiteaduse instituut
Informaatika õppekava

Ted Edward Õunap

Veebisaidi loomine ettevõttele Rigor OÜ

Bakalaureusetöö (9 EAP)

Juhendaja: Ljubov Jaanuska

Kaasjuhendaja: Lidia Feklistova

Tartu 2018

Veebisaidi loomine ettevõttele Rigor OÜ

Lühikokkuvõte:

Käesoleva bakalaureusetöö eesmärgiks on luua uus veebisait ettevõttele Rigor OÜ. Töö sisaldab vana veebisaidi analüüsi ja kliendi poolt kehtestatud nõudeid. Töö käsitleb veebisaidi turvalisuse aspekte, annab ülevaate kasutatud tehnoloogiatest ning tehtud tööst.

Võtmesõnad:

Rigor OÜ, WordPress, Bootstrap, turvalisus

CERCS: P175 Informaatika

Creating a website for Rigor OÜ

Abstract:

The goal of the present thesis is to create a new website for Rigor OÜ. The thesis contains an analysis of the old website, client requirement for the new website, website security aspects, an overview of the used technologies and the work done.

Keywords:

Rigor OÜ, WordPress, Bootstrap, security

CERCS: P175 Informatics

Sisukord

Sissejuhatus

Rigor OÜ on 1992. aastal asutatud tellimuste alusel käsitöömööblit valmistav ettevõte Eestis. Viimastel aastatel on suuremat rõhku pandud avaliku sektori tellimustele. Firma klientidele/partneritele nähtavamaks ja kättesaadavamaks muutmiseks pööras firma tähelepanu veebikanalitele ja võimalustele.

Firma vana veebisait on jäänud poolikuks nii sisult, kui ka ülesehituselt. Infoajastu mõjutusel otsustas firma oma veebisaidile suuremat rõhku pöörata. Firma soovib lihtsasti hallatavat veebisaiti, mille haldamine oleks neile endile jõukohane (ei nõua suuri eelteadmisi veebiarenduses). Selle tagamiseks otsustati kasutada sisuhaldussüsteemi WordPress koos selle juurde kuuluvate lisadega.

Antud bakalaureusetöö raames valmis Rigor OÜ-le uus veebisait, millega asendatakse vana veebisait (www.rigor.ee). Töö esimeses peatükis tutvustatakse töös esinevaid mõisteid ja termineid; teises peatükis vaadeldakse vana veebisaiti; kolmandas peatükis tuuakse välja kliendi nõuded uuele veebisaidile. Töö neljas peatükk räägib sisuhaldussüsteemidest ja käsitleb kasutatud tehnoloogiaid; viies peatükk käsitleb veebisaidi turvalisust ning kuuendas peatükis kirjeldatakse uut veebisaiti.

1 Mõisted ja terminid

Käesolevas peatükis on antud peamised töös kasutatavad mõisted ja terminid.

Back end – „tagasüsteem, tagakomponent vms, sõltuvalt kontekstist; kasutajale nähtamatu töötlev, talletav, käitlev jne põhiosa" [1].

Back-up – varundama [2].

Front end – „eessüsteem, eeskomponent vms, sõltuvalt kontekstist; inimkasutajat või kasutavat süsteemi tagaosaga liidestav osa" [3].

Jõurünne (ingl *brute-force*) – „parooli, krüptovõtme vms mõistatamine kõigi võimalike variantide läbiproovimise teel" [4].

Kujundusteema (ingl *theme*) – failide kogum, mis loob veebilehe graafilise liidese ja lisab veebilehele funktsionaalsust [5].

Liugur (ingl *slider*) - automaatne slaidiesitlus.

Open-source – tarkvara, mille lähtekood on kasutajale kättesaadav uurimiseks, muutmiseks ja sellest midagi uut tuletamiseks [6].

Pistikprogramm (ingl *plugin)* – hõlpsalt installeeritav olemasoleva tarkvarakomponendi võimalusi laiendav lisandprogramm [7].

Postitus – blogi sissekanne.

Sisuhaldussüsteem (ingl *content-management system*) – „tarkvara, mis hõlbustab teabesisu (võrgus) kirjastamist, redigeerimist ja muutmist, võimaldades vastavate töövoogude haldust rühmatöö keskkonnas" [8].

2 Rigor OÜ taust ja vana veebisait

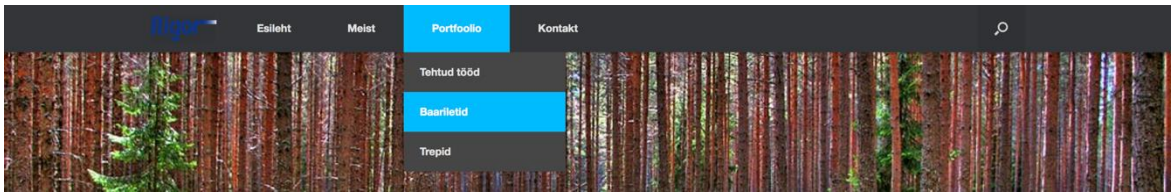
Käesolevas peatükis tutvustatakse ettevõtet Rigor OÜ, kirjeldatakse vana veebisaiti ja põhjendatakse uue veebisaidi vajadust.

Rigor OÜ on 1992. aastal asutatud tellimuste alusel käsitöömööblit valmistav ettevõte Eestis. Tootmine toimub Pärnumaal, Tori vallas. Firma tegevusvaldkonda kuuluvad eramute mööbli ja avaliku ruumi sisustuse valmistamine ja paigaldamine. Viimastel aastatel on suuremat rõhku pandud avaliku sektori tellimustele. Firma tehtud tööde hulka kuuluvad näiteks Lottemaa, Pärnu erinevad majutusasutused ja pubid/baarid üle Eesti.

Vana veebisait on valminud 2014. aastal (www.rigor.ee). Selle peamiseks eesmärgiks oli tutvustada külastajatele teostatud töid ja tegevusvaldkondi. Lisaks sellele pidi veebisait andma edasi piisavalt infot tootmise ja tellimise kohta. Vana veebisaidi loomisel on eelmine autor kasutanud olemasolevat WordPressi tasuta teemat „Vantage" ja tasuta pistikprogramme. MySQL-i andmebaasi kasutati läbi phpMyAdmin töövahendi, mida haldas veebisaidi autor. Enamus lehe sisust on lisatud läbi WordPressi sisuhaldussüsteemi. Serverisse paigaldati antud hetkel kõige uuem WordPressi versioon (mida sai läbi WordPressi töölaua uuendada), vajaminev teema ja kujunduseks vajalikud failid.

2.1 Navigeerimine vanal veebisaidil

Vana veebisaidi navigeerimisribal on firma logo (toimib kui *home* nupp), neli lehte („Esileht", „Meist", „Portfoolio", „Kontakt") ja otsingu võimalus (vt Joonis 1).

