LAPIN AMK
Lapland University of Applied Sciences

NETTISIVUJEN TIETOTURVA WORDPRESS-LIITÄNNÄISILLÄ

Rönkkö Vertti

Opinnäytetyö

Tieto- ja viestintätekniikka
Insinööri (AMK)

2023

LAPIN AMK
Lapland University of Applied Sciences

Opinnäytetyön tiivistelmä

Tieto- ja viestintätekniikka
Insinööri (AMK)

Tekijä	Vertti Rönkkö	**Vuosi**	2023
Ohjaaja	Aku Kesti		
Toimeksiantaja	Veitsiluodon Metsämiehet ry		
Työn nimi	Nettisivujen tietoturva WordPress-liitännäisillä		
Sivumäärä	35		

Tässä opinnäytetyössä lähdin rakentamaan uusia nettisivustoja metsästysyhdistykselle korvaamaan edellisen nettisivuston. Sivustoon liitettiin tietoturvaliitännäisiä sekä tutkittiin tietoturvaa yleisellä tasolla.

Työn tavoitteena oli luoda tietoturvallinen nettisivusto liitännäisien ja palveluiden avulla sekä oppia tietoturvallisuudesta lisää. Tässä käytin pohjana kahta versiota WordPress-alustasta, jotta sain myös kokemusta alustojen toimivuudesta ja saatavuudesta. Työhön myös kuuluivat palvelimien ja verkkotunnuksien tilaus, niiden asentaminen sekä konfigurointi.

Tuloksena syntyivät modernit nettisivut, tietoturvaliitännäisen tutkimukset sekä yleistiedostaminen tietoturvasta. Tästä opinnäytetyöstä on hyötyä henkilöille, joilla on halu rakentaa nettisivuja tulevaisuudessa ja saada ideoita ja tietoa tästä aihealueesta.

Avainsanat ohjelmointi, protokolla, tietoturva, verkkotunnukset, WWW-sivut

LAPIN AMK
Lapland University of Applied Sciences

Abstract of Thesis

Study Programme in Information
and Communication Technology
Bachelor of Engineering

Author	Vertti Rönkkö	**Year**	2023
Supervisor	Aku Kesti		
Commissioned by	Veitsiluodon Metsämiehet ry		
Title	Website Security with WordPress-Plugins		
Number of pages	35		

The aim of this thesis study was to build a new website for a hunting association to replace the association's previous website.

A secure website with plugins and services was created using two versions of the WordPress-platform as a basis. That gave also a possibility for the author to gain experience of the functionality and availability of the platforms. The website was integrated with security plugins, and security was explored on a general level. The study also included subscribing to servers and domains, installing them and configuring them.

The result was a modern website, studies of security plugins and an overview of security. This thesis will be useful for people who want to build websites in the future and get ideas and information on this topic.

Keywords: data security, domain names, programming, protocols, web pages

SISÄLLYS

KÄYTETYT LYHENTEET JA TERMIT

2FA	Two-Factor Authentication, kaksivaiheinen todennus
botti	komentoja suorittava tietokoneohjelma
CAPTCHA	Completely Automatic Public Turing test to tell Computers and Humans Apart, henkilön varmistus ja autentikaatio käyttäjänä
CDN	Content Delivery Network, sisällönjakeluverkko
DNS	Domain Name System, nimipalvelujärjestelmä
DoS	denial-of-service, palvelunestohyökkäys
HTTPS	Hypertext Transfer Protocol Secure, protokolla suojattuun tiedon siirtoon
NVD	National Vulnerability Database, amerikkalainen tietoturvasivusto
spämmi	roskapostia, haitallisia sähköpostiviestejä
XSS	cross-site scripting, WWW-sivustojen tietoturva-aukko

1 JOHDANTO

Nykyaikana nettisivustojen laaja saatavuus on luonut mahdollisuuksia kaikenlaisen tiedon kokoamiseen ja jakamiseen ympäri maailmaa, minkä mukana on tullut myös ongelmallisia tekijöitä. Nämä tekijät yrittävät kaapata tiedonlähteitä sekä päästä mahdollisesti käsiksi sivustojen tietoihin, jotka ovat piilossa julkiselta puolelta. Tämän takia tietoturvallisuus on relevantti aihe, jota työstetään jokaisessa ammattimaisessa yksikössä. Vaikka tietoturvallisuus saattaa vaikuttaa hankalalta, on sen tarkoitus avustaa jokaista henkilöä.

Nettisivustojen tekemistä varten on tehty erilaisia pohjia, joita käyttäjät voivat hyödyntää. Näitä varten toiset kehittäjät voivat avustaa luomalla liitännäisiä, joita yhdistetään pohjiin. Nämä voivat tuoda erilaisia ominaisuuksia, ja turvallisuus on yksi näistä ominaisuuksista.

Tässä opinnäytetyössä käyn läpi WordPress-alustaa ja siihen liittyviä liitännäisiä, jotka auttavat suojaamaan sekä kehittäjiä että käyttäjiä. Tämän toteuttamiseksi olen luonut modernin nettisivuston Veitsiluodon Metsämiehet ry:lle, jotka korvaavat yli kymmenen vuotta vanhan nettisivuston. Käyn läpi kehittämisprosessia, sivustoon liitettäviä liitännäisiä sekä muita liitännäisiä, joita voi käyttää mahdollisesti, jos käyttämäni työkalut eivät sovellu erityistapauksiin.

Lähdin tekemään tätä opinnäytetyötä oman osaamiseni laajentamiseksi insinöörialalla sekä nettisivujen tekemisestä että tietoturvan osaamisesta. Pääsin harjoittamaan monta eri osa-aluetta tässä työssä, jotka edistävät ammattiosaamistani.

2 NETTISIVUT TIETOTURVAN KANNALTA

2.1 Yleinen tietoturva

Tietoturvan relevanttisuus on nousussa. Yritykset ja kehittäjät ovat kehittämässä uusia laitteita ja tapoja käyttää niitä, esimerkiksi internettiä, minkä mukana tulee kaikki haavoittuvuudet ja virheet. Tiedon arvokkuuden tiedostaminen sekä haavoittuvuuksien ja rikkomuksien opiskelu on ensimmäinen askel hyvässä tietoturvassa.

Yleisiin hyökkäystapoihin kuuluu DoS- ja XSS-hyökkäykset, väsytyshyökkäykset, ja SQL:ään liittyvät ongelmat, esimerkiksi NoSQL-injektiot. Nämä kaikki käyttävät hyödykseen joko suoria haavoittuvuuksia järjestelmissä tai kehittäjien virheitä. (Bassi 2023a.) Esimerkiksi väsytyshyökkäyksen tarkoitus on yrittää pakolla löytää käyttäjän salasana kokeilemalla yleisiä salasanoja niin kauan aikaa, kun hyökkäys on päällä. Tätä varten sivustoilla on yleisesti aikakatkaisu, kun on monta kertaa yrittänyt kirjautua sisään. Järjestelmä katsoo, että sama IP-osoite on yrittänyt kirjautua monta kertaa sisään tietyn ajan sisällä ja lukitsee kirjautumiset tietyksi ajaksi. Tämä aiheuttaa sen, että yksi botti ei pysty pakottamaan itseään sisälle nopeasti eli prosessissa kestäisi liian kauan aikaa ollakseen efektiivinen. (Zieniūtė 2023.)

Myös yleinen ongelma on verkkourkinta eli tietojen kalastelu, jossa käyttäjän henkilöllisyys voidaan varastaa tai päästä käsiksi pankkitietoihin tai muihin palveluihin, joihin on rahaa liitetty. Tämä ongelma on erityisesti tehokas, jos henkilö, joka esiintyy toisena käyttäjänä, on osannut piilottaa kaikki epäilykset, esimerkiksi väärinkirjoitukset, pahat kuvanmuokkaukset, ja niin edelleen. ”Kalastajat” ovat yleisesti myös tehneet valesivustoja, jotka näyttävät oikeilta sivustoilta, mutta verkkotunnus saattaa olla hieman erilainen. Tämän ongelman takia on viisasta tarkistaa linkit, joita saatetaan lähettää esimerkiksi sähköpostin kautta. Joskus linkit saattavat tulla hakkeroiduista posteista, joten varmuuden vuoksi ei välttämättä kannata edes koskea linkkeihin. Nämä saattavat tulla jopa omista kontakteista ilman varoitusta. (F-Secure 2023.)

Näitä haavoittuvuuksia ja virheitä varten kehittäjien on pitänyt olla varuillaan jo kymmeniä vuosia internetin laajentuessa. Joka päivä jotain uutta löytyy, ja joka

päivä niitä yritetään korjata kehittäessä ja päivittäessä sivustoja. Tietoturva-kurssit ovat tämän takia hyvin tärkeitä ja aktiivisia, erityisesti tietoteknisillä urilla. Jo pelkästään muutaman perustiedon oppiminen ja osaaminen auttaa massiivisesti millä tahansa uralla, vaikka ei tekisikään tietoteknisiä asioita työkseen. Nettisivujen tekemisen aikana nämä tiedot ovat tärkeitä.

Tärkein neuvo mitä voi ottaa vastaan nettisivujen tietoturvasta on se, että sivusto ei saa koskaan luottaa automaattisesti tietoon, joka on lähetetty sivustoon. Kaikki tieto kannattaa alustavasti puhdistaa kaikesta haitasta ja varmistaa ennen kuin sitä lukee, käynnistää, tai esittää, esimerkiksi haittaohjelmista. Yleistiedot mitkä vaikuttavat tähän turvaan ovat myös HTTPS:n vaikutus nettisivuihin, työkalujen käyttö, sekä tallenna vain tietoa mitä tarvitset. (MDN Web Docs 2023.)

