TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Anli Gea Põldemaa

Veebilehe turvalisuse võimalused

Bakalaureusetöö

Juhendaja: Karl-Erik Karu
MSc

Tallinn 2023

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Anli Gea Põldemaa

08.05.2023

Annotatsioon

Käesolev bakalaureusetöö keskendub veebilehtede turvalisuse uurimisele ja analüüsimisele, sealhulgas võimalustele ja turvalisuse saavutamiseks loodud vahenditele. Töö eesmärk on välja selgitada kõige tõhusamad meetodid veebilehtede turvalisuse parandamiseks, milleks testitakse ja rakendatakse neid veebilehe turvalisuse tõstmiseks. Konkreetse näitena teostatakse analüüs WordPressi veebilehele, mis on arendatud Web Design Agency OÜ kliendile.

Eesmärgi saavutamiseks antakse esmalt ülevaade veebilehtede turvalisusest, selle vajalikkusest ning tutvustatakse erinevaid tegureid, mis mõjutavad veebilehtede turvalisust. Seejärel kirjeldatakse spetsiifilisemalt WordPressi sisuhaldussüsteemi turvalisust, kaasnevaid ohte ning võimalusi nende vältimiseks. Lisaks analüüsitakse erinevaid turvalisuse mõõdikuid ja tööriistu, mis on mõeldud veebilehtede analüüsimiseks ja turvalisuse edendamiseks. Lõpuks viiakse läbi praktiline analüüs Amidisain OÜ veebipoe baasil ning teostatakse selle turvaliseks muutmine. Seejärel kirjeldatakse lehe turvalisuse saavutamise protseduure ja efektiivsuse hindamise meetodeid.

Töö lõpptulemusena valmib Amidisain OÜ turvatud veebileht ning koostatakse metoodika ja soovituslike turvalisustoimingute loetelu, mis aitavad WordPressi baasil arendatud veebilehtede arendajatel luua jätkusuutlikumaid ja turvalisemaid veebilehti, seeläbi tõstes ettevõtete edukust ning klientide rahulolu.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 51 leheküljel, 6 peatükki, 25 joonist, 6 tabelit.

Abstract

Website security options

This bachelor's thesis focuses on researching and analyzing the security of web pages, including the goals, possibilities and tools designed to achieve security. The aim of the thesis is to find out the most effective methods for improving the security of web pages, for which they are tested and implemented to increase the security of the web page. Specifically, the analysis is performed on a WordPress website developed for a client of Web Design Agency OÜ.

In order to achieve the goal, an overview of the security of websites, its necessity, and various factors that affect the security of websites are first given. Then, the security of the WordPress content management system, accompanying threats and ways to avoid them are described more specifically. In addition, various security metrics and tools available for analyzing web pages and improving security are analyzed. Finally, a practical analysis will be carried out on the basis of Amidisain OÜ's online store, and it will be made secure. Then the procedures for achieving page security and methods for evaluating effectiveness are described.

As a final result of the thesis, a secured website of Amidisain OÜ will be created and a list of methodology and recommended security actions will be prepared, which will help the developers of websites developed on the basis of WordPress to create more sustainable and secure websites, thereby increasing the success of companies and customer satisfaction.

The thesis is in Estonian and contains 51 pages of text, 6 chapters, 25 figures, 6 tables.

Lühendite ja mõistete sõnastik

API	*Application Programming Interface* on tarkvara komponent, mis võimaldab erinevatel rakendustel omavahel suhelda ja andmeid vahetada
Bruce-force rünnak	Küberrünnak, mis kasutab paroolide või krüpteeritud sõnumi sisu murdmiseks katse-eksituse meetodit
CDN	*Content Delivery Network* ehk sisu edastamise võrgustik
CMS	*Content management system* ehk sisuhaldussüsteem
Cross Site Scripting (XSS)	Küberrünnak, mille käigus sisestatakse pahatahtlikke skripte veebirakenduse koodi, mis käivitatakse kasutaja veebibrauseris
CSS	*Cascading Style Sheets* on märgistuskeel, mida kasutatakse peamiselt veebilehtede disaini ja paigutuse kujundamiseks
DoS/DDoS rünnak	*Distributed Denial of Service* on küberrünnak, kus suunatakse suur hulk päringuid veebiserverile, et tekitada ülekoormus ja takistada õigustatud kasutajate juurdepääs veebilehele
Gutenbergi plokiredaktor	Plokipõhine WordPressi redaktor, mis võimaldab paindlikumalt sisu luua, lisades kohandatavate plokkidega veebilehele elemente, nagu pildid, lõigud, loendid ja nupud
HTML	*HyperText Markup Language* ehk hüperteksti märgistuskeel
HTML *iframes*	Tekstisisene raam, mis võimaldab veebilehele lisada teise veebilehe sisu
HTTPS	*Hypertext Transfer Protocol Secure* on turvaline andmeedastusprotokoll, mis tagab veebilehe ja brauseri vahelise krüpteeritud ühenduse
JavaScript	Programmeerimiskeel, mida kasutatakse interaktiivsete veebilehtede loomiseks
MySQL	Avatud lähtekoodiga struktureeritud andmebaasi haldussüsteem
PHP	Skriptimiskeel, mida kasutatakse peamiselt veebilehtede dünaamilise sisu loomiseks

Plugin	Pistikprogramm või moodul, mis võimaldab tarkvarasüsteemidele lisada lisafunktsionaalsusi
reCaptcha	*Google'i* poolt välja töötatud tehnoloogia, mis aitab eristada inimesi arvutiprogrammidest veebilehtede külastamisel
SEO	*Search Engine Optimization* ehk veebilehe otsingumootorite optimeerimine
SQL *Injection*	Küberrünnak, mile käigus sisestatakse veebilehele pahatahtlikku SQL-koodi, et pääseda ligi ja manipuleerida andmebaasi sisuga
SSL	*Secure Sockets Layer* on turvatehnoloogia, mis krüpteerib andmeedastuse veebiserveri ja brauseri vahel
URL	*Uniform Resource Locator* ehk veebiaadress
WordPress	Avatud lähtekoodiga sisuhaldustarkvara, mis võimaldab luua ja hallata veebilehti

Sisukord

Jooniste loetelu

Tabelite loetelu

1 Sissejuhatus

Veebilehtede turvalisus on tänapäeval äärmiselt oluline. Veebilehtede abil teostatakse kliendi andmetega toiminguid, mistõttu on oluline tagada andmete turvalisus. Turvaline veebileht peaks kliendile garanteerima privaatsuse, kindlustunde ning usaldusväärsuse, mis on tähtis nii kliendi kui ka ettevõtte jaoks.

Turvalise veebilehe puudumine võib kaasa tuua tõsiseid tagajärgi nii ettevõttele kui ka kliendile. Kliendi jaoks tähendab see riski tema isikuandmete ja rahaliste vahendite turvalisusele. Kliendid usaldavad ettevõtteid, kellel on turvalised veebilehed, kuna see annab neile kindlustunde, et nende isikuandmed ja muu tundlik info on kaitstud. Turvamata veebileht võib olla kliendi jaoks pettumust valmistav, kui nad satuvad pettuse ohvriks või nende privaatsus on ohus. Teisisõnu, turvalisuse puudumine võib kahjustada ettevõtte mainet. Kvaliteetne ja turvaline veebileht tagab aga kliendi rahulolu ning usalduse, mis omakorda tõstab ettevõtte kuvandit ning vähendab kahjusid. Seega on turvaline veebileht ettevõttele oluline investeering, mis tagab nende klientide usalduse ja kaitseb nende mainet ja vara.

Antud bakalaureusetöö eesmärk on anda ülevaade veebilehtede turvalisuse olulisusest ning tutvustada erinevaid meetodeid ja vahendeid, mis aitavad saavutada optimaalse turvalisuse taseme. Eesmärgi saavutamiseks kirjeldatakse detailselt tegureid, mis võivad mõjutada veebilehe turvalisust. Lisaks tuuakse välja mõõdikuid, mille abil saab hinnata turvalisuse taset ning pööratakse tähelepanu tööriistadele, mis võimaldavad nende analüüsimist. Töö autor töötab veebidisaineri ja -arendajana ettevõttes Web Design Agency OÜ, kus veebilehtede kvaliteet ja turvalisus on prioriteet ning peamiselt kasutatakse arendamisel WordPressi sisuhaldussüsteemi, mistõttu uuritakse töös põhjalikult antud süsteemi turvalisuse võimalusi.

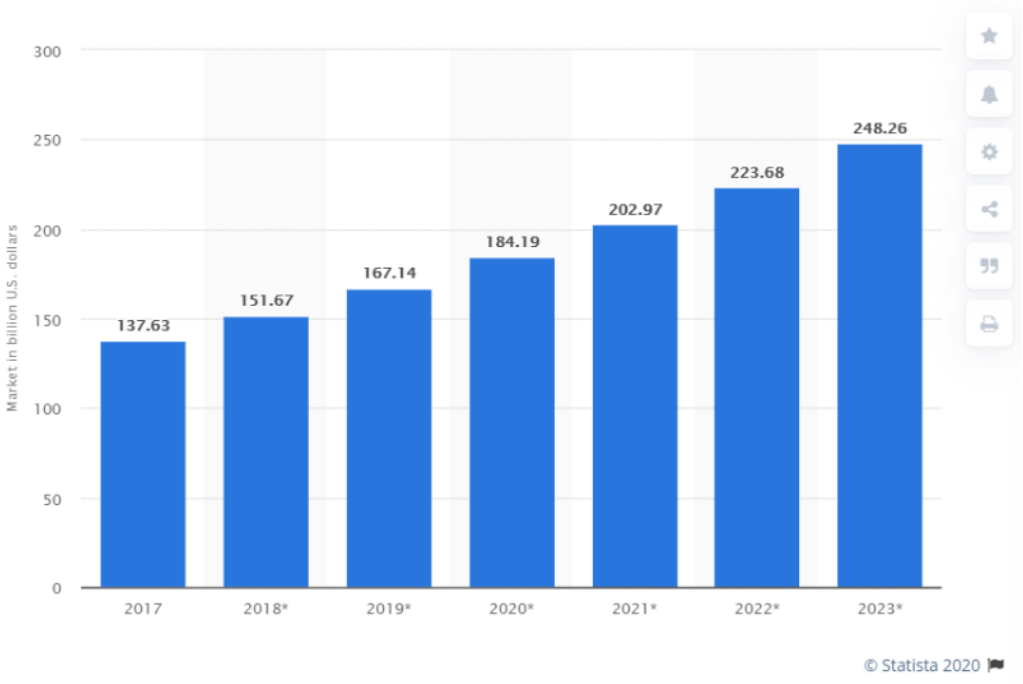
Esimene peatükk annab ülevaate probleemist ning kirjeldab turvalisuse vajalikkust veebilehtede puhul. Kirjeldatakse erinevaid tegureid, mis mõjutavad veebilehtede turvalisust ning uuritakse nende rakendamisviise. Teises peatükis keskendutakse spetsiifilisemalt WordPressi sisuhaldussüsteemi turvalisusele ning tutvustatakse

erinevaid turvalisuse vahendeid. Töös võrreldakse erinevaid meetodeid ning tuuakse välja nende tugevused ja nõrkused. Seejärel analüüsitakse turvalisuse mõõdikuid ning tööriistu, mis on saadaval veebilehtede analüüsimiseks ja turvalisuse parandamiseks. Kolmandas peatükis viiakse läbi praktiline osa, kus analüüsitakse Amidisain OÜ veebipoodi ning seejärel teostatakse selle turvaliseks muutmine, rakendades eelnevalt analüüsitud metoodikaid ja vahendeid. Lisaks selgitatakse turvalisuse saavutamise toiminguid ning hinnatakse erapooletult turvatud veebilehte ja turvalisusmeetodite efektiivsust. Lõpuks koostatakse nimekiri soovituslikest ja eelistuslikest toimingutest, mida arendajad saavad järgida, et saavutada veebilehtede parim võimalik turvalisus.

2 Veebilehtede turvalisus

Uuringud on näidanud, et veebilehtede arv maailmas kasvab pidevalt ning ainuüksi 2023. aasta seisuga on maailmas umbes 1,13 miljardit veebilehekülge [1]. Samal ajal suureneb ka küberrünnakute arv, mille sihtmärkideks on üha enam veebirakendusi. Ameerika Ühendriikides on veebilehtede vastu suunatud rünnakud 2020. aastast kasvanud umbes 400% ning FBI teada andnud kuni 4000 küberrünnakust päevas [2]. Lisaks on hinnangu kohaselt 2023. aastaks oodata ülemaailmsete DDoS-rünnakute koguarvu kasvu üle 15,4 miljoni [2]. Küberrünnakud muutuvad aina komplitseeritumaks ning kõik veebilehed võivad olla turvalisuse ja privaatsuse rikkumiste suhtes suure ohu all. Seetõttu on teadmine, kuidas oma veebilehekülgi erinevate küberrünnakute eest kaitsta, äärmiselt oluline nii veebirakenduse omanikule, ettevõttele kui ka kasutajate andmete kaitsmiseks.

Oluline on välja tuua ka eelpool mainitud infost tingitud küberturvalisuse turu kasvu (Joonis 1), mis on muutunud väga konkurentsivõimeliseks ning uute toodete ja teenuste väljatöötamisel pööratakse suurt tähelepanu innovatsioonile ja turvalisusele. Üha enam ettevõtteid tunnistab, et küberturvalisus on oluline ja vajalik investeering. [3]



Joonis 1. Küberturvalisuse turu suurus US dollarites aastatel 2017-2023 [3].

2.1 Veebilehtede turvalisuse eesmärk

Veebilehe turvalisuse tagamine hõlmab meetmeid, mille eesmärk on tagada, et veebilehe sisu ja andmed oleksid kaitstud küberkurjategijate eest ja veebisaidi mis tahes viisil ärakasutamise eest [4]. Turvalisuse toimingud aitavad kaitsta veebilehe privaatseid andmeid, riistvara ja tarkvara eksisteerivate erinevat tüüpi rünnakute eest. Lisaks tagab see kasutajate privaatsuse ja andmekaitse vastavalt kohaldatavatele seadustele ja regulatsioonidele [2].

Tähtis on meeles pidada, et turvalisus ei ole ühekordse seadistusega lahendus. See on pidev protsess, mis nõuab tihedat hindamist ja täiustamist, et vähendada üldist riski ning tagada lehe turvalisus nii praegu kui ka tulevikus. See on lehe haldamise oluline osa. [5]

2.2 Veebilehtede turvamise olulisus

Veebisaitide turvalisuse tagamine on väga oluline, sest tänapäeval kasutatakse veebikeskkonda laialdaselt oluliste toimingute ja tehingute sooritamiseks. Turvamata veebilehed on vastuvõtlikumad erinevatele rünnakutele. Järgnevalt on lähemalt selgitatud viis peamist põhjust koos näidetega, miks igal veebisaidil peaks olema korralik turvakaitse.

Ettevõtte maine kaitse - Veebisaidi turvalisus on oluline ettevõtte, maine ja usaldusväärsuse säilitamiseks. Kui veebileht on kergesti haavatav rünnete ja andmete varguse suhtes, siis võib see kahjustada ettevõtte mainet ning külastajad võivad kaotada usalduse ettevõtte vastu. Näiteks, kui ründaja saab juurdepääsu e-poe klientide andmetele, võib see põhjustada ettevõttele kahju, kuna kaob külastajate usaldus ning võidakse eelistada osta tooteid hoopis konkurendi veebisaidilt. Halvimal juhul võib see viia ettevõtte tegevuse lõpetamiseni. [6]

Veebisaidi kättesaadavus - Küberkurjategijad võivad kasutada erinevaid meetodeid, et häirida veebisaidi teenust või muuta see kasutajatele kättesaamatuks. Turvarünnakud mõjutavad veebisaidi tööd ja põhjustavad teenuste katkemist. Näiteks, kui veebisait on häkitud ja blokeeritud, võib see kaotada kuni 98% oma liiklusest [2]. DDoS-rünnakud on üks levinumaid meetodeid, mida ründajad kasutavad veebisaidi kättesaadavuse häirimiseks. Antud juhul saadetakse veebisaidile tohutul hulgal võltsliiklust mitmest allikast, püüdes serverit üle koormata [2]. Kui e-pood saab DDoS-rünnaku osaliseks, võib

see takistada kasutajatel sisse logida, tooteid osta või makseid sooritada. Kui saidi omanikud ei suuda rünnakuga kiiresti toime tulla, on jällegi tõenäoline kaotada kliente, kes võivad eelistada teisi konkurente, kus teenus töötab sujuvalt ja turvaliselt. [5]

Kulukas rünnakust taastumine - Turvameetmete investeeringud võivad tunduda kulukad, kuid küberrünnakutest tulenevad kahjud võivad olla see-eest palju suuremad. Kui ettevõte ei pea veebisaidi turvalisust piisavalt oluliseks ning ei rakenda piisavalt turvameetmeid, võib see põhjustada tõsiseid turvariske. Pärast küberrünnakut veebilehe puhastamine ja taastamine võib olla väga kulukas ja aeganõudev protsess. Sinna alla ei kuulu mitte ainult pahavara puhastusteenus, vaid ka saamata jäänud tulu ja mainekahju. Pahavara puhastamise toiming seisneb turvaaukude ja häkkeri mõtteviisi tundmises. Veebisaidi puhastamine ja taastamine võib hõlmata erinevaid kulutusi, nagu professionaalsete turvaekspertide palkamine, turvavigade parandamine, pahavara ja viiruste eemaldamine, andmete taastamine ja saidi taastamine. Näiteks 2021. aasta uuringute kohaselt kulutati pahavara eemaldamiseks keskmiselt 613 dollarit WordPressi veebilehe kohta, kus kõrgeim makstud hind oli 4800 ja madalaim 50 USA dollarit [7]. [8]

Andmete kaitse - Veebisaitide turvamine on oluline, et kaitsta nii ettevõtte kui ka kasutajate andmeid. Isikuandmete vargus on üks levinumaid küberkuritegusid ja võib põhjustada tõsist kahju. Identiteedivargus, andmete edasimüük või lekitamine võivad olla suhteliselt lihtsa teostusega, kui häkkeril on juurdepääs piisavatele isikuandmetele. Veebisaidi turvamine hõlmab tugevat autentimist ja volituste kontrollimist, et piirata juurdepääsu tundlikele andmetele. Kui inimene logib veebisaidile sisse, siis autentimisprotsess peaks veenduma, et see inimene on tõesti see, kes ta väidab end olevat, ja ei ole keegi teine, kes püüab pettuse teel lehele ligi pääseda. Kui ettevõtte andmed satuvad kurjategijate kätte, võib see põhjustada suurt rahalist kahju, mis võib olla tingitud näiteks GDPR nõuete rikkumisest. [6]

Pahavara ja küberrünnakuid võib olla raske märgata - Pahavara ja küberrünnakud on muutunud üha keerulisemaks ja salakavalamaks ning võivad tihti veebilehtedel esineda. Näiteks võib ründaja manipuleerida veebilehe koodiga, et varastada isiklikke andmeid või paigaldada pahavara arvutitesse või nutiseadmetesse. Kui ründajad teevad seda tõhusalt, ei pruugi veebilehe omanik märgata, et midagi oleks valesti ning ettevõtte ja klientide turvalisus on tõsiselt ohustatud. Sarnaste rünnakute populaarsus tõuseb jätkuvalt, kasvades 2021. aastal sellele eelneva aastaga võrreldes 23%. [4]

2.3 Veebilehtede ründamise põhjused

Veebilehekülgede loomise populaarsus kasvab igapäevaselt ning loob suure võimaluste spektri kurjategijatele, kes soovivad selles keskkonnas oma ebaseaduslikke tegevusi läbi viia [1]. Veebilehtede rünnakud on liigitatud kaheks: tahtlik või juhuslik [9]. Peaaegu kõik veebilehed kuuluvad juhuslike rünnakute valdkonda [9]. Tahtlik küberkuritegu sooritatakse tavaliselt raskesti ligipääsetavate, suurema avalikkuse tähelepanu all või suurema turuväärtusega ettevõtete/isikute veebirakenduste pihta [9]. Siinkohal toob autor välja erinevad eesmärgid ründamiseks:

1. **Rahaline kasu** - Veebilehtede ründajad võivad rünnata veebilehti, et varastada andmeid, mida kasutada identiteedivarguseks või nende andmete müümiseks. Antud motiivi puhul on levinud automatiseeritud tehnikad, millest võib järeldada, et suurem osa rünnakutest toimuvad juhuslikult valitud veebilehtedel.

    - Üks levinud toiming on ründaja poolt tehtud rämpsposti saatmine, mis sisaldab näiteks õngitsuskirju, mille abil petturid püüavad saada inimesi jagama oma krediitkaardiandmeid, paroole või muud tundlikku teavet [10].

    - Teine levinud võimalus on nõudmiste ja lunaraha väljapressimine, kus ründajad blokeerivad veebilehe juurdepääsu ja nõuavad raha, et veebilehe juurdepääs taastada [11].

2. **Ideoloogiliste või poliitiliste vaadete propageerimise eesmärgil** - Mõnikord võivad veebilehti rünnata ründajad, kes soovivad propageerida oma ideoloogilisi või poliitilisi vaateid. Siinkohal valib ründaja tahtlikult kindla rünnatava veebilehe. Näiteks võivad nad rünnata valitsusasutuste või poliitiliste organisatsioonide veebilehti, et väljendada oma vastuseisu nende tegevusele või avaldada survet valitsusele või organisatsioonile. [12]

    - Üks võimalikest variantidest mainitud vaadete propageerimiseks on veebilehe *defacement* ehk veebilehe kaaperdamine. Sellisel juhul ründavad ründajad veebilehte, muudavad selle sisu ning asendavad selle näiteks poliitiliste või ideoloogiliste sõnumitega. [13]

3. **Lõbu pärast** - Vahel võib veebilehti rünnata ka inimesed, kes soovivad lihtsalt lõbutseda või testida oma häkkerioskusi. Sellised ründajad võivad olla nii algajad

kui ka professionaalsed häkkerid ning kannatada saavad veebilehed valitakse enamjaolt juhuslikult. [11]

2.4 Veebilehtede peamised turvaprobleemid

Veebilehtede turvaprobleemid võivad tunduda väikesed, kuid nende ignoreerimine võib põhjustada suuri tagajärgi nii ettevõttele kui ka lehe kasutajatele. Järgnev loetelu kirjeldab peamisi veebilehtede turvaauke:

1. **Nõrk juurdepääsu kontroll** - Kasutajad võivad kasutada liiga lihtsaid paroole või sama parooli mitmesugustel kontodel, mis muudab nende kontod haavatavaks häkkerite rünnakute suhtes. Lisaks on kriitiline ohumärk kaheastmelise autentimise mittekasutamine, harv paroolide uuendamine või HTTPS-ühenduste puudumine. [14]

2. **Süsteemisisesed turvavead –** Uuendamata pluginad ja tundlike andmete kaitsmata käsitlus veebilehel on tõhusad võimalused küberrünnaku sooritamiseks. Näiteks tuleks lehel krüpteerida tundlikud andmed nii nende saatmisel kui salvestamisel ning pidevalt uuendada pluginaid. [15]

3. **Jagatud veebimajutus** – See on veebimajutus, kus mitmed veebilehed jagavad ühte füüsilist serverit ja selle ressursse. Haavatavust seal majutavatele lehtele tekitab olukord, kui üks veebisait on haavatav või sissemurdmise ohuga, sest siis võib see ohustada ka teisi lehti, mis jagavad sama serverit. [16]

2.5 Veebilehtede ründamise meetodid

On oluline, et veebilehe omanikud oleksid teadlikud võimalike ründemeetodite olemasolust ja rakendaksid meetmeid nendest hoidumiseks, et seeläbi kaitsta veebilehe ja selle kasutajate andmeid. Siin on ülevaade mitmetest tänapäeval laialdaselt levinud küberkurjategijate ründe meetmetest koos näidetega [5]:

1. **SQL *Injections*** (SQL süstimine) on ründemeetod, mille käigus ründaja sisestab andmebaasi päringusse spetsiaalselt loodud SQL-käsu, et saada juurdepääs andmetele, mida ta ei tohiks näha või muuta andmeid, mida ta ei tohiks muuta. Täpsemalt saab ründaja antud meetodit rakendades luua uue

administraatoritaseme kasutajakonto, mille kaudu saab täieliku juurdepääsu veebisaidile. Lisaks saab ründaja seda meetodit kasutada uute andmete sisestamiseks lehe andmebaasi, mis võib hõlmata pahatahtlikke linke või rämpsposti veebisaite.

2. ***Cross-Site Scripting*** **(XSS)** (Saitidevaheline skriptimine) on ründemeetod, kus ründaja sisestab pahatahtliku koodi veebilehele, et saada juurdepääs kasutaja brauseri küpsistele või varastada kasutaja andmeid. XSS-rünnak võib toimuda siis, kui veebilehel on tagatud nõrk sisendandmete turvalisus ja sisestatud andmed ei ole piisavalt filtreeritud. Näiteks võib ründaja sisestada veebisaidile pahatahtliku koodi, mis saadab kasutaja andmed ründaja serverisse.

3. ***Brute Force*** **rünnakud** (Jõuga ründamine) on ründemeetod, kus ründaja proovib automaatselt genereeritud paroolide kombinatsioone, et leida õige parool. Ründaja võib kasutada jõuga ründamist, kui veebisaidil ei ole piisavalt tugevat paroolipoliitikat ja paroolid on lihtsad, nagu kasutajanimed, sünniajad jms. Näiteks võib ründaja proovida jõuga ründamist sisselogimisvormis, et leida õige parool ja saada juurdepääs konto andmetele.