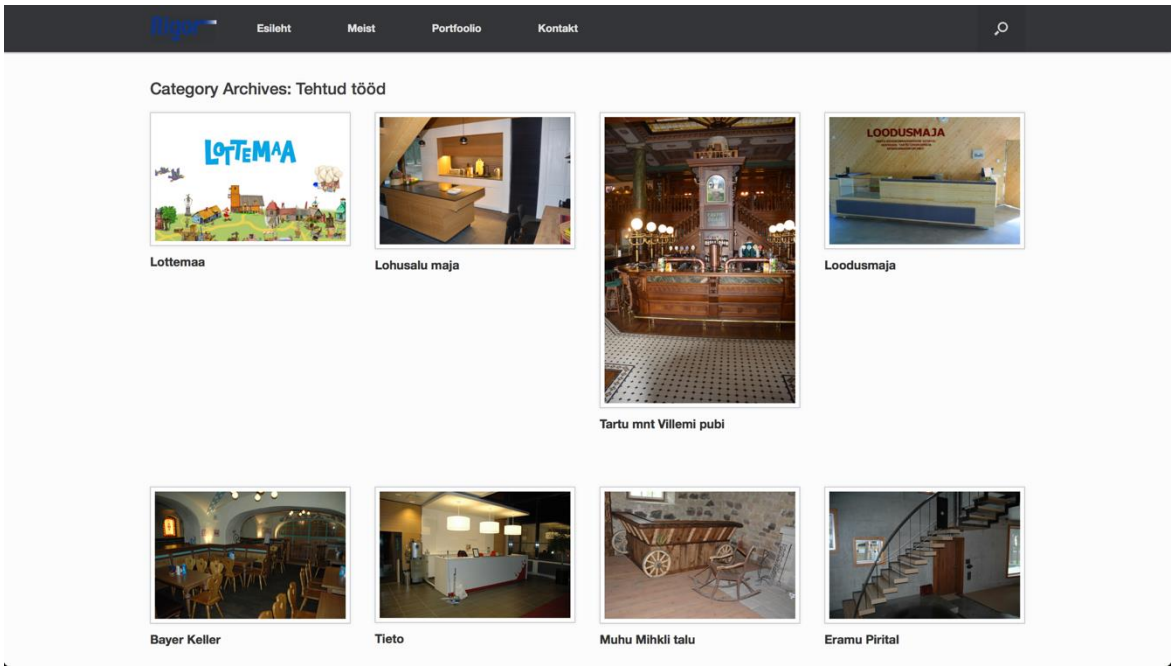


Joonis 1. Vana veebisaidi navigeerimiriba

Portfoolio leht jaguneb kolmeks alamleheks („Tehtud tööd", „Baariletid" ja „Trepid"). Sellest alammenüüst on „Baariletid" leht valesti suunatud, sest see suunab lehele, kus on pilt trepist. Navigeerimisribal asuv firma logo on raskesti loetav (liiga tume kiri koos tumeda taustaga, logol on taustavärv mis erineb navigeerimisriba taustast) ja rikub kogu ülejäänud navigeerimisriba visuaali.

2.2 „Portfoolio" leht ja eraldi galerii lehed

Firma veebisaidi peamine eesmärk on tehtud tööde esitlemine ja seetõttu peaks portfoolio leht olema visuaalselt silmapaistva kujundusega ja kasutajale mugav kasutada. Lehel „Portfoolio" – „Tehtud tööd" on ühel tehtud tööl vertikaalpaigutusega pilt ja see lükkab järgmist postituste rida allapoole, jättes tühja ruumi (vt Joonis 2).



Joonis 2. „Tehtud tööde" lehekülg

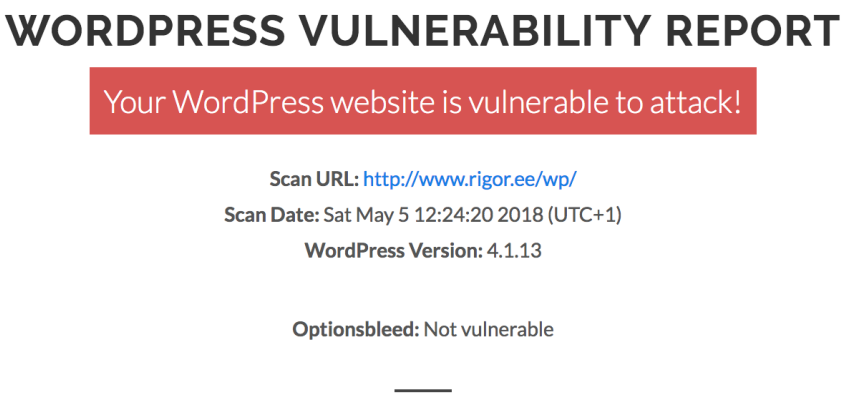
Kui ülejäänud veebisait on eestikeelne, siis „Portfoolio" alamlehtedele on jäetud enne alamlehe nimetust ingliskeelne sõnapaar „Category Archives: ", mis jätab veebisaidi üles-ehitusest ebaprofessionaalse mulje. „Portfoolio" – „Trepid "lehekülg on tühi ja kuvab ainult pealkirja. Alamgaleriides on näha, et osad pildid on skaleerimata ja avanedes tuleb korralikult lehes välja suumida, et näha tervet pilti.

2.3 Muud vead veebisaidil

Järgnevalt on toodud välja vana veebisaidi muud puudused:

1. avalehe liuguril on üks pilt, aga kursoriga peale liikudes kuvatakse mõlemas ääres noole kujutisi;
2. avalehel on osa infost jäänud poolikuks;
3. alamlehtedel on kohati vähe infot ja liiga palju tühja ruumi;
4. veebisaidilt puudub otse maili saatmise võimalus;

5. „Info” lehel asuvad mailiaadressid ei reageeri peale vajutamisele (vormistatud tavatekstina);
6. veebisaidi jalus muudab oma suurust vastavalt sisu hulgale (mida vähem sisus seda pikemaks ennast venitab) ja see tekitab suure kontrastierinevuse osadel alamlehtedel;
7. vana veebisaidi galeriis avanevad pildid ei reageeri aknasuuruse muutmisele;
8. vana veebisait ei ole turvaline (vt Joonis 3) [9].



Joonis 3. Vanale veebisaidile tehtud WPScans

2.4 Analüüsi tulemused

Vanal veebisaidil on palju pisimaid ja suuremaid vigu, mis on seotud olemasoleva kujundusteemaga ja pistikprogrammidega. Vigade parandamiseks, muutmiseks ja täiendamiseks peaks looma uue alamkujundusteema. Seetõttu otsustasid klient ja töö autor luua uue kujundusteema. Järgnevas peatükis on kirjeldatud kliendi poolt seatud nõuded uuele veebisaidile.

3 Kliendi nõuded uuele veebisaidile

Kliendiga koostöös valmis uuele veebisaidile seatud nõuete loetelu. Kliendiga suhtlemine oli perioodiliti keeruline, sest muud projektid olid kliendile prioriteetsemad kui uue veebisaidi loomine. Klient eelistas visuaalselt sarnast veebisaiti, kuid andis veebisaidi kujunduse osas vabad käed antud bakalaureusetöö autorile. Veebisaidi kujunduseks loodi ja võrreldi mitmeid kavandeid, mille seast klient valis endale kõige meelepärasema. Kujundusteema loomisel oli kliendile oluline lihtne info lisamise ja muutmise võimalus.

