Karelia-ammattikorkeakoulu
Tradenomi (AMK), tietojenkäsittelyn koulutus

WordPress-sivuston tietoturva

Haavoittuvuudet, suojausmenetelmät ja kyberuhkien hallinta

Aatu Kärnä

Opinnäytetyö, toukokuu 2025

www.karelia.fi

Karelia AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Helmikuu 2025
Tietojenkäsittelyn koulutus

Tikkarinne 9
80200 JOENSUU
+358 13 260 600

Tekijä
Aatu Kärnä

Nimeke
WordPress-sivuston tietoturva : haavoittuvuudet, suojausmenetelmät ja kyberuhkien hallinta

Toimeksiantaja
Sisustuspalvelut Minna Nevalainen Oy

Tiivistelmä

Opinnäytetyö käsittelee WordPress-sivustojen tietoturvaa ja pyrkii luomaan kattavan ja käytännönläheisen tietoturvaoppaan. Oppaan tavoitteena on auttaa WordPress-sivustojen ylläpitäjiä suojaamaan WordPress-sivustonsa tehokkaasti erilaisia uhkia vastaan sekä opastaa heitä hyödyntämään saatavilla olevia tietoturvatyökaluja ja lisäosia. Työssä perehdytään kattavasti erilaisten lisäosien tarjoamiin tietoturvaratkaisuihin.

Opinnäytetyössä on toteutettu kirjallisuuskatsaus, jossa on hyödynnetty akateemisia julkaisuja, tietoturvaraportteja ja WordPress-dokumentaatiota. Tietoturvaratkaisujen testaamiseen on käytetty WordPressiä ja WAMP-ohjelmistoa, ja kaikki vaiheet on dokumentoitu. Työssä