4. **DoS/DDoS** (Jaotatud teenuse keelamise rünnakud) ründemeetodid takistavad kasutajate juurdepääsu veebisaidile, häirides või ülekoormates veebisaidi serverit. Ründaja võib kasutada DoS/DDoS rünnakut, kui veebisaidil ei ole piisavalt tugevat turvalisust ja ründaja suudab kasutada võrgus olevaid seadmeid, et saata suur hulk päringuid veebisaidile, mis võib põhjustada serveri ülekoormuse ja veebisaidi töö lõpetamise. Näiteks võib ründaja kasutada antud rünnakut, et häirida pangateenuseid või valitsuse veebilehti, et takistada kasutajatel nende veebisaitidele juurdepääsu.

2.6 Veebilehtede rünnakute tõkestamine

Veebisaidi turvalisuse tagamine võib pidevalt areneval maastikul olla keeruline teema, kuna küberturvalisuse valdkond areneb kiiresti ja pidevalt tulevad turvaohtude uued variatsioonid. See tähendab, et turvalisuse meetmed, mis olid veel mõni aeg tagasi piisavad, võivad tänasel päeval olla ebaefektiivsed ja ohtlike rünnete vastu haavatavad. Selle tõttu nõuab turvalisuse tagamine pidevat tähelepanu, vastavaid teadmisi ning

ajakohasust. Antud alapeatükis selgitatakse erinevaid võimalusi, kuidas hoiduda küberrünnakute ohvriks sattumisest ning tuuakse välja ka nende spetsiifilised eelised.

2.6.1 Firewall ehk tulemüür

Tegemist on turvamehhanismiga, mis aitab kaitsta veebisaiti volitamata juurdepääsu eest. Tulemüür töötab võrgukihis, kontrollides kõiki sissetulevaid ja väljaminevaid võrguliikluse vooge, lubades ainult turvalisi või lubatud ühendusi. [17]

Tulemüürid võivad olla nii riistvara- kui tarkvaralahendused, mis asuvad veebisaidi serveris. Need analüüsivad ja filtreerivad kogu võrguliiklust vastavalt seatud reeglitele ja poliitikatele. Tulemüür blokeerib potentsiaalselt ohtlikke liiklusevooge, mis võivad sisaldada pahavara, ründetarkvara, spämmi või muud ebasoovitavat sisu. [17]

Tulemüüri eelised:

- Turvalisus: Tulemüür aitab kaitsta teie veebisaiti rünnakute, häkkimise, pahavara ja muude võimalike ohtude eest.
- Liikluse kontroll: Tulemüür võimaldab teil kontrollida ja filtreerida sissetulevat ja väljaminevat võrguliiklust vastavalt oma reeglitele ja poliitikatele.
- Juurdepääsu kontroll: Tulemüür võimaldab teil kontrollida, millised ühendused on lubatud või keelatud teie veebisaidiga. [17]

2.6.2 SSL (Secure Sockets Layer)

SSL-sertifikaat on digitaalne sertifikaat, mis tõendab veebisaidi autentsust ja võimaldab krüpteeritud ühendust. SSL turvaprotokoll loob krüpteeritud ühenduse veebiserveri ja veebibrauseri vahel ning tagab turvalise andmeedastuse. Antud sertifikaatide kasutamine on oluline, et kaitsta veebisaidi külastajate andmeid, näiteks krediitkaardinumbreid, isikukoode jne. SSL aitab takistada kurjategijaid neid andmeid lugemast või muutmast, kui need edastatakse kahe süsteemi vahel. [18]

Kui SSL-sertifikaat on veebisaidile edukalt installitud, siis kuvatakse veebibrauseri aadressiribal ikooni, mis kujutab tabalukku. See näitab, et veebisait on SSL-ga kaitstud ja külastajad saavad oma andmeid turvaliselt sisestada. SSL-sertifikaat on kasutusel HTTPS kaudu, mis on turvaline krüpteeritud ühendus. [18]

SSL-protokolli eelised:

- Autentimine: SSL-protokoll võimaldab veebisaidil autentimist ja kinnitada külastaja identiteeti, mis aitab vältida pettusi ja andmete vargusi.
- Usaldusväärsus: SSL-sertifikaadid annavad külastajatele kindluse, et veebileht on autentne ja privaatse teabe jagamiseks turvaline. [18]

2.6.3 Backup ehk varukoopia

Varukoopia on oluline osa veebisaidi turvalisuse tagamisest. Koopia tegemine tähendab veebisaidi andmete (sh failide, piltide, videote, tekstide) varundamist teise asukohta või serverisse, mis tagab nende turvalisuse ning võimaldab neid taastada juhul, kui tekib probleeme, näiteks andmete kadumine, häkkimine, rikutud või hävitatud failid. [19]

Varukoopia eelised:

- Andmete kaitsmine: Andmete turvalisus on üks peamisi põhjuseid, miks on oluline regulaarselt teha varukoopiaid oma veebisisust. See aitab tagada, et kõik veebisaidi andmed on kaitstud ja säilivad, hoolimata sellest, mis juhtub.
- Aja ja raha säästmine: Kui mõni osa veebisaidist kaob ja puudub sellest varukoopia, peab kulutama aega ja ressursse, et see uuesti taastada. See võib hõlmata saidi taasloomist algusest peale.
- Veebisaidi migreerimine: Kui on soov oma veebisait üle kanda uude serverisse või muuta oma praeguse majutamise teenuse pakkujat, on varukoopiate kasutamine selle protsessi jaoks oluline. Varukoopia kasutamine muudab kogu protsessi lihtsamaks ja vähendab riski, et midagi kaduma läheks. [19]

2.6.4 Tugev paroolipoliitika

Parooli parimad tavad näevad ette tugevate ja ainulaadsete paroolide kasutamist, mis on piisavalt pikad, et muuta need ründajate jaoks raskesti äratuntavaks. Lisaks peaksid paroolid sisaldama erinevaid tähemärke, numbreid ja sümboleid. Soovitatav parooli pikkus on 16 tähemärki. [20]

Paroolide regulaarne vahetamine on samuti oluline, kuna see vähendab ründajate võimalusi pikka aega sama parooli kasutamiseks. Paroolid peaksid olema hästi kaitstud,

hoides neid turvalistes paroolihaldurites või kasutades kaheastmelist autentimist. Veebisaidi omanikud peaksid kasutama just sellist paroolipoliitikat, mis aitab kaitsta nende konto- ja kliendiandmeid, et seeläbi ennetada küberrünnakuid. [20]

2.6.5 Tarkvara värskendamine

Kui veebisaidi tarkvara ei ole ajakohane, võib selles esineda turvavigu, mida kurjategijad saavad ära kasutada, et saidile juurde pääseda või sealt andmeid varastada. Vananenud tarkvara võib sisaldada tuntud haavatavusi, mida on lihtne rünnata. Tarkvara värskendamise eesmärk on edendada tarkvara turvalisust, parandades sellega turvaauke ja haavatavusi, mis on leitud varasematest versioonidest. [21]

Seega on oluline tarkvara värskendada regulaarselt, et saada kasutada uusimaid vastava tarkvara turvapoliitikaid ja kaitsta seeläbi veebilehte uute rünnakute eest. Kuigi paljud seadmed ja rakendused suudavad värskendusi automaatselt installida, on mõnikord vaja ka kasutaja sekkumist. Seetõttu on oluline jälgida, millal uued värskendused saadaval on, et need õigeaegselt installida. [21]

3 WordPressi veebilehtede turvamine ja analüüsimine

Antud peatükis kirjeldatakse autori töökoha ehk ettevõtte Web Design Agency OÜ (vDisain) veebilehtede arendusel peamist kasutatavat tehnoloogiat, milleks on WordPress. Tuuakse välja antud sisuhaldussüsteemi kasutatavate veebilehtede levinud turvariskid ja kuidas nendest hoiduda. Lisaks uuritakse mõõdikuid, mille abil saab hinnata turvalisuse taset WordPressi veebilehtedel ning tutvustatakse tööriistu, mis võimaldavad nende analüüsimist.

3.1 WordPress sisuhaldussüsteem

WordPress on üks enimkasutatavaid sisuhaldussüsteeme (CMS), mis võimaldab kasutajatel luua ja hallata veebilehti. WordPress loodi algselt blogimisplatvormina, mida arendasid Matt Mullenweg ja Mike Little. Esimene WordPressi versioon ilmus 2003. aastal ning alates sellest ajast on platvormi pidevalt täiustatud ja arendatud. WordPress pakub kasutajatele palju funktsioone, näiteks erinevad teemad, mis määravad veebilehe kujunduse ning pluginad, mis lisavad funktsioone, et luua dünaamilisi veebilehtede lahendusi [22]. [24]

Hetkel kasutab 810 miljonit veebilehte WordPressi platvormi ning igapäevaselt luuakse sellega üle 500 uue veebilehekülje. Allpool joonisel on välja toodud enim kasutatavate sisuhaldussüsteemi platvormide turuosad alates aastast 2014 kuni käesoleva aasta jaanuarini. Joonise 2 põhjal on antud platvorm olnud kõige kiiremini kasvav CMS vaadeldaval perioodil, võrreldes konkurentidega ning moodustab 2023. aasta seisuga 43,1% kõigist maailma veebisaitidest, tõstes ta kindlale turuliidri positsioonile [23]. [24]

CMS PLATFORM	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023 (JAN 1)
None	**64.8%**	61.7%	56.6%	53.3%	51.3%	45.3%	43.1%	38.3%	33.8%	32.3%
WordPress	21.0%	23.3%	25.6%	27.3%	29.2%	32.7%	35.4%	39.5%	**43.2%**	43.1%
Shopify	0.1%	0.3%	0.4%	0.6%	0.9%	1.4%	1.9%	3.2%	**4.4%**	3.8%
Joomla	3.3%	3.3%	3.3%	**3.4%**	3.2%	3.0%	2.6%	2.2%	1.7%	1.8%
Drupal	1.9%	2.0%	2.1%	2.2%	**2.3%**	1.9%	1.7%	1.5%	1.3%	1.2%
Wix	0.1%	0.1%	0.2%	0.3%	0.4%	1.0%	1.3%	1.5%	1.9%	**2.4%**
Squarespace	0.1%	0.2%	0.4%	0.5%	0.7%	1.4%	1.5%	1.4%	1.8%	**2.0%**

Peak year for every CMS bolded

Joonis 2. WordPressi turu osakaal teiste CMS-idega [23].

WordPress on avatud lähtekoodiga platvorm, mis tähendab, et seda saab tasuta alla laadida, kasutada ja kohandada. Täpsemalt on see PHP programmeerimiskeeles kirjutatud sisuhaldussüsteem, mis rakendab MySQL andmebaasi [25]. WordPressi veebilehe loomiseks vajab kasutaja vaid domeeninime ja veebimajutuskontot. Seda saab kasutada mis tahes veebimajutuse paketi abil, mis vastab sobivatele nõuetele. [27]

WordPress pakub kasutajatele suurt valikut erinevaid teemasid, mis võimaldavad luua oma veebisaidile unikaalse ja atraktiivse kujunduse. Iga teemat on võimalik reaalajas enne paigaldamist eelvaadata, mis annab kasutajale võimaluse visuaalselt näha, kuidas teema võiks nende saidi välimust mõjutada. Lisaks on teemasid võimalik igal ajal vahetada, et muuta oma veebisaidi välimust ja sisu paigutust vastavalt soovile. [27]

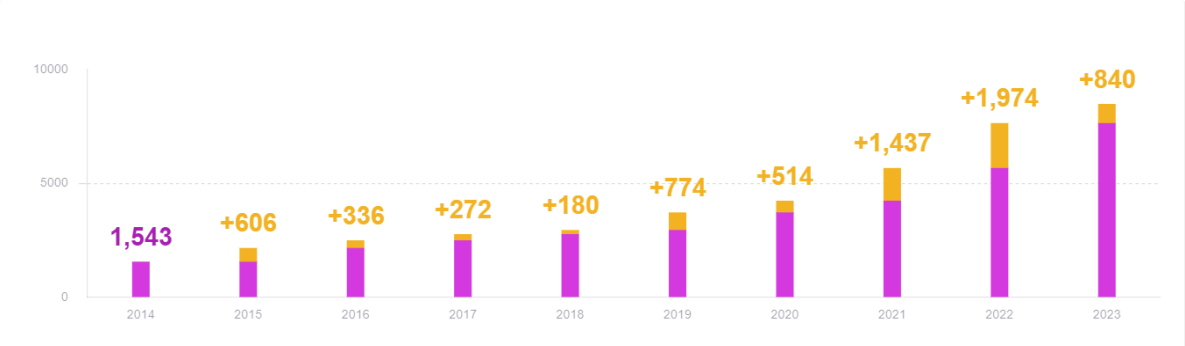
WordPressi pluginate abil saab lisada veebisaidile palju funktsioone ja võimalusi, mida platvorm vaikimisi ei paku. Hetkel on maailmas 60 324 WordPressi pluginat [26]. Kõige populaarsemad pluginate tüübid on e-kaubandus, turvalisus, SEO, kontaktvormid ja lehe koostajad (*page builders*). Installitud pluginate abil on võimalik lisada näiteks

sotsiaalmeedia jagamise nuppe, optimeerida oma veebisaidi SEO-d, lisada kontaktvorme või analüüsida statistikat. [27]

Süsteemi eelised võivad kaasa tuua ka negatiivseid pooli. Nimelt mõjutavad lehe kiirust paljude funktsioonide ja lisamoodulite olemasolu. Näiteks suured pildifailid, pluginate lisamine, halvasti optimeeritud teemad ja suurem külastajate arv aeglustada veebilehe kiirust. Lisaks on WordPressi kasutamine muutunud väga populaarseks erineva skoobiga veebilehtede loomiseks, sest platvorm on avatud lähtekoodiga ning selle rakendamine on tasuta. Välja toodud aspektidest järeldades on see sihtmärgiks paljudele pahavara ründajatele, mis toob esile antud süsteemi ühe peamise puuduse - turvalisuse. [28]

3.2 WordPressi turvalisuse ohud

On üldiselt teada, et iga interneti kasutamisega seotud tegevus hõlmab erinevaid turvariske, mida tuleks teada ja ennetada. Antud aspekt kehtib ka WordPressi puhul. WordPressi turvanõrkused ei tulene ainult selle tuumast, vaid lõviosa haavatavusest moodustavad hoopis veebilehele installeeritud pluginad ja väiksema osa ka teemad. 2022. aastal jälgiti WordPressi turvameeskonna poolt 1779 erinevat turuvaauku, millest 93,25% oli seotud pluginatega, 5,45% teemadega ja 1,29% põhiosaga [29]. Turvariskide hulk suureneb iga aastaga WordPressi populaarsuse, häkkerite oskuste ning kasutajate hooletuse kasvamise tõttu (Joonis 3). Järgnevalt uuritakse detailsemalt süsteemi võimalikke turvariske.



Joonis 3. WordPressi turvaaukude kasv aastatega [30].

Aegunud põhitarkvara

WordPress annab regulaarselt välja oma tarkvara uusi versioone, kuid ainult 54,3% kasutajatest kasutab tarkvara uusimat versiooni [3]. Osa kasutajatest ei ole teadlikud uue versiooni olemasolust, osad aga kardavad oma WordPressi veebisaite värskendada. Arvatakse, et uuendus ei suuda kohaneda nende veebilehega ning rikub selle. Siinkohal on abiks esimeses peatükis mainitud *backup* ehk varukoopia veebilehest, mis aitab veebilehe taastada, kui uuendades peaks midagi katki minema. [31]

Kui kasutaja ei värskenda platvormi, jäetakse veebileht tahtlikult turvaohtudele avatuks. Aja jooksul leiavad häkkerid juba avastatud ning vanal versioonil veel parandamata jäänud turvaaugud ning saavad neid kasutades võimaluse rünnata veebilehte [31]. Iga WordPressi uus versioon parandab teadaolevad turvaaugud ja kriitilised turvaprobleemid. Näiteks WordPressi versioon 5.8.1 sisaldas parandusi kolmele suurele haavatavusele, sealhulgas *Cross-Site Scripting* haavatavusele Gutenbergi plokiredaktoris. [31]

Aegunud või mitte usaldusväärsed pluginad ja teemad

Antud peatüki sissejuhatavas lõigus tõi autor välja, et enamus turvaaukudest on seotud just pluginate või teemadega. Erinevaid pistikprogramme ja teemasid on palju ning paraku ei ole WordPressi turvameeskonnal võimalik kõikide usaldusväärsust kontrollida. Neid võivad näiteks vabatahtlikud käsitsi üle vaadata, mis ei garanteeri nende ohutust. Kui arendaja on plugina edasiarendamise lõpetanud, saavad kasutajad seda ikka edasi kasutada, mille tagajärjel jääb tähelepanuta nii võimalikud olemasolevad kui ka aja jooksul tekkinud haavatavused, mis ohustavad veebilehe turvalisust. [33]

Üldiselt värskendavad arendajad siiski pistikprogramme ja teemasid regulaarselt, parandades avastatud turvaaugud ning lisades funktsionaalsust. Siinkohal langeb veebilehe avatus turvariskidele tihti kasutaja kaela, kes lihtsalt ei uuenda enda veebilehte, jäädes kasutama moodulite vananenud versioone. Võttes näiteks Wordfence'i uuringu, kus selgus, et 1032-st häkitud veebilehest 55,9% olid põhjustatud uuendamata pluginatest, mille aegunud versioonidel avastatud turvavead olid uutel versioonidel juba parandatud. [32], [33]

Määratlemata kasutajarollid

WordPressil on viis peamist kasutajarolli: tellija (*subscriber*), kaastööline (*contributor*), autor (*author*), toimetaja (*editor*), administraator (*administrator*). Igal rollil on oma

kindlad õigused, mis lubavad või piiravad kasutajatel sooritada konkreetseid toiminguid. Administraatoril on juurdepääs kõigile võimalikele veebisaidi toimingutele, samal ajal kui tellijal on võimalus ainult sisu lugeda. [34]

Turvariskide vähendamiseks tuleb veenduda, et kõigil saidi kasutajatel oleksid ainult need õigused, mis on neile vajalikud. Kui veebilehel on mitu kasutajat ja kõik peaksid olema administraatorid, on rünnakukatset sooritaval häkkeril palju suurem tõenäosus saada juurdepääs tervele lehele ehk tegutseda administraatori rolli all. Halvasti määratletud rollid suurendavad haavatavust, sest tagajärjena võivad need ründajale anda lehe üle täieliku kontrolli, mille kaudu on lihtsam teostada erinevaid ründemeetodeid nagu *Cross-Site Scripting* ja *Bruce-force* rünnakud. [31]

3.3 WordPressi turvamise meetodid

Võttes arvesse kõiki eelpool peatükkides mainitud turvaohtusid on olemas ka mitmeid erinevaid meetodeid, mida saab kasutada, et veebilehtede turvalisust parandada. Järgnevalt tuuakse välja turvameetmed, mida on soovituslik rakendada:

1. **Elementaarsete turvameetmete rakendamine**

   Turvalisuse tagamiseks tuleks kasutada alati uusimaid WordPressi ja PHP versioone. Teemasid ja pistikprogramme tuleks alla laadida ainult usaldusväärsetest allikatest, näiteks mooduli arendaja enda veebileheküljelt või ametlikest WordPressi hoidlatest, oluline on see juures hoida neid ajakohastena. Turvaaukude teket vähendab ka pluginate ja teemade eemaldamine, mis veebilehel enam kasutust ei vaja. [36]

   Lisaks on soovitatav kasutada tugevaid paroole ja muuta neid regulaarselt, järgides tugevat paroolipoliitikat. Lisaturvalisuse tagamiseks võimalusel kasutada kaheastmelist autentimist, mis nõuab lisaks paroolile kasutaja tuvastamiseks täiendavat ajatundlikku koodi teisest seadmest, näiteks nutitelefonist. See minimeerib peaaegu täielikult *Bruce-force* rünnakute potentsiaalse õnnestumise [35]. [36]

2. **Vormide turvamine**

   Teiseks WordPressi saidi turvalisemaks muutmise võimaluseks on vaikimisi sisselogimislehe peitmine. Tavaliselt tuleb igale WordPressi veebisaidile sisselogimiseks lisada veebilehe lingi (URL) lõppu: */wp-admin* ning seejärel avaneb sisselogimisevorm. Seda linki muutes on võimalik tõhusalt peita enda lehe sissepääs

ning seeläbi on rünnakute sooritamine häkkeritele raskem. Lisaturvalisuse saavutamiseks on võimalik pluginate abiga piirata ka sisselogimiskatseid. [37]

Teine põhiline vorm veebilehel on kasutajale täitmiseks mõeldud vorm, kuhu tavaliselt sisestatakse kontaktandmeid. Soovituslik oleks vormidele lisada *reCaptcha*, mis on automaatne test, mis eristab inimesi arvutiprogrammidest, tagades, et sisestatud teave tuleb inimeselt, mitte automatiseeritud tarkvaralt. See on oluline, kuna roboteid kasutatakse paljude küberrünnakute meetodite puhul. Siinkohal saab jälle välja tuua levinumad häkkimisstrateegiaid *Cross-Site Scripting* ja *Bruce-force* rünnakud, mis mainitud turvaauku ära kasutavad. [37]

3. Turvapluginad

Turvapluginate kasutamine on üks olulisi turvameetmeid, mida WordPressi saitidel tuleks rakendada, sest need lisavad veebisaidile täiendava kaitsekihi. Iga veebisait on ainulaadne ja võib sisaldada erinevaid turvaprobleeme. E-pood, mis töötleb klientide krediitkaardiandmeid võib vajada palju mahukamat kaitset oma funktsionaalsuste tõttu, võrreldes näiteks lihtsama fotograafi portfoolio kodulehega. WordPress pakub varieeruvate funktsionaalsustega pluginaid, mille täpsemaid omadusi uuritakse lähemalt järgmises alapeatükis. [38]

3.4 Turvamisvahendid

WordPressi veebilehtede turvalisuse tagamiseks on võimalik kasutada erinevate turvamiseks loodud pistikprogrammide funktsionaalsusi, mis aitavad tuvastada ja lahendada erinevaid turvalisusprobleeme ning tagada, et veebileht oleks kaitstud küberrünnakute eest. Autor toob esile kuus olulisemat funktsiooni, mis aitavad oluliselt tugevdada WordPressi veebilehtede kaitsekihti ning mida tuleks arvesse võtta turvalisuse plugina valikul [39]:

- **Veebirakenduse tulemüür (WAF) -** kaitseb saiti rünnakute eest, tuvastades ja blokeerides pahatahtlikud IP-aadressid veebiserverist ning teatud tüüpi rünnakud nagu näiteks *Brute-Force* ja DdoS/DoS, piirates administraatori sisselogimislehe sisselogimiskatsete arvu.

- **Pahavara skanner -** skaneerib veebilehte pahavara ja muude turvaohtude suhtes, blokeerides päringud, mis sisaldavad pahatahtlikku koodi või sisu.

- **Ründest teavitamine** - tuvastab ründeid ja hoiatab nende kohta, saates kasutajale meilihoiatuse.
- **Pahavara eemaldamine -** aitab eemaldada leitud pahavara.
- **Kaheastmeline autentimine** - lisab lehele sisselogimiseks täiendava turvakihi, nõudes sisselogimiseks lisateavet lisaks kasutajanimele ja paroolile.
- ***reCAPTCHA*** - väldib robotite sisselogimist ja piirab rämpsposti, kontrollides, et sisse logiv või kommentaare postitav isik on tõepoolest inimene.

Turvamisvahendite võrdlus

Järgnevalt uuritakse detailselt kolme populaarseimat WordPressi veebilehtede turvalisuse tagamise jaoks mõeldud pluginat: *Wordfence*, *iThemes* ja *Sucuri*, võrreldes nende eeliseid ja puudusi, et seeläbi leida nende hulgast autori arvates optimaalseim valik. Iga plugina funktsionaalsus, positiivsed ja negatiivsed aspektid ning hinnastus on täpsemalt esitatud töö lisades (Lisa 2, Lisa 3, Lisa 4). Järgnevates tabelites on välja toodud kolme plugina olulisemate turvalisuse funktsioonide võrdlus. Funktsioonid on jaotatud nelja kategooriasse: monitooring ja skaneerimine, kaitse kombineerituna tulemüüridega, WordPressi turvameetmed ning pahavara ja jõudluse eemaldamine. Esimeses tabelis on esitatud pluginate üldine informatsioon. (Tabel 1, Tabel 2, Tabel 3, Tabel 4, Tabel 5)

Tabel 1. Wordfence, iThemes, Sucuri turvapluginate üldine info.

Üldine info			
Plugin/Funktsioon	**Wordfence**	**iThemes**	**Sucuri**
Aktiivsed paigaldused	3+ miljonit	900 000+	700 000+
Hinnangute arv	3572	3830	338
Hinnang (1-5)	4,8	4,7	4,4
Tasuta versioon	Jah	Jah	Jah
Premium (aastane litsents)	Alates 99 $	Alates 80 $	199,99 $

Tabelist 1 saab välja lugeda, et kõik kolm pluginat on kõrgelt hinnatud ning populaarsed. Wordfence võtab siiski liidri koha endale, arvestades paigalduste ja hinnangute arvu ning hinnangute suurust. Kui tasuta versioonide funktsionaalsused jäävad oma võimekuselt soovitule alla, siis on väikse eelarve puhul mõistlikuim variant iThemes plugin.