3.1 Kliendi nõuete loetelu uuele veebisaidile

Allpool on toodud kliendi poolt esitatud nõuded loodavale veebisaidile:

- esileht annab selge ülevaate firma tegevusvaldkonnast.
- „Kontakt" lehelt on otse võimalik saata e-mail, mis sisaldab külastaja nime, meiliaadressi, sõnumi teemat ja sisu. Kui vorm on valesti täidetud, siis reageeritakse teatud viisil:
    - kui külastaja ei täida kõiki kohustuslikke välju, siis annab veebisait vastava veateate;
    - kõik kohustuslikud väljad peavad olema täidetud korrektselt (põhirõhk mailiaadressi väljal);
    - peale korrektset täitmist ja saatmist kuvatakse teade, mis kinnitab kas kiri sai edastatud või annab vastava veateate;
- veebisaidil on firma juriidilised andmed ja kontaktandmed;
- „Tehtud tööd" lehel kuvatakse kõiki tehtud tööde postituste tunnuspilte;
- veebisait peab olema mobiilisõbralik;
- veebisaiti on lihtne kasutada olenemata seadmest;
- info leidmine peab olema lihtne ja konkreetne.

Nõuete täitmiseks veebisaidil jagati töö kolmeks etapiks – kõigepealt visuaalselt alamlehed paika, seejärel hakati neisse funktsionaalseid omadusi implementeerima ja viimasena korrektset sisu postituste näol.

4 Kasutatud tehnoloogiad

Alljärgnevas peatükis tutvustatakse veebisaidi loomisel kasutatud tehnoloogiaid ning põhjendatakse nende kasutamist.

4.1 Sisuhaldustarkvarad

Sisuhaldustarkvara on sisu haldamise rakendus, mis võimaldab erinevate õigustega kasutajatel hallata veebisaidi sisu (näiteks luua või muuta) ilma, et kasutaja omaks põhjalikke teadmisi veebiarendusest ja veebitehnoloogiatest. Samuti säästab sisuhaldustarkvara kasutamine aega, sest *back-end* osa on juba loodud, tuleb vaid lisada kujundus ja sisu. [10]

1and1 [11] veebisaidi järgi on viis kõige populaarsemat *open-source* sisuhaldustarkvara WordPress, Joomla!, Drupal, TYPO3 ja Contao. Järgnevalt tuuakse välja nende sisuhaldustarkvarade plussid ja miinused vastavalt 1and1 [11] veebisaidile.

WordPress on kõige laialdasemalt levinud sisuhaldustarkvara maailmas umbes 18 miljoni installeerimisega. WordPressis on üle 14 000 tasuta kujundusteema ja üle 18 000 lisa, mis hõlmavad avaldamist ja haldamist soodustavaid töövahendeid [11].

WordPressi miinusteks loetakse seda, et sisuhaldussüsteemi funktsiooni täitmiseks on vaja lisa töövahendeid, pistikprogrammidel võivad esineda turvaaugud, kõrge külastatavus võib põhjustada ebastabiilsust lehe toimimises ja tihedad turvalisuse uuendused nõuavad lisa administreerimist [11].

Wordpressi plussideks on suur kommuun, kes pidevalt arendab uusi võimalusi. Paigaldamine on lihtne ja kiire, kasutajaliides muudab veebisaidi sisu haldamise lihtsaks, ja pistikprogrammide ning muude lisade integreerimine on tehtud väga lihtsaks. [11]

2,5 miljoni paigaldusega **Joomla!** on suuruselt teine sisuhaldustarkvara. Tarkvara kasutamine on keerulisem kui WordPressil, kuid erinevalt WordPressist on Joomla! funktsionaalsus ilma lisadeta kohe olemas [11].

Joomla! miinusteks loetakse ebaadekvaatset õiguste haldamist, lisatöövahendid võivad olla kallid ja nende implementeerimine nõuab tihti rohkem tööd [11].

Plussideks on küllaltki lihtne paigaldamine, suur valik lisasid ja disaine ning kasutajasõbralik teema loomine [11].

Drupal on väga lihtsa baaspaigaldusega sisuhaldustarkvara, mida saab laiendada läbi moodulite. Baaspaigaldusele lisaks on rohkem kui 36 000 laiendusmoodulit [11].

Miinusteks on keerukas seadistamine seoses nõrga *back-end* ühilduvusega. Baaspaigaldus vajab palju lisade paigaldamist, ja mooduleid on võimalik paigaldada ainult läbi serveri. Plussideks on kompakte tarkvara, suur valik lisasid ja mitme domeeni haldamise tugi. [11]

TYPO3 on mõeldud ettevõtetele sisu haldamiseks. Ta on väga hea valik suurte korporatsioonide portaalidele ja e-poe platvormidele [11].

Miinusena nõuab TYPO3 veebiarenduse oskusi ja teadmisi, et implementeerida, muuta ja administreerida veebisaiti. Tema suur funktsionaalsus tõstab nõudmisi serveri poole pealt, ja väljaõpe TYPO3 kasutamiseks on ajamahukas protsess. [11]

Plussideks on suur arendajate kommuun, palju erinevaid funktsioone, paindlikkus ja võimalus laiendada lehte. [11]

Contao on lihtne ja kasutajasõbralik sisuhaldustarkvara. Süsteem on intuitiivne, *back-end* on mitmekeelne, ja administreerimise kiht on lihtne ja selge. [11]

Miinustena tuuakse välja, et Contao ei sobi keerukamatele veebisaitidele. Tarkvara ei toeta mitmetasandilisi lehti ja tal on küllaltki väike kasutajaskond. Plussidena on hästi toimiv arhitektuur, kasutajasõbralik paigaldus ja haldamine ning hea turvalisus. [11]

Analüüsides kõigi populaarsete sisuhaldussüsteemide plusse ja miinuseid ning arvestades kliendi nõudeid otsustas töö autor koostöös kliendiga jääda WordPressi juurde, sest sellega on kliendil kokkupuude olemas ja selle haldamine läbi WordPressi töölaua on lihtne.