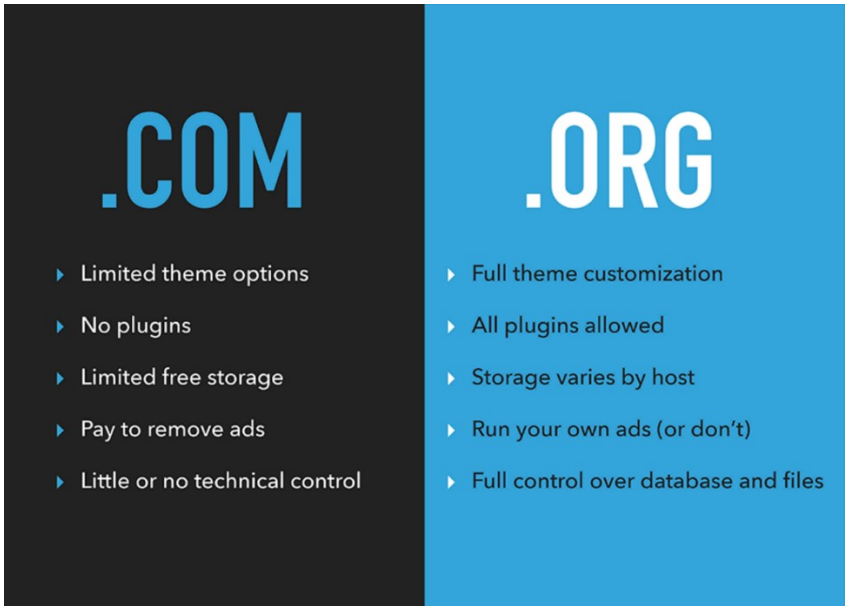
Perusasiat, kuten vahvojen salasanojen käytännön asetus, päivityksien asentaminen ja sivustojen puhtaana pitäminen ovat myös hyvin tärkeitä asioita, jotka pysyvät ajankohtaisina, vaikka ne saattavatkin vaikuttaa jopa liian yksinkertaisilta. Koskaan ei voi liikaa muistuttaa näistä asioista, joskus ne saattavat unohtua ja siinä vaiheessa saattaa olla jo liian myöhäistä. Myös muiden palveluiden ja työkalujen valitseminen on tärkeää. Vaikka palvelu saattaa olla ilmainen tai halpa, ei kannata olettaa, että ne ovat tarpeeksi. Arvostelut ja ammattilaisten mielipiteet ovat tärkeitä ja niitä kannattaa seurata, mutta myös kannattaa kriittisesti tiedustaa kaikenlainen tieto. (Bassi 2023b.)

Tärkeitä ovat myös varmuuskopiot. Aina on mahdollisuus, että tietoturvarikos tuhoaa sivut ja palvelut kokonaan. Tätä varten, jos varmuuskopioita ei ole olemassa, kaikki työ ja tieto ovat hukassa ja menetetty. Palveluita on olemassa, mitkä tekevät tämän automaattisesti käyttäjälle, mutta parhainta olisi oma muistaminen asian suhteen, koska jopa nämä palvelut saattavat pettää jokin päivä. Palmu (2019) kertoo lisää varmuuskopioinnin tärkeydestä ja miten tiedostot voi varmuuskopioida artikkelissaan ”Miksi varmuuskopiointi on tärkeää – Näin turvaat tiedostosi”. Jos nämä asiat ovat liikaa kehittäjälle, kannattaa harkita alan ammattilaisen palkkaamista (Bassi 2023b). Tosin tämä ei ole kaikille mahdollista, joten sen voi pitää viimeisenä vaihtoehtona. Kun nämä osuudet ovat varmistettu, pääsee kehittäjä seuraavaan osioon, eli työkalujen varmistamiseen.

2.2 Alustat, palvelut ja tilaukset

Työn aikana tuli monenlaisia vaiheita vastaan ja niiden mukana päätöksiä. Etsin kumpaa WordPress-versiota käytän, verkkotunnuksien hankkiminen ja monta muuta kohtaa. Käytin seuraavia palveluita työssäni, ja vertaan myös WordPressin versioita, jotta version valitseminen ei olisi haasteliasta. Yhtenä tavoitteena oli myös tehdä sivusto mahdollisimman edullisesti. Joten kun valitsin alustoja ja palveluita, piti tarkkaan tutkia mitä tarvitsin ja kuinka paljon ne maksavat minimissään. Mutta piti myös varmistaa, ettei saa olla niin halvat palvelut, että tietoturva kärsii.

WordPress-alustalla on kaksi versiota, wordpress.com ja wordpress.org (kuvio 1). Com on tarkoitettu kevyemmälle käytölle, esimerkiksi blogin ylläpitämistä tai muita kevyemmän päivityksen sivustoja varten. Org taas on raskaamman taakan versio, jossa saa enemmän vaikutusvaltaa, liitännäiset ja vapautta muokata sivut mihin tahansa kuntoon. (Thibodeau 2022.) Dils (2016) osoittaa, että jos muokkaavuuden vapaudessa tai myynnissä on ongelmia com-versiossa, on org-versio parempi vaihtoehto. Org-versiossa on tosin se ongelma, että käyttäjän pitää itse maksaa ja hankkia esimerkiksi verkkotunnukset ja tallennustilat webbihotellien ja verkkotunnustilauksien kautta.



Kuvio 1. Vertailun kohteet molemmille WordPress-versioille (Dils 2016)

Koska tässä työssä liitännäiset ovat suuri osuus kokonaisuudesta, oli org-version hankinta pakollinen. Tässä muutenkin ilman teemojen muokkaavuusominaisuutta olisi com-versio ollut alempana listalla alustojen suhteen.

Webbihotelli/hostauspalvelun suhteen DigitalOcean oli nimi, joka tuli etsiessä monesti esille. DigitalOceanin palveluista saa edullisesti itselle palvelimen käyttöön jopa 5 - 6 dollarilla kuussa, nopean asiakaspalvelun sekä kohtuulliset nopeudet. Kyseiseltä palvelulta myös sai WordPress-aloituspalvelun, joka nopeutti prosessia huomattavasti. DigitalOceanilla on myös laaja valikoima tilauksia eri tarpeisiin, joten ei tarvitse miettiä onko tarpeeksi isoa pakettia saatavilla. Ainoa ongelma on se, että DigitalOcean-palvelu ei tarjoa palomuuria ja muita tietoturvaominaisuuksia. (SolarWinds Worldwide 2023.) Nämä tosin eivät ole ongelmia, kun käyttäjä osaa käyttää muita palveluita avukseen, esimerkiksi Cloudflare-palvelua. Nettivertailut.com (2023) kertoo asiasta tarkemmin DigitalOceanin palveluista ja hinnoitteluista artikkelissa ”DigitalOcean”.

Cloudflare on CDN-palvelu, joka tarjoaa tietoturvaa nettisivustoille pilvipalvelupohjaisilla palveluilla, esimerkiksi DoS-hyökkäyksiltä suojaaminen, palomuurien ja SSL-suojauksien jakaminen sekä optimisaatiota sivustoille (Cloudflare 2023). Shim (2023) kommentoi kuinka tärkeä Cloudflare on palveluillaan, kuinka paljon optimisaatiota se suorittaa parantaakseen selaamista monilla sivustoilla ja kuinka tarpeellisia Cloudflaren tapaiset yhtiöt ovat. Käytin tätä palvelua suojaamaan nettisivuston IP-osoitteen nimen, jotta hyökkääjät eivät pääsisi palvelimen oikeaan osoitteeseen.

Namecheap.com on DNS-palvelu, josta tilasimme nimen nettisivustolle. Tavoitteena oli hankkia lyhyt, mutta osuva nimi, jonka muistaa helposti, ja namecheap.com-sivustolta saimme .org-lopun sivustoon. Tarkistin myös hintahaarukkaa ja .org on noin 10 euroa kuukaudessa, joka verrattaessa muihin verkkotunnuksiin on huomattavasti halvempi. Tätä voi verrata tätä samalla sivustolla .com-muotoon, josta pitäisi maksaa yli 7000 euroa ensimmäisellä kerralla.

2.3 Työhön liittyvää terminologiaa

Seuraavia termejä käytän useasti opinnäytetyöni aikana. Näistä jokainen liittyy tiukasti liitännäisiin tai yleiseen tietoturvaan.

DNS on nimipalvelujärjestelmä, joka yhdistää IP-osoitteen verkkotunnukselle. Sivustot tulevat omien nimiensä kanssa ja DNS-järjestelmä on se, joka mahdollistaa nämä nimet. Jos tätä järjestelmää ei olisi, käyttäjien pitäisi toimia IP-osoitteiden kanssa sivustoja etsiessä tai hakiessa, mitkä olisi mahdotonta muistaa. Tämä myös tuo tietoturvariskinsä, jos IP-osoite olisi esillä julkisesti. (Šimonėlytė 2023.)

CAPTCHA on termi metodille, jossa haastetaan käyttäjä kertomaan mitä kuvassa näkyy. Tämän avulla sitten ohjelma pystyy kertomaan, onko käyttäjä ihminen vai robotti, poistaen suurimmat mahdolliset haittatapaukset. Näihin kuviin kuuluu suositut kaikkien liikennevalojen valitsemin tai kuvan tekstin kirjoittaminen, mutta on myös palveluita, jotka tekevät tämän automaattisesti piilossa, esimerkiksi Googlen reCAPTCHA. Piilotetut CAPTCHA-toiminnot ovat mainioita heille, joilla menee usein aikaa CAPTCHA-kuvien kanssa tai eivät pääse niistä läpi. (Stytch 2022.) Nielsen (2023) mainitsee, että tutkimukset kertovat kymmenen sekunnin olevan vakio CAPTCHA-pulmille, jos käyttäjä pääsee läpi koko ominaisuudesta. Tosin vaikka CAPTCHA vaikuttaa hankalalta, tietoturvan tarkoitus ei ole olla helppoa, koska jos se olisi, niin olisi sen hakkerointi myös.

HTTPS on HTTP-protokollan ja TLS/SSL-salausprotokollan yhdistelmä, joka on kehitetty tarjoamaan suojatun yhteyden käyttäjän selaimen ja sivuston palvelimen välillä. Tämä auttaa pitämään molemmat selaimen ja palvelimen tietoturvan kunnossa tiettyyn asteeseen. (Jukarainen 2019.) Hakkarainen (2016) kommentoi, että joissakin selaimissa tämä protokolla on ollut pakollinen jo monta vuotta, esimerkiksi Googlen Chrome-verkkoselaimessa.

2FA on metodi, jolla lisätään tietoturvakerros salasanan päälle käyttäjän tiliin (Kenton 2022). Twilio (2023) mainitsee, että salasanat ovat alkamassa olemaan vanhanaikaisia ja käyttäjät päätyvät käyttämään yksinkertaisia tai uusiksi käytettyjä salasanoja palveluihin, jotka on helppo murtaa. 2FA on tätä varten kehitetty, käyttäjä asettaa 2FA-sovelluksen tiliin ja saa esimerkiksi uuden koodin joka kerta kun kirjautuu sisälle, mikä on vaikea murtaa käyttäjän puolelta.