Tabel 2. Wordfence, iThemes, Sucuri turvapluginate võrdlus. Monitooring ja skaneerimine.

Monitooring ja skaneerimine			
Plugin/Funktsioon	**Wordfence**	**iThemes**	**Sucuri**
Plaanitud turvakontrollid	Pro versioon ainult	Pro versioon ainult	Pro versioon ainult
Pahavara tuvastamine	Jah	Jah	Jah
Musta nimekirja monitooring	Ainult Google'i ohutu sirvimine	Musta nimekirja olekukontroll	Jah
SSL monitooring	Ei	Jah	Jah
Teavitused	Jah	Jah	Jah
Rämpsposti kontroll	Pro versioon ainult	Jah	Jah
Turvalogid	Jah	Jah	Algeline

Tabel 2 näitab kõigi kolme plugina üsna tugevat taset monitooringu ja skaneerimise funktsioonide seisukohalt. Monitooringu vaatenurgast on Wordfence'i reaalajas liikluse funktsioon suureks eeliseks, kuid musta nimekirja monitooring on iThemes ja Sucuril siiski tõhusam. SSL monitooringu puhul on nõrgim lüli Wordfence ning logifailide olemasolu võimekusest jääb Sucuril vajaka.

Tabel 3. Wordfence, iThemes, Sucuri turvapluginate võrdlus. Kaitse kombineeritud tulemüüridega.

Kaitse kombineerituna tulemüüridega			
Plugin/Funktsioon	**Wordfence**	**iThemes**	**Sucuri**
Veebirakenduse tulemüür (WAF)	Piiratud	404 tuvastamine	Jah
DDoS kaitse	Ei	Ei	Jah
Brute Force kaitse	Jah	Jah	Jah
Häkkimiskatsete blokeerimine	Jah	Osaline	Jah
Täiustatud käsitsi blokeerimine	Jah	Ei	Ei

Tabel 3 põhjal saab välja tuua selgeimad pluginate omavahelised erinevused. Arvestades, et iThemes kasutab vaid 404 tuvastamisi, mis ei kaitse veebilehte reaalsete rünnakute eest, võib väita, et iThemes ei kasuta tegelikku tulemüüri veebiturbe meetodit. Sucuri tulemüür ning sellega seotud enamik olulised funktsioonid on võrreldes teistega tugevaima

jõudlusega ning automatiseeritud. Manuaalse blokeerimise puhul on eelistatuim Wordfence, mis võimaldab üksikuid riike eraldi blokeerida, mis on manuaalse häkkimise puhul boonuseks.

Tabel 4. Wordfence, iThemes, Sucuri turvapluginate võrdlus. WordPressi turvameetmed.

WordPressi turvameetmed			
Plugin/Funktsioon	**Wordfence**	**iThemes**	**Sucuri**
Andmebaasi varukoopiad	Ei	Jah	Ei
Teabe peitmine	Ei	Jah	Ei
Kirjutamiskaitse	Ei	Jah	Ei
Paroolihaldus	Ei	Jah	Ei
Kaheastmeline autentimine	Premium	Premium	Ei

Tabel 4, mis annab ülevaate Wordpressi platvormi üldistest turvameetmetest, näitab, et liidripositsioonil antud kategoorias on kindlasti iThemes, sest tasuta versioon pakub ulatuslikku kaitset ning premium versioonis on oluline välja tuua kaheastmeline autentimine. Kuna Wordfence ja Sucuri ei keskendu WordPressi turvamise toimingutele, jäävad nad antud olukorras nõrgaks.

Tabel 5. Wordfence, iThemes, Sucuri turvapluginate võrdlus. Pahavara eemaldamine ja jõudlus.

Pahavara eemaldamine ja jõudlus			
Plugin/Funktsioon	**Wordfence**	**iThemes**	**Sucuri**
Pahavara eemaldamine	Premium	Puudub	Premium
Automaatne puhastamine	Osaline	Puudub	Osaline
Turvalünkade sulgemine	Premium	Puudub	Premium
Varukoopiad	Ei	Puudub	Jah

Tabel 5 põhjal saab öelda, et Sucuri ja Wordfence on siin kategoorias olemuselt sarnased. Mõlema puhul on pahavara eemaldamiseks vaja Premium versiooni. See-eest iThemes ei paku pahavara eemaldamise funktsionaalsust. Jõudluse puhul on oluline välja tuua, et kuna Sucuri pakub CDN-i (sisu edastamise võrgustik) ja tulemüüri integreeritud

funktsionaalsust, võimaldab see parandada veebilehe jõudlust eriti välismaa külastajate jaoks. [42]

Eelnevate tabelite põhjal võib järeldada, et kõikidel pluginatel on oma eelised ja puudused ning valik tuleks teha vastavalt veebilehe olemusele ning turvalisuse eesmärgile. Sellest hoolimata leiab autor, et efektiivsemaid ja kasutajasõbralikumaid võimalusi veebilehtede turvamiseks pakub Wordfence, mis on WordPressi populaarseim turvalisuse plugin. Wordfence-i fookus on suunatud kahele olulisemale turvaplugina elemendile nagu tulemüür ja turvakontrollid, pakkudes juba tasuta versioonis täielikku tulemüüri. Premium versioonis integreeritakse funktsioone konkreetselt ja mõistlikult. Lisaks on selle seadistamine lihtne, arusaadav ning ei vaja suuri tehnilisi oskuseid, mis võib miinuseks olla teiste pluginate puhul. Wordfence-i suurimaks miinuseks on serveriressursi kasutus skaneeringute puhul, kuid viga saab lahendada plugina korrektse seadistusega, vältimaks jõudlusprobleeme.

Wordfence on kasutusel enamikel Web Design Agency OÜ-s arendatud veebilehtedel, sest antud plugina funktsionaalsus ühtib ettevõtte teenuste turvalisuse standarditega. Seega puutub töö autor antud turvaplugina rakendamisega igapäevaselt kokku. Autori isikliku positiivse kogemuse põhjal ning vDisainis Wordfence kasutamise võimaluse olemasolu tõttu, kasutatakse pluginat ka antud lõputöö praktilises osas reaalse kliendi veebilehe turvamiseks. Turvaplugina rakendamise kogemuse põhjal on koos Wordfence-ga mõistlik kasutada täiendavaid pluginaid nagu *Headers Security Advanced &* HSTS WP ja *WP Hardening*. Nende tugevateks külgedeks on veebilehele suunatud päringute krüpteerimine ning turvaseadete kasutajasõbralik kohandamine.

3.5 Mõõdikud turvalisuse hindamiseks

Veebilehe turvamõõdikud on turvalisuse hindamiseks kasutatavad mõõtevahendid, mis aitavad kvantitatiivselt mõõta kindla aspekti alusel lehe turvataset. Turvamõõdikute eesmärk on aidata tuvastada ja hinnata turvaprobleeme, et saaks nende vastu tõhusalt võidelda. Järgnevalt on loetletud peamised turvamõõdikud, mille alusel saab hõlpsamalt hinnata veebilehe üldist turvaseisundit [44]:

- **Pahavara tuvastus** – mõõdik pahavara või viiruste avastamiseks, mis on tuvastatud analüüsitaval veebilehel.

- **Tulemüüri olemasolu** – mõõteriist, mis kontrollib, kas analüüsitaval veebilehel on olemas peamine küberrünnakute eest kaitsev vahend ehk tulemüür.

- **Musta nimekirja kuuluvus** – mõõdik, mis tuvastab, kas veebisait on määratud turvaohtlikuks või ebasoovitavaks ja seetõttu blokeeritud või piiranud juurdepääsu teatud võrguliiklusele.

- **Siseserveri errorid** – mõõtevahend, mis teeb kindlaks, kas veebilehel on siseserveri vigu, mis paljastava serveri konfiguratsiooniteavet, tundlikke andmeid või muid turvavigu.

- **Veebilehe ajakohasus** – mõõdik, mis kontrollib analüüsitava veebilehe WordPressi ja PHP versioone, et leht omaks viimaseid turvaparandusi ja uuendusi ning toimuks sujuv süsteemi käitamine serveris.

- **HTTP-turvapäiste olemasolu ja korrektne seadistus –** mõõtevahend, mis kontrollib erinevate päiste eksisteerimist ning kas need on õigesti konfigureeritud, et piirata brauseri ja serveri lubatud käitumist, kui veebirakendus töötab [43].

3.6 Vahendid veebilehtede analüüsimiseks

Veebilehtede turvalisuse analüüsimine on oluline, sest see aitab kindlaks teha analüüsitava lehe hetke turvaseisundi ning tuvastada põhjused, mis võivad mõjutada turvalisust. Selleks on olemas erinevaid veebilehe analüsaatorid, mis aitavad hinnata ja analüüsida veebisaidi turvalisust, tuvastada turvariskid ja soovitada parandusmeetmeid.

Antud protsessi on oluline läbi viia enne mistahes veebilehe turvaliseks tegemist, et vältida või tuvastada turvalisusprobleeme, mis võivad kahjustada veebisaidi mainet, kasutajate privaatsust ja andmete turvalisust. Autor toob välja kaks turvalisuse analüsaatorit *SiteCheck* ja *Security Headers*, mis aitavad analüüsida veebilehe turvalisust ja leida puudusi, mis vajaksid parendamist turvariskide langetamiseks.

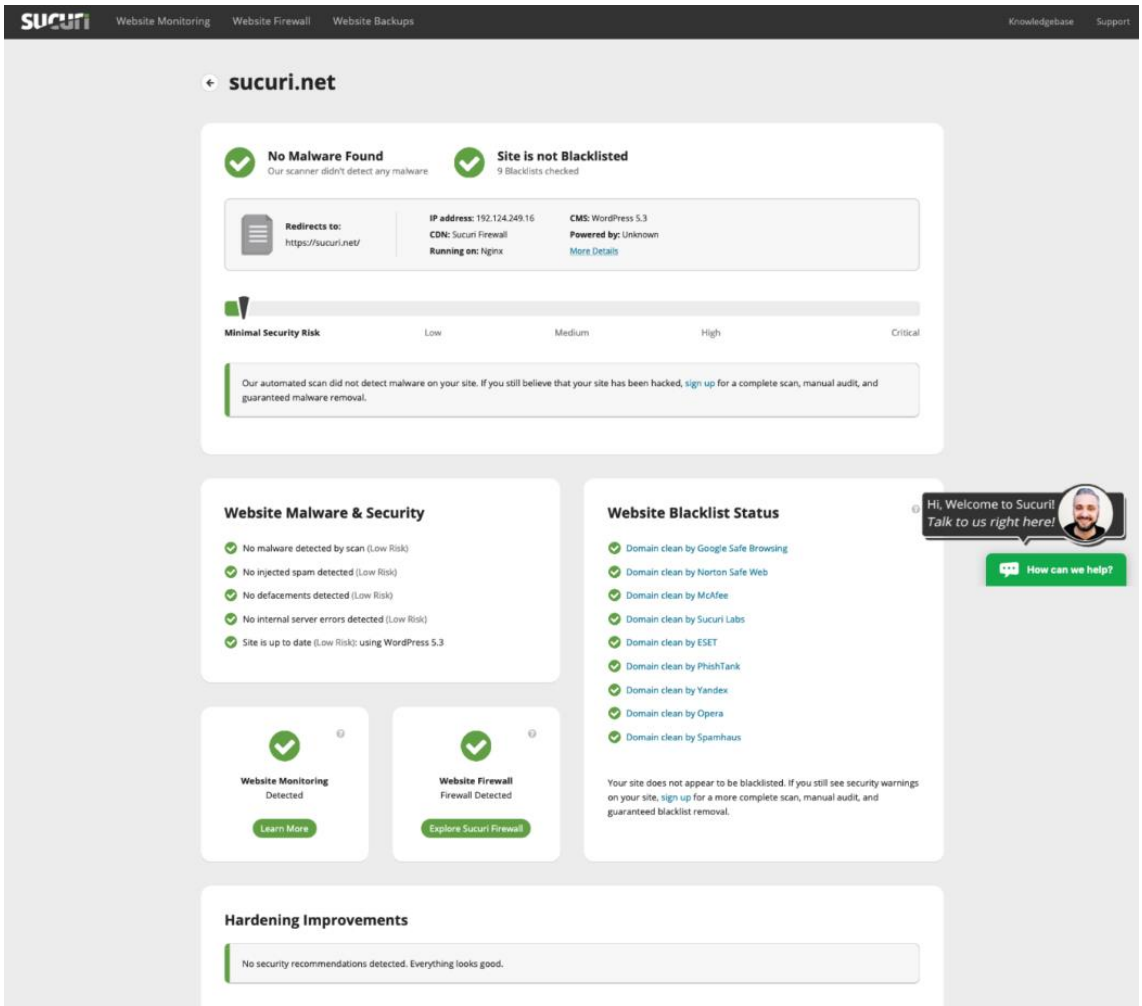
3.6.1 SiteCheck

SiteCheck on üks populaarsemaid veebilehe analüsaatoreid, mida pakub veebiturbeettevõte Sucuri. Täpsemalt on tegemist kaugskanneriga ehk veebilehe

külastamine toimub samamoodi nagu teevad kõik selle lehe veebikülastajad (või otsingumootori robotid), kontrollides lehte pahavara suhtes. [44]

SiteCheck skannib veebilehe erinevaid osi, sealhulgas HTML-i, JavaScripti ja CSS-i faile, analüsaator teeb kindlaks manustatud objektid või pluginad ning uurib andmebaasi sisu ja serveri konfiguratsiooni. Skannimisprotsess on automaatne ja võtab tavaliselt vaid mõne minuti. [44]

Kui skaneerimine on lõpetatud, annab analüsaator veebilehe turvaseisu kohta üksikasjaliku raporti. See sisaldab informatsiooni tuntud pahavara, pahavara mustrite, veebisaidi vigade, aegunud tarkvara, pahatahtliku koodi ning turvalisuse soovituste kohta. Lisaks sisaldab raport ka teavet veebilehe reputatsiooni ja musta nimekirja kuulumise kohta (Joonis 4). [44]



Joonis 4. Näidistulemused SiteCheck analüsaatoris [43].

3.6.2 Security Headers

Lisaks eelnevalt kirjeldatud analüsaatorile on mõistlik lehte skaneerida ka Security Headersi analüsaatoriga, et saada detailsemaid tulemusi HTTP-turvapäiste konfiguratsiooni kohta, et seeläbi kindlustada usaldusväärse ja ohutu teabe edastamist veebisaidi külastajatele.

Päised (*Headers*) on osa HTTP protokollist, mida kasutatakse veebilehe andmete edastamiseks veebiserverist brauserisse. Need sisaldavad teavet veebisaidi ja selle sisu kohta ning tagavad selle tõrgeteta toimimist. Halvasti konfigureeritud päised võivad jätta veebisaidi haavatavaks rünnakutele, näiteks *Cross-Site Scripting* (XSS). [43]

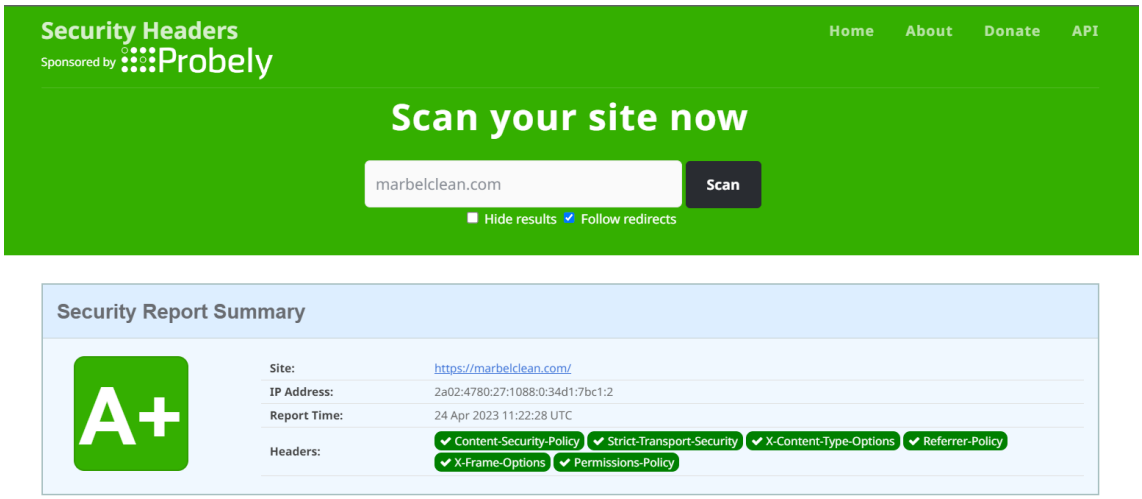
Kuna HTTP-protokolli päiste ajakohasus muutub pidevalt, on turvalisuse tagamiseks oluline jälgida ja parandada nende konfiguratsiooni vastavalt parimatele tavadele. Näiteks võib turvalisuse tagamiseks keelata ohtlikud päised, nagu *Serveri header*, mis annab kurjategijatele teavet kasutatava veebiserveri kohta. Peamised turvalisusele suunatud päised, mida tuvastab ka Security Headers analüsaator on järgmised [43]:

- **HTTP *Strict-Transport-Security* (HSTS - Range transpordi turvalisus)** - võimaldab tagada, et leht ja kõik selle alamdomeenid kasutavad ainult SSL sidet ehk brauser külastab veebisaiti alati HTTPS-i kaudu, isegi kui kasutaja sisestab aadressiribale ainult HTTP-ühenduse. See turvameede tagab, et kõik andmed, mis edastatakse veebirakenduse ja veebibrauseri vahel, on krüpteeritud ja kaitstud.

- ***Content-Security-Policy* (CSP - Sisu turvalisus poliitika)** - võimaldab kontrollida, millist tüüpi sisu saab veebisaidile laadida. Antud turvameede aitab vältida *Cross-Site Scripting (XSS*) rünnakuid, sest piirab, milliseid skripte saab veebisaidile lisada. CSP aitab määrata, millistest allikatest saab veebibrauser laadida erinevaid ressursse, nagu näiteks pildid ja skriptid.

- ***X-Frame-Options* (X-raami valikud)** – võimaldab teha kindlaks, kuidas leht teiste veebisaitide raamides (HTML *iframes*) kuvatakse. See meetod aitab kaitsta veebilehte rünnete eest, kus ründaja kasutab veebisaidi välimust või toiminguid, näiteks *Cross-Site Scripting* (XSS) rünnakud, mis hõlmavad HTML-i *iframe*.

Security Headers analüsaator on arendajale hea abivahend, mis kontrollib automaatselt HTTP-turvapäiste olemasolu ja õigsust ning annab soovitusi vigade kõrvaldamiseks (Joonis 5).



Joonis 5. Näidistulemused Security Headers analüsaatoris [46].

3.6.3 Analüsaatori valik

Veebilehe analüsaatori valimisel on oluline arvesse võtta mitut aspekti. Tuleks arvestada eelnevalt välja toodud turvalisuse hindamise mõõdikutega ehk analüsaatori ulatuse keerukusega. Teine oluline aspekt on kasutusmugavus, mille alla kuuluvad seadistamise, kohandamise ja automatiseerimise lihtsus, tulemusraportite detailsus ja nende genereerimise kiirus ning valehäirete esinemise sagedus. Kindlasti on tähtis tähelepanu pöörata ka analüsaatori hinnastusele ja mainele. [47]

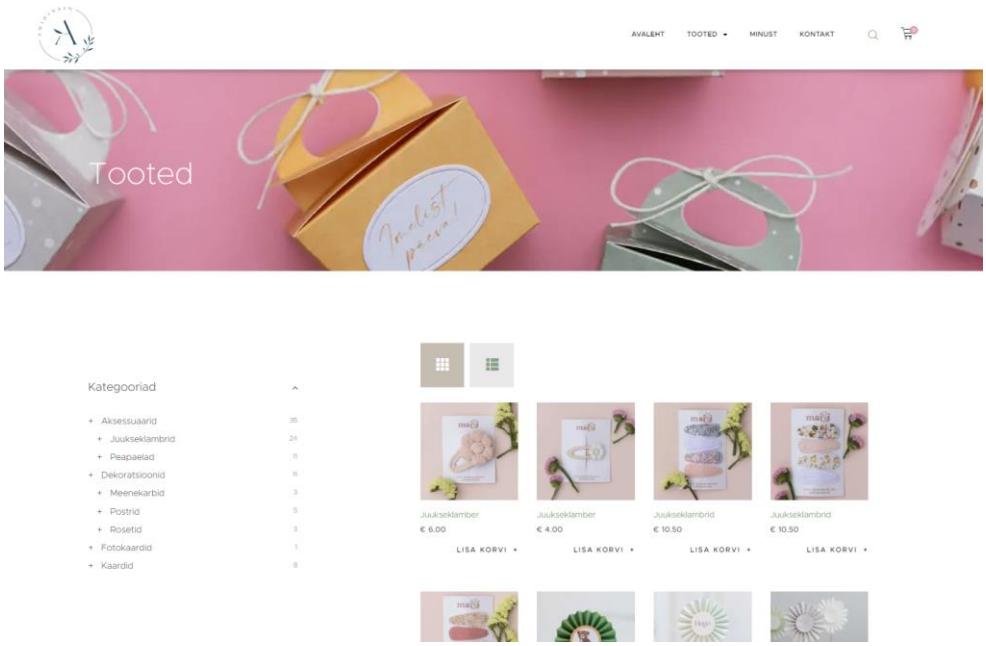
Iga analüsaator pakub erinevaid funktsionaalsusi ning valik tuleks teha analüüsitava veebilehe turvalisuse eesmärgi saavutamiseks vajaminevate toimingute vaatenurgast ehk milliseid aspekte peetakse prioriteetideks turvamise puhul. Kuna ettevõttes vDisain, kus töö autor töötab, kasutatakse eelpool mainitud analüsaatoreid ning autor ise on uurinud nende tausta ning võimekust, kasutatakse nende kahe kooslust ka töö viimases peatükis veebilehe turvamise tõhusama tulemuse saavutamiseks.

4 Ettevõtte Amidisain OÜ e-poe analüüs ja turvamine

Käesoleva bakalaureusetöö praktilise osa eesmärk on uurida Amidisain OÜ kodulehe turvalisust, seejärel rakendada turvamismeetodeid ning lõpuks võrrelda tulemusi turvamise järgselt. Vastavalt analüüsitulemustest rakendatakse turvalisuse meetodeid ja vahendeid, mis on kirjeldatud töö varasemates peatükkides, et parandada veebilehe üldist turvalisust ning seeläbi ka ettevõttes kasutusel olevaid teemakohaseid meetmeid. Viimase osana viiakse läbi pahavara monitooring, et hinnata kasutatavate meetodite efektiivsust. Turvamise tulemuse eesmärgiks on kasutada töös mainitud turvalisuse mõõdikuid ning tagada, et analüsaatori *SiteCheck*-i aruanne annaks veebilehe turvalisuse kohta madala turvariski taseme (*Low Security Risk*) ning *Security Headers* analüsaatori tulemus oleks tasemel A+.

4.1 Analüüsitav veebileht

Amidisain OÜ on Eestis tegutsev erinevate käsitöötoodete valmistamise ja müügiga tegelev väikeettevõte, kes on vDisaini klient ning kellele arendas koduleheküljе antud töö autor (Joonis 6). Tegemist on e-poega, mis kogub ja töötleb isikuandmeid, nagu kliendi nimi, aadress, e-posti aadress ja krediitkaardiandmed. Need isikuandmed on küberkurjategijate jaoks hinnaline sihtmärk, mida saab kasutada kahjulike tegevuste sooritamiseks. Seetõttu on vajalik tagada, et kõik Amidisaini e-poe külastajate andmed oleksid turvaliselt kaitstud.



Joonis 6. Amidisain OÜ kodulehe e-poe vaade.

Amidisaini koduleht on arendatud WordPressi sisuhaldussüsteemi platvormi peal, mille versioon on töö kirjutamise ajal 6.0 (uusim: 6.2) ning PHP versiooniks antud hetke seisuga on 7.4.0 (uusim: 8.1.16). Veebimajutaja on *Zone* ning ka domeen on seal registreeritud. Kasutatakse Apache veebiserverit ja MySQL andmebaasi. Veebileht on arendatud kasutades *WooCommerce* moodulit, mis on tasuta avatud lähtekoodiga e-poe pistikprogramm WordPressi veebisaitidele. See võimaldab hõlpsalt luua veebipoe ning müüa tooteid või teenuseid internetis. Antud veebilehe teemaks valis autor „*Craftise*“, sest sellel on olemas *WooCommerce* tugi. Lehel on enne turvalisuse meetodite rakendamist aktiveeritud 21 ning aktiveerimata 2 pluginat, millest 4 on uuendamata. Ükski aktiveeritud plugin ei oma turvalisuse funktsionaalsust. Veebilehe aadressiks on https://amidisain.ee.