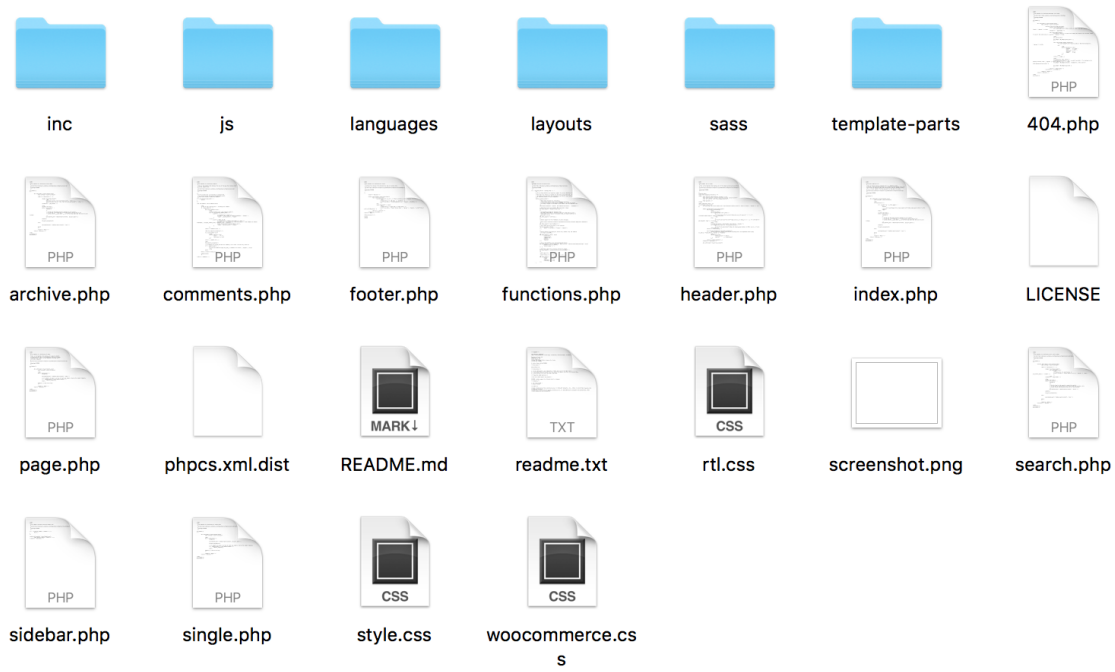
4.2 WordPressi kujundusteema loomine

Käesolev alampeatükk käsitleb WordPressis uue kujundusteema loomist. WordPressi baaskujundusteema peab vastavalt WordPressi arenduse kodulehele [12] koosnema vähemalt järgnevatest failidest:

- style.css
- index.php
- comments.php
- screenshot.png

Lisaks nendele failidele on WordPressis võimalik kujundada mitmeid lehemalle, et muuta erinevate lehtede ja/või postituste välimust. Lisa funktsionaalsuse tõstmiseks on fail *functions.php* ja erinevad JavaScripti failid.

Uue kujundusteema loomisel on käsitsi kõikide vajaminevate failide loomine ajamahukas ja seetõttu on optimaalsem kasutada WordPressi alustusteemat, mis sisaldab kõiki baas-kujundusteema faile ja siis hakata neid vastavalt vajadusele modifitseerima. Sellist võimalust pakub näiteks underscores.me lehekülg, kus tuleb täita kujundusteema nimi, kujundusteemat loova autori nimi ja lühikirjeldus kujundusteema kohta. Kui see on tehtud, siis automaatselt genereeritakse kõik vajaminevad failid kujundusteema loomiseks. Underscores on Automatticu (haldab WordPressi [13]) poolt loodud alustusteema ja see on mõeldud WordPressi kujundusteemade loomiseks, et säästa arenduselt mitmeid tunde kõikide failide ise loomiseks. WordPressi alustusteema on eraldiseisev teema, mida saab hõlpsasti muuta. Eriti kasulik on see juhtudel, kus on loodud staatiline HTML/CSS lehekülg ja tuleb lihtsalt muuta see WordPressi jaoks sobilikuks. [14] Underscores veebisait genereerib järgnevad failid (vt Joonis 4).



Joonis nr 4 Underscores.me genereeritud failid

Nendest failidest kustutas antud bakalaureusetöö autor järgnevad failid:

- sass
- archive.php

- readme.txt
- rtl.css

Need failid said eemaldatud, sest nad ei ole WordPressi kujundusteema nõutud failide hulgas ja kliendi poolt veebisaidile seatud nõuete täitmiseks ei ole nende kasutamine vajalik.

Lisaks underscores.me genereeritud failidele lõi bakalaureusetöö autor juurde järgnevad failid:

- home.php (avalehe jaoks)
- header-home.php (avalehe navigatsiooniriba)
- page-contact.php („Kontakt" lehemalli jaoks)
- page-portfolio.php (tehtud tööde kuvamiseks)
- page-services.php (firma pakutavate teenuste kuvamiseks)

Genereeritud failidest tuli muuta järgnevaid faile:

- 404.php
- footer.php
- functions.php
- header.php
- page.php
- single.php
- style.css

Algselt sisaldasid kõik need failid baaskujundusteema sisu, aga kliendi nõuete tagamiseks ja kujunduse muutmiseks tuli neid faile muuta ja täiendada.

4.3 Bootstrapi kasutamine veebisaidi kujundamisel

Antud osa tutvustab, mis on Bootstrap ja seletab, miks otsustas bakalaureusetöö autor seda antud veebisaidi loomisel kasutada.

Bootstrap on tasuta *front-end* tarkvara, mis teeb veebisaitide kujunduse loomise lihtsamaks ja kiiremaks. Bootstrap sisaldab endas HTML ja CSS disainimalle ning JavaScripti lisasid, et muuta veebisaitidel asuvate elementide kujundust ja paigutust. Bootstrapi suur eelis on mobiilisõbralikkus, ehk kõik sisseehitatud kujunduselemendid on juba loodud ennast kohandama vastavalt kasutatavale seadmele. Bootstrapi kasutamise eelisteks on lihtne kasutatavus, juba sisseehitatud mobiilisõbralikkus ja erinevate veebibrauserite tugi. [15]

Veebisaidi kujunduse osas kasutatakse Bootstrap kujundusmalli ja selle peale ehitatud kujundust nimega „Agency" Start Bootstrap veebisaidilt [16]. Tegemist on staatilise HTML/CSS ühelehelise veebilehega. Agency Bootstrapi teemast sai WordPressi kujundusteemasse implementeeritud järgnevad elemendid:

- avalehele pilt
- avalehele kolm kasti koos avaneva mooduliga
- navigeerimisriba
- veebisaidi jalus
- teenuste lehekülje kujundus

4.4 Juurde loodud lehemallide kirjeldus

4.4.1 Veebisaidi „Avaleht" mall

Avalehele implementeeris bakalaureusetöö autor staatilisest Bootstrapi teemast ühe pildi koos lühikese teksti ja nupuga, mis viib lehel järgmise sektsioonini. Avalehel on kolm infokasti, mis on kõik seotud eraldi WordPressi postitustega. WordPressi postitusest võetakse pealkiri ja eraldi avanevas moodulis kuvatakse postituse sisu. Kaks infokasti kuvavad postitust ja üks infokast sisaldab suunaviita tehtud tööde galerii juurde.

4.4.2 Veebisaidi „Teenused" leht

Teenuste lehele implementeeris töö autor staatilisest Bootstrap kujundusest kolm tulpa, et kuvada firma poolt pakutavaid teenuseid. Iga tulp on eraldi seotud WordPressi postitusega ja selle sisu saab kergesti muuta WordPressi tööriistaribalt.

4.4.3 Veebisaidi „Tehtud tööd" leht

Tehtud tööde leht on seotud kindla WordPressi lehega, kuhu on võimalik lisada galeriisid tehtud tööde postitustest ja lühikirjeldusi nende kohta. Leht küsib WordPressi andmebaasist postituse sisu kohta infot ja kuvab seda tehtud tööde lehel.