3 NETTISIVUJEN SUUNNITTELU JA TOTEUTUS

3.1 WWW-sivujen suunnittelu ja mallikappaleen luominen

Toimeksiantajan vaatimuksena työlle oli sivustojen nykyaikaisuus toimivuudelta, saatavuudelta sekä ulkonääöltä. Tähän kuului sivustojen saatavuus eri laitteistoissa, esimerkiksi puhelimen pystymuoto pitäisi olla toimiva ja helppokäyttöinen. Näiden lisäksi vanhoista tiedoista piti valita, mitä tuon sivustoille takaisin ja mitä voin jättää vanhoille sivuille. Myös tiedon uusiminen kuului tähän osuuteen päivittämisestä, koska tietyt linkit esimerkiksi eivät toimineet enää toisille sivustoille. Ulkonäön suhteen sivustoissa pitää olla nykyaikainen ulkonäkö, johon toimeksiantaja halusi yhdistää vanhan ajan tunnetta yhdistyksen perinteitä kunnioittaen. Koska lähdin tekemään sivustoja ilman, että käytin vanhaa sivustoa suoraan pohjana, sain vapauden lisätä vain tärkeimmän tiedon sen sijaan, että pitäisi poistaa kaikki vanhentuneet tiedot ensimmäisenä.

Jotta pääsin tutkimaan liitännäisiä tarkemmin ja luomaan sivustoa, aloitin luomalla nettisivustoille mallikappaleen, josta sain ideoida mitä tarvitsin tai mitä pystyin olemaan lisäämättä vanhentuneiden ominaisuuksien suhteen. Alkuideana oli luoda moderni ulkonäkö ja toimivuus sekä saatavuus eri resoluutioissa, mutta otin vanhoista sivustoista tutun sommittelun, jotta edelliset kävijät löytävät kaiken tarvittavan tiedon. Vanhojen sivustojen päälle tein uusien sivustojen mallikappalenäkymän, jotta teknisesti pidettiin linkkien paikat samana ja artikkelien asettelu olisi samassa kohdassa. Muutoksia tosin ovat yläpalkki, johon asetin eri ominaisuuksia. Oikealle puolelle kuvien sijaan on nyt kävijälaskuri, joka oli vanhoilla sivustoilla vasemmalla puolella, sekä artikkelit saavat uutta ulkonäköä saatavuuden kannalta.

Tärkeintä oli varmistaa, että tiesin mitä lähdin tekemään sivuston suhteen. Kuviossa 2 on esitetty vanha sivusto, joita lähdin tutkimaan ja parantamaan uusilla sivuilla.

Kuvio 2. Alkuperäinen sivusto

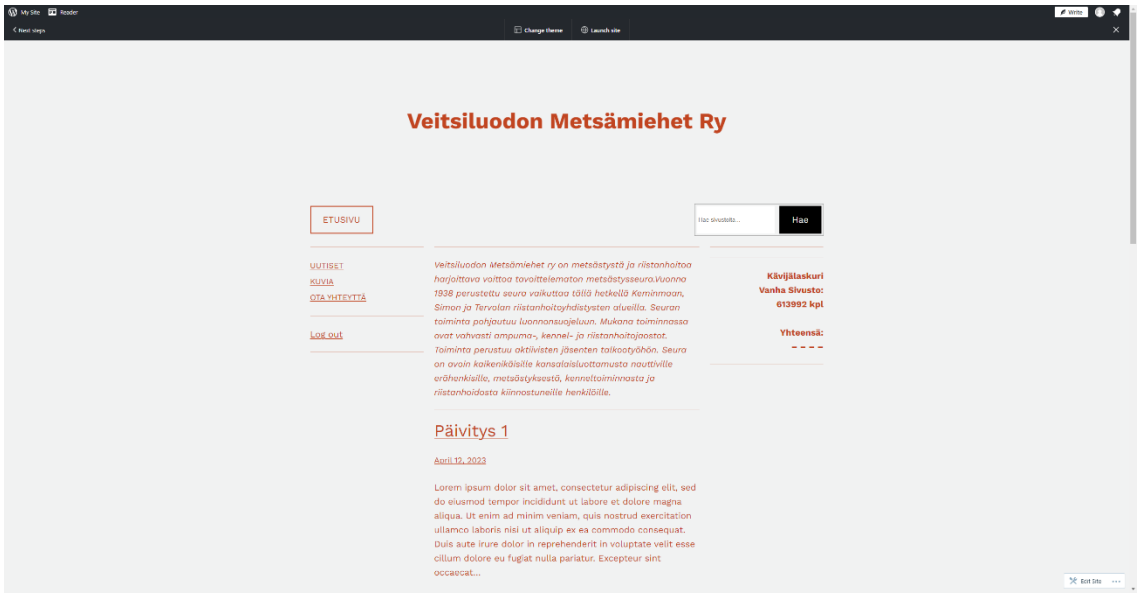
Kuviossa 3 on esitetty mallikappale, jota seurasin pohjana työn aikana. Näkyvillä on etusivu, jossa on päivityksien malli sekä vanhoja ominaisuuksia siirrettynä uusiin paikkoihin.

Kuvio 3. Sivustojen ensimmäinen mallikappale

Toimeksiantaja sitten hyväksyi tämän mallikappaleen ja aloin tuomaan sitä WordPressin .com-versioon. Samalla pääsin tutustumaan alustan toimivuuteen sekä käyttäjäkokemukseen. Kävin läpi WordPressin tarjoamat teemat ja etsimisen jälkeen löysin yhden, joka sopi hyvin mallikappaleen kanssa. Koska

wordpress.com-versiossa teemoja ei pysty itse tekemään ilman maksua ja muutenkin alusta oli hyvin rajoitettu muokkaamisen ja saatavuuden suhteen, siirryin tekemään sivustoa wordpress.org-versioon.

Tämän aloitin sen jälkeen, kun olin päässyt tiettyyn vaiheeseen pohjan tekemisessä eli saanut tiettyjä ominaisuuksia toimimaan, kuten sivupalkin ja artikkelit. Testasin ensin muutamaa uutta ominaisuutta ennen siirtymistä, esimerkiksi hakupalkkia, koska sivustolla on usein päivitettyjä artikkeleja ja niiden löytäminen ja tutkiminen helpottuisi hakutoiminnolla. Hakupalkki-ominaisuus parantaisi sivustojen saatavuutta uusille sekä vanhoille käyttäjille. Kuviossa 4 on esitetty WordPressin näkymä sivustosta WordPressin teeman kanssa ilman suurempia muokkauksia.

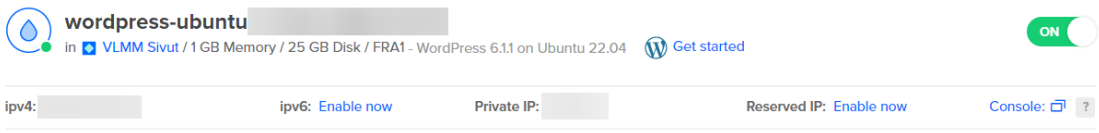


Kuvio 4. Ensimmäinen versio WordPress-sivustolla

3.2 WWW-sivujen hostaus ja toiminnallisuus

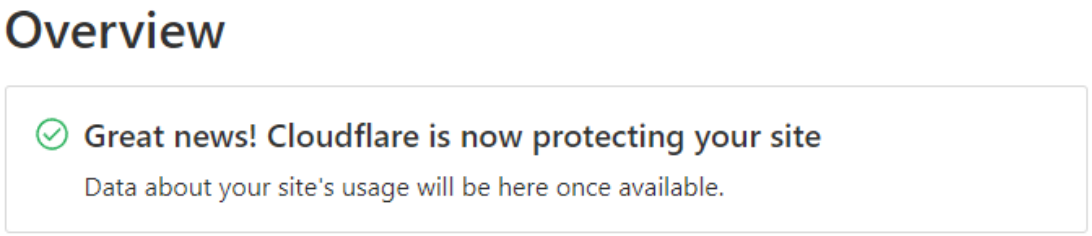
Ennen kuin pääsin vaihtamaan sivustojen paikkaa, tarvitsin hostauspalvelun, johon sivusto liitetään. Tein tilauksen sivustolle DigitalOcean, joka on tunnettu, luotettava ja halpa webbihotelli. Webbihotellissa on saatavilla myös WordPress-asennuspaketti, jota käytin tässä vaiheessa. Käynnistin sen, tein perusasennuksen, johon sisältyi konsolin käynnistäminen ja konfigurointi. Lopulta pääsin IP-osoitteen kautta katselemaan nettisivuja sekä tuomaan teeman ja asettelun,

jonka olin luonut aikaisemmin. DigitalOceanissa myös näkyi, että kaikki on toiminnassa sivuston asetuksien näkymässä (kuvio 5).



Kuvio 5. DigitalOcean-sivuston näkymä minun ”Dropletista”

Kun olin tuonut sivuston org-versioon ja asentanut tarpeelliset ominaisuudet, lähdin hankkimaan verkkotunnuksia sekä asettamaan DNS:ää palvelimelle. Päädyin tilaamaan verkkotunnuksen namecheap.com-sivustolta, ja DNS tuli Cloudflare-palvelulta (kuvio 6). Tämä varmistaa sen, että jos joku henkilö tai botti koittaa hyökätä sivustoon käyttämällä sivuston IP-osoitetta, menee hyökkäys sen sijaan Cloudflaren palveluun. Tämä vuorostaan varmistaa sen, että hyökkäys ei toimi. Tämän voi todistaa komennolla *”dig <verkkotunnus> a”*. Kun tätä komentoa käyttää, se palauttaa IP-osoitteen. Jos Cloudflare ei ole päällä, IP-osoite olisi nettisivuston oikea osoite, mutta Cloudflaren ollessa päällä se palauttaa yhden heidän monesta IP-osoitteesta, johon hyökkäykset yhdistetään. Edward (2022) kirjoittaa tästä komennosta lisää artikkelissaan ”How to Use the Dig Command in Linux”.



Kuvio 6. Cloudflare-sivuston toteamus toimivuudesta

Aloin jälkeenpäin työstämään sivuston toimivuutta, ennen kuin aloin lisäämään työhön tarvittavia liitännäisiä. Tätä varten toimeksiantajan kanssa kävin läpi mitä otan mukaan edelleen vanhoilta sivustoilta. Olin alustavasti päättänyt, että sivustoon tulee artikkelit, kuville galleria, osa vanhoista linkeistä sekä kirjautumisen taakse tulevia toimintoja, esimerkiksi kartat ja kokouksien pöytäkirjat seuran jäsenille.

3.3 Sivuston tietoturvavaatimukset

Tehtäväkseni tuli varmistaa, että nettisivusto on turvallinen ja ei pääse kaatuilemaan herkästi, kirjautumissivut tietyille tiedoille sekä tietoturvallisuus järjestelmänvalvojille. Tosin ennen kuin pääsin lisäämään näitä, tietty asetus, jonka piti vaan asettaa HTTPS päälle sivustossa, rikkoi sivuston kokonaan ja monen tunnin jälkeen jouduin uudelleenasentamaan koko sivuston muutamaa asetusta lukuun ottamatta. Tällä kertaa aloin tekemään varmuuskopioita ja pääsin pidemmälle työn kanssa. Tämä auttoi myös siinä, että en lisäillyt työhön muita tarpeettomia asetuksia testaillessani mikä toimii.