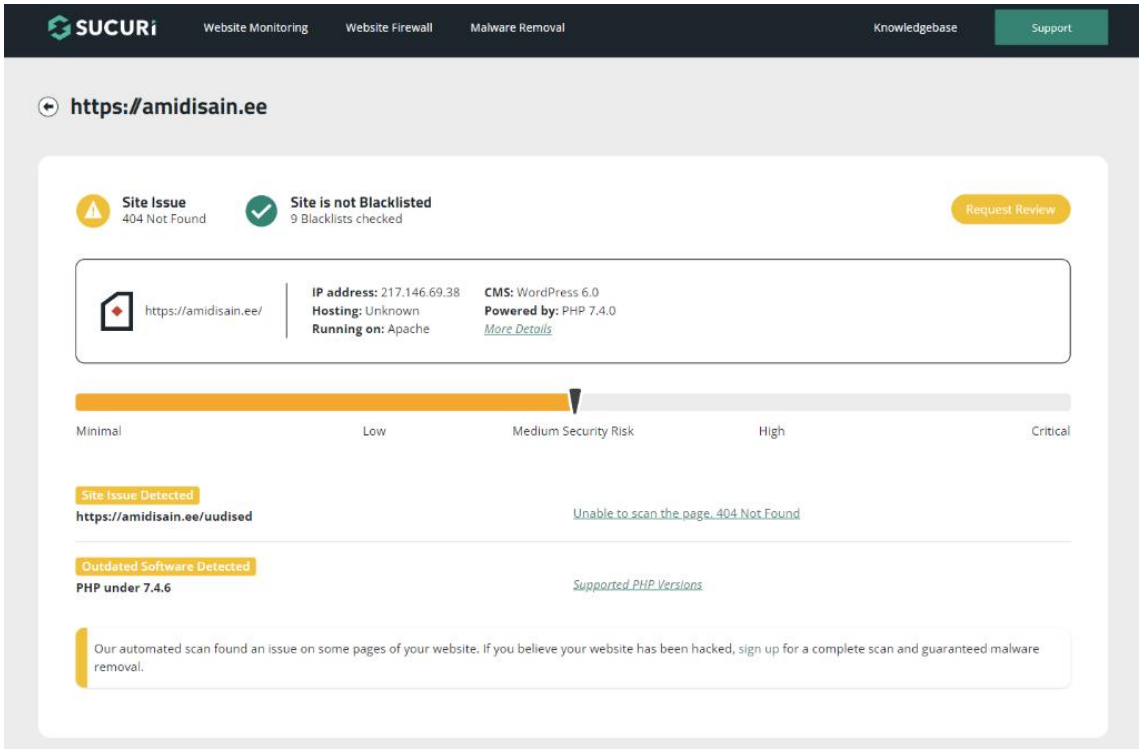
4.2 Veebilehe analüüs

Enne turvameetmete rakendamist on oluline teada veebilehe hetkelist turvaseisundit ja tuvastada olemasolevad ja võimalikud turvariskid, mis ohustavad veebilehte. Selleks on soovitatav kasutada erinevaid analüsaatoreid, sest igaüks neist keskendub erinevatele turvalisuse aspektidele ning nende tulemuste ühendamisel saab parima ülevaate lehe turvalisuse seisundist. Antud peatükis analüüsitakse Amidisaini veebisaidi turvaseisu

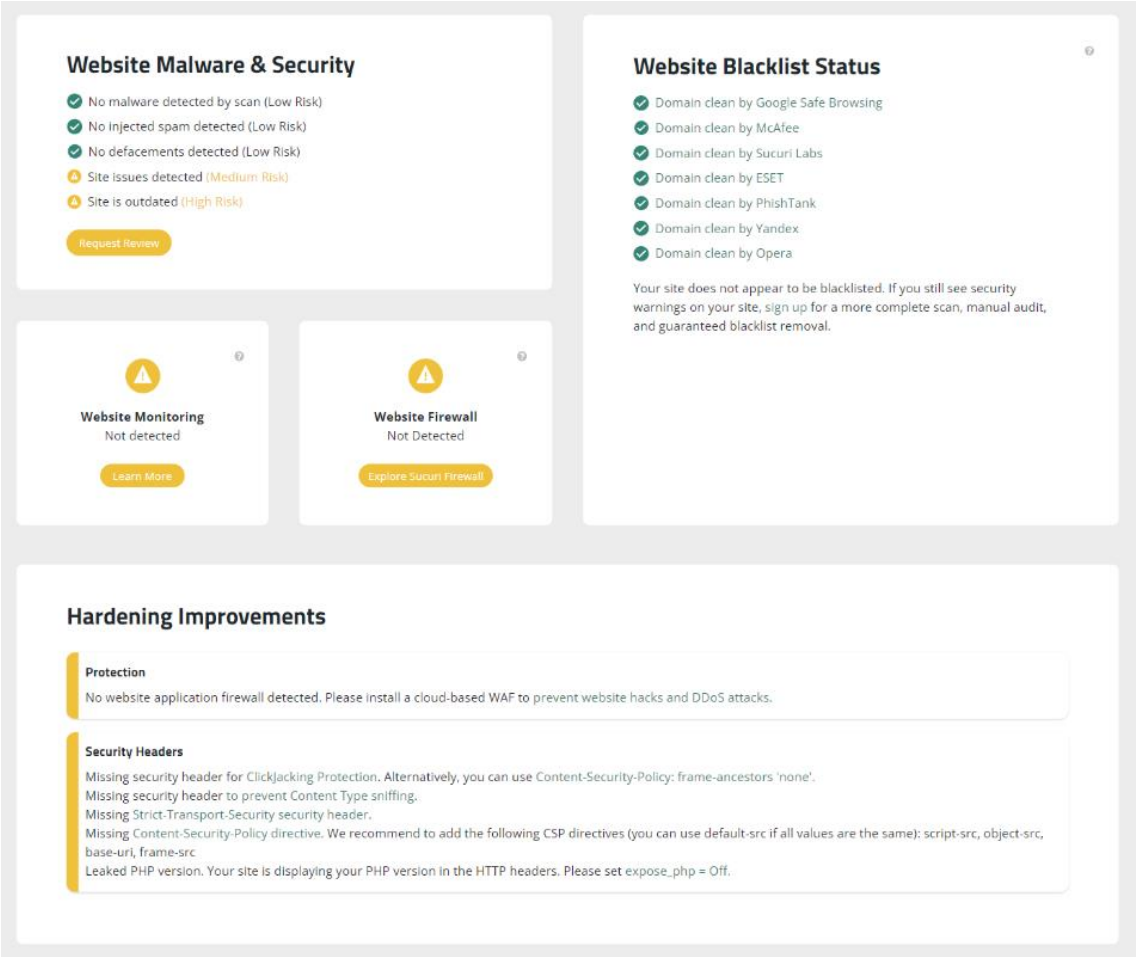
kasutades *SiteCheck* ja *Security Headers* analüüsimise tööriistade tasuta versioone. Seejärel kirjeldatakse detailselt nende aruannetest saadud analüüsitulemusi.

4.2.1 SiteCheck analüüsitulemused

Joonis 7 ja Joonis 8 näitavad Amidisaini kodulehe turvaseisundi aruande tulemusi SiteCheck analüsaatorist.



Joonis 7. SiteChecki esialgsed analüüsitulemused 1.



Joonis 8. SiteChecki esialgsed analüüsitulemused 2.

SiteChecki aruande põhjal on tulemused pigem kehvad, sest turvalisuse oht on määratud keskmisele riskitasemele. Tase tuleneb mitme avastatud probleemi koosmõjul. Nii WordPressi kui ka PHP versioonid on värskendamata. Uusim WordPressi versioon on hetke seisuga 6.2, kuid analüüsitava veebisaidi versiooniks on paraku 6.0. PHP kõige viimasem uuendus on 8.1.16., lehel aga on see hetkel vaid 7.4.0. Selle tõttu on skanner avastanud saidil probleemi nimega „*Outdated Software Detected*“ ehk tuvastati aegunud tarkvara, mis on liigitatud kõrgeks riskiks (*High Risk*). Aegunud tarkvara versioonid on kergem sihtmärk pahatahtlikele isikutele, kes otsivad haavatavaid veebilehti.

Teise aspektina saab raportist välja tuua keskmise tasemega (*Medium Risk*) probleemi mitteeksisteeriva lehe kohta. Nimelt oli kunagi antud lehel uudistesektsioon, kuid veebilehe omanik on selle eemaldanud. Menüüribale on jäänud siiski link, mis viitab lehele, mida ei ole võimalik leida serverist, kus see peaks olema, andes veakoodi 404. Antud viga veebilehel võib kasutajakogemust halvendada, sest veebileht ei suuda

kasutajale vajalikku sisu kuvada. Lisaks kahjustab see otsingumootori optimeerimist (SEO) ning annab teavet failistruktuuri ja kasutavate tehnoloogiate kohta, mida saab ründaja enda kasuks ära kasutada.

Kolmandana on oluline välja tuua tulemüüri puudumine (*No website application firewall detected*), mis on peamine turvalisuse meetod erinevate turvariskide vähendamiseks. Tulemüüri puudumine veebilehel võib põhjustada turvaaugud, mis avavad kurjategijatele tee veebilehele ja sealt edasi kasutajate andmetele. Tulemüür kaitseb veebiserverit ja sellega seotud seadmeid erinevate rünnakute eest. Lisaks ei ole antud veebilehel turvalisuse monitooringu funktsionaalsust (*Website Monitoring Not detected*). Turvalisuse monitooring aitab jälgida veebilehe turvalisust ja avastada turvavigu või ründeid enne nende laialdast levikut.

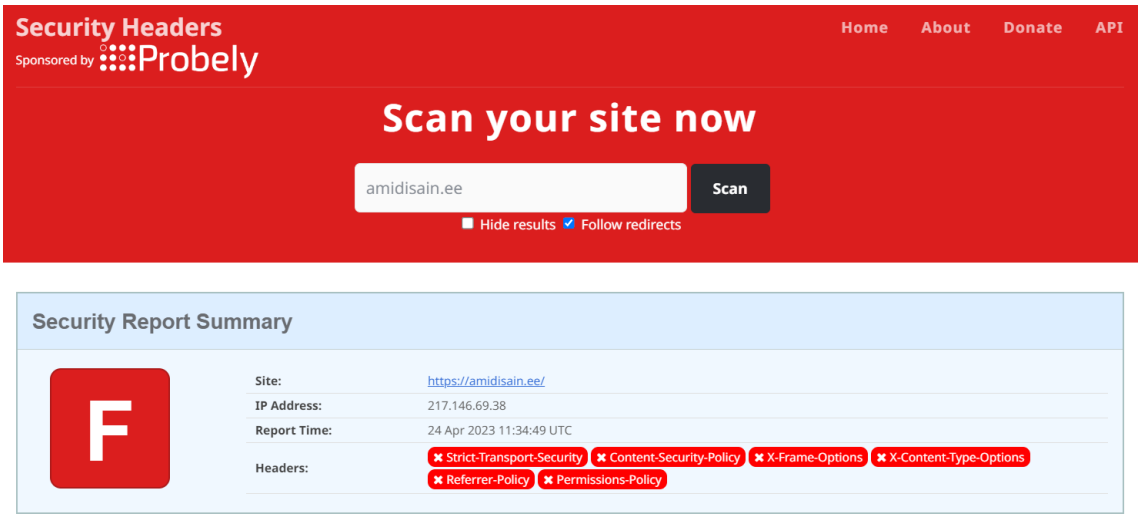
Neljanda turvariskina leiame raporti täiustuste (*Hardening Improvements*) alt turvapäiste probleemid (*Security Headers*) koos seadistuse soovitustega. Antud aruande põhjal on puudu olulised HTTP turvapäised, mida SiteCheck soovitab lisada veebisaidile, et suurendada selle turvalisust. Kui need päised puuduvad, võib see suurendada selle haavatavust erinevate veebirünnete vastu. Täpsemalt analüüsitakse erinevaid päiseid, nende korrektseid seadistusi ja vajalikkust järgmises alapeatükis Security Headers analüsaatori raporti tulemuste baasil. (peatükk 4.2.2)

Viimasena on mainitud, et saidil on HTTP päises avalikult nähtav PHP versiooninumber. Kui ründaja teab veebisaidi PHP versiooni, saab ta otsida teadaolevaid turvavigu, mida võib selles versioonis esineda. See võimaldab ründajal leida ja ära kasutada turvaauke, läbi mille saab lehte rünnata. Üks võimalus, mida soovitab ka SiteCheck on määrata PHP seadistustes *"expose_php = Off"*. See takistab PHP versiooni näitamist *HTTP* päistes ja aitab kaitsta seeläbi veebisaidi turvalisust.

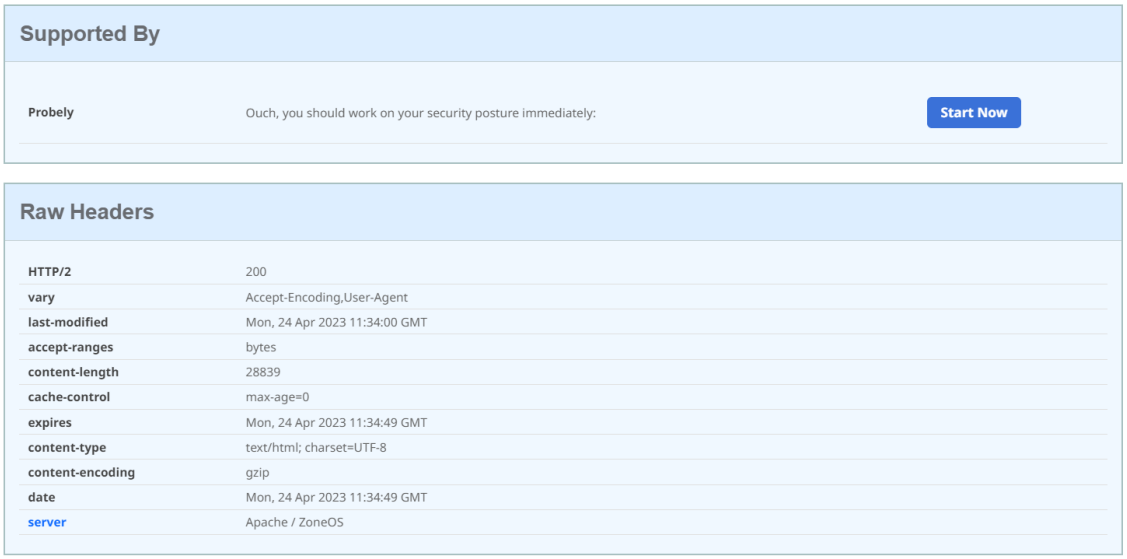
Positiivse poole pealt saab välja tuua, et lehelt ei tuvastatud pahavara, rämpsposti ega muid rikkumisi, mis ohustaks veebisaidi turvalisust. Kui analüsaator ei leia midagi sellist, siis ei sisalda veebileht mingeid pahatahtlikke koodijuppe ning ei kujuta ohtu kasutajatele**.** Lisaks ei kuulu veebileht musta nimekirja. *McAfee, Google, Yandex, Opera, Sucuri Labs, PhisTank, ESET* musta nimekirja andmebaasidest Amidisaini lehte ei leitud, mis tähendab, et veebisait pole määratud turvaohtlikuks. See tõstab kasutajate usaldust ja vähendab riski, et nende andmed või seadmed võiksid olla ohustatud.

4.2.2 Security Headers analüüsitulemused

Joonis 9 ja Joonis 10 annavad ülevaate analüüsitava veebilehe turvaseisundi aruande tulemustest Security Headers analüsaatorist.



Joonis 9. Security Headers esialgsed analüüsitulemused 1.



Joonis 10. Security Headers esialgsed analüüsitulemused 2.

Security Headersi analüsaator annab analüüsitavale lehele turvataseme hinde vastavalt turvapäiste olemasolule ja nende õigele seadistusele vahemikus A-F. Amidisaini koduleheküg pälvis raporti põhjal hinde F, mis on madalaim võimalik hinne. Vastav hinne on igati põhjendatud väga oluliste turvalisust tagavate turvapäiste puudumise tõttu. Täpsemalt on puudu järgmised turvapäised:

- ***HTTP Strict-Transport-Security* (HSTS) –** päise seadistamisel talletavad brauserid teavet, et veebisaidi külastamisel on alati vaja HTTPS-i protokolli (peatükk 3.6.2).

- ***Content-Security-Policy* (CSP) -** annab juhiseid, millist sisu võib kuvada või laadida veebisaidile. See aitab vältida *Cross-Site Scripting* (XSS) rünnakuid, mis on üks levinumaid veebiründe tüüpe (peatükk 3.6.2).

- ***X-Frame-Options* -** piirab, kuidas saidi sisu kuvatakse teiste veebisaitide raamide sees. Päis tagab *ClickJackingu* kaitse ehk kaitse rünnaku eest, kus ründaja paneb oma pahavara või muu sisu kuvatava veebisaidi peale ja meelitab kasutaja sellele klikkima, ilma et ta seda teaks (peatükk 3.6.2).

- ***X-Content-Type-Options* –** võimaldab kontrollida, kuidas veebibrauserid tüübimäärangut (MIME tüüp) kasutavad, keelates brauseritel seda automaatselt muuta. Tüübimäärang on viis, kuidas veebiserverid teatavad brauseritele, millist tüüpi sisu nad tagastavad, näiteks HTML, CSS, JavaScript, pilt või muud tüüpi fail. See on oluline turvameede, sest mõned ründajad võivad manipuleerida sisu tüübimääranguga, et saada juurdepääs kasutaja brauserile või rakendusele. [48]

- ***Referrer-Policy* -** päis määrab, millist teavet viitaja saadab päringut edastavale serverile. Viitaja sisaldab teavet, mis näitab, kust kasutaja veebilehele saabus. See võib olla kas teine veebileht, otsingumootor või mõni muu allikas. Kui päis puudub, võib ründaja saada juurdepääsu viitaja infole ja seega koguda isiklikke andmeid, nagu näiteks otsingumootorisse sisestatud otsingupäringud või sotsiaalmeedia lehe külastused, mis rikuvad kasutaja privaatsust. [49]

- ***Permissions-Policy* -** See header määrab, milliseid API-sid ja muid funktsioone on lubatud veebilehel kasutada. Näiteks saab päise abil keelata veebikaamerate ja mikrofonide kasutamist, piirata JavaScript koodi ligipääsu teistele domeenidele, keelata teatud andmete salvestamist küpsistesse ning palju muud. Antud päis on mõeldud asendama varasemaid funktsioonidega seotud päiseid nagu *Feature-Policy* ja *Document-Policy*, kuna see võimaldab veebisaidi omanikel määrata ühe üldise poliitika kõigi funktsioonide jaoks, mis võivad olla ohtlikud või põhjustada turvariske. Kui päis puudub, võib ründaja kasutada ohtlikke API-sid või funktsioone, mis võivad kahjustada veebilehe turvalisust. [50]

4.2.3 Järeldused tulemustest

Analüüsitulemuste põhjal on võimalik järeldada, et antud veebileht vajab mitmete turvalisuse meetmete rakendamist, et kuuluda usaldusväärsete ning turvaliste veebirakenduste tasemele. Halvad analüüsitulemused on tingitud mitmetest turvalisuse probleemidest. Esmatähtsaks on kindlasti uuendamata tarkvara, mille alla saab liigitada nii WordPressi kui ka PHP aegunud versioonid. Teisena on oluline välja tuua tulemüüri puudumine, mis on üks tõhusamaid turvameetmeid saidi kaitsmiseks. Lisaks tuli aruannetest välja mitme olulise turvapäise puudumine. Kõik eelpool mainitud turvariskid vähendavad oluliselt veebilehe turvalisuse taset, mis seeläbi muudavad lehe kõikvõimalikele turvaohtudele kättesaadavamaks.

Analüüsitulemustest paljastatud turvariske võetakse arvesse järgnevas peatükis, kus proovitakse nendest erinevate turvamise meetmetega täielikult vabaneda.

4.3 Veebilehe turvamine

Analüüs ettevõtte Amidisain OÜ kodulehele erinevate analüsaatoritega baasil tõi esile erinevaid turvariske, mis avaldavad lehe turvalisusele suurt mõju. Analüüsi läbiviimiseks valitud tööriistad andsid mitmeid soovitusi avastatud riskidest vabanemiseks. Antud soovitusi ja turvamise protsessile seatud eesmärki silmas pidades proovib autor kõik ilmnenud turvaaugud likvideerida, samal ajal järgides ka üldisi WordPressi veebilehtede turvalisusemeetmeid, vahendeid ja mõõdikuid, millele on antud töös tähelepanu pööratud. Prioriteediks on tagada turvaline leht nii veebisaidi omanikule kui ka selle külastajatele, ehk analüsaatorite tulemused antud veebilehele peaksid viitama madalale turvariskile ja kõrgele turvalisuse tasemele. Järgnevates alampeatükkides on samm-sammult kirjeldatud veebilehe turvamise protseduuri läbiviimist.

Pärast igat läbiviidud muudatust on oluline testida veebibrauseris veebilehe jätkuvat toimimist. See kehtib nii väikeste kui ka suurte muudatuste puhul, sest muutuse tegemine võib kaasa tuua rikkeid veebilehe töövõimes. Kuna veebileht on *live* keskkonnas, siis vea korral on vaja kiiresti tegutseda, et veebilehe külastajate kasutajakogemus ei halveneks. Antud toimingut rakendab autor igas järgnevas turvamise etapis.

4.3.1 Veebilehe varukoopia

Veebilehe varukoopia aitab vältida olukorda, kus lehel olevad andmed ja informatsioon kaovad või muutuvad kättesaamatuks. Kuna turvamiseprotsess näeb ette veebilehel mitmete muudatuste läbiviimist, on mõistlik kindlasti teha varukoopia, et lehe muudatuste eelset versiooni saaks vajadusel taastada. Autor kasutas antud turvamise meetodi teostamiseks WordPressi pistikprogrammi *All In One Migration*, mille funktsionaalsus võimaldab hõlpsalt eksportida veebirakenduse fail arvuti kõvakettale [51].

4.3.2 Tarkvara, teema ja pluginate uuendamine

SiteChecki analüüsitulemustest selgus, et üheks turvaohuks oli antud veebilehe aegunud tarkvara. Vea parandamiseks uuendas autor WordPressi versiooni 6.0 sellel ajahetkel uusima ehk 6.2 peale. PHP versioon uuendati 7.4.0 pealt samuti uusimale, milleks oli 8.1.16. Järgmise vajaliku turvalisuse tagamise sammuna uuendatakse lehe teema ja pluginad. Seejärel kustutatakse mittevajalikud teemad ja pluginad. Kõik mainitud uuendused saab teostada WordPressi adminpaneelil valides menüüribalt „Uuendused“. Ebavajalikud teemad ja pluginad saab eemaldada valides menüüst vastavalt „Teemad“ ja „Pluginad“ sektsioonid.

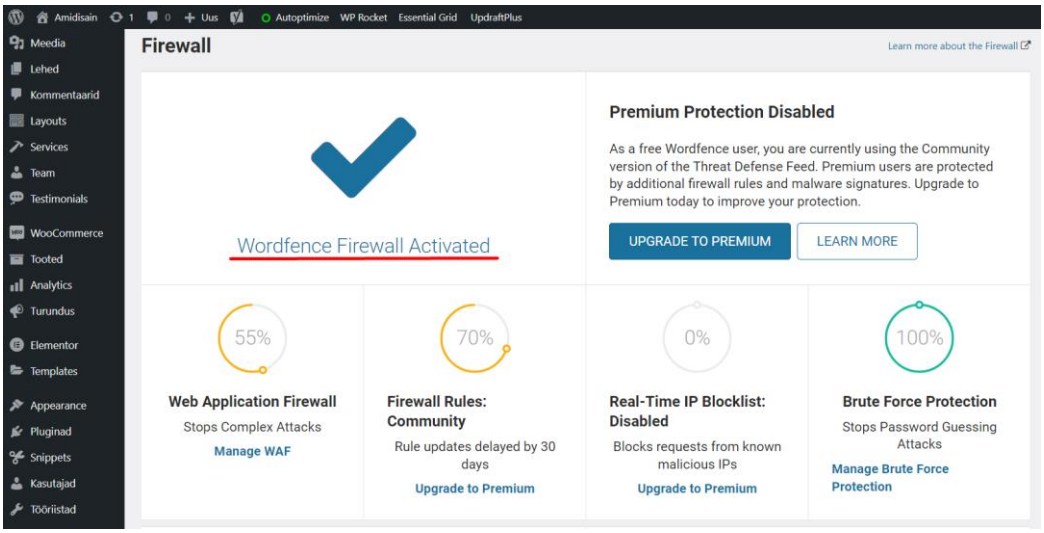
Kõik tehtud toimingud tarkvara, teemade ja pluginatega olid eesmärgil vähendada neis leiduvate või veel avastamata turvaaukude poolt võimalikku tekitava kahju suurust.