4.4.4 Veebisaidi „Kontakt" leht

„Kontakti" lehele kasutas bakalaureusetöö autor pistikprogramme Contact Form 7 [17] ja selle Bootstrapi [18] lisa. Nende pistikprogrammidega loodi maili saatmise vorm, mis on üles ehitatud nii, et ta küsib külastajalt nime, mailiaadressi, teemat ja sõnumi sisu. Kui mingi väli on puudulik või valesti täidetud, siis annab lehekülg vastavasisulise teate. Kui

kõik on korrektselt täidetud ja maili saatmine õnnestus, siis annab veebisait teate, et sõnum on edastatud.

4.5 Kasutatud pistikprogrammid

Antud veebisaidi loomisel kasutas töö autor WordPressi viit pistikprogrammi. Neli neist on tasuta ja üks on tasuline. Tasuta pistikprogrammidest kasutatakse Sucuri Security [19], Login LockDown [20], Contact Form 7 [17] ja selle Bootstrapi [18] lisa pistikprogramme. Esimene neist tagab veebisaidi turvalisust ja teine piirab sisselogimiskatseid, et hoida ära *brute-force* ründeid. Contact Form 7 ja selle Bootstrapi lisa pistikprogramm võimaldab veebisaidilt otse maili saatmise ja teeb kontaktivormi loomise ja muutmise lihtsaks. Tasulistest programmidest otsustasid klient ja bakalaureusetöö autor kasutada Essential Grid [21] pistikprogrammi. Antud programm sisaldab erinevaid kujundusi galeriide loomiseks ja annab kasutajale ilma koodi oskamata suure mänguruumi enda veebisaidil asuvate galeriide kujundamiseks. Pistikprogramm maksis 29€, kõik aktiveerimiskoodid ja failid edastati kliendile, ning klient saatis rakenduse koopia bakalaureusetöö autorile. Hetkel testkeskkonnas kasutatakse aktiveerimata rakendust, ning kui kogu veebisait on kolitud ümber õigesse veebiserverisse, siis aktiveeritakse rakendus.

Arendamise käigus kasutas bakalaureusetöö autor pistikprogrammi Show Current Template [22], mis kuvab veebisaidil olles hetkel kasutuses oleva lehemalli ja selle osad. See pistikprogramm hõlbustab arendamist ja annab lisainformatsiooni, mis failid antud lehel viibides kasutuses on.

5 WordPressi turvalisus

Käesolevas peatükis käsitletakse WordPressi turvalisusega seonduvaid probleeme ja võimalusi nende ärahoidmiseks.

5.1 Lihtsad turvameetmed, mida kasutusele võtta

WordPressi turvalisuse tõstmiseks on mõned lihtsad võtted, mille kasutusele võtmine suurendab märgatavalt lehe turvalisust ja aitab ära hoida *brute-force* ründeid [23, 24]:

- WordPressi ja pistikprogrammide õigeaegne uuendamine – sellest saab alguse kogu lehe turvalisus;
- tugevad paroolid ja kasutajate õigused süsteemis (WordPress, andmebaasid, e-mail jne);
- ära kasuta „admin" või muud levinud kasutajanime;
- hostingu serveri poolne turvalisus (enne valiku langetamist tutvu serveri turvalisusega).

5.2 WordPressi pistikprogrammid turvalisuse tõstmiseks

Järgnev loetelu toob veel välja erinevaid pistikprogramme WordPressi jaoks, mis aitavad parandada veebisaidi turvalisust:

- veebisaidi varundamine – aitab taastada veebisaiti ja varundada veebisaidi sisu (pistikprogrammid VaultPress või BackupBuddy);
- auditeerimine – annab infot lehel toimuva kohta (pistikprogramm Sucuri Scanner);
- Web App Firewall (WAF) – veebirakenduse tulemüür (pistikprogramm Sucuri Scanner tasuline liides).

Parimaks pistikprogrammiks turvalisuse tõstmiseks peetakse Sucuri Scannerit ja Login LockDown, sest oma baasseadistusega katab ära enamus turvalisuse jaoks vajalikke samme [23, 24].

Sucuri Security [19] on pistikprogramm, mis on mõeldud auditeerimiseks ja veebisaidi tegevuse jälgimiseks. Lisaks sellele on seal võimalus lisada turvameetmeid – piirata ja peita infot veebisaidi ja seal asuvate failide kohta (vt Joonis 5).

Joonis 5. Sucuri Security pistikprogrammi turvameetmed

Käesolevas töös rakendati kõiki tasuta saadavalolevaid meetmeid. Ainsana jäi rakendamata Veebisaidi tulemüüri osa, mis kuulub antud rakenduse tasuliste meetmete juurde.

Login LockDown [20] – Login LockDown on WordPressi pistikprogramm, mis aitab piirata sisselogimiskatseid ja blokeerida uusi sisselogimisi teatud ajaks. Selle pistikprogrammi kasutamine aitab ära hoida *brute-force* ründeid.

Mõlemaid pistikprogramme (Sucuri Scanner ja Login LockDown) on kasutatud veebisaidi arendamisel.

5.3 Käsitsi tehtavad muudatused ja muudatused *back-end* koodis.

Mõned turvalisuse tõstmise võtted nõuavad koodi või süsteemi andmebaasi muutmist. Näiteks tuuakse välja järgmisi soovitusi [23, 24, 25, 26]:

- keelata WordPressis failide muutmine. Faile saab muuta ainult läbi serveri;
- keelata php koodi käivitamine alamkaustas /wp-contents/uploads/;
- piirata sisselogimiskatseid ja seadistada juurdepääsu keeld kasutaja IP-aadressile, kes ületab selle;
- andmebaasi viide ära muuta (baasseadistuses on see wp_ kõigi andmebaasi tabelite jaoks);
- peida lehelt WordPressi versiooni info;

- muuda algne WordPressi administreerimise lehekülje suunaviit;
- piira WordPress admin ja login lehekülg eraldi parooliga.

Antud töös olid kasutatud järgmised võtted:

- **Admin kasutajanime vahetamine** – selle jaoks on mitu erinevat moodust. Üheks variandiks on luua WordPressis uus admin kasutaja ja siis läbi selle kasutaja kustutada vana. Teiseks variandiks on teha seda läbi phpMyAdmini. Antud töös kasutati esimest varianti ja loodi WordPressis uus kasutaja ja kustutati vana.
- **.htaccess failis tehtud muudatused** – keelamaks lähtefailide uurimist, serveri signatuuri peitmiseks ja XML-RPC päringute blokeerimiseks on tehtud .htaccess failis muudatusi (vt Joonis 6).

```
# Disable directory listing and browsing
Options All -Indexes

# Disable server signature
ServerSignature Off

# Block WordPress xmlrpc.php requests
<Files xmlrpc.php>
order deny,allow
deny from all
allow from 123.123.123.123
</Files>
```

Joonis 6 .htaccess failis tehtud muudatused

Need koodijupid olid lisatud faili lõppu, mis laeti üles serverisse samasse kohta. XML-RPC päringute keelamine on turvalisuse seisukohalt väga oluline – see sisaldab *system.multicall* meetodit. Antud meetod lubab saata mitu käsklust ühe päringuga, ehk läbi selle on võimalik ühe päringuga proovida läbi sadu paroole [27].