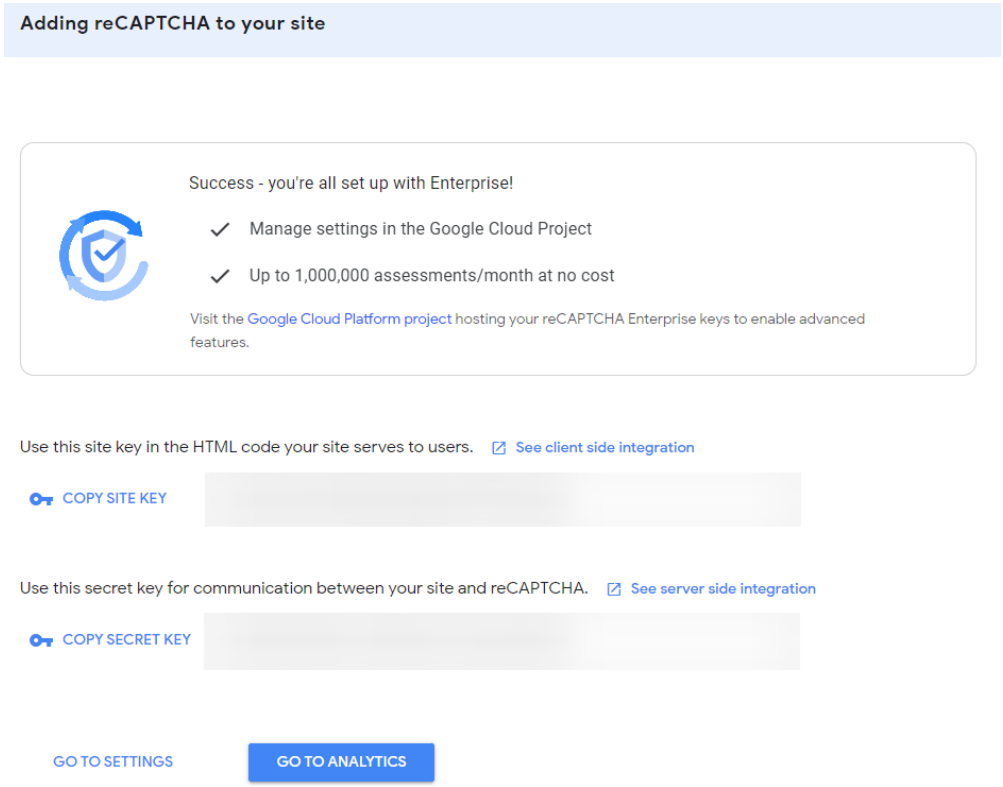
Asensin sivustolle SSL-liitännäisen myös nimeltä Really Simple SSL. Tämä on liitännäinen, joka varmistaa SSL-yhteyden sivustoon, minkä avulla tietoliikenne IP-osoitteiden suhteen on suojattu HTTPS-protokollalla. Tämä liitännäinen on toimiva, mutta hyvin tarkka asetuksien ja tietojen mukaan. (Really Simple Plugins 2023.) Perusolosuhteissa tämä olisi kaikki tarvittava tietoturva nettisivuille, kun yhdistää Cloudflaren ja SSL-suojaukset, mutta siirryin tarkistamaan, jos pystyisin lisäämään tietoturvaa.

DigitalOceanin WordPress-paketin kanssa tulee myös valmiiksi asennettu liitännäinen nimeltä WP fail2ban, joka antaa statistiikkaa kirjautumisista ja sivuston eheydestä (Lecklider 2023). Koska keskityn muihin liitännäisiin, joita pitää asentaa erikseen, en koske fail2ban-liitännäisen asetuksiin muuten kuin korjaan eheyttä tarvittaessa.

Lähdin aluksi etsimään yleistä turvallisuutta. Liitännäisellä pitää olla palomuuri, haittaohjelmien skanneri, sekä 2FA-mahdollisuus kirjautumisiin järjestelmänvalvojille. Näiden avulla saan yleisen tietoturvatason korkealle ja suojaamme samalla järjestelmänvalvojia kirjautumisia varten. Seuraavaksi tarvitsin tietyille sivuille salasanasuojauksen ja CAPTCHA:n. WordPressissä on jo sisäänrakennettu järjestelmä salasanoille tietyillä sivuilla, mutta yhdistin tähän CAPTCHA:n, jotta sivustossa varmistui tiedon eheys ja turvallisuus. Liitännäinen yleiselle tietoturvalle oli tiedossa, mutta erikseen piti asentaa liitännäinen CAPTCHA:lle.

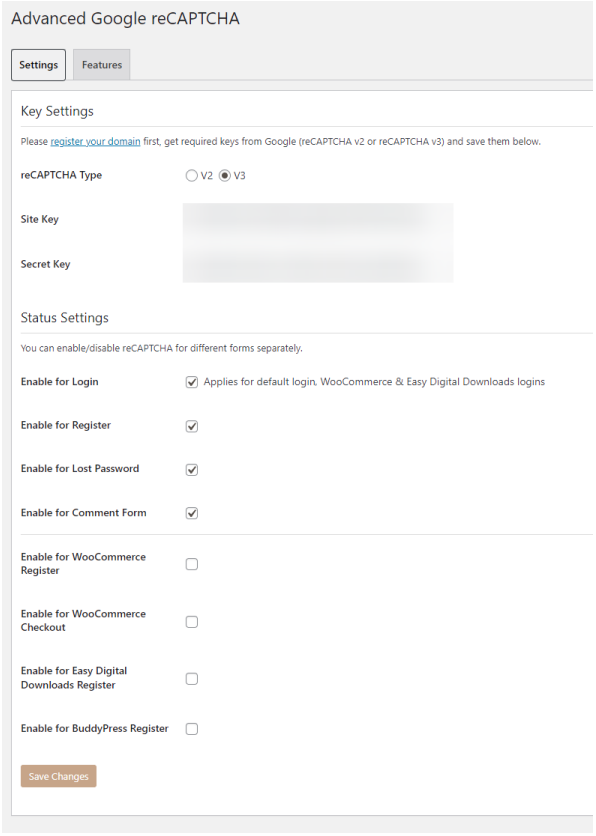
CAPTCHA-metodia varten asensin liitännäisen nimeltä Advanced Google reCAPTCHA (WP Concern 2023). Tämä on Googlen oma CAPTCHA-metodi, jota

mainostetaan ”vaikea boteille, helppo ihmisille”-myyntipuheella (Vaishnavi 2022). Astari (2023) esitti, että reCAPTCHA on efektiivinen, koska se adaptoi koneälyllä uusimpien bottien hyökkäyksiä vastaan, joten asentamani liitännäinen pysyy ajan tasalla. Ensimmäinen valinta oli V2 tai V3 reCAPTCHA-sivulla. V2 on käyttäjälle näkyvä, jossa käyttäjä painaa nappia tai muita mahdollisia vaihtoehtoja, kun taas V3 on näkymätön ja toimii taustalla perustuen käyttäjän toimintaan. Koska halusin käyttäjäkokemuksen olevan helppoa, valitsin V3:n, loin avaimet Googlen reCAPTCHA-sivustolta, testasin kirjautumisia ja kaikki toimi kuten piti (kuvio 7). Nyt sivustossa on uusi suojaus kirjautumisia varten. CAPTCHA:n kanssa pitää olla varovainen, koska jos ei seuraa ohjeita oikein, voi kehittäjä menettää pääsyn sivustoon. Tätä varten kannattaa erillisellä ikkunalla kirjautua sisään ja varmistaa, että metodi toimii.



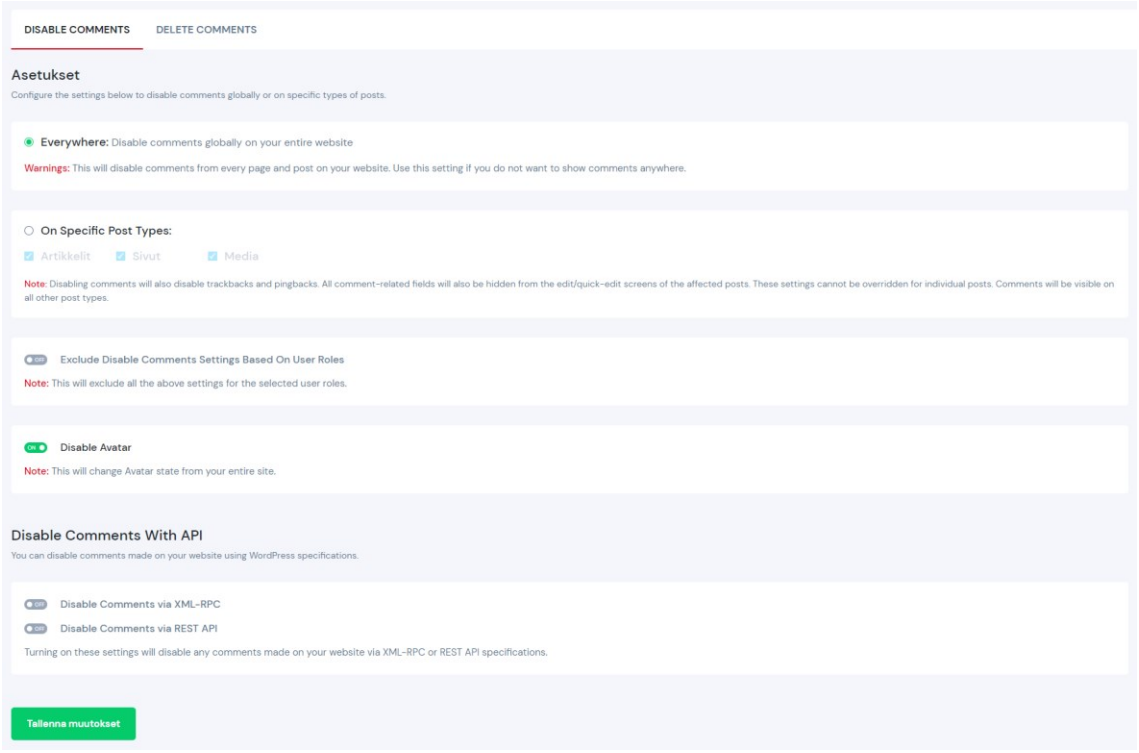
Kuvio 7. Google reCAPTCHA:n autentikaatio sivu

Liitännäisessä kävin asettamassa oikeat asetukset ja liitännäinen alkoi toimimaan. Kuviossa 8 on esitetty liitännäisen asetukset, esimerkiksi mihin sivuille liitännäinen vaikuttaa.