4.3.3 Turvalisuspluginate installeerimine

Wordfence

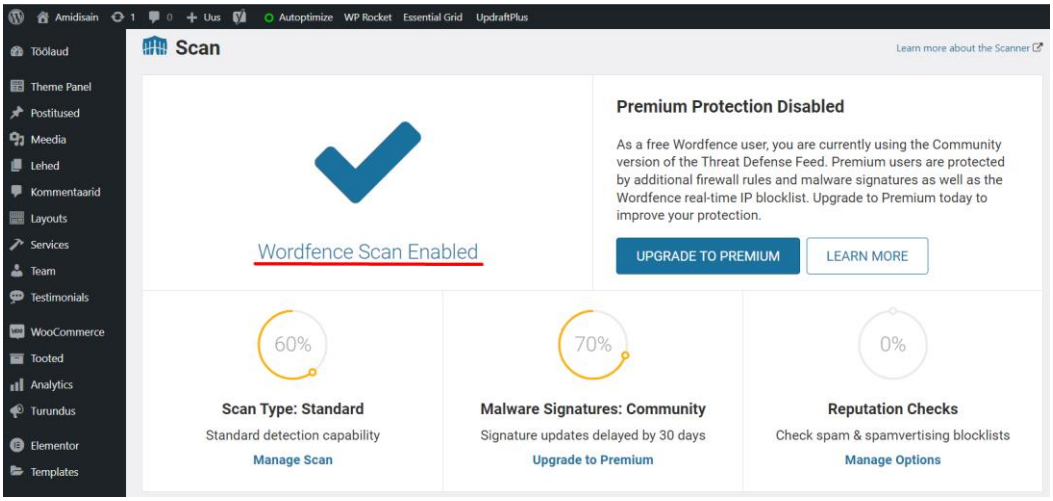
Oluliseimaks installeeritavaks turvalisuse pluginaks on Wordfence, mis pälvis liidripositsiooni erinevate populaarseimate turvamisvahendite analüüsimisel. Antud plugina tasuta versioon võimaldab veebilehel kasutusele võtta järgmised turvalisust tagavad funktsioonid [52]:

- **Tulemüür** - veebipõhine tulemüür, mis töötab reaalajas ja analüüsib kogu veebisaidi liiklust, blokeerides automaatselt kõik ründajad ja pahavara rünnakud (Joonis 11).



Joonis 11. Wordfence tulemüüri aktiveerimine.

- **Pahavara monitooring ja puhastus** – funktsioon võimaldab tuvastada ja eemaldada veebisaidil leiduva pahavara, skaneerides regulaarselt pahavara, vigaseid ja muudetud faile. Kui pahavara tuvastatakse, antakse arendajale teada, millised failid sisaldavad pahavara. Lisaks pakub Wordfence võimalust neid faile automaatselt puhastada või käsitsi kustutada (Joonis 12).

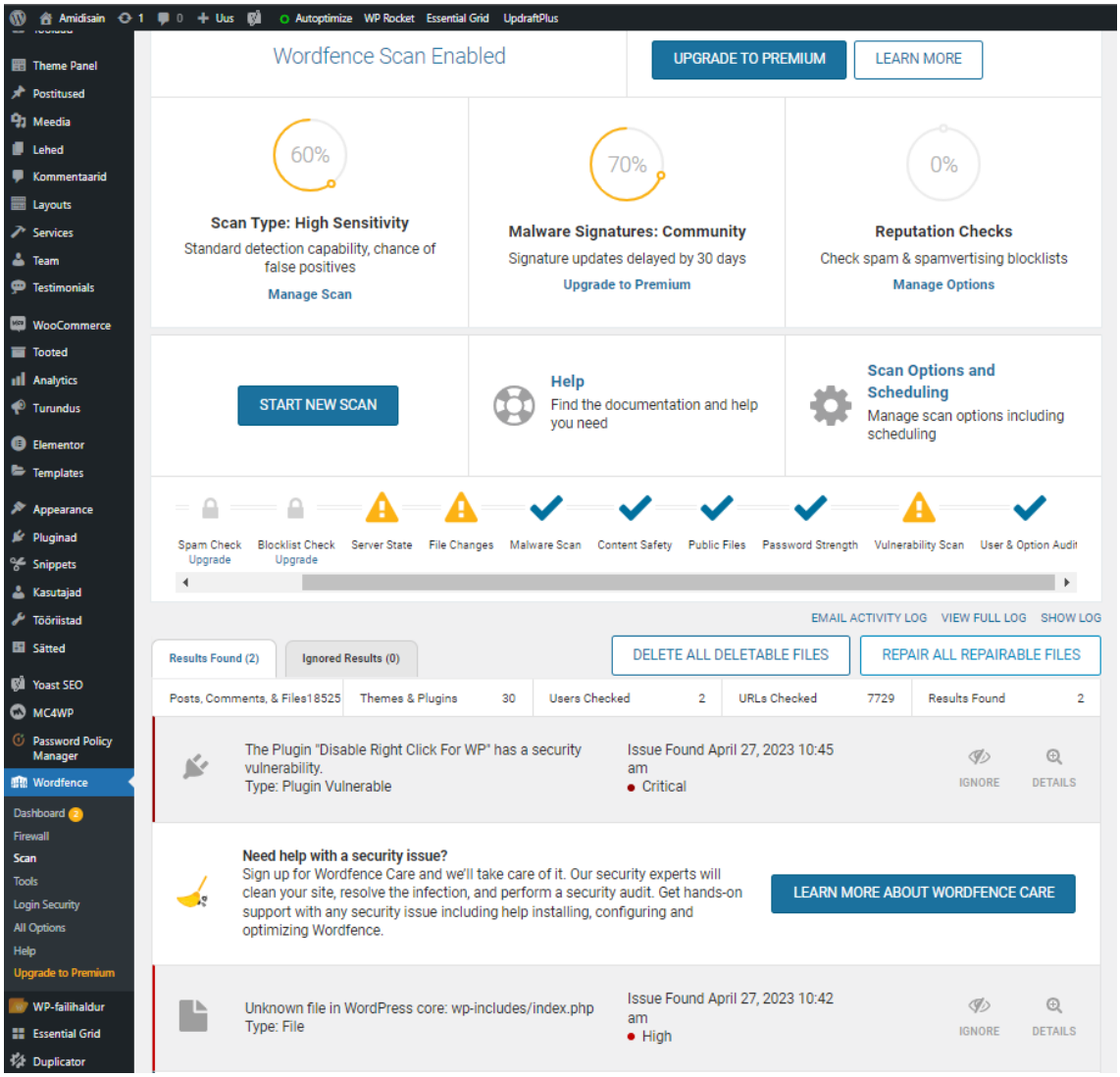


Joonis 12. Wordfence monitooringu aktiveerimine.

- **Haavatavuse tuvastamine** - Wordfence jälgib järjepidevalt teadaolevaid turvaaukusid vananenud ning haavatavatel pluginatel ja teemadel, pakkudes automaatseid turvaparanduste uuendusi.

- **Sisselogimise turvalisus** – kaheastmelise autentimise funktsioon.

Järgnevalt teostab autor pahavara monitooringu, et tuvastada võimalikke haavatavusi lehe hetkeseisundis (Joonis 13).



Joonis 13. Wordfence turvamonitooring 1.

Turvamonitooringu tulemuste põhjal tuvastati kaks probleemi. Esimene neist on turvaauke sisaldav plugin, mis on määratud kriitilisele riskitasemele (*Critical*). Ohu kõrvaldamiseks deaktiveerib ja kustutab autor haavatavusega pistikprogrammi. Teiseks turvalisuse alandajaks on välja toodud tundmatu fail, mis asub WordPressi põhifailide asukohas, kuid seda ei levitata koos antud ehk uusima WordPressi versiooniga. See fail on pärit vanemast WordPressi versioonist ning kuna see versioon võib sisaldada tundmatuid turvaauke, on selle olemasolu riskantne ning seetõttu liigitatud kõrgele riskitasemele (*High)*. Mainitud fail kustutatakse WordPressi põhifailide hulgast, et vähendada turvariskide olemasolu.

Sarnaste tundmatute failidega seotud turvaohtude vältimiseks programmeeris autor koodi, mis blokeerib vastavas kaustas PHP failide jooksutamise (Lisa 6). Autori enda kogemusest on *wp-content/uploads* kaust populaarne rünnakuallikas häkkeritele, kes loovad kausta PHP faili, mis sisaldab turvaauku, mille kaudu saab veebiserverile ligi. *Uploads* kaustas hoitakse kõiki veebisaidile üles laetud faile, näiteks pilte, videoid, dokumente jne. Selle tõttu turvati antud kaust ära, luues sinna *.htaccess* fail, mis sisaldab ülal mainitud blokeerimise funktsionaalsuse koodi. Loodud kood aitab turvaohte vähendada takistades potentsiaalselt ohtlikke või pahavara sisaldavate failide jooksutamist serveris.

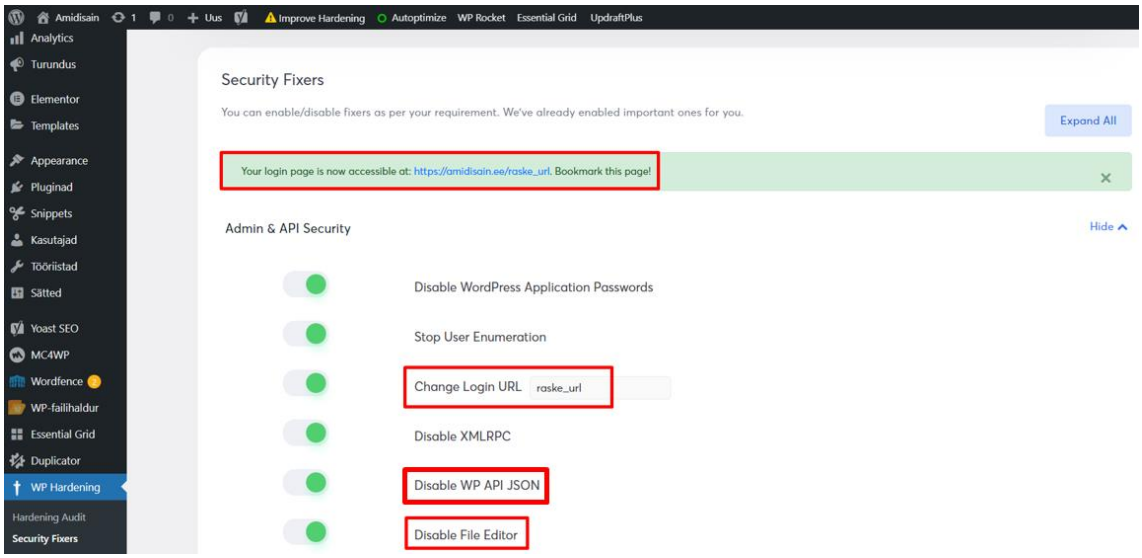
Sama monitooringu protsess viiakse läbi ka peatükis 4.4.3, kui kõik vajalikud turvameetmed on juba lehele paigaldatud, et saaks veenduda rakendavate toimingute turvalisuses.

Kuna Wordfence ei võimalda kõiki töös välja toodud turvamise meetodeid tagada, võetakse kasutusele ka täiendavad pistikprogrammid, millega saavutatakse puuduvad turvalisuse meetmed.

WP Hardening

Vajalikku lisaabi pakub turvamisel plugin nimega *WP Hardening*. Autor seadistab selle vastavalt installimisel ning aktiveerimisel omandab veebileht järgnevad turvaohte madaldavad parandused [53]:

- Muudetakse WordPressi sisselogimislehe URL-i, et sisselogimisevormi leidmine oleks raskendatud (Joonis 14).
- Keelatakse faili muutmise (*File Editor*) võimalus. See tagab, et ainult veebisaidi serveri administraatoritel on juurdepääs failidele ja funktsioonidele, mis vähendab ründajal võimalust faile muuta ja seeläbi kahjustada veebilehte (Joonis 14).
- Keelatakse WP API JSON funktsionaalsus, mis takistab kolmandatel isikutel või rakendustel juurdepääsu API kaudu WordPressi saidi sisule ja andmetele (Joonis 14).



Joonis 14. Sisselogimislehe URL muutmine, WP API JSON ja failide muutmise keelamine.

Headers Security Advanced & HSTS WP

Veebilehe analüüsimise peatükis kerkis Security Headersi analüsaatori aruandes esile HTTP turvapäiste puudumise turvaprobleem. Selle vea aitab lahendada *Headers Security Advanced &* HSTS WP plugin, võimaldades lisada lehele kõik turvapäised, mis analüüsiaruande põhjal olid puudu [54]:

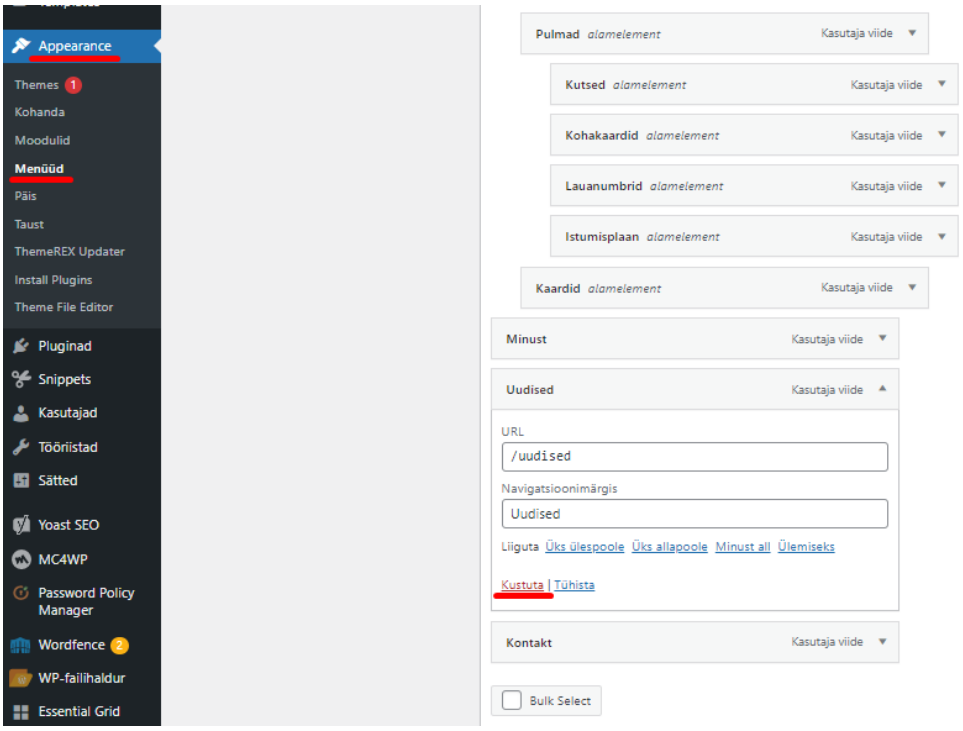
- *HTTP Strict-Transport-Security* (HSTS)
- *Content-Security-Policy* (CSP)
- *X-Frame-Options*
- *X-Content-Type-Options*
- *Referrer-Policy*
- *Permissions-Policy*

Detailsemalt on erinevate turvalisuse päiste funktsionaalsuste kohta informatsiooni peatükkides 3.6.2 ja 4.4.2.

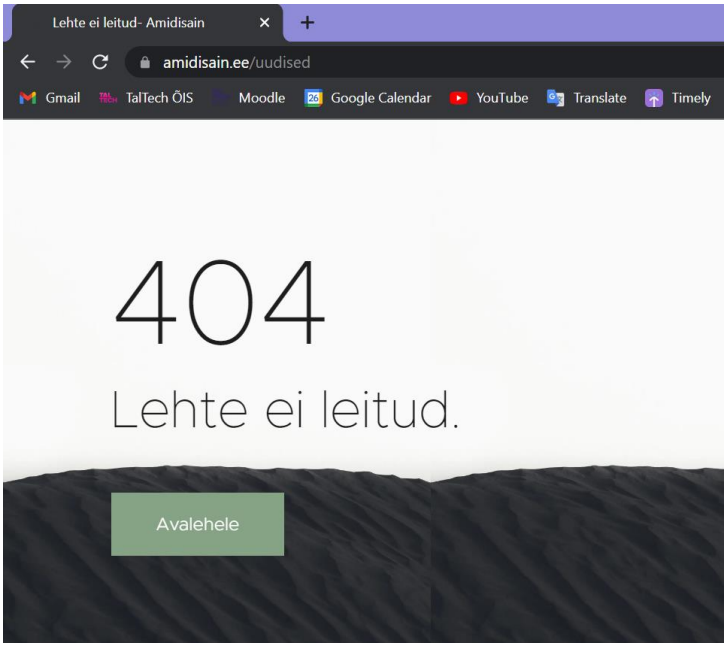
4.3.4 404 veakoodi linkide eemaldamine

Peatükis 4.2.1, kus viidi läbi veebilehe analüüs enne turvamise protsessi, leidis analüsaator mitteeksisteerivale lehele viitava lingi. Antud lingile vajutades ei leita serverist vastavat päringut ning kuvatakse spetsiaalne veateate leht, mis juhatab kasutaja

tagasi veebilehe avalehele (Joonis 15). Selle probleemi lahendamiseks kustutas kasutaja menüüribal paikneva lingi „Uudised“, sest sellele viitavat lehte ei ole antud lehel enam vaja (Joonis 16). Oluline on tagada, et veebisaidi linkidele vastaksid tegelikud lehed, et vältida kasutajate segadust ja vähendada vigade arvu lehel.



Joonis 15. 404 veakoodi lingi eemaldamine menüüst.



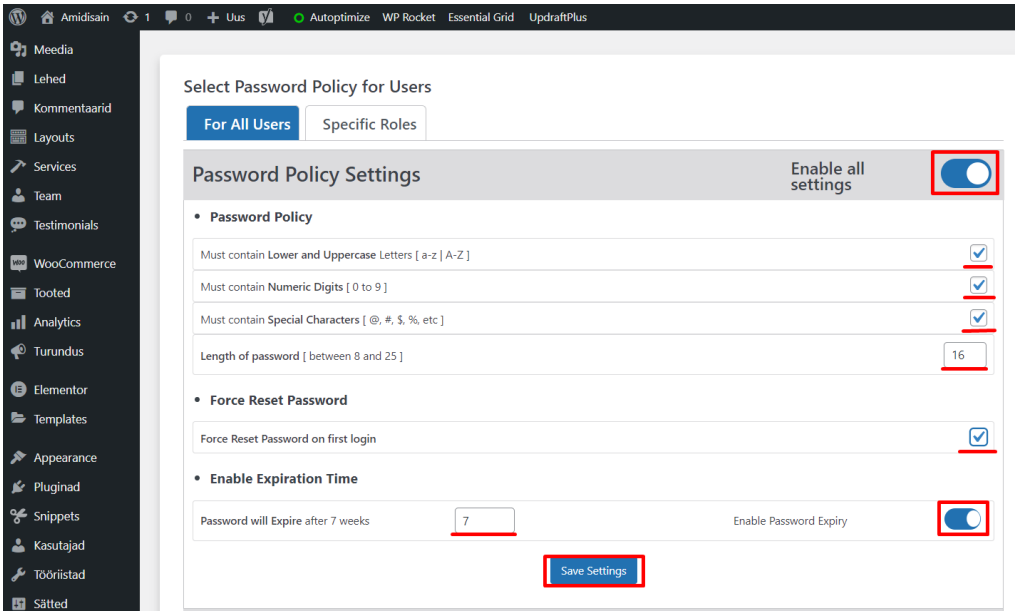
Joonis 16. Mitteeksisteeriva lehe veateate vaheleht.

4.3.5 Tugeva paroolipoliitika loomine

Tugeva parooli haldamine

Paroolihalduri (*Password Policy Manager)* plugin on tööriist, mis võimaldab määrata oma lehel tugevad paroolipoliitikad. Autor seadistas veebilehel järgnevad reeglid kasutaja paroolidele (Joonis 17) [55]:

- Minimaalse ja maksimaalse parooli pikkuse nõue.
- Suurtähti, väiketähti ja numbreid sisaldava parooli nõue.
- Parooli muutmise nõue pärast esimest sisselogimist.
- Parooli aegumise perioodi määramine.
- Pärast määratud perioodi möödumist parooli muutmise nõue.



Joonis 17. Tugeva paroolipoliitika loomine Paroolihalduriga.

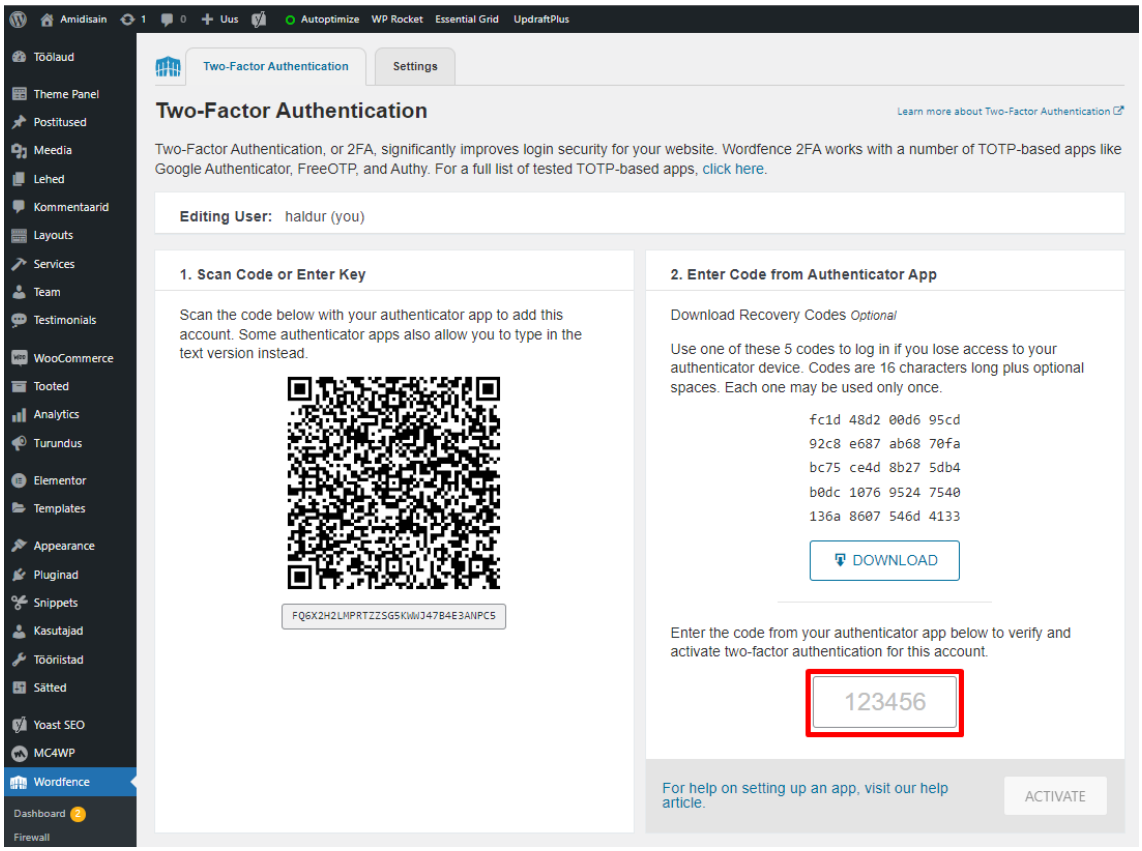
Kasutajanime ja parooli muutmine

Autor muutis administraatori kasutajanime ning parooli, järgides peatükis 2.6.4 tugeva paroolipoliitika soovitusi ning paroolihalduri plugina funktsionaalsusega määratud nõudeid. Parool peaks sisaldama erinevaid tähemärke, numbreid, sümboleid ning olema pikkusega vähemalt 16 tähemärki. Lisaks on kohustuslik vahetada parooli vastavalt määratud aegumise perioodi möödumisel, milleks autor valis 7 nädalat (Joonis 17).

Kaheastmelise autentimise lisamine

Peatüki alguses installeeris autor Wordfence plugina, mille seadete alt seadistati mainitud funktsionaalsus tugeva paroolipoliitika ja lisaturvalisuse tagamiseks. Täpsemalt tuleb

oma nutiseadmesse installeerida mõni autentimise rakendus, näiteks *Google Authenticator*, millega tuleb skaneerida WordPressis Wordfence seadete all olevat QR-koodi. Seejärel genereerib rakendus koodi, mis tuleb sisestada WordPressi, et kinnitada ja aktiveerida antud konto kaheastmeline autentimine (Joonis 18).



Joonis 18. Kaheastmelise autentimise lisamine.

4.3.6 Vormide turvamine

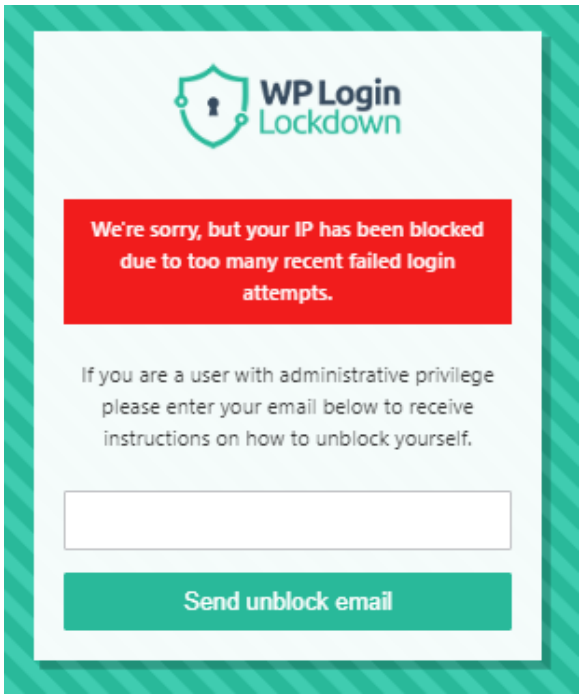
Sisselogimiselehe URL muutmine

Eelpool installeeritud turvalisuse plugin WP Hardening omab funktsiooni, mille abil muutis autor sisselogimislehele viitava URL-i nime, et sisselogimisvormil oleks lisaturvalisuse kiht pahatahtliku tegevuse eest (Joonis 14).