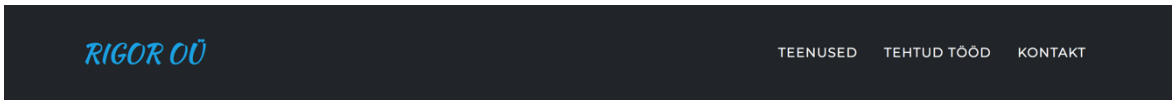
Veebisaidi turvalisuse kontrollimiseks ja turvaaukude leidmiseks oli kasutatud lehekülg www.wpscans.com ja rakendus NIKTO.

6 Uue veebisaidi kirjeldus

Käesolev peatükk tutvustab lühidalt uue veebisaidi elemente ja alamlehti ning esitab veebisaidil tehtud testide tulemusi.

6.1 Veebisaidi päis

Veebisaidi kõikidel lehtedel on ühesugune päis, ainus erinevus on avalehel suunaviit „*Rigor OÜ*" viitel (avalehel viib ta lehekülje ülesse, muudel lehtedel avalehele). Veebisaidi päis koosneb Rigor OÜ nimest ja navigeerimisribast (vt Joonis 7). Päis liigub lehekülje-ga üles-alla kerides kaasa (muutub allapoole kerides väiksemaks, et jätta lehele rohkem ruumi).



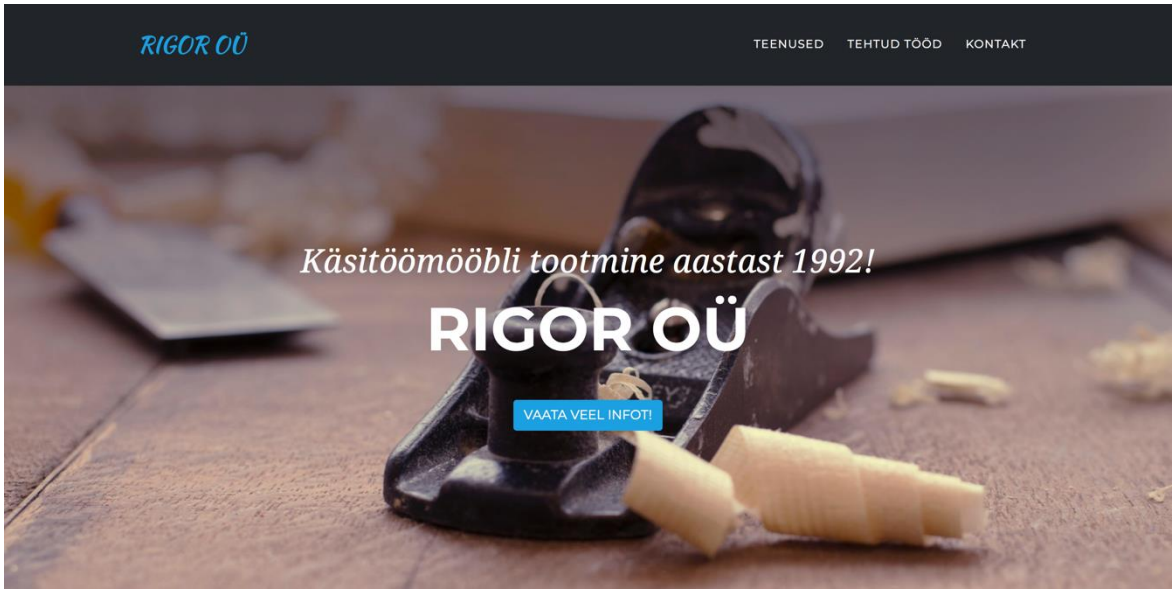
Joonis 7 Rigor OÜ uue veebisaidi päis.

Navigeerimisriba struktuur:

- „Rigor OÜ" (toimib kui *home* nupp)
- „Teenused"
- „Tehtud tööd"
- „Kontakt"

6.2 Veebisaidi avaleht

Veebisaidi avalehel on pilt, millel on lühike kirjeldus ja nupp, mis suunab leheküljel järgmise sektsioonini (vt Joonis 8). Järgmises sektsioonis on kolm tulpa, mis avavad lisamooduli, et kuvada erinevaid postitusi. Vasakpoolne on „Meist" info, keskmine on „Tehtud tööd" ja parempoolne on „Lisainfo". Neile peale vajutades avaneb lisamoodul, kus on kirjas täpsem info.



Joonis 8 Veebisaidi avalehe pilt.

6.3 Muud lehed veebisaidil

„**Teenused”** lehel on kolm tulpa, igaüks on seotud erineva postitusega. Leht kuvab postituse päisepildi ja seejärel selle sisu.

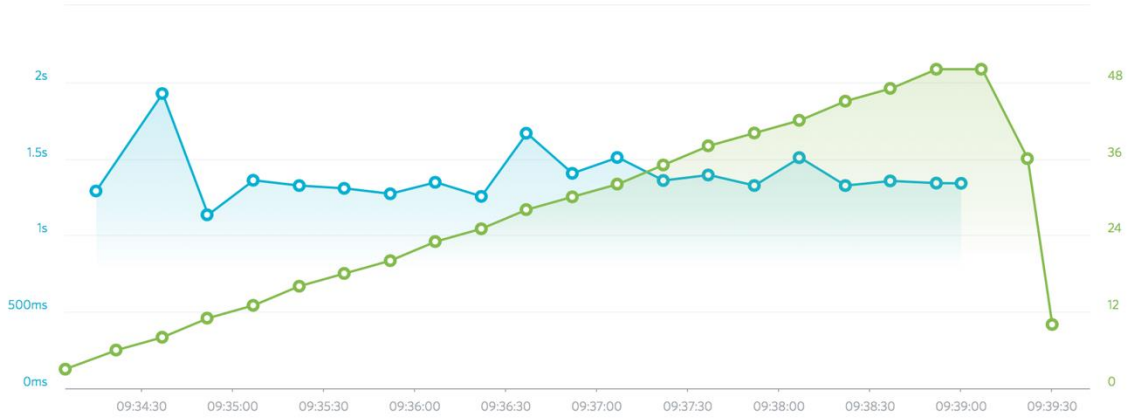
„**Tehtud tööd”** lehekülg sisaldab kõikide tehtud tööde postitusi. Leht kuvab kõikide postituste tutvustavad pildid ja kursoriga pildi peale liikudes ka selle nime.

„**Kontakt”** leheküljelt saab saata Rigor OÜ-le e-maili. Vormis tuleb täita oma nimi, e-mail, sõnumi teema ja sõnumi sisu. Peale saatmist kuvab leht teate, kas kiri sai edastatud või annab vastava veateate.