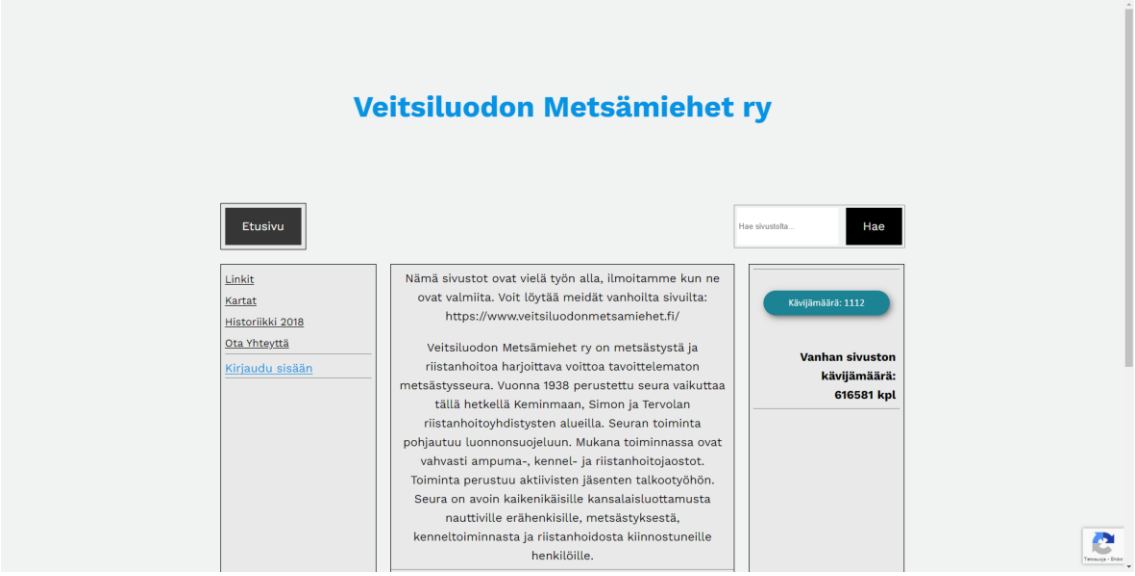
Kuvio 8. Advanced Google reCAPTCHA-liitännäinen

Myöhemmin tuli lisättyä muutama liitännäinen lisää tietoturvaa ja päivityksien helpottamista varten sekä PDF-esikatselua varten. Liitännäinen nimeltä Disable Comments – Remove Comments & Stop Spam tuli lisättyä, jotta sain poistettua valmiiksi asennetun ominaisuuden kommenteille (kuvio 9). Kommentit lisäävät tietoturvariskejä, antavat paikan spämmiviesteille sekä tekevät sivustojen päivittämisestä hankalampaa järjestelmänvalvojille. Järjestelmänvalvojien pitäisi tarkistaa enemmän tulevaa tietoa ja useammin, jos pitäisin kommentit päällä. Liitännäisellä pystyy myös poistamaan automaattisesta kaikki tai tietynlaiset kommentit. (WPDeveloper 2023.) Tämä korjaisi osittaisen hankaluuden järjestelmänvalvojille, mutta ei kokonaan, joten käytän liitännäistä kommenttien poistamiseen kokonaisuudessa.



Kuvio 9. Disable Comments-liitännäinen

Seuralla on myös historiikki saatavilla vuodelta 2018 PDF-muotona, minkä päätin esittää suoraan sivustolla ilman toista sivua. Tätä varten asensin PDF Embedder-liitännäisen, koska se näyttää sivustolla esikatselun tiedostosta (WP PDF Embedder Team 2023). Saatavuutta varten varmistin, että PDF-sivuja varten asetetut painikkeet ovat aina esillä, koska muuten toiminnallisuus olisi rikki puhelimen näytössä sekä vaikeakäyttöinen tietokoneella. Kuviossa 10 on näkyvillä toimiva sivusto ennen teeman viimeistelyä. Oikeassa alanurkassa esimerkiksi näkyy reCAPTCHA:n painike, joka huomauttaa käyttäjille, että se on toiminnassa.



Kuvio 10. Sivusto ennen viimeistelyä

4 TIETOTURVA

4.1 Liitännäisien tietoturva

Kun moni aloittaa tekemään nettisivuja, tätä varten on tärkeää tutkia mitä ominaisuuksia käyttäjä haluaa ja miten voidaan varmistaa, että toiminnot eivät aiheuta tietoturvariskejä pidemmällä aikavälillä. Tähän liittyen liitännäiset ovat mainioita, koska kun alkaa tekemään nettisivuja wordpress.org-sivustolla, on moni tietoturvaliitännäinen saatavilla heti laatikosta. Kokonaisuuspaketteja ja pienempiä yhden ominaisuuden liitännäisiä on saatavilla, jotka antavat monta vaihtoehtoja kehittäjille.

On hyvä aloittaa kokonaispakkauksilla, koska jos on vain muutama alue, joissa tarvitaan tietoturvaa, on näillä paketeilla yleisesti kaikki mitä tarvitsee, esimerkiksi palomuurit ja skannaustoiminnot. Siitä eteenpäin käyttäjä tarkistaa mitä tarvitsee ja alkaa asentamaan ja implementoimaan liitännäisiä. Esimerkiksi SSL-liitännäiset, jotka tekevät HTTPS-protokollan automaattisesti ovat hyviä asettamaan tietoturvaprotokollat.

Mutta liitännäisiin kuuluu myös riskejä. Kuten melkein kaikkeen nettiin liittyviin osiin, liitännäisiin voi syntyä murtoja sekä haavoittuvuuksia, jotka auttavat hyökkääjiä murtautumaan sivustoihin liitännäisien kautta. On myös mahdollista, että liitännäinen ei tarpeeksi nopeasti tai ei ollenkaan huomaa uusia haavoittuvuuksia, joita syntyy. Vaikka monen asennuksen työkalut ovat yleensä parhaimpia tietoturvan vuoksi, ovat ne myös eniten hakkereiden kohteena. Joten kannattaa tarkistaa onko liitännäinen usein päivitetty ja varsinkin lähiaikoina sekä kuinka hyvin tekijät vastaavat käyttäjille ongelmien syntyessä. Päivittämättömät työkalut sekä vähän aktiivinen kehittäjä tai tiimi ovat yleensä ensimmäinen kohde liitännäisen luotettavuuden tarkastamiseen.

Näitä varten voit seurata NVD:n palveluiden tarjoamia statistiikkoja. NVD:n tarkoituksena on tarkkailla tietoturvahaavoittuvuuksia, kun ne syntyvät ja raportoida murroista. Palveluista löytyy esimerkiksi näytönohjaimien ja muiden tietoteknisien laitteiden asennuksien haavoittuvuuksia, bottien toimintaa esimerkiksi Discord-sovellusalustalla ja muita näihin soveltuvia ongelmia. NVD on suurin raportoija

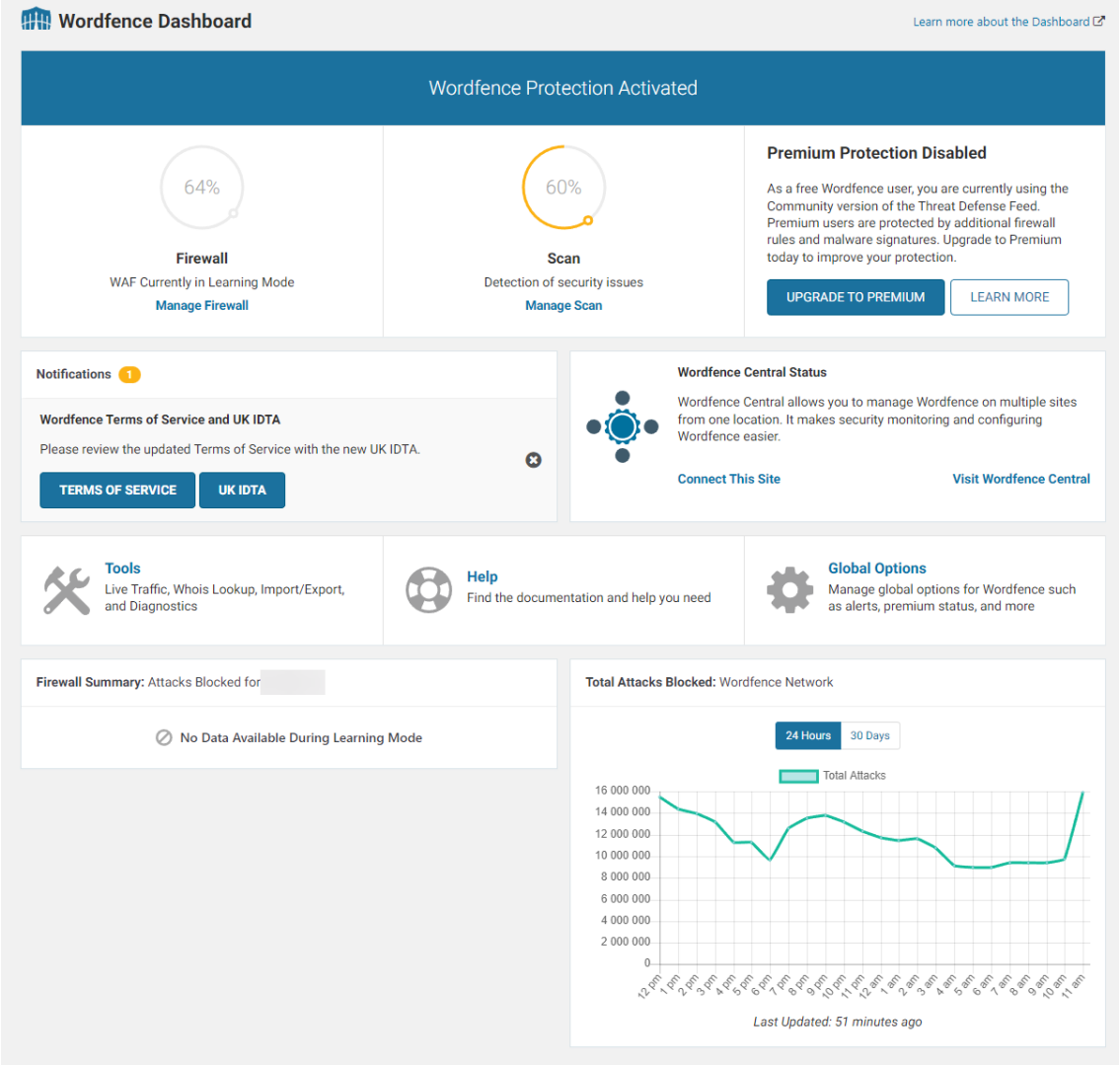
riskeille, joten tietoturvan vuoksi kannattaa tarkistaa tietyn väliajoin, miten siellä raportoidaan asioista. (Appknox 2023.)