Sisselogimisekatsete piiramine

Login Lockdown plugin aitab takistada *Brute Force* rünnakuid sisselogimise lehe kaudu. Selle paigaldamisel jälgib plugin sisselogimiskatsete ajalugu ja piirab teatud aja jooksul edutuid sisselogimiskatseid. Antud sisselogimisvormi turvamise meetod aitab kaitsta veebisaiti nii reaalsete kui ka automaatsete rünnakute eest. Kui vale parool sisestatakse

mitu korda järjest, kuvatakse teade, mis informeerib kasutajat ajutisest blokeeringust või piirangut sisselogimisele ning soovitatakse oodata teatud aeg enne uuesti sisselogimise proovimist (Joonis 19). [56]



Joonis 19. Login Lockdown blokeerimise teade kasutajale.

reCaptcha lisamine kontaktivormile

reCAPTCHA on *Google'i* poolt välja töötatud turvameede, mida kasutatakse veebilehtedel inimeste eristamiseks automaatsetest robotitest. Rakendusest on tehtud kaks erinevat versiooni, vanem on *reCAPTCHA v2* ning uuem on *reCAPTCHA v3*. Vanem versioon kasutab meetodit, kus kasutaja peab lahendama pildipõhiseid küsimusi, näiteks tuvastama pildil olevaid objekte. *reCAPTCHA v3* kasutab aga uuenduslikku lähenemist, kus kasutaja ei pea midagi lahendama. Selle asemel kogub see taustal automaatselt kasutaja tegevuse kohta teavet, genereerides kasutaja käitumise põhjal skoori vahemikus 0-1. Kui tulemus on nulli lähedal, on tegemist tõenäoliselt robotiga ning kui see on 1 lähedal, on see suurema tõenäosusega inimene. [57]

reCAPTCHA v3 versiooni paigaldamise protsess Amidisain OÜ veebilehele on esitatud töö lisades (Lisa 5).

4.3.7 Kodeeritud turvameetmed

Lisaturvameetmetena programmeeris autor paar lahendust, mis lisavad turvalisuse kihte veebilehele juurde, need on järgmised:

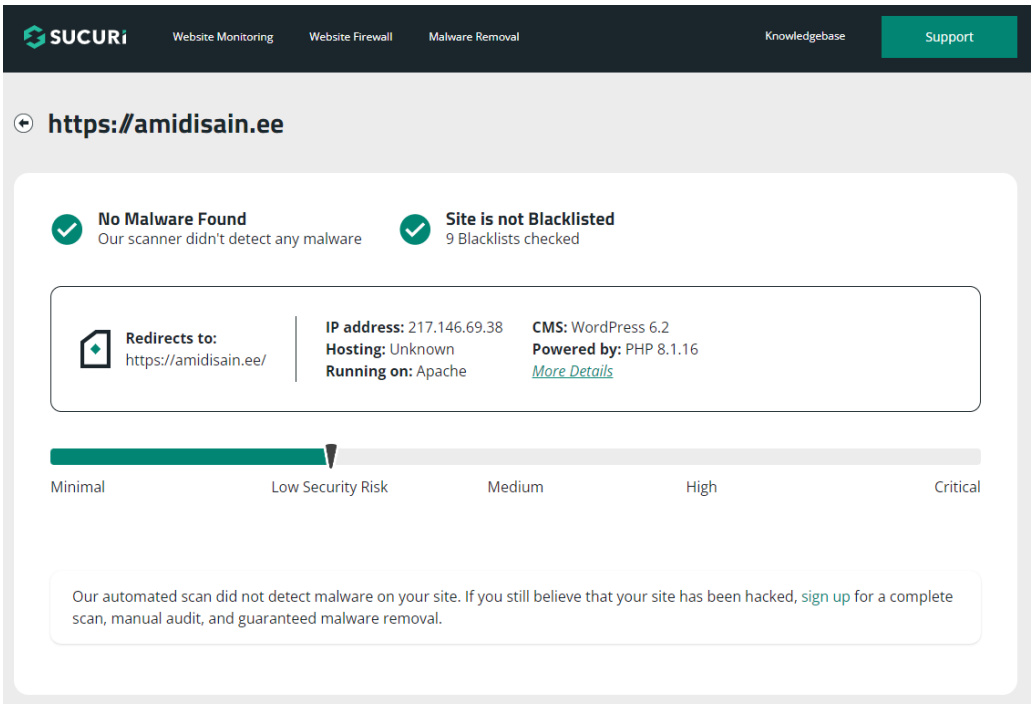
- WordPressi versiooni eemaldamise funktsiooni koodi lisamine *functions.php* faili. Kui ründaja teab lehe WordPressi versiooni, on lihtsam leida tuntud turvaauke, millele vastava versiooni puhul rakendatud parandusi ei ole veel tehtud. On oluline, et WordPressi põhiteemat ei muudetaks otse, sest kõik muudatused, mida tehakse, kaovad, kui põhiteemat värskendatakse. Selleks kasutab autor alamteemat *„Craftis Child“*, võimaldades säilitada veebisaidi põhiteema terviklikkust (Lisa 6).
- Juurdepääsu piiramise kodeeringu lisamine *.htaccess* faili kaudu aadressidele *wp-login.php* ja */wp-admin/*, mis blokeerib POST päringud (nt. parooli või sisu värskendamine) ja juurdepääsu sisselogimislehele (*wp-login.php ja wp-admin*), kui need päringud ei ole pärit määratud domeenist. Lubatud kasutajad saavad aga tavapäraselt sisse logida (Lisa 6).
- *wp-config.php* faili lukustamise kodeeringu lisamine, et kaitsta lehe üht olulisemat faili, mis sisaldab lehe konfiguratsiooni andmeid, sealhulgas andmebaasi kasutajanime ja parooli. Kood takistab juurdepääsu failile väljaspool WordPressi rakenduse kataloogi (Lisa 6).

4.4 Turvatud veebileht

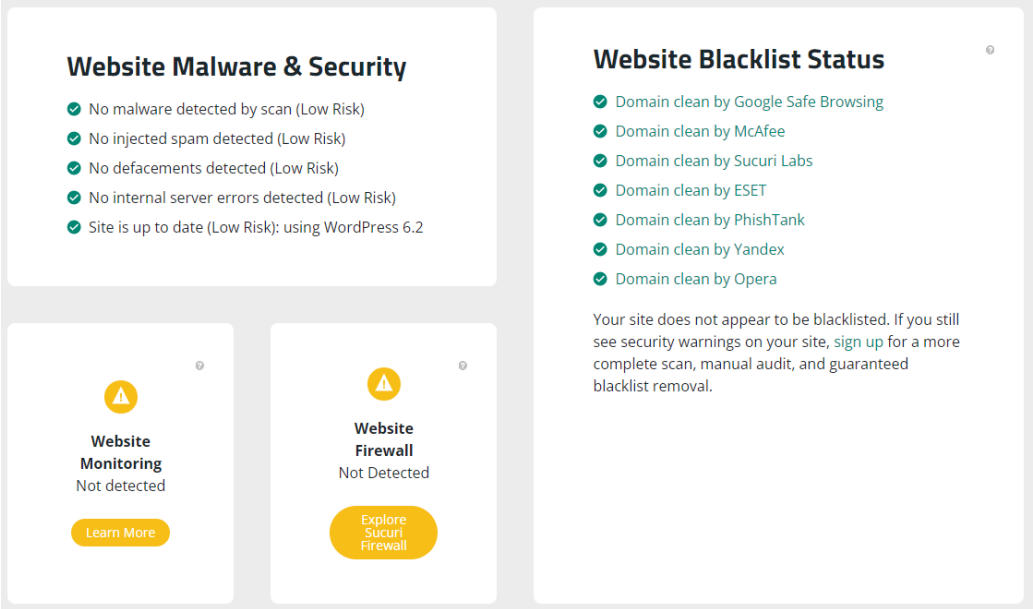
Antud peatükis hinnatakse Amidisain OÜ veebilehele jõustatud turvamise meetodite efektiivsust. Tulemuste hindamiseks ning muutuste nägemiseks kasutatakse kahte sama analüsaatorit nagu algse veebilehe puhul: *SiteCheck* ja *Security Headers*. Lisaks kasutab autor tulemuste tõestamiseks veel *Securityforeveryone* analüsaatorit, mille kasutamise vajadust selgitatakse järgmises alapeatükis. Kõikide analüsaatorite aruannete põhjal tuuakse välja turvaohtude ja turvalisuse taseme erinevused algse ja lõpliku veebilehe vahel. Lisaks teostatakse eelmises peatükis installeeritud Wordfence pahavara monitooringu funktsioon, et viia turvariskid miinimumini ja veenduda lehe turvalisuses.

4.4.1 SiteCheck analüüsitulemused pärast turvamise protsessi

Joonis 20 ja Joonis 21 näitavad turvatud Amidisani kodulehe turvaseisundi aruande tulemusi SiteCheck analüsaatorist.



Joonis 20. SiteCheck analüüsitulemused pärast turvamise protsessi 1.



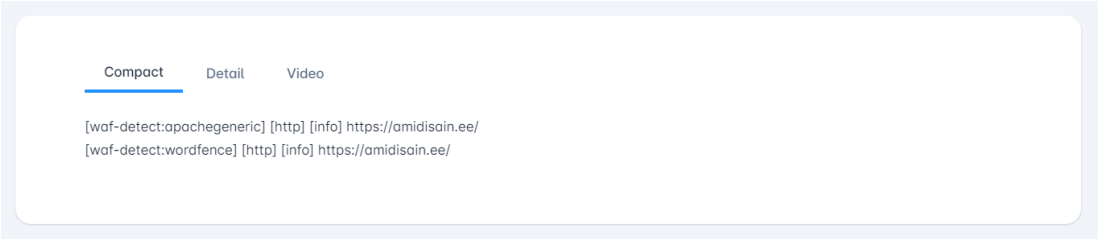
Joonis 21. SiteCheck analüüsitulemused pärast turvamise protsessi 2.

SiteChecki tulemused on kõvasti paremad võrreldes esialgsete tulemustega. Esiteks on turvalisuse oht langenud keskmiselt madalale riskitasemele. Riski langusele aitas kaasa enne suureks probleemiks olnud WordPressi ja PHP värskendamata versioonid, mis on mõlemad hetkel kõige uuemal võimalikul versioonil, vastavalt 6.2 ja 8.1.16. Enne turvamist olid need aga vastavalt 6.0 ja 7.4.0. Lisaks langetas riski kindlasti enne keskmisele tasemele hinnatud riskiga mitteeksisteeriva lehe olemasolu veebilehel. Antud vigade parandamine vähendas turvaaukude olemasolu ning seeläbi parandas turvalisust ja ka kasutajakogemust.

Kui enne oli aruandes miinusena välja toodud turvapäiste puudumine, siis pärast turvameetmete rakendamist on viga parandatud. Täpsema ülevaate HTTP turvapäiste seisunditest pärast turvamise protsessi leiab järgmisest alapeatükist, kus kirjeldatakse Security Headersi turvamise järgseid veebilehe analüüsitulemusi (peatükk 4.4.2).

Autorile tekitasid muret siiani mittetuvastatud monitooring ja tulemüür, teades, et installeeritud populaarse ning võimeka plugina Wordfence funktsionaalsused peaksid võimaldama reaalset toimivat pahavara monitooringut ja tulemüüri. Lisaks kontrollis autor peatükis 4.3.3 mõlema funktsiooni aktiveeritust lehel ning lisatud on ka vastavad pildid. Pärast lähemat uurimist selgus, et kuna antud analüsaator on välja töötatud veebisaidi turva- ja kaitseplatvormi Sucuri poolt, suudab see tuvastada vaid Sucuri turvalisuse plugina poolt aktiveeritud tulemüüri ja monitooringut [58].

Kuna Sucuri turvalisuse plugin on tasuline ning eesmärki saab täita ka ilma selleta, jääb autor siiski Wordfencile kindlaks. Wordfence funktsionaalsuse toimivuse tõestamiseks on vajalik kasutada alternatiivset analüsaatorit, mille nimeks on *Securityforeveryone*. Antud analüsaator tuvastab veebirakenduse tulemüüri (*Web Application Firewall* (WAF)) olemasolu ning näitab ka täpsemalt, mis tulemüüriga on tegemist. Lisaks teeb see kindlaks ka veebilehe serveri. Raporti tulemused tuvastavad Wordfence tulemüüri olemasolu ning *Apache* on serveritüübi nimi, kus antud veebileht paikneb (Joonis 22). [59]



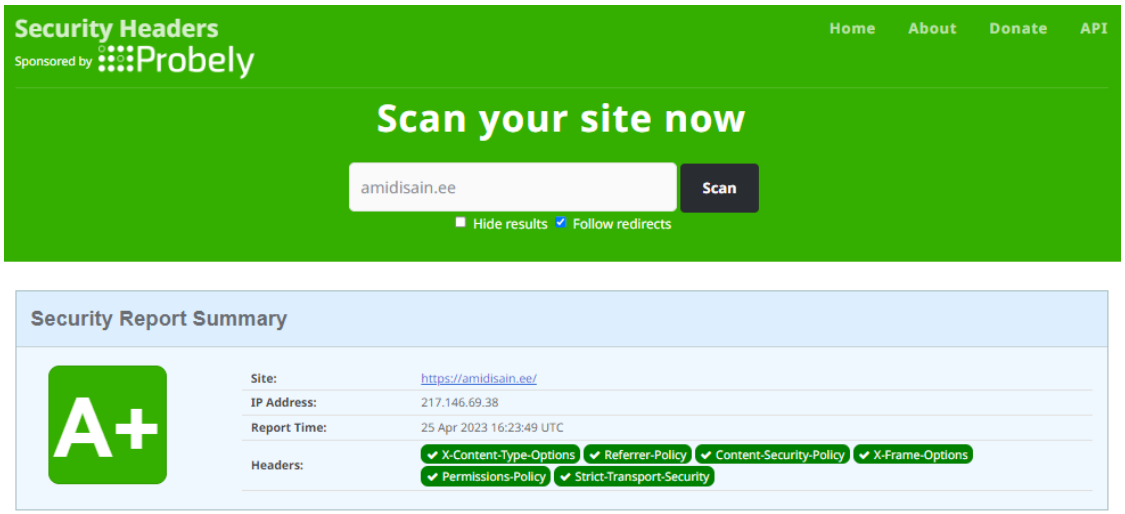
Joonis 22. Securityforeveryone analüüsitulemused pärast turvamise protsessi.

Samas seisundis on kõik algse veebilehe analüüsitulemuste positiivsed aspektid. Veebilehel ei tuvastatud pahavara, rämpsposti ega muid rikkumisi, mis tõstaks turvariske. Lisaks ei kuulu Amidisaini kodulehekülg endiselt ka musta nimekirja, mis näitab, et veebilehel vajalike toimingute tegemine ei ohusta kasutajat.

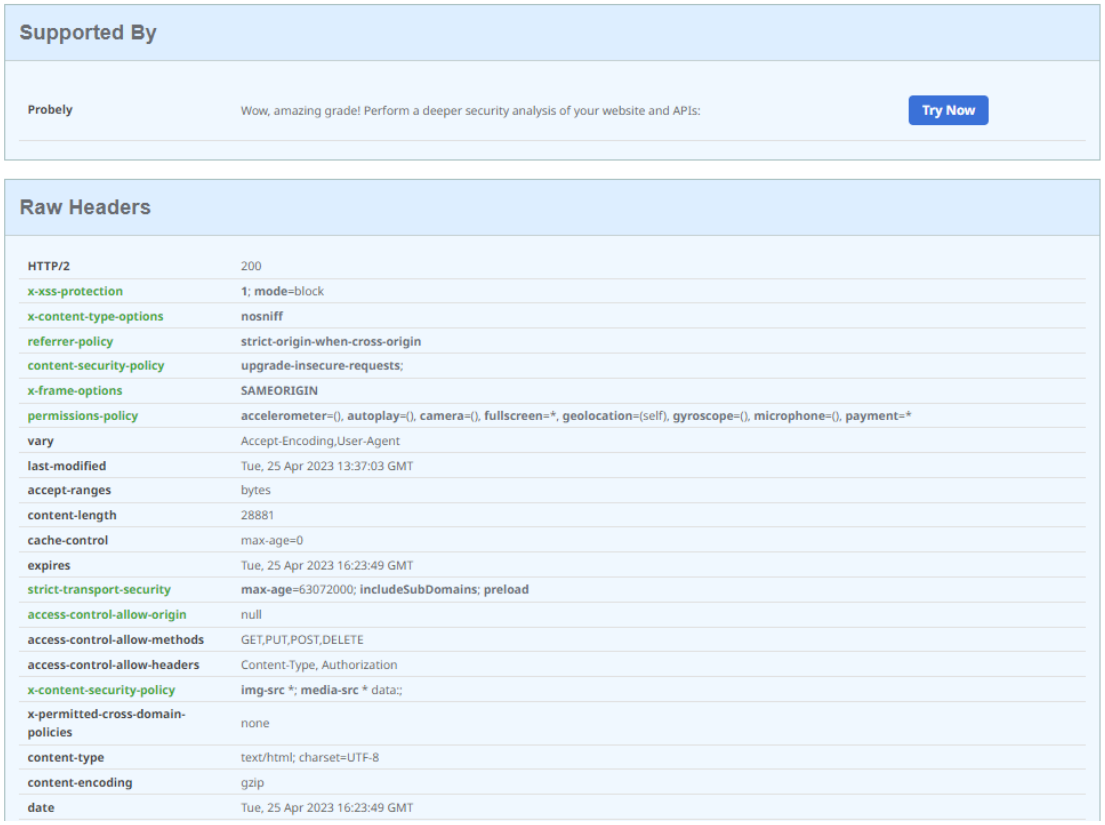
Arvestades SiteChecki analüsaatori puudusi tulemüüri ja monitooringu tuvastamises ning selle tõttu kasutusele võetud Securityforeveryone analüsaatorit, mis tõestas Wordfence funktsionaalsuse olemasolu, võib öelda, et seatud turvalisuse taseme eesmärk sai siiski edukalt täidetud.

4.4.2 Security Headers analüüsitulemused pärast turvamise protsessi

Joonis 23 ja Joonis 24 heidavad pilgu turvatud veebilehe turvaseisundi tulemustele Security Headersi analüsaatorist.



Joonis 23. Security Headers analüüsitulemused pärast turvamise protsessi 1.



Joonis 24. Security Headers analüüsitulemused pärast turvamise protsessi 2.

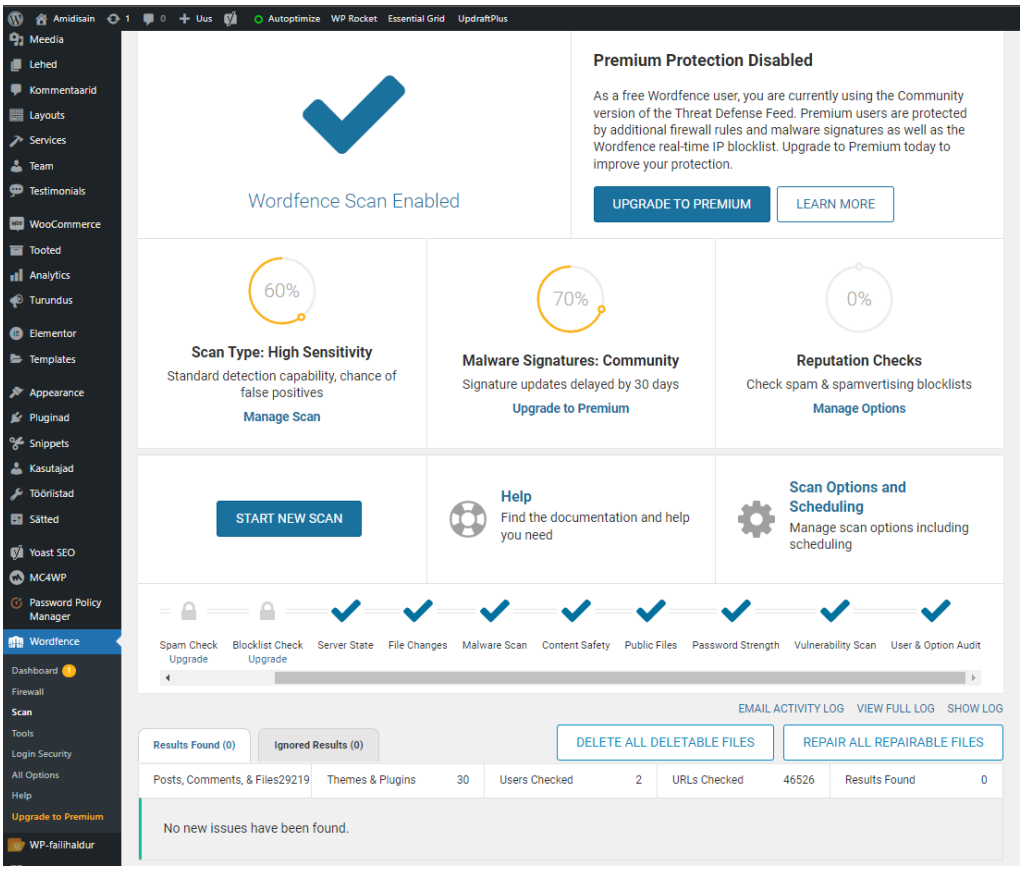
Turvatud veebilehe tulemused Security Headersi analüsaatorist on positiivsed, sest Amidisaini kodulehe tase tõusis hindelt F hindele A+, mis on parim võimalik hinne. Kõik eelnevalt puudulikud HTTP turvapäised on nüüd ilusti tuvastatud:

- *HTTP Strict-Transport-Security* (HSTS)
- *Content-Security-Policy* (CSP)
- *X-Frame-Options*
- *X-Content-Type-Options*
- *Referrer-Policy*
- *Permissions-Policy*

Puuduvate turvapäiste probleemi lahendamisele aitas kaasa *Headers Security Advanced & HSTS WP* funktsionaalsuse rakendamine antud veebilehel. Nüüd on täiendava turvalisuskihi olemasolu turvapäiste näol veebisaidil olemas. Autori eesmärgiks oli saavutada kõrgeim võimalik hinne antud analüsaatorist ning see sai edukalt täidetud.

4.4.3 Pahavara monitooring

Kuna kõik olulised turvalisust edendavad meetodid on läbi viidud, sooritab autor veelkord turvalisuse monitooringu Wordfence abiga, mis tuvastab võimalikud ohtu kujutavad tegurid monitooritaval veebilehel (Joonis 25).



Joonis 25. Wordfence turvamonitooring 2.

Läbiviidud monitooring ei tuvastanud ühtegi haavatavust lehel, mis näitab, et turvalisus on hetkel ohutul tasemel ning võimalikud riskid on viidud miinimumini. Siinkohal tuleb esile tuua, et veebilehe turvalisus ei ole ühekordne tegevus, sest küberkurjategijate taktikad ja meetodid muutuvad pidevalt ning arenevad aja jooksul. Seetõttu on suureks kasuks Wordfence regulaarne pahavara monitooringu funktsioon, mis aitab pidevate skaneeringutega hoida lehe turvalisuse taset, käies turvariskide arenguga kaasas.

5 Tulemuste analüüs ja järeldused

Ettevõtte Amidisain OÜ koduleheküljе turvamiseprotsessi võib lugeda positiivselt sooritatuks. Autori poolt valitud turvalisust tagavate toimingute jõustamine veebilehele suutis parandada mõõdikute väärtusi kasutatud analüsaatorite tulemusi arvestades. Püstitatud eesmärgiks oli kasutada turvalisuse hindamisel töös välja toodud mõõdikuid ja turvamise meetodeid ning tagada, et analüsaatori SiteCheck veebilehe turvalisuse kohta antav aruanne näitaks madalat turvariski taset ning Security Headers analüsaatori tulemus turvapäiste kohta oleks kõrgeimal A+ tasemel. Mõlemad analüsaatori aruanded suutsid näidata oodatud tulemusi, ehk eesmärk sai täidetud. Sellest järeldades on läbiviidud turvalisuse tagamise protsessist võimalik esile tuua tulemusrikkaid strateegiaid, mis suure tõenäosusega tõstavad kõikide veebilehtede turvalisust.

Analüüsitav veebileht ei suutnud saada kõikides analüsaatorites ideaalset turvalisuse tagasisidet. Selle põhjuseks ei olnud mitte rakendatud turvamise meetodite ebaefektiivsus, vaid analüsaatori funktsionaalsus, mis oli suunatud ühele kindlale tasulisele turvapluginale. Antud töös kasutati ainult tasuta pluginaid ja versioone, millest antud juhul piisas eesmärgi saavutamiseks ehk tasulisi turvapluginaid ei analüüsitud. Seda aspekti arvesse võttes on võimalik, et erinevate turvalisuse pluginate tasulisi funktsioone rakendades saaks saavutada veelgi suurema veebilehe turvalisuse. Siiski ei pruugi see alati nii olla, sest ka tasuta pluginate versioonid suudavad pakkuda piisavat turvalisust vastavalt konkreetsele vajadusele, mis tuli ka antud töö analüüsist välja.

Järgnev tabel toob lühidalt välja töös mainitud oluliste turvamõõdikute ja -funktsioonide olekud enne ja pärast veebilehe turvamiseks rakendatud meetodeid (Tabel 6).

Tabel 6. Turvalisuse mõõdikute ja funktsioonide seisund enne ja pärast turvalisuse protseduuri.