6.4 Testid

Jõudlus

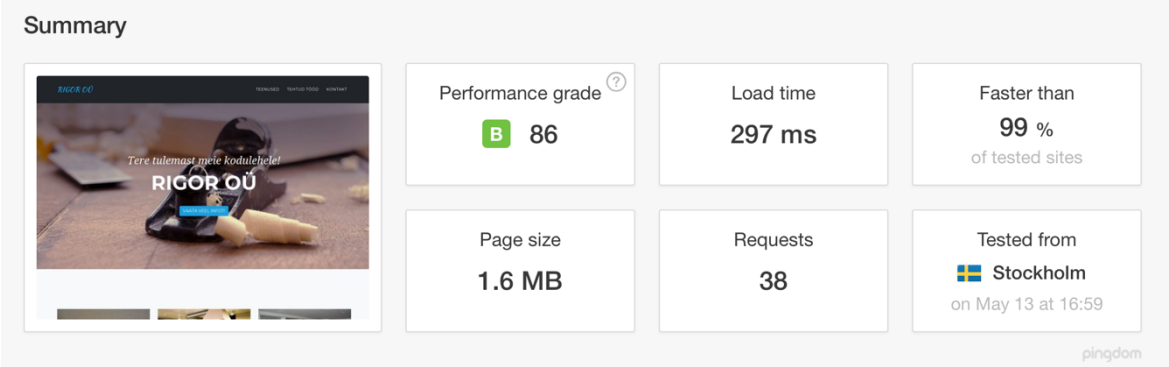
Jõudluse testimiseks kasutati tööriista Load Impact [28]. Testi käigus külastas valminud Rigor OÜ veebisaiti 50 virtuaalset kasutajat. Kasutajad lisati ükshaaval ning iga kasutaja puhul mõõdeti lehe laadimiseks kulunud aega. Testi tulemustest on näha (vt Joonis 9), et alguses on lehe laadimiseks kulunud aja hüppeline kasv, mille järel langes see kiiresti tagasi.



Joonis 9. Jõudlustest (sinine – lehe laadimise aeg, roheline – kasutajate arv lehel).

Kiirus

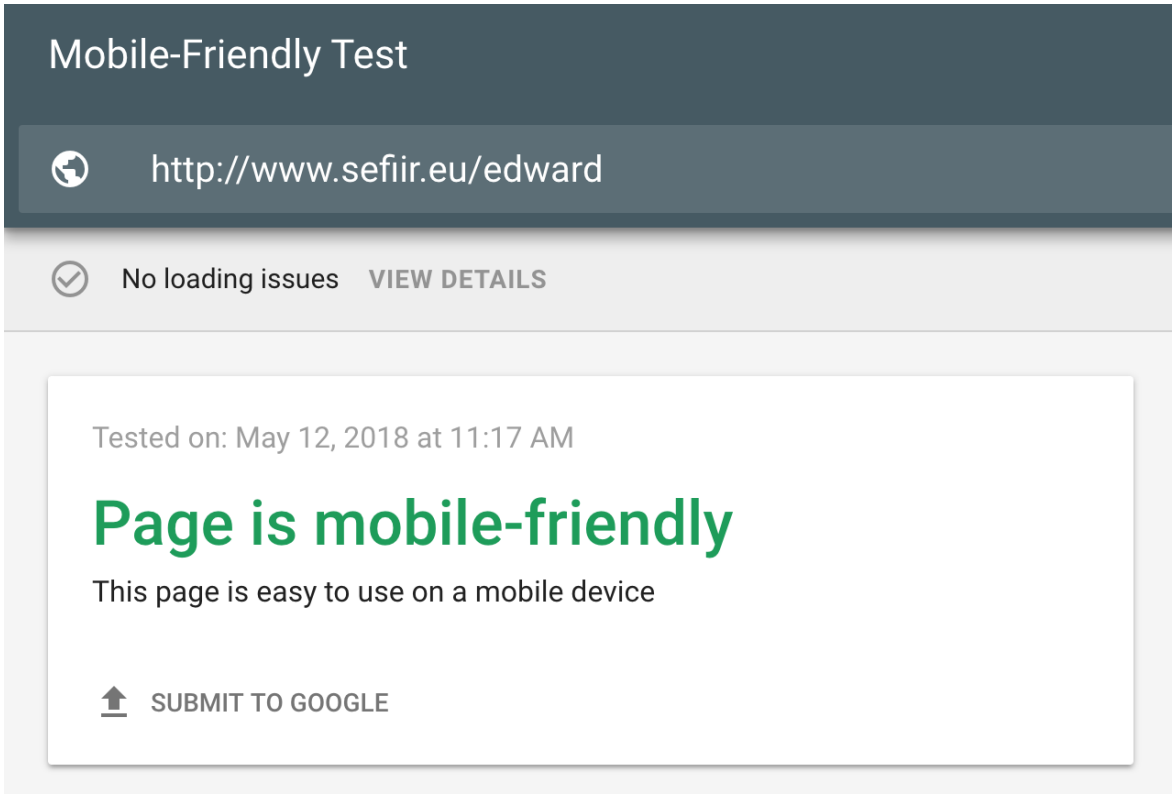
Veebisaidi kiirust testiti Pingdom [29] kiirust mõõtva tööriistaga (vt Joonis 10). Testi tulemused näitasid, et lehe laadimine võttis aega 297 ms. Kokku tehti lehele Stockholmist 38 päringut – lehe laadimine on kiirem kui 99% antud tööriistaga testitud veebisaitidest. Rigor OÜ veebisaidi hindeks kujunes 86/100 Pingdomi hinnangul.



Joonis 10 Pingdom kiiruse test veebisaidile.

Mobiilisõbralikkus

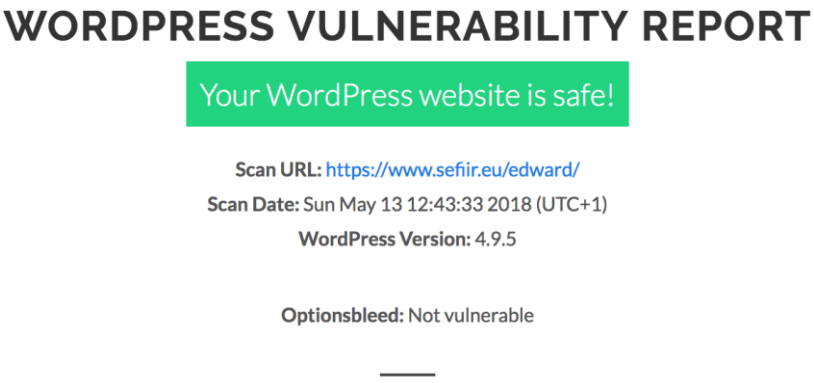
Mobiilisõbralikkust testiti Google'i „Mobile-Friendly-Test" [30] tööriistaga. Uus Rigor OÜ veebisait läbis selle testi ja on mobiilisõbralik (vt Joonis 11).



Joonis 11. Mobiilisõbralikkuse test.

Turvalisus

Veebisaidi turvalisust testiti WP-Scans [31] tööriistaga. Testi tulemusena selgus, et veebisait on turvaline (vt Joonis 12).



Joonis 12. WP Scans turvalisuse testi tulemused.

7 Kokkuvõte

Käesoleva bakalaureuse töö raames on loodud uus veebisait Rigor OÜ-le.

Töö koosneb vana veebisaidi analüüsist, annab ülevaate kliendi ja töö autori vahel kokkulepitud nõuetest veebisaidile, veebisaidi turvalisuse tagamise võimalustest, kasutatud tehnoloogiatest ja uue veebisaidi tutvustusest.