4.2 Wordfence-liitännäinen

Kaikkien liitännäisien tutkimisen jälkeen päätin asentaa nettisivuille Wordfence-liitännäisen. Wordfence on kokonaisuuspaketti tietoturvalle. Tähän kuuluu palomuuri, jonka tehtävänä on estää kaikenlainen spämmi ja haitallinen liikenne ja haittaohjelmien skannausohjelma, joka estää haittaohjelmien pääsyn järjestelmiin. Saatavilla on myös 2FA-authentikaatiojärjestelmän suojaamaan järjestelmänkäyttäjiä. Wordfence myös tarjoaa CAPTCHA-ominaisuuden kirjautumisille ja muita ominaisuuksia Premium-tilauksen takana. (Wordfence 2023.)

Valitsin tämän liitännäisen, koska se on aktiivisin ja korkeasti arvosteltu liitännäinen, joka takaa laajimman valikoiman tietoturvaominaisuuksia. Vaikka moni toiminnallisuus on Premium-tilauksen takana, on ilmaisversiossa tarpeeksi sisältöä, jotta voin liittää sen työhön ja varmistaa yleistason tietoturvalle. Tämän liitännäisen kanssa kannattaa tosin tarkistaa, onko lähiaikoina ollut tietomurtoja tai muita ongelmia. Vaikka tutkimukseni mukaan on se hyvin päivitetty, saattaa suuri määrä asennuksia kertoa sen, että hakkerit pitävät silmällä tätä liitännäistä ja joskus menee jokin läpi.

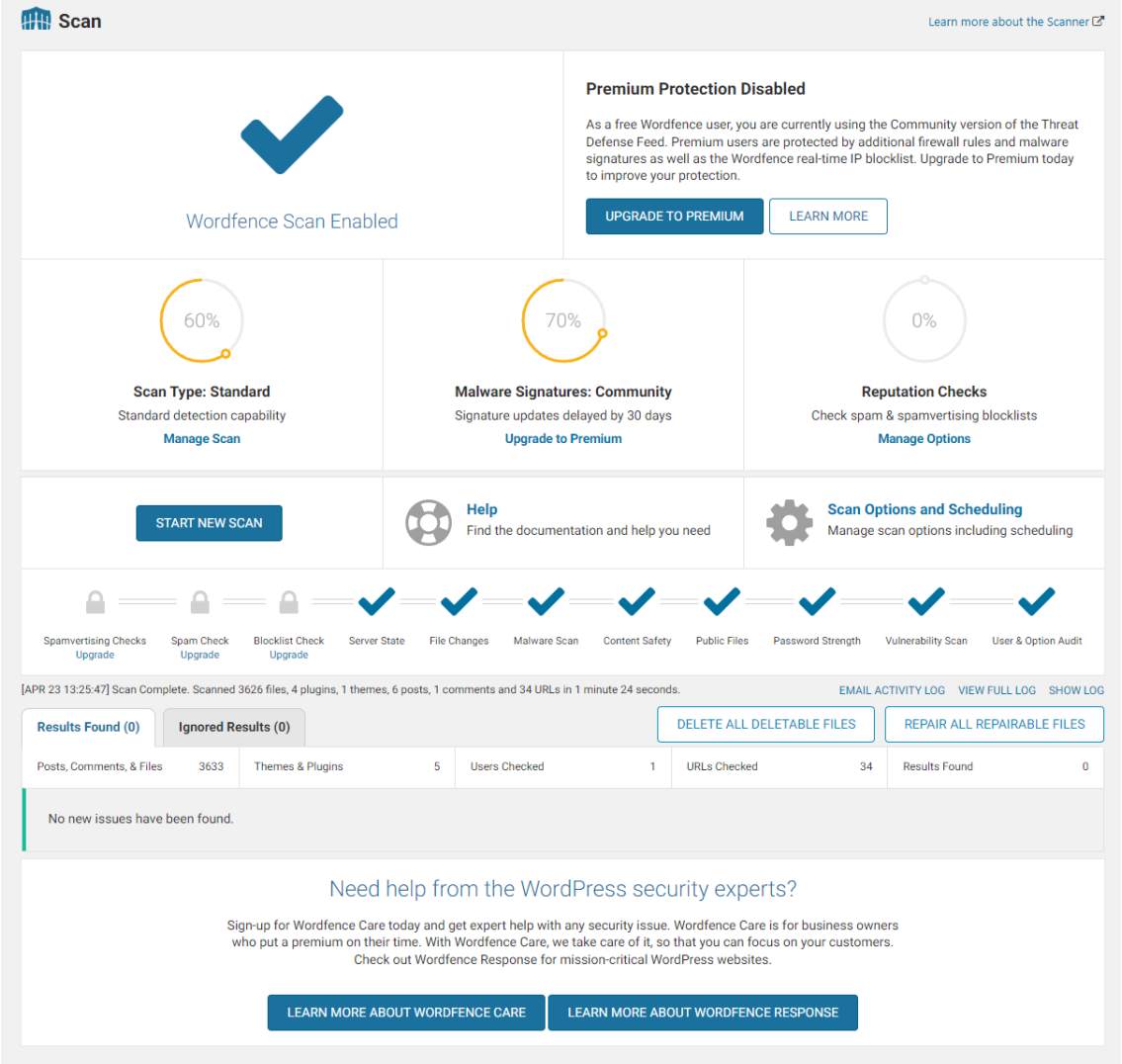
Alussa syntyi ongelmia tietoliikenteen kanssa, joka mahdollisesti oli ongelmia liitännäisen palvelimien kanssa, mutta tunnin odotuksen jälkeen sain liitännäisen asennettua. Asennukseen kuului tilaussuunnitelman valitseminen, joka tässä työssä oli ilmainen pohja, ja sen jälkeen lisenssiavaimen hankkiminen. Lopuksi kävin laittamassa päälle turvaominaisuuksia tai laittamassa ne käynnistymään (kuvio 11) ja sitten siirryin seuraavaan osuuteen liitännäisessä.



Kuvio 11. Wordfence Dashboard-etusivunäkymä

Huomioitavaa ilmaisessa versiossa on se, että ohjelma toimii oppimistilassa, kun sen asentaa. Ohjelman pitää pyöriä seitsemän päivää, ennen kuin se toimii täydellä teholla palvelimien ja optimisaation vuoksi. Joten jos menee ilmaisella versiolla, pitää odottaa viikko ennen kuin näkee efektiivisyyden liitännäisessä. Tähän kuuluu palomuuri, joka neuvotaan laittamaan päälle vasta viikon päästä, kun oppimistila on tehnyt tehtävänsä.

Wordfence-liitännäiseen kuuluu myös skannausominaisuus, jossa liitännäinen skannaa mahdolliset haittaohjelmat järjestelmässä, salasanan vahvuuden, tiedostot ja muut sisäänkirjautumiset (kuvio 12). Tämä suoritetaan automaattisesti tietyin väliajoin, mutta käyttäjä voi itse skannata milloin tahansa.

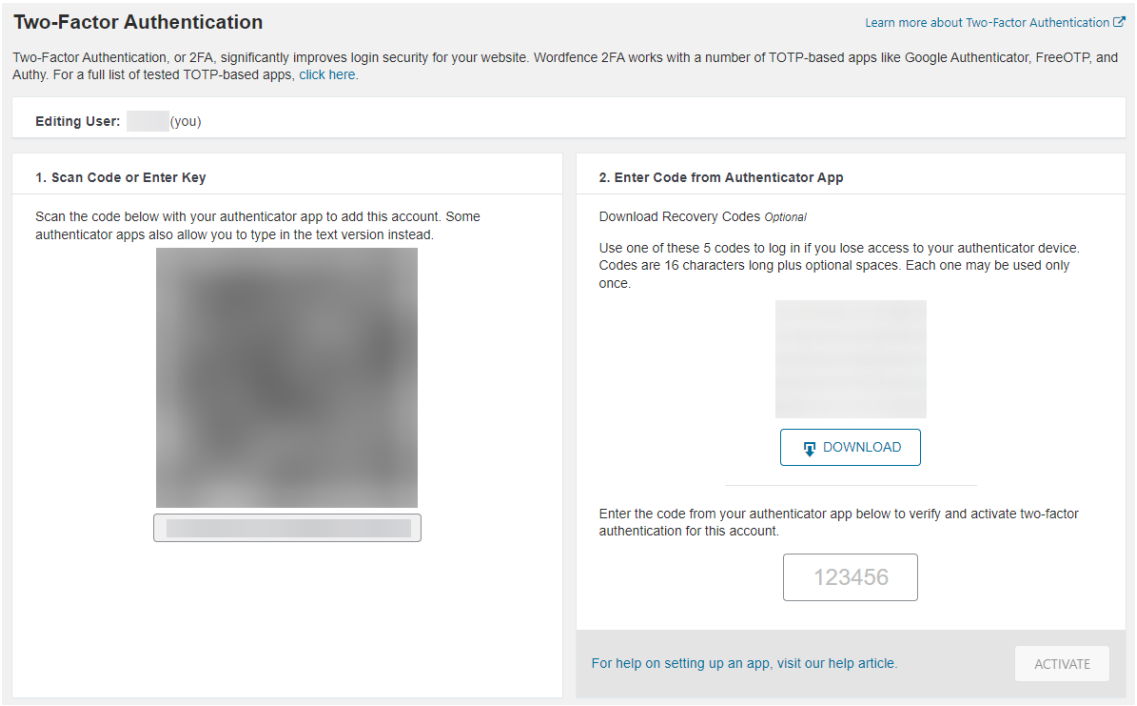


Kuvio 12. Wordfence Scan-näkymä liitännäisessä

Kuten huomataan, kaikki on toiminnassa ensimmäisellä skannauksella. Skannaus ei huomannut mitään ongelmia sivustossa.

Jokaisella sivulla on prosenttimääriä näkyvissä, mitkä kertovat miten kehittäjä voi parantaa suojaavuutta sivustoille. Nämä ovat erinomaisia siksi, että kehittäjä saa yksityiskohtaisen näkymän parantamista varten sen sijaan, että on piilotettua statistiikka pelkässä tekstin muodossa. Skannaussivustolta voi nähdä aluksi, että ensimmäinen ja toinen prosenttimäärä on 60 – 70. Nämä johtuvat siitä, että Premium-tilausta ei ole hankittu, joten kaikkea toiminnallisuutta ei ole saatavilla. Viimeinen osuus on nolla prosenttia, koska spämmiä varten tarkistuksia ei ole asetettu. Nämä ovat myös Premium-ominaisuuksia, joten voimme tarkistaa tämän toisella sivustolla tai liitännäisellä, jos kehittäjä ei halua käyttää rahaa Premiumiin.

Wordfence-liitännäiseen voi myös yhdistää käyttäjille 2FA-metodin, joka suojaa sivuston pääkäyttäjiä (kuvio 13). Vaikka sivuston kirjautumiset pidetään minimiä, on tärkeää, että järjestelmänvalvojat käyttävät tätä ominaisuutta.



Kuvio 13. 2FA-sivu liitännäisessä

Wordfence-liitännäisen avulla sain myös reaaliajassa tiedon mitä spämmiä varten tehdyt botit koittavat käyttää kirjautumiseen. Esimerkiksi käyttäjätunnus admin on usein käytetty tunnus bottien mukaan, joten kannattaa varmistaa, ettei tule käytettyä yleisiä nimiä tunnuksille. Myös käyttäjäasetuksista kannattaa asettaa uusi nimimerkki, koska jos artikkeleissa näkyy oikea käyttäjänimi, botit saattavat yrittää käyttää sitä. Huomattavaa myös on siinä, että botit eivät huomaa ääkkösiä, joten kirjautumisyritykset epäonnistuvat enemmän, jos käyttäjä käyttää ääkkösiä (taulukko 1).

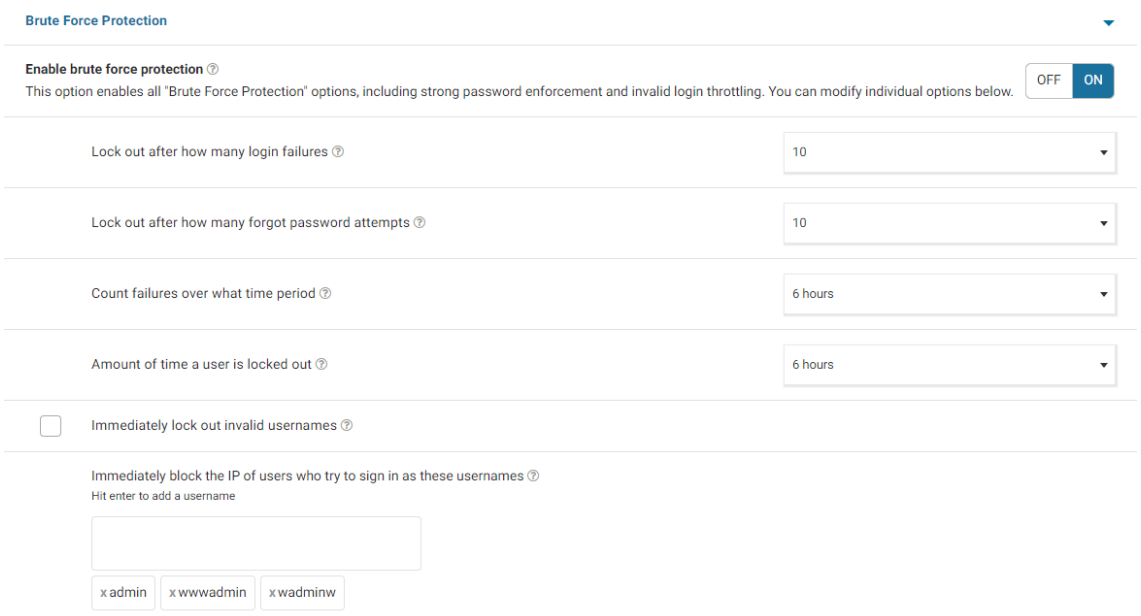
Taulukko 1. Bottien kirjautumisyritykset viikon sisällä

Top 5 Failed Logins

Username	Login Attempts	Existing User
admin	145	No
wwwadmin	12	No
Vertti Ronkko	10	No
wadminw	5	No

Update Login Security Options

Liitännäisessä kehittäjä voi myös asettaa oman määrän kirjautumisyrityksiä. Kuviossa 14 on esitetty kirjautumisyritys-näkymä, jossa voi asettaa yrityksien määrän, käyttäjän lukitusajan sekä tietyt nimet voi asettaa estoon.



Kuvio 14. Lisäasetukset kirjautumisyrityksille

4.3 Muita käytettäviä liitännäisiä

Wordfence-liitännäisen lisäksi WordPressin sivustolta löytyy monia muita liitännäisiä, joita voi käyttää tietoturvan lisäämiseksi. Tähän kuuluu muita yleispaketteja, sisäänkirjautumiseen liittyviä, spämmin estoa sekä optimoimiseen liittyviä,

mitkä myös auttavat tietoturvassa. Käyn läpi valintoja, joilla on ollut hyvät arvioinnit, mutta eivät soveltuneet sivustoihini.

Yleisiin kokonaispaketteihin kuului esimerkiksi Defender, iThemes ja BulletProof. Jokaisessa on moni ominaisuus saatavilla, mutta oli myös puuttuvia ominaisuuksia, joita on saatavilla toisissa. Esimerkiksi iThemes-liitännäisestä puuttuu palomuuri, kun taas BulletProof-liitännäisessä CAPTCHA on primitiivisempi. Kaikki kolme tosin ovat usein päivitettyjä ja ovat pysyneet ajan tasalla hyvin arvosteltuina. (AITpro Website Security 2023; iThemes 2023; WPMU DEV 2023.)

Jos haluaa varmistaa turvallisen sisäänkirjautumissivun, kehittäjä voi ladata ja asentaa Limit Login Attempts Reloaded-liitännäisen. Limit Login Attempts Reloaded-liitännäinen rajaa kirjautumisyritykset, lisää IP-osoitteiden rajaamista sekä pystyy laittamaan sähköpostia kirjautumisyrityksistä tilannekatsausta varten. (Limit Login Attempts Reloaded 2023.) Tämä on sitä varten, jos haluaa muutenkin lisätä ominaisuuden, jossa käyttäjä ei pysty kirjautumaan niin monta kertaa kun haluaa sisälle. Huonoja puolia tosin tässä liitännäisessä on se, että osa kokonaispaketeista tarjoaa tämän jo. Myös tutkimukseni mukaan tämä liitännäinen oli kaksi ja puoli vuotta sitten raportissa, joka mainitsi, että liitännäinen olisi mahdollisesti haitallinen. Liitännäisellä on pääsy käyttäjävalvojien tietoihin ja pystyy aiheuttamaan XSS-ongelman, mutta tämä on mahdollisesti korjattu. (National Vulnerability Database 2020.)

Lopuksi käyn läpi kaksi muuta liitännäistä. Ensimmäinen on Spam Protection, AntiSpam, FireWall by CleanTalk. Tämä liitännäinen perustuu kaiken spämmin pysäyttämiseen ja poistamiseen kaikesta mediasta, esimerkiksi kommenteista, kontakteista, äänestyksistä ja niin edelleen. Kaikki palomuuriin tarvittavat ominaisuudet löytyvät tästä liitännäisestä, jolla on erinomainen määrä asennuksia verrattuna arvioihin. Ainoa heikkous on se, että se alkaa maksuttomana, mutta siirtyy maksullisesti kokeilun jälkeen 12 dollarilla vuodessa. (CleanTalk 2023.) Sitten on vielä EWWW Image Optimizer, jonka päätavoite on kuvien optimisaatio, mutta myös tarjoaa SSL-suojan (Exactly WWW 2023). Joten jos on tarvetta optimoida kuvia sekä parantaa tietoturvaa, on tämä liitännäinen sopiva siihen työhön.

Liitännäisistä löytyy paljon vaihtoehtoja. Tärkeintä tosin on tarkistaa, kuinka monta asennusta liitännäisellä on ja siihen vertailee, kuinka monta arvostelua siihen on liitetty. On turhaa asentaa liitännäinen, jolla on monta asennusta, mutta arvosteluissa näkyy monta yhden tai kahden tähden arvostelua, eikä tarpeeksi ylemmän arvon arvostelua. Käyttäjät arvioivat liitännäiset usein, joten kannattaa tarkistaa statistiikat ennen kuin asentaa mitään.

5 POHDINTA

Opinnäytetyön tavoitteena oli rakentaa nettisivusto yhdistykselle ja samalla tutkia tietoturvaliitännäisiä sekä yleisesti sivustojen tietoturvaa. Osana tavoitteina oli myös oppia, miten WordPress-alustaa käytetään ja miten sivusto yhdistetään nettiin DNS:n ja webbihotellin avulla.

Tuloksena syntyi toimiva sivusto, joissa tietoturva on syvästi tutkittu ja mahdollistettu monella eri lähteellä, liitännäisien sekä palveluiden avulla. Opin mitä liitännäisiä tarvitaan, mitkä ominaisuudet ovat tärkeitä, ja mitä voi lisätä, jos nykyiset lakkaavat toimimasta. Yleiseen tietoturvaan liittyvät aiheet on myös opittu ja käyty läpi sivustojen tekemisen aikana.

Opinnäytetyön haastavuus tuli kaiken tiedon keräämisestä ja asettamisesta. Liitännäiset piti varmistaa sekä onko tieto oleellista, koska moni artikkeli oli vanhentunutta tietoa. Internetti on siinä vaiheessa tietoteknistä osaamista, että asiat saattavat muuttua yön aikana, joten relevanttisuus oli iso osa kaikkea. Vaivattomiin osuuksiin kuuluivat itse liitännäisien asennus ja sivuston rungon kasaaminen. WordPress tarjoaa helppokäyttöisen liitännän liitännäisien asentamista varten sekä aloituspaketin asettamista varten.

Liitännäisien luotettavuus on todistettu tutkimalla käyttäjien antamia arviointeja lukemalla sekä omalla tutkimuksella. Hyödynnettävyys on myös todistettu sillä, että yleisestä tietoturvasta oli löytynyt tietoa ja taitoa tehdä tietoturvallinen nettisivusto. Työn avulla löytyi myös vaihtoehtoja, jos jokin menee pieleen.

Osa liitännäisien tuomia haasteita olivat myös hinta sekä toimivuus ensimmäisellä asennuksella. Monissa liitännäisissä kaikki parhaimmat ominaisuudet olivat tilauksen takana ja tietoturvan vuoksi pidin liitännäiset ilmaisina. Tämä lisäsi haastavuutta, mutta ei paljon, koska liitännäisistä löytyi paljon vaihtoehtoja. Ensimmäisen asennuksen haastavuus tuli siinä, että joskus liitännäiset eivät toimineet ensimmäisellä asennuksella tai ei ollenkaan. WordPress-versionumerointi vähensi taakkaa, mutta osa liitännäisistä ei toiminut, vaikka arvostelut olivat positiivisia. Testaaminen on aina tarpeellista, koska joskus saattaa olettaa, että esimerkiksi jokin takaosa-liitännäinen toimii ilman näkyvää vaikutusta, mutta se ei toimikaan.

Työn tarkoitus oli myös esittää kehittäjille uusia vaihtoehtoja luoda nettisivustoja ilman, että pitää miettiä tietoturvaa liian monimutkaisesti. Tosin tietoturvallisin tapa luoda nettisivusto olisi luoda itse työkalut tai antaa ammattilaisen luoda sivusto ilman liitännäisiä, mutta tämä tapa antaa tämän hetken mukaan hyvin tietoturvallisen sivuston. Myös palvelut ovat iso osa tietoturvaa. Webhotellin, DNS:n ja muiden valinta on yhtä tärkeää kuin tarkistaa liitännäiset ja asentaa ne. Pelkät liitännäiset voivat riittää lyhytikäisille tai vähäkäyttöisille nettisivuille, mutta molemmat liitännäiset sekä palvelut ovat osa isompaa kokonaisuutta.

Vaikka loin sivuston käyttäen julkisia liitännäisiä, kehittäjän pitää tarkistaa hyvin väliajoin onko päivityksiä saatavilla tai ovatko liitännäiset edes toimimassa. Hyvän tietoturvan takaa sillä, että itse käy asentamassa päivitykset sen sijaan, että antaisi sivuston automaattisesti asentaa ne. Kannattaa myös tarkistaa onko ollut tietomurtoja tai haavoittuvuuksia.

Jatkotutkimusta voidaan harjoittaa tekemällä laajempi sivusto, joissa on enemmän käyttäjäkokemusta ja käyttäjäsyöttöä saatavilla. Tiedon tallentaminen ja jakaminen automaattisesti on tärkeää tehdä oikein, ja tästä pystyy tekemään jatkokehittämiseen liittyvän aiheen.

Lopputuloksena on sivusto, jossa tietoturvan taso on korkealla, muokattavana ja optimoituna. Järjestelmänvalvojat voivat kirjautua sisään ja muokata ilman huolia CAPTCHA:n ja 2FA:n ansiosta, sivustoon DoS ja muut samankaltaiset hyökkäykset eivät toimi SSL/HTTPS:n avulla, ja sivustolla on palomuuri ja skannaustoiminnot toiminnassa. Nämä asetukset auttavat myös modulaarisesti kaiken tiedon suojassa pitämisessä, jos sivustolle lisää tietoa. Palvelut on valittu asiakastukea ajatellen, jotta jos jotain sattuu palvelimelle, voi saada yhteyden tukeen helpommin. Työssä ei valittu palvelinta heikolta sivustolta halvemmalla, millä on historiaa ongelmallisesta asiakastuen saatavuudesta tämän vuoksi.

Lähitulevaisuuden jatkokehittäminen sivustoille on kaiken tiedon viimeistely ja teemojen kehittäminen, jonka jälkeen voi julkaista sivuston. Sitten voi harkita, josko tulevaisuudessa tarvitsee lisäturvaa, kun liitännäiset päivittyvät tai poistuvat, uusia tietoturva-aukkoja tapoja löytyy tai WordPressissä asiat muuttuvat.

Mutta nyt kun liitännäiset päivitetään tietyin välinajoin sekä tilaukset uusitaan oikein, sivusto tulee pysymään pystyssä hyvin pitkän ajan ja pysyvät tietoturvallisina.

LÄHTEET

AITpro Website Security 2023. BulletProof Security. Viitattu 25.4.2023 https://wordpress.org/plugins/bulletproof-security.

Appknox 2023. National Vulnerability Database. Viitattu 7.5.2023 https://www.appknox.com/cyber-security-jargons/national-vulnerability-database.

Astari, S. 2023. What Is reCAPTCHA? Everything You Need to Know. Hostinger 1.3.2023. Viitattu 4.5.2023 https://www.hostinger.com/tutorials/what-is-recaptcha.

Bassi, B. 2023a. 6 Common Website Security Vulnerabilities. Viitattu 7.5.2023 https://www.commonplaces.com/blog/6-common-website-security-vulnerabilities.

Bassi, K. 2023b. 8 Simple Ways to Improve your Website Security. Viitattu 7.5.2023 https://www.commonplaces.com/blog/8-simple-ways-to-improve-your-website-security.

CleanTalk 2023. Spam protection, AntiSpam, FireWall by CleanTalk. Viitattu 25.4.2023 https://wordpress.org/plugins/cleantalk-spam-protect.

Cloudflare 2023. So what is Cloudflare? Viitattu 7.5.2023 https://www.cloudflare.com/learning/what-is-cloudflare.

Dils, C. 2016. How You Know it’s Time to Move from WordPress.com to WordPress.org. Viitattu 26.4.2023 https://carriedils.com/move-from-wordpress-com-to-wordpress-org.

Edward, S. 2022. How to Use the Dig command in Linux. Hostinger 23.11.2022. Viitattu 2.5.2023 https://www.hostinger.com/tutorials/how-to-use-the-dig-command-in-linux.

Exactly WWW 2023. EWWW Image Optimizer. Viitattu 25.3.2023 https://wordpress.org/plugins/ewww-image-optimizer.

F-Secure 2023. Mitä on tietojenkalastelu? Viitattu 7.5.2023 https://www.f-secure.com/fi/articles/what-is-phishing.

Hakkarainen, A. 2016. HTTPS-protokollan käyttö pakolliseksi myös Google Chromessa. Telia 16.9.2016. Viitattu 2.5.2023 https://www.telia.fi/yrityksille/artikkelit/artikkeli/https-protokollan-kaytto-pakolliseksi.

iThemes 2023. iThemes Security. Viitattu 25.4.2023 https://wordpress.org/plugins/better-wp-security.

Jukarainen, M. 2019. Https-salaus ja mitkä ovat http ja https erot. Viitattu 8.5.2023 https://mikaeljukarainen.com/https-salaus.

Kenton, W. 2022. What Is Two-Factor Authentication (2FA)? How It Works and Example. Dotdash Meredith 8.9.2022. Viitattu 8.5.2023 https://www.investopedia.com/terms/t/twofactor-authentication-2fa.asp.

Lecklider, C. 2023. WP fail2ban. Viitattu 7.5.2023 https://wordpress.org/plugins/wp-fail2ban.

Limit Login Attempts Reloaded 2023. Limit Login Attempts Reloaded. Viitattu 25.4.2023 https://wordpress.org/plugins/limit-login-attempts-reloaded.

MDN Web Docs 2023. Website Security. MDN 25.2.2023. Viitattu 25.4.2023 https://developer.mozilla.org/en-US/docs/Learn/Server-side/First_steps/Website_security.

National Vulnerability Database 2020. Raportti CVE-2020-35589 22.12.2020. Viitattu 4.5.2023 https://nvd.nist.gov/vuln/detail/CVE-2020-35589.

Nettivertailut.com 2023. DigitalOcean. Viitattu 2.5.2023 https://nettivertailut.com/hostingpalvelut/digitalocean.

Nielsen, S. 2023. Mikä on CAPTCHA. Kotimikro 28.1.2023. Viitattu 26.4.2023 https://kotimikro.fi/tietoturva/pc-suojaus/mika-on-captcha.

Palmu, P. 2019. Miksi varmuuskopiointi on tärkeää – Näin turvaat tiedostosi. Etevä tietopalveluyhtiö 10.2019. Viitattu 7.5.2023 https://www.etevat.fi/blogi/miksi-varmuuskopiointi-on-tarkeaa-nain-turvaat-tiedostosi.

Really Simple Plugins 2023. Really Simple SSL. Viitattu 25.4.2023 https://wordpress.org/plugins/really-simple-ssl.

Shim, T. 2023. Everything You Need to Know About Cloudflare (and Some You Don’t). Web Hosting Secret Revealed 18.4.2023. Viitattu 2.5.2023 https://www.webhostingsecretrevealed.net/blog/security/everything-you-need-to-know-about-cloudflare.

Šimonėlytė, M. 2023. DNS: aloittelijan opas internetin nimipalvelujärjestelmään. Nord Security 4.4.2023. Viitattu 8.5.2023 https://nordvpn.com/fi/blog/mika-on-dns.

SolarWinds Worldwide 2023. What is DigitalOcean? Viitattu 8.5.2023 https://www.papertrail.com/solution/guides/digitalocean.

Stytch 2022. What is CAPTCHA, and how does it work? Viitattu 8.5.2023 https://stytch.com/blog/what-is-captcha.

Thibodeau, T. 2022. WordPress.com vs WordPress.org: What’s the Difference. WordPress 29.4.2022. Viitattu 7.5.2023 https://www.webhostingsecretrevealed.net/blog/security/everything-you-need-to-know-about-cloudflare.

Twilio 2023. What Is Two-Factor-Authentication (2FA)? Viitattu 26.4.2023 https://authy.com/what-is-2fa.

Vaishnavi 2023. reCAPTCHA: Easy for Humans and Hard for bots. NamLabs Technologies 23.2.2022. Viitattu 8.5.2023 https://www.atatus.com/blog/what-is-recaptcha.

Wordfence 2023. Wordfence Security – Firewall, Malware Scan, and Login Security. Viitattu 25.4.2023 https://wordpress.org/plugins/wordfence.

WP Concern 2023. Advanced Google reCAPTCHA. Viitattu 26.4.2023 https://wordpress.org/plugins/advanced-google-recaptcha.

WPDeveloper 2023. Disable Comments – Remove Comments & Stop Spam [Multi-Site Support]. Viitattu 1.5.2023 https://wordpress.org/plugins/disable-comments.

WPMU DEV 2023. Defender Security – Malware Scanner, Login Security & Firewall. Viitattu 25.4.2023 https://wordpress.org/plugins/defender-security.

WP PDF Embedder Team 2023. PDF Embedder. Viitattu 1.5.2023 https://wordpress.org/plugins/pdf-embedder.

Zieniūtė, U. 2022. Mikä on brute force -hyökkäys eli väsytyshyökkäys. Nord Security 7.6.2022. Viitattu 8.5.2023 https://nordvpn.com/fi/blog/vasytyshyokkays.