Mõõdik/funktsioon	**Enne turvamist**	**Pärast turvamist**
Tulemüür	Ei	Jah
Pahavara tuvastamine	Ei	Jah
Musta nimekirja kuuluvus	Ei	Ei
Siseserveri errorid	Jah	Ei

Mõõdik/funktsioon	Enne turvamist	Pärast turvamist
WordPressi versioon	6.0	6.2
PHP versioon	7.4.0	8.1.16
HTTP-turvapäised	Ei	Jah
SSL sertifikaat	Jah	Jah
Varukoopia	Ei	Jah
Uuendamata pluginad	3	0
Uuendamata teemad	1	0
Failide muutmise keelamine	Ei	Jah
Tugev paroolipoliitika	Ei	Jah
Kaheastmeline autentimine	Ei	Jah
Sisselogimiselehe URL muutmine	Ei	Jah
Sisselogimisekatsete piiramine	Ei	Jah
WP API JSON funktsionaalsuse keelamine	Ei	Jah
404 veakoodid	Jah	Ei
reCAPTCHA	Ei	Jah

Läbiviidud analüüs näitas, et turvalisuse parandamine võib veebilehte omavale ettevõttele tuua ärikasu pikemas perspektiivis, tõstes kasumit, vältides kahjusid, suurendades klientide lojaalsust ja usaldust ning seeläbi parandades ettevõtte mainet. Vaid mõne hetkelise veebilehe kättesaamatuse tagajärjeks võib olla klientide kaotus. Monitooring ja tulemüür hoiavad veebilehe töökorras ehk külastajad pääsevad saidile, ilma et neid takistaksid pahatahtlikud tegevused (näiteks DDos rünnakud). Töös välja toodud SSL-i sertifikaat ja seda vahendav HTTPS ühendus tagavad usaldusväärse andmeedastuse kliendi ja veebilehe vahel (URL-i ees SSL-i tabaluku sümbol). Nii suureneb tõenäosus, et klient tunneb end turvaliselt, soovib oma andmeid jagada, ostu sooritada ning teenust ka teistele soovitada. Kliendi usalduse teenimine on müügi võti ning turvaline veebileht mängib selles suurt rolli.

Analüüsist saab järeldada, et WordPressi veebilehe turvalisuse parandamiseks on vajalik võtta kasutusele mitmeid meetmeid ning pöörata tähelepanu erinevatele turvaohtudele. Samuti tuleb arvestada veebilehe enda olemusega, et valida sobivad turvameetmed.

Ainuõiget lähenemist turvalisusele ei ole ning iga veebileht vajab erinevat lahendust, mis arvestaks konkreetse veebilehe vajadusi.

Järgnevalt on välja toodud antud töös rakendatud turvalisuse meetmete põhjal loetelu põhilistest nõuannetest, mida WordPressi veebilehtede turvalisuse tagamiseks ja efektiivseks turvaohtude langetamiseks tuleks rakendada:

- **Veebilehe turvaseisundi analüüs** - enne turvameetmete rakendamist tuleb kindlaks teha lehe hetkeline seisund, et teada, millele turvamisel rõhku panna. Selleks saab kasutada erinevate funktsionaalsustega analüsaatoreid, näiteks *SiteCheck* ja *Security Headers*.
- **Varukoopia** - kui midagi läheb valesti, näiteks tahtmatu muudatus, häkkimiskatse või andmete kadumine, saab lehe taastada tagavarakoopiaga. Oluline on tagada, et varukoopiaid tehakse regulaarselt ja neid hoitakse turvalises asukohas. Soovitatav WordPressi plugin selle jaoks on *All In One Migration.*
- **Tarkvara, teemade ja pluginate uuendus** - uuendused parandavad sageli leitud turvaaugud ja aitavad vältida tarkvara terviklikkuse rikkumist. Tähtis on ka kasutada usaldusväärseid teemasid ja pluginaid ning mittevajalikud eemaldada. Kasutades vananenud või ebausaldusväärseid tarkvara, teemasid või pluginaid, on leht kindlasti haavatavam rünnakutele.
- **Tulemüür** - filtreerib kogu võrguliikluse, et takistada nakatunud failide, pahavara ja viiruste sattumist veebilehele, kaitstes näiteks populaarsete DDoS rünnakute eest. See on iga turvalisuse arhitektuuri tähtsaim osa.
- **Pahavara monitooring ja puhastus** - aitab avastada ja kõrvaldada pahavara, mis juba on veebilehel. Oluline on monitooringut teostada regulaarselt, et ohte avastada ja lahendada kiiremini. Lisatõhusust annab juurde kasutaja kohene teavitamine riski tuvastamisel.
- **Failide muutmise (*File Editor*) võimaluse keelamine** – kui kurjategija pääseb lehele ligi, keelab antud funktsioon WordPressi failide redigeerimise võimaluse, mis tõttu ei saa ründaja failidesse pahavara sisestada. Tähtis on piirata failide redigeerimise võimalusi ainult juurdepääsu omavatele administraatoritele.
- ***HTTP* turvapäised** - tagavad, et veebisaidi kasutajate brauserid suhtlevad veebilehega turvaliselt. Need aitavad kaitsta mitmesuguste rünnakute eest, näiteks *Cross-Site Scripting* (XSS). Olulisemad päised, mis peaksid igal lehel olema:

HTTP Strict-Transport-Security (HSTS), *Content-Security-Policy* (CSP), *X-Frame-Options.*

- **Tugev paroolipoliitika** - tugev parool peaks olema vähemalt 16 tähemärki pikk ning sisaldama erinevaid tähemärke, sealhulgas numbreid, suuri ja väikeseid tähti ning sümboleid. Lisaks tuleks vältida sagedaste paroolide kasutamist ning neid tuleks regulaarselt muuta. Parooli haldamiseks on soovitatav kasutada WordPressi paroolihalduri pistikprogrammi, mis aitab seadistada eelpool mainitud nõuded kasutajale kohustuslikuks.
- **Kaheastmelise autentimise lisamine** – turvameede, mis nõuab lisaks tavapärasele kasutajanimele ja paroolile ka teist kinnitust, näiteks mobiilse autentimisrakenduse abil saadetud kinnituskoodi. Kasutajanimi ja parool ei pruugi olla piisavad turvaliseks autentimiseks.
- **Sisselogimiselehe URL muutmine** – WordPressi vaikimisi sisselogimisleht on teadaolevalt */wp-admin*, mis teeb selle lihtsaks rünnakute sihtmärgiks. Sisselogimise URL-i muutmine raskendab ligipääsu lehele.
- **Sisselogimisekatsete piiramine** – aitab vältida sisselogimisrünnakuid, kus kasutatakse automatiseeritud tööriistu, et proovida sisse logida kasutajanimede ja paroolide kombinatsioonidega. Nende piiramisel on võimalik blokeerida IP-aadresse, mis ületavad lubatud sisselogimiskatsed.
- ***reCAPTCHA*** – aitab tuvastada, kas sisselogimiskatsed või kontaktvormi sisestused on inimeste või automatiseeritud robotite poolt tehtud. Soovitatav on kasutada selle uusimat versiooni *v3*, kus tuvastamine toimub ilma kasutajapoolsete toiminguteta ning paigaldada see igale lehel asuvale vormile, kuhu saab andmeid sisestada.

Neid nõuandeid rakendades on võimalik vähendada turvariski ja kaitsta WordPressi veebilehte küberkurjategijate eest. Samuti tuleks turvalisust pidevalt jälgida ja uuendada, et vältida potentsiaalseid rünnakuid ja nende negatiivseid tagajärgi. Veebilehe turvalisuse tagamine peaks kindlasti kuuluma lehe omaniku prioriteetide hulka, võttes protsessi tõsiselt ning seda mittealahinnata.

Arvestades, et kõik veebilehed on oma ülesehituse, funktsionaalsuse ja eesmärgi poolest omanäolised, turvariskide madaldamise variante on hulgaliselt ning küberründajate taktikad ja meetodid muutuvad pidevalt, võivad töö autori valikust erinevad turvalisuse tagamise võimalused anda teistsugused tulemused. Lõpliku otsuse turvameetodite

rakendamise kohta tuleks teha pärast hoolikat uurimist ja kaalutlemist, lähtudes konkreetsest olukorrast ja vajadustest.

5.1 Edasiarendus

Kuigi autor on juba rakendanud mitmeid efektiivseid turvalisusmeetmeid, et tagada veebilehe turvalisus, on alati võimalik olemasolevat veelgi täiendada, et kaitsta veebilehte potentsiaalsete tuleviku ohtude eest. Autor toob välja mõned võimalikud täiendavad turvalisuse tagamise võimalused, mida tasuks tulevikus kaaluda, kuid millele antud töös ei keskendatud.

Analüüsi põhjal selgus, et investeering turvalisusesse tasub ettevõttele kindlasti ära, arvestades turvalisuse võimet tõsta kasumlikkust ning turvalisuse puudumise võimalike kahjudega. Kuna antud töös kasutati vaid tasuta turvalisuse pluginate versioone, siis oleks järgmiseks sammuks minna üle Wordfence tasulisele versioonile, mis sisaldab täiendavalt ka reaalajas tulemüüri ja monitooringu värskendusi, Wordfence tugitiimi ööpäevaringset tuge probleemide lahendamiseks ning nendepoolset pahavara eemaldamist [39]. See tagaks ohtude veelgi kiirema likvideerimise ning veebilehe omanik saaks keskenduda südamerahus äritegevusele, sest lehega tegelevad professionaalid.

Juba eelpool töös mainitud olulist aspekti arvesse võttes, et turvalisuse tagamine on pidev protsess, tuleks ka edaspidi regulaarselt lehte kontrollida ning hoida ajakohasena. Lisaks kuna Amidisaini veebilehele on juurdepääs ka kliendile endal ning ta sooritab iseseisvalt lehel mitmeid toiminguid, tuleks talle selgitada antud töös käsitletud meetmeid ning nende olulisust. Alustades näiteks tugeva paroolipoliitika regulaarsest järgimisest. Nii suureneb teadmine antud valdkonnas ning seeläbi väheneb turvarisk.

6 Kokkuvõte

Veebilehtede turvalisus on üha olulisem teema tänapäeva digitaalses maailmas, kus aina rohkem tegevusi toimub internetis ja erinevaid andmeid hoiustatakse veebis. Turvaline veebileht on oluline nii veebilehe kasutajate kui ka omanike jaoks, kuna küberrünnakud on muutunud üha levinumaks ning võivad põhjustada andmeleket, raha -ja mainekahju.

Käesoleva bakalaureusetöö eesmärgiks oli analüüsida erinevaid meetodeid ja vahendeid, mis võimaldavad tagada WordPressi platvormi veebilehtede turvalisuse. Eesmärgi saavutamiseks selgitati veebilehtede turvalisuse vajalikkust, tutvustati üldisi tegureid, mis mõjutavad nende turvalisust, kirjeldati mõõdikuid ja meetmeid, mida kasutada veebilehtede turvamiseks, hindamiseks ja analüüsimiseks. Pärast analüüsi viidi läbi turvalisuse testimine Web Design Agency OÜ kliendi veebilehel, et välja selgitada tõhusaimad viisid WordPressi veebilehtede turvalisuse tõstmiseks ning suurendada kliendi lehe turvalisust.

Töö peamine tulemus on ettevõtte Amidisain OÜ turvatud veebileht, mis vastab töös seatud turvalisuse tõstmise eesmärkidele ning mille turvariski tase on viidud miinimumini, järgides turvalisuse parimaid tavasid. Töö lisaväärtusena koostas autor ülevaatliku loendi nõuannetest ja tegevustest, mille eesmärgiks on aidata luua efektiivne turvakiht WordPressi sisuhaldussüsteemi veebilehtedele, mis kaitseb erinevate ohtude eest, see juures pannes mõistma turvalisuse vajalikkuse aspekte.

Läbiviidud veebilehe turvamise analüüsi tulemustest võib järeldada, et veebilehe turvalisuse parandamiseks on vajalik rakendada erinevaid meetmeid ning nende valik sõltub peamiselt veebilehe enda funktsionaalsusest. Kõige tähtsamateks neist on veebilehe varukoopia hoiustamine, tarkvara, teemade ja pluginate värskendamine, lehe sisene ja brauseri vaheline regulaarne monitooring pahavara eemaldamiseks ning tugeva paroolipoliitika järgimine. Antud meetmeid rakendades on võimalik tõsta veebilehe turvalisust ja vähendada potentsiaalseid riske, mis tulenevad küberrünnakutest. Siiski on oluline meeles pidada, et turvalisus on pidev protsess ning turvameetmete rakendamine on vajalik ka pärast veebilehe loomist ja käiku laskmist.

Kasutatud kirjandus

[1] N. Huss, „How Many Websites Are There in the World?,“ 16 02 2023. [Võrgumaterjal]. Available: https://siteefy.com/how-many-websites-are-there/. [Kasutatud 27 03 2023].

[2] R. Tomasis, „What is Website Security? Plus 7 Steps to Secure Your Website,“ 17 01 2023. [Võrgumaterjal]. Available: https://www.wix.com/blog/2022/01/website-security. [Kasutatud 26 03 2023].

[3] J. Chambers, „55 Astounding Cybersecurity Statistics in 2023,“ 07 01 2023. [Võrgumaterjal]. Available: https://www.ukwebhostreview.com/cybersecurity-statistics/?fbclid=IwAR2CfMXxF-1eCg3Mvl7Go7aRbTl-GRH5zLvxYGmRhZMzWFqVOEMgwO-Qzdo. [Kasutatud 30 03 2023].

[4] SiteLock, „Website Security Definition & How to Keep Your Site Protected,“ 27 07 2022. [Võrgumaterjal]. Available: https://www.sitelock.com/blog/what-is-website-security/. [Kasutatud 20 03 2023].

[5] Sucuri, „Website Security & Protection: How to Secure a Website,“ 2023. [Võrgumaterjal]. Available: https://sucuri.net/guides/website-security/. [Kasutatud 2023 03 26].

[6] C. Greenlees, „4 Reasons Why Website Security Is Important,“ 20 10 2020. [Võrgumaterjal]. Available: https://sectigo.com/resource-library/why-is-website-security-important-and-why-should-businesses-care. [Kasutatud 27 03 2023].

[7] Patchstack, „State Of WordPress Security In 2021,“ 04 03 2022. [Võrgumaterjal]. Available: https://patchstack.com/whitepaper/the-state-of-wordpress-security-in-2021/. [Kasutatud 26 03 2023].

[8] A. Talalaev, „5 Reasons Why Website Security Is Important,“ 03 04 2021. [Võrgumaterjal]. Available: https://patchstack.com/articles/reasons-why-website-security-important/. [Kasutatud 26 03 2023].

[9] T. Perez, „Why Websites Get Hacked,“ 26 02 2015. [Võrgumaterjal]. Available: https://blog.sucuri.net/2015/02/why-websites-get-hacked.html. [Kasutatud 29 03 2023].

[10] Graphus, „What Is the Goal Behind Phishing Emails?,“ 16 12 2022. [Võrgumaterjal]. Available: https://www.graphus.ai/blog/what-is-the-goal-behind-phishing-emails/. [Kasutatud 28 03 2023].

[11] A. Talalaev, „Why Are Hackers Attacking Websites?,“ 23 02 2021. [Võrgumaterjal]. Available: https://patchstack.com/articles/hackers-attacking-websites/. [Kasutatud 27 03 2023].

[12] Checkpoint, „What is Hacktivism?,“ 2023. [Võrgumaterjal]. Available: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-hacktivism/. [Kasutatud 28 03 2023].

[13] B. Martin, „2014 Website Defacements,“ 01 01 2015. [Võrgumaterjal]. Available: https://blog.sucuri.net/2015/01/website-hacks-defacements-2014.html. [Kasutatud 25 03 2023].

[14] Comodo Security Solutions, „The security issues with websites that must be avoided at all cost,“ 2023. [Võrgumaterjal]. Available: https://cwatch.comodo.com/security-issues-with-websites.php. [Kasutatud 25 03 2023].

[15] G. Kalman, „10 Common Web Security Vulnerabilities,“ 08 12 2022. [Võrgumaterjal]. Available: https://www.toptal.com/security/10-most-common-web-security-vulnerabilities. [Kasutatud 28 03 2023].

[16] K. Krishnamoorthy, „How Do Websites Get Hacked?,“ 13 04 2020. [Võrgumaterjal]. Available: https://www.indusface.com/blog/how-do-websites-get-hacked/. [Kasutatud 16 04 2023].

[17] A. Freda, „What Is a Firewall and Why Do You Need One?,“ 23 02 2023. [Võrgumaterjal]. Available: https://www.avast.com/c-what-is-a-firewall. [Kasutatud 27 03 2023].

[18] Kaspersky Lab, „What is an SSL certificate – Definition and Explanation,“ 2023. [Võrgumaterjal]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate. [Kasutatud 20 03 2023].

[19] ICDSoft, „Website Backups – Do You *Really* Need Them? (Yes, You Really Do),“ 30 07 2021. [Võrgumaterjal]. Available: https://www.icdsoft.com/blog/website-backups-do-you-really-need-them/. [Kasutatud 30 03 2023].

[20] UC Santa Barbara Information Technology, „Password Best Practices,“ 2023. [Võrgumaterjal]. Available: https://www.it.ucsb.edu/secure-compute-research-environment-user-guide/password-best-practices. [Kasutatud 22 03 2023].

[21] National Cyber Security Center, „Device Security Guidance,“ 2023. [Võrgumaterjal]. Available: https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date. [Kasutatud 20 03 2023].

[22] E. Gregersen, „WordPress content management system,“ 17 03 2023. [Võrgumaterjal]. Available: https://www.britannica.com/technology/WordPress. [Kasutatud 13 04 2023].

[23] R. Brandl ja C. Ellis, „WordPress Market Share (2023),“ 11 01 2023. [Võrgumaterjal]. Available: https://www.tooltester.com/en/blog/wordpress-market-share/. [Kasutatud 05 04 2023].

[24] A. Silkalns, „WordPress Statistics: How Many Websites Use WordPress in 2023?,“ 09 04 2023. [Võrgumaterjal]. Available: https://colorlib.com/wp/wordpress-statistics/. [Kasutatud 13 04 2023].

[25] K. Muldoon, „What Is WordPress? What Can It Do & Is It Right For You? A Beginner’s Guide,“ 19 01 2023. [Võrgumaterjal]. Available: https://www.wpkube.com/what-is-wordpress/. [Kasutatud 10 04 2023].

[26] Wordpress, „Plugins,“ 2023. [Võrgumaterjal]. Available: https://wordpress.org/plugins/. [Kasutatud 12 04 2023].

[27] E. Deckers, „Why WordPress? 7 benefits of WordPress websites,“ 04 10 2021. [Võrgumaterjal]. Available: https://www.godaddy.com/garage/why-wordpress-benefits-wordpress-websites/. [Kasutatud 12 04 2023].

[28] J. Odukoya, „Why Use WordPress: Pros and Cons,“ 17 10 2022. [Võrgumaterjal]. Available: https://translatepress.com/wordpress-pros-and-cons/. [Kasutatud 11 04 2023].

[29] D. Knauss, „The 2022 WordPress Vulnerability Annual Report,“ 10 04 2023. [Võrgumaterjal]. Available: https://ithemes.com/blog/the-2022-wordpress-vulnerability-annual-report/. [Kasutatud 11 04 2023].

[30] WPScan, „WordPress Vulnerability Statistics,“ 2023. [Võrgumaterjal]. Available: https://wpscan.com/statistics. [Kasutatud 28 04 2023].

[31] J. Juviler, „14 WordPress Security Issues & Vulnerabilities You Should Know About [New Research from WCEU 2022],“ 23 06 2022. [Võrgumaterjal]. Available: https://blog.hubspot.com/website/wordpress-security-issues. [Kasutatud 11 04 2023].

[32] D. Moen, „How Attackers Gain Access to WordPress Sites,“ 23 03 2016. [Võrgumaterjal]. Available: https://www.wordfence.com/blog/2016/03/attackers-gain-access-wordpress-sites/. [Kasutatud 11 04 2023].

[33] B. Jackson, „Is WordPress Secure? Here’s What the Data Says,“ 12 07 2022. [Võrgumaterjal]. Available: https://kinsta.com/blog/is-wordpress-secure/. [Kasutatud 11 04 2023].

[34] T. Anderson, „What WordPress User Roles Are and How to Manage Them for Your Website,“ 23 04 2023. [Võrgumaterjal]. Available: https://www.bluehost.com/blog/what-wordpress-user-roles-are-and-how-to-manage-them-for-your-website/. [Kasutatud 12 04 2023].

[35] Ithemes editorial team, „5 Common WordPress Security Issues,“ 06 01 2023. [Võrgumaterjal]. Available: https://ithemes.com/blog/wordpress-security-issues/. [Kasutatud 15 04 2023].

[36] E. Staff, „11 Top Reasons Why WordPress Sites Get Hacked (& How to Prevent it),“ 18 04 2023. [Võrgumaterjal]. Available: https://www.wpbeginner.com/beginners-guide/reasons-why-wordpress-site-gets-hacked/. [Kasutatud 19 04 2023].

[37] B. Dreisbach, „6 WordPress Security Tips and Best Practices Every Site Owner Should Know,“ 28 02 2023. [Võrgumaterjal]. Available: https://wpengine.com/resources/wordpress-security-tips-best-practices/. [Kasutatud 15 04 2023].

[38] D. Sears, „9 Best WordPress Security Plugins to Protect Your Website,“ 28 03 2023. [Võrgumaterjal]. Available: https://www.bluehost.com/blog/best-wordpress-security-plugins/. [Kasutatud 15 04 2023].

[39] Editorial Team, „Wordfence Review: The Good, the Bad, and the Secure,“ 29 03 2023. [Võrgumaterjal]. Available: https://www.malcare.com/blog/wordfence-review/. [Kasutatud 16 04 2023].

[40] J. Benz, „WordPress Security: How useful are security plugins really?,“ 16 03 2023. [Võrgumaterjal]. Available: https://raidboxes.io/en/blog/security/wordpress-security-plugins/. [Kasutatud 17 04 2023].

[41] Z. Banach, „HTTP security headers: An easy way to harden your web applications,“ 21 10 2022. [Võrgumaterjal]. Available: https://www.invicti.com/blog/web-security/http-security-headers/. [Kasutatud 17 04 2023].

[42] Sucuri, „Free website malware and security checker,“ 2023. [Võrgumaterjal]. Available: https://sitecheck.sucuri.net/. [Kasutatud 17 04 2023].

[43] A. Martori, „5 Malware & Virus Scanning Tools You Need to Check Out,“ 16 12 2019. [Võrgumaterjal]. Available: https://blog.sucuri.net/2019/12/website-malware-virus-scanners.html. [Kasutatud 17 04 2023].

[44] S. Helme, „Scan your site now,“ 2023. [Võrgumaterjal]. Available: https://securityheaders.com/. [Kasutatud 15 04 2023].

[45] S. Fadilpašić, „Best free web security scanners of 2023,“ 27 04 2023. [Võrgumaterjal]. Available: https://www.techradar.com/best/best-free-web-security-scanners-of-year. [Kasutatud 28 04 2023].

[46] S. Helme, „Hardening your HTTP response headers,“ 24 03 2015. [Võrgumaterjal]. Available: https://scotthelme.co.uk/hardening-your-http-response-headers/. [Kasutatud 20 04 2023].

[47] S. Helme, „A new security header: Referrer Policy,“ 17 02 2017. [Võrgumaterjal]. Available: https://scotthelme.co.uk/a-new-security-header-referrer-policy/. [Kasutatud 20 04 2023].

[48] S. Helme, „Goodbye Feature Policy and hello Permissions Policy!,“ 07 09 2020. [Võrgumaterjal]. Available: https://scotthelme.co.uk/goodbye-feature-policy-and-hello-permissions-policy/. [Kasutatud 20 04 2023].

[49] Y. Iliev, B. Angelov ja P. J. Iliev, „All-in-One WP Migration,“ 2023. [Võrgumaterjal]. Available: https://et.wordpress.org/plugins/all-in-one-wp-migration/. [Kasutatud 22 04 2023].

[50] Wordfence Security, wfryan, WFMattR ja wfmatt, „Wordfence Security – Firewall, Malware Scan, and Login Security,“ 2023. [Võrgumaterjal]. Available: https://wordpress.org/plugins/wordfence/. [Kasutatud 22 04 2023].

[51] Astra Security, A. Krishna ja Shikhil, „WP Hardening – Fix Your WordPress Security,“ 2023. [Võrgumaterjal]. Available: https://wordpress.org/plugins/wp-security-hardening/. [Kasutatud 22 04 2023].

[52] Andrea ja Augusto, „Headers Security Advanced & HSTS WP,“ 2023. [Võrgumaterjal]. Available: https://wordpress.org/plugins/headers-security-advanced-hsts-wp/. [Kasutatud 23 04 2023].

[53] miniorange, „Password Policy Manager | Password Manager,“ 2023. [Võrgumaterjal]. Available: https://wordpress.org/plugins/password-policy-manager/. [Kasutatud 25 04 2023].

[54] WebFactory, „Login Lockdown – Protect Login Form,“ 2023. [Võrgumaterjal]. Available: https://wordpress.org/plugins/login-lockdown/. [Kasutatud 26 04 2023].

[55] DataDome, „ReCAPTCHA v2 vs. v3: Are they really efficient for bot protection?,“ 20 08 2022. [Võrgumaterjal]. Available: https://datadome.co/bot-management-protection/recaptchav2-recaptchav3-efficient-bot-protection/. [Kasutatud 26 04 2023].

[56] Paul, „Sucuri: “No firewall detected”,“ 2021. [Võrgumaterjal]. Available: https://wordpress.org/support/topic/sucuri-no-firewall-detected/. [Kasutatud 27 04 2023].