Töö tulemusena valmis nii arvuti-, kui ka mobiilisõbralik veebisait, mida toetab sisuhaldussüsteem WordPress koos oma pistikprogrammidega. Veebisaidil on võetud kasutusele erinevaid turvalisust tagavaid samme.

Klient on avaldanud rahulolu valminud tulemusega. Koostöö jätkub testserverist (www.sefiir.eu/edward) veebisaidi ümber kolimiseni õige domeeni alla (www.rigor.ee). Ümber kolimine toimub 2018. aasta suvel.

8 Viidatud kirjandus

[1] Cybernetica AS, „ANDMEKAITSE JA INFOTURBE LEKSIKON,“ [Võrgumaterjal]. Available: https://akit.cyber.ee/term/2412-back-end. [Kasutatud 09 05 2018].

[2] Eesti Keele Instituut, [Võrgumaterjal]. Available: https://keeleabi.eki.ee/index.php?leht=0. [Kasutatud 09 05 2018].

[3] Cybernetica AS, „ANDMEKAITSE JA INFOTURBE LEKSIKON,“ [Võrgumaterjal]. Available: https://akit.cyber.ee/term/2413-front-end. [Kasutatud 09 05 2018].

[4] Cybernetica AS, „ANDMEKAITSE JA INFOTURBE LEKSIKON,“ [Võrgumaterjal]. Available: https://akit.cyber.ee/term/639-brute-force-attack. [Kasutatud 09 05 2018].

[5] WordPress, [Võrgumaterjal]. Available: https://codex.wordpress.org/Themes. [Kasutatud 09 05 2018].

[6] Cybernetica AS, „ANDMEKAITSE JA INFOTURBE LEKSIKON,“ [Võrgumaterjal]. Available: https://akit.cyber.ee/term/598-open-source-software-1. [Kasutatud 09 05 2018].

[7] Cybernetica AS, „ANDMEKAITSE JA INFOTURBE LEKSIKON,“ [Võrgumaterjal]. Available: https://akit.cyber.ee/term/2437-plugin-pistikprogramm. [Kasutatud 09 05 2018].

[8] Cybernetica AS, „ANDMEKAITSE JA INFOTURBE LEKSIKON,“ [Võrgumaterjal]. Available: https://akit.cyber.ee/term/2551-content-management-system. [Kasutatud 09 05 2018].

[9] Triop AB, „WP Scans,“ [Võrgumaterjal]. Available: https://wpscans.com/scan/?id=4a4d6320015643b3ae839c648443e701. [Kasutatud 09 05 2018].

[10] Comentum, [Võrgumaterjal]. Available: http://www.comentum.com/what-is-cms-content-management-system.html. [Kasutatud 09 05 2018].

[11] 1&1, [Võrgumaterjal]. Available: https://www.1and1.com/digitalguide/hosting/cms/cms-comparison-a-review-of-the-five-best-platforms/ [Kasutatud 10 04 2018].

[12] WordPress.org, [Võrgumaterjal]. Available: https://developer.wordpress.org/themes/release/required-theme-files/ [Kasutatud 24 04 2018].

[13] Automattic, [Võrgumaterjal]. Available: https://automattic.com./ [Kasutatud 05 05 2018].

[14] Torgue Magazine, [Võrgumaterjal]. Available: https://torquemag.io/2017/08/beginners-guide-to-creating-a-theme-underscores/ [Kasutatud 05 05 2018].

[15] W3Schools, [Võrgumaterjal]. Available: https://www.w3schools.com/bootstrap/bootstrap_get_started.asp. [Kasutatud 05 05 2018].

[16] Start Bootstrap, [Võrgumaterjal]. Available: https://startbootstrap.com/template-overviews/agency/ [Kasutatud 01 04 2018].

[17] „WordPress plugins - Contact Form 7,“ [Võrgumaterjal]. Available:

https://wordpress.org/plugins/contact-form-7/ [Kasutatud 12 05 2018].

[18] „WordPress plugins - Bootstrap for Contact Form 7,“ [Võrgumaterjal]. Available: https://wordpress.org/plugins/bootstrap-for-contact-form-7/ [Kasutatud 12 05 2018].

[19] „WordPress plugins - Sucuri Scanner,“ [Võrgumaterjal]. Available: https://wordpress.org/plugins/sucuri-scanner/ [Kasutatud 12 05 2018].

[20] „WordPress plugins - Login LockDown,“ [Võrgumaterjal]. Available: https://wordpress.org/plugins/login-lockdown/ [Kasutatud 12 05 2018].

[21] ThemePunch, „Essential Grid WordPress plugin,“ [Võrgumaterjal]. Available: https://essential.themepunch.com/ [Kasutatud 12 05 2018].

[22] „WordPress plugind - Show Current Template,“ [Võrgumaterjal]. Available: https://wordpress.org/plugins/show-current-template/ [Kasutatud 12 05 2018].

[23] CodeinWP, [Võrgumaterjal]. Available: https://www.codeinwp.com/blog/secure-your-wordpress-website/ [Kasutatud 09 05 2018].

[24] WPBeginner, [Võrgumaterjal]. Available: http://www.wpbeginner.com/wordpress-security/ [Kasutatud 09 05 2018].

[25] WordPress.org, [Võrgumaterjal]. Available: https://codex.wordpress.org/Hardening_WordPress. [Kasutatud 09 05 2018].

[26] Yoast BV, [Võrgumaterjal]. Available: https://yoast.com/wordpress-security/ [Kasutatud 09 05 2018].

[27] Sucury Security, [Võrgumaterjal]. Available: https://blog.sucuri.net/2015/10/brute-force-amplification-attacks-against-wordpress-xmlrpc.html. [Kasutatud 01 05 2018].

[28] „Load Impact,“ [Võrgumaterjal]. Available: https://app.loadimpact.com/tests/3928403/runs/1?charts=type=1%3Bsid=__li_user_load_time%3A1%3BdataKey=value%3B%3Btype=1%3Bsid=__li_bandwidth%3A1%3BdataKey=avg%3B%3Btype=1%3Bsid=__li_requests_per_second%3A1%3BdataKey=avg%3B%3Btypeh [Kasutatud 13 05 2015].

[29] Pingdom, [Võrgumaterjal]. Available: https://www.pingdom.com/ [Kasutatud 13 05 2018].

[30] Mobile-Friendly-Test, [Võrgumaterjal]. Available: https://search.google.com/test/mobile-friendly?utm_source=gws&utm_medium=onebox&utm_campaign=suit&id=IwJbrdRLqjT95lg5PpztTw. [Kasutatud 12 05 2018].

[31] „WP Scans,“ [Võrgumaterjal]. Available: https://wpscans.com/ [Kasutatud 13 05 2018].

Lisad

I. Litsents

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, **Ted Edward Õunap**,
(*autori nimi*)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose
Veebisaidi loomine ettevõttele Rigor OÜ,
(*lõputöö pealkiri*)

mille juhendaja on Ljubov Jaanuska ja kaasjuhendaja Lidia Feklistova.
(*juhendaja nimi*)

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.
2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.
3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, **14.05.2018**