[57] S. F. Everyone, „Web Application Firewall (WAF) Detection Scanner,“ 2023. [Võrgumaterjal]. Available: https://securityforeveryone.com/tools/waf-detection-scanner. [Kasutatud 27 04 2023].

[58] Ithemes, „iThemes Security Pro Review PROS & CONS (2023) How Good It Is In Protecting Site?,“ 13 01 2023. [Võrgumaterjal]. Available: https://www.kasareviews.com/ithemes-security-pro-review/. [Kasutatud 15 04 2023].

[59] S. Ravoof, „Sucuri vs Wordfence: WordPress Security Plugins Showdown,“ 30 01 2023. [Võrgumaterjal]. Available: https://kinsta.com/blog/sucuri-vs-wordfence/. [Kasutatud 16 04 2023].

Lisa 1 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks[1]

Mina, Anli Gea Põldemaa

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Veebilehe turvalisuse võimalused“, mille juhendaja on Karl-Erik Karu
   1.1. reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
   1.2. üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.
2. Olen teadlik, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.
3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest ning muudest õigusaktidest tulenevaid õigusi.

08.05.2023

1 Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal vastavalt üliõpilase taotlusele lõputööle juurdepääsupiirangu kehtestamiseks, mis on allkirjastatud teaduskonna dekaani poolt, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil. Kui lõputöö on loonud kaks või enam isikut oma ühise loomingulise tegevusega ning lõputöö kaas- või ühisautor(id) ei ole andnud lõputööd kaitsvale üliõpilasele kindlaksmääratud tähtajaks nõusolekut lõputöö reprodutseerimiseks ja avalikustamiseks vastavalt lihtlitsentsi punktidele 1.1. ja 1.2, siis lihtlitsents nimetatud tähtaja jooksul ei kehti.

Lisa 2 – Wordfence ülevaade

Funktsionaalsus

Wordfence on üks maailma populaarsemaid WordPressi veebiturvalisuse pluginaid, mis pakub laias valikus funktsioone ja vahendeid, et kaitsta lehte pahatahtlike rünnakute ja häkkimise eest. Wordfence-il on lokaliseeritud tulemüür ehk sisaldab serveripoolset sügavamal tasemel skaneerimist. See on mõistlik valik täiesti uutele või väikese eelarvega veebilehtedele. [39]

Plussid

Wordfence pakub kasutajatele kergesti mõistetavat ja intuitiivset kasutajaliidest. Pluginat on lihtne seadistada ja kasutada ka neil, kellel puudub tehniline taust. Wordfence hoolitseb enamiku turvaaspektide eest ise ning tasuta versioonis saab otse juurdepääsu kogu tulemüüri spektrile. Lisaks on kõrgelt hinnatud reaalaja liikluse skaneerimise funktsionaalsust. Oluline on mainida, et arvustuse kohaselt on see parim tasuta versiooniga turvaplugin. [39]

Miinused

Potentsiaalse probleemina võib välja tuua mõju serverile, sest Wordfence teostab skannimist veebilehe enda serveris ning võib see tõttu mõjutada veebisaidi jõudlust. Plugin skanneerib pahavara põhifailides, mittepreemium pluginates ja teemades, kuid ei suuda tuvastada pahavara andmebaasis, mis on sageli pahavara sihtmärk. Lisaks on pahavara eemaldamine keeruline ning nõuab kallimale plaanile üleminekut. [39]

Hinnastus

Wordfence'i hind sõltub sellest, millist versiooni soovitakse kasutada. Tasuta versioon sisaldab põhifunktsioone, kuid piiratud funktsionaalsusega. Tasulised versioonid sisaldavad täiendavaid funktsioone, nagu näiteks arendaja tugi, pahavara eemaldamine ja tegevusjärgsete aruannete koostamine. Hinnad algavad 99 dollarist aastas. [39]

Lisa 3 – iThemes ülevaade

Funktsionaalsus

iThemes on teine populaarne WordPressi turvalisuse plugin, mis suurendab WordPressi veebisaidi turvalisust ja kaitset. Pistikprogramm tuvastab ja blokeerib automaatselt kahtlase tegevuse, suurendades samal ajal paroolide ja andmete turvalisust. Tänu kasulikele WordPressi turvameetmetele on plugin soovitatav sisult lihtsamate lehtede turvataseme tõstmiseks, mis ei vaja mahukat skaneerimist ja tulemüüri. [40]

Plussid

iThemes pakub *AwayMode* turvafunktsiooni, millega saab teie WordPressi paneeli muuta teatud kellaaegadel kättesaamatuks, kui kasutaja on passiivne, nii et keegi teine ei pääse lehele ligi ega saaks seda muuta. iThemes *Magic Links* funktsioon on kiire ja usaldusväärne viis WordPressi sisselogimiseks, eriti kui kasutaja on juurdepääsu kaotanud. Kui kasutaja on *Local Brute-Force* kaitse funktsiooni tõttu välja lülitatud, saab taotleda erisõnumit, mille kaudu saate unikaalse tagasilogimisviisi. [40]

Miinused

iThemes võib vahel kogeda raskusi teatud veebimajutusteenuste pakkujatega, eriti nende teenusepakkujate puhul, mille RAM-i (juhusliku juurdepääsu mälu) maht on piiratud. Limiteeritud maht põhjustab rohkema info töötlemisel jõudluse vähenemist. Selles olukorras võib iThemes'i plugin toimimine olla ebastabiilne, eriti kui kasutatakse täiustatud funktsioone nagu failimuudatuste jälgimine või eesliidete muutmine. Lisaks on võrgust pärinev teave juurdepääsetav ainult Pro versioonis. [40]

Hinnastus

iThemes Security põhipakett on tasuta, kuid pro funktsioonidega versioon maksab alates 80 dollarist aastas. Tasuta versioon ei sisalda funktsioone nagu *Magic Links* ja kaheastmeline autentimine. Pro versioon on saadaval kolmes hinnaklassis, mis sisaldavad ühe aasta värskendusi ja kliendituge. Pro versioonis on mõned elemendid, mida konkurendid pakuvad tasuta, kuid antud plugin annab üpris tugevat kaitset ning investeering tasub ära. [40]

Lisa 4 – Sucuri ülevaade

Funktsionaalsus

Sucuri on populaarne pilvepõhine veebisaitide turvatööriist veebisaitide turvamiseks. See filtreerib kogu veebisaidi liikluse enne, kui see hostimisserverisse jõuab. Sucuri Firewall teeb tulemusrikka töö *DDoS*-i rünnakute, kuritarvitavate robotite ja kliendi andmete kahjustamise vastu. Plugin on soovituslik kui oluline on CDN-i kasutamine ehk teisi sõnu veebileht pakub oma sisu rahvusvahelisel turul ning prioriteet on suure külastavuse tõttu veebilehe laadimiskiiruse efektiivsus. [41]

Plussid

Sucuri automatiseerib enamiku oma turvafunktsioonidest, nii et kasutajal tuleb need vaid ühe korra seadistada. Samuti ei pea muretsema plugina värskendamise ega hooldamise pärast. Kuna Sucuri veebirakenduse tulemüür on pilvepõhine, ei vaja see kasutaja poolset tehnilist hooldust. Sucuri kasutab CDN-i, et kiirendada veebisaidi laadimisaega. [41]

Miinused

Tasuta Sucuri pistikprogramm rakendab mõningaid standardseid turvameetmeid, kuid see ei ole loodud veebisaidi vastu suunatud suuremate rünnakute vältimiseks. Üks esmatähtsaid funktsioone nagu tulemüür tuleb kaasa ainult premium versiooniga. Lisaks ei teosta Sucuri serveri tasemel sügavat skannimist. [41]

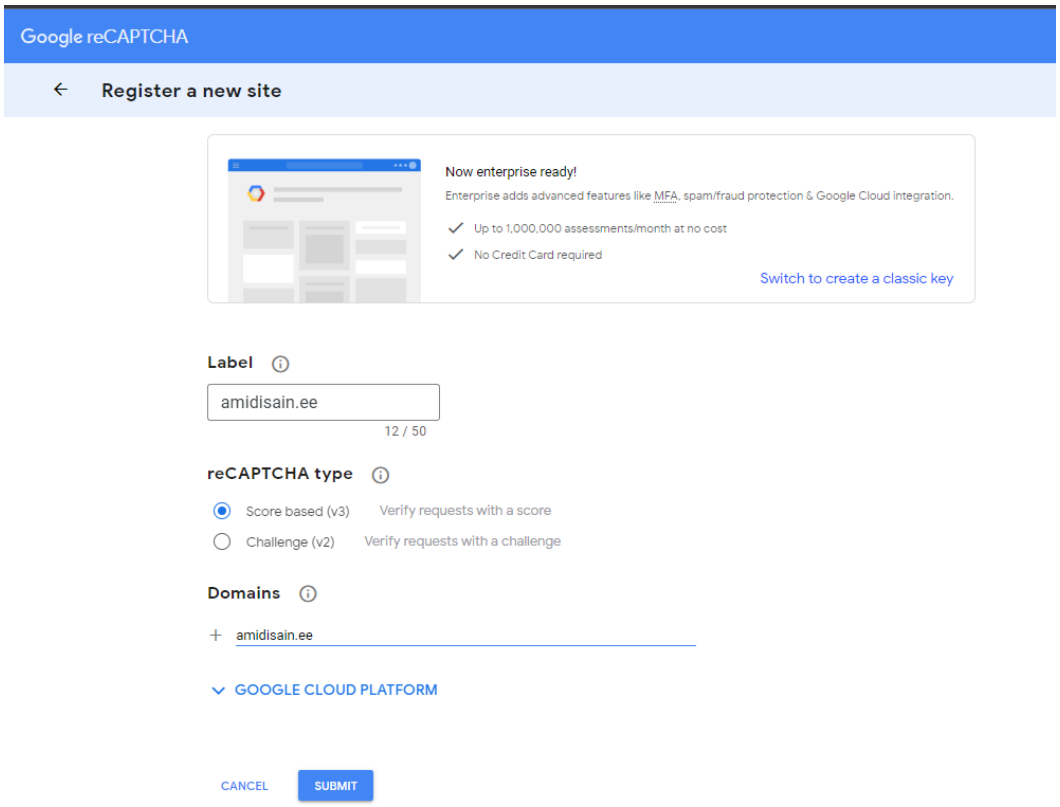
Hinnastus

Sucuri hind on alates 199,99 dollarist aastas. See pakett sisaldab iga-aastast põhjalikku turvakontrolli, päevast pahavara skannimist ja eemaldamist, DDoS kaitset, reaalajas teavitusi, pidevat jälgimist ja muud. Sucuri pakub ka mitmeid teisi teenuseid, sealhulgas professionaalset pahavara eemaldamist ja pahavara eemaldamise garantiid, mida saab osta eraldi. [41]

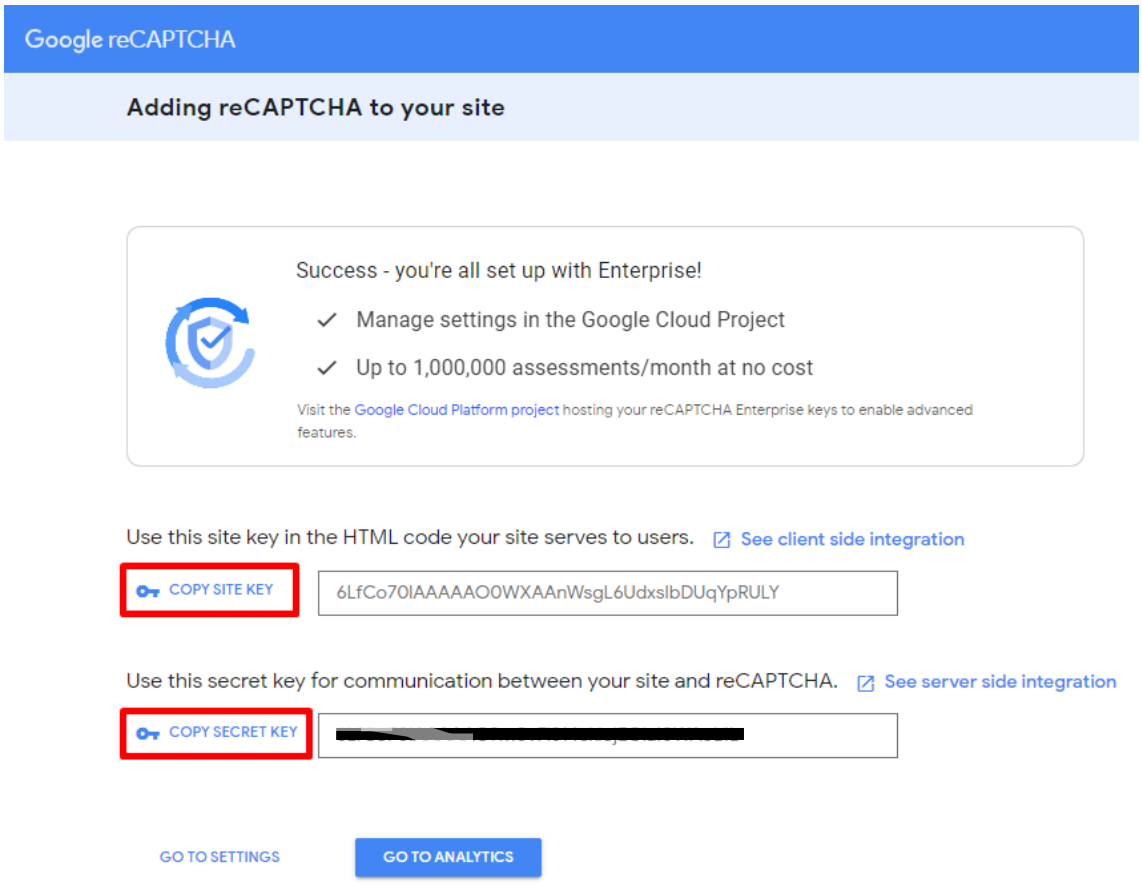
Lisa 5 – reCAPTCHA v3 versiooni paigaldamise protsess veebilehele

Järgnevalt on koos piltidega välja toodud *reCAPTCHA v3* versiooni paigaldamise protsess veebilehele:

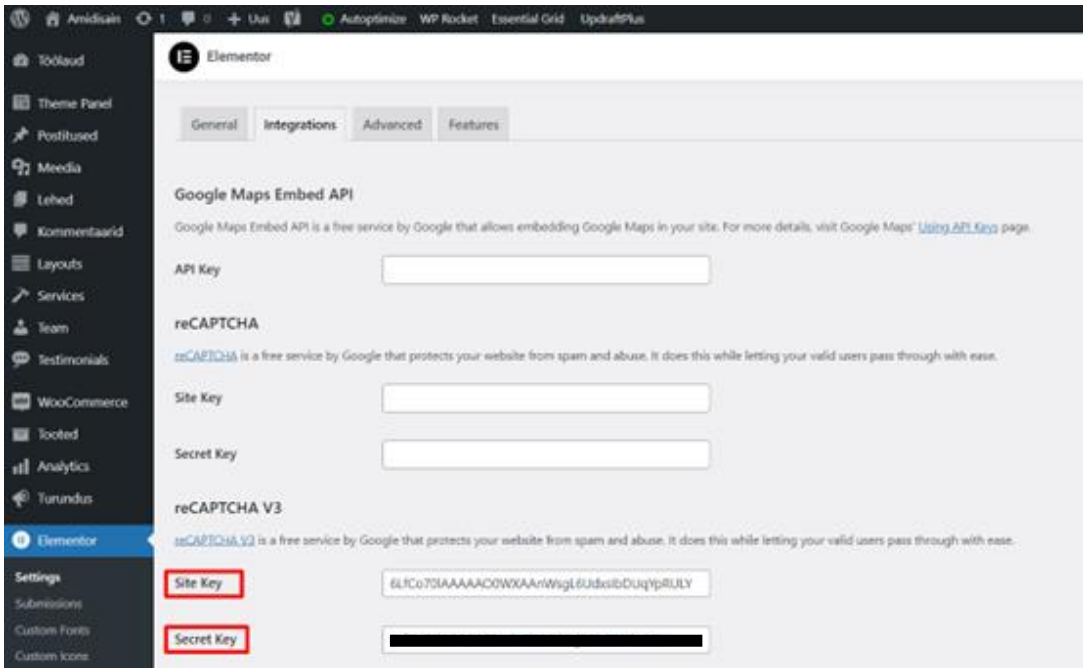
1. Esmalt registreerib autor *Google reCAPTCHA* lehel Amidisaini veebilehe, kus tuleb lisada vastav *Label*, domeeni nimi ning valida *reCAPTCHA* tüüp.



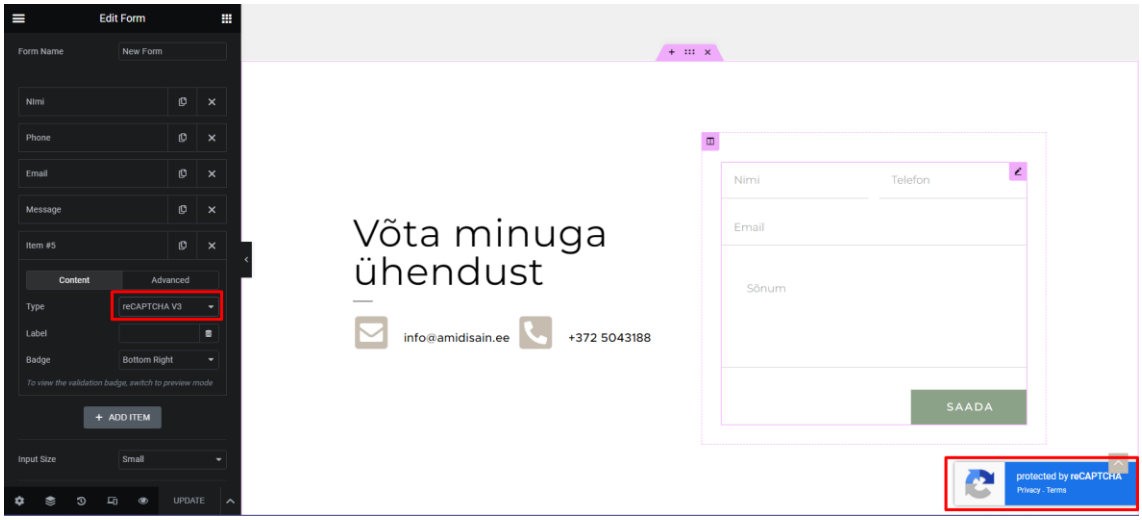
2. Seejärel genereeritakse kaks võtit, saidivõti (*Site Key*) ning salavõti (*Secret Key*). Esimest kasutatakse veebilehel antud teenuse käivitamiseks ning teist serveripoolse valideerimise teostamiseks.



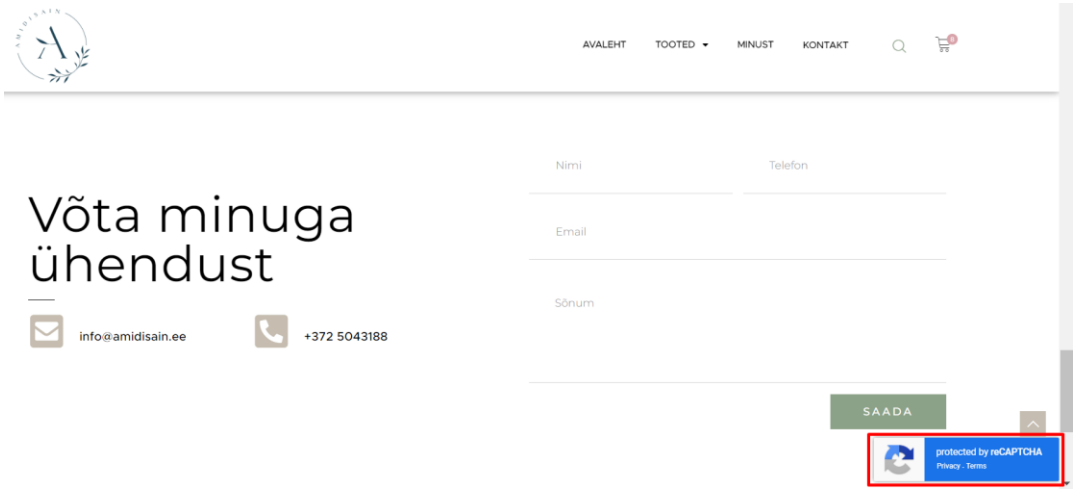
3. Antud veebileht kasutab visuaalset WordPressi veebisaitide koostamise pluginat *Elementor*, kuhu on sisseehitatud *reCAPTCHA* vidin, mis võimaldab hõlpsasti lisada antud turvalisuse funktsionaalsuse oma veebilehele. Saadud võtmed sisestatakse *Elementori* integratsiooni menüüsse, mis asub WordPressi adminpaneelil.



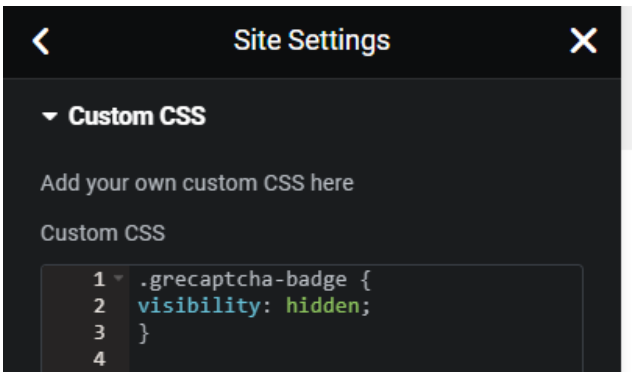
4. Nüüd on aeg lisada *reCAPTCHA* ka kontaktivormi külge. Täpsemalt avas autor *Elementoris* lehe, kus kontaktivorm asub ning lisas sinna *reCAPTCHA v3* tüübi.

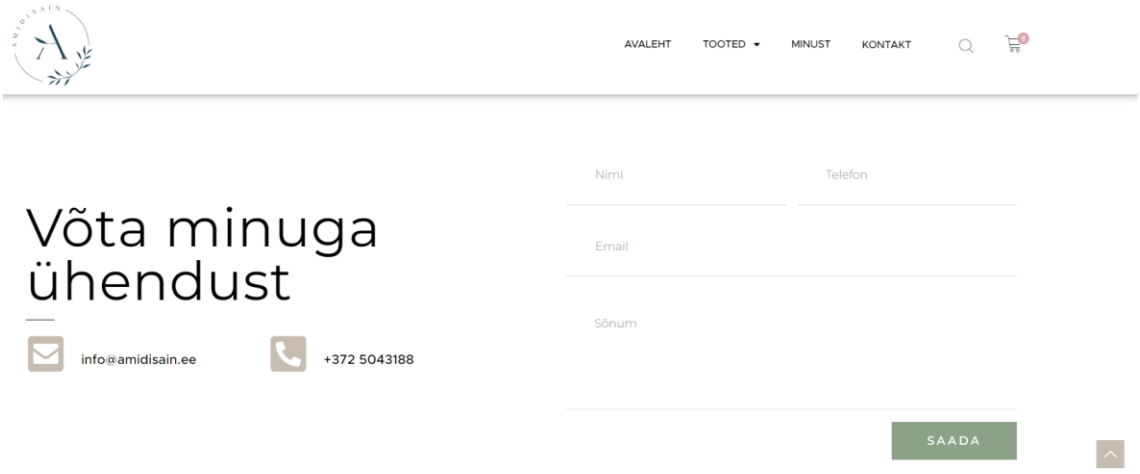


5. Veebilehte brauseris uuendades on *reCAPTCHA* olemasolu kinnitamiseks ka visuaalselt näha.



6. Kuna *reCAPTCHA v3* ei nõua kasutajapoolseid eritoiminguid, pole selle märgi nähtavus veebilehel oluline. Puhtama veebilehe vaate jaoks peitis autor järgneva CSS koodiga *reCAPTCHA* märgi ära, kuid turvameetodi funktsionaalsus säilib sellest hoolimata. Antud samm ei avalda mingit mõju lehe turvalisusele ning selle võib vahele jätta.





Lisa 6 – Veebilehele lisatud kodeeritud turvameetmed

1. **Htaccess kood PHP failide jooksutamise blokeerimiseks**

```
<FilesMatch "\.(?i:php)$">
<IfModule !mod_authz_core.c>
Order allow,deny
Deny from all
</IfModule>
<IfModule mod_authz_core.c>
Require all denied
</IfModule>
</FilesMatch>
```

2. **Functions.php faili kood WordPressi versiooni viidete eemaldamiseks**

```
remove_action('wp_head', 'wp_generator');

function eemalda_wp_versioon() {
return '';
}
add_filter('the_generator', 'eemalda_wp_versioon');
```

3. **Htaccess kood juurdepääsu piiramiseks aadressile /wp-admin**

```
<IfModule mod_rewrite.c>
RewriteEngine on
RewriteCond %{REQUEST_METHOD} POST
RewriteCond %{HTTP_REFERER} !^https://(.*)?amidisain\.ee [NC]
RewriteCond %{REQUEST_URI} ^(.*)?wp-login\.php(.*)$ [OR]
RewriteCond %{REQUEST_URI} ^(.*)?wp-admin$
RewriteRule ^(.*)$ - [F]
</IfModule>
```

4. **Wp-config.php faili lukustamise kood**

```
<Files wp-config.php>
Order deny,allow
Deny from all
</Files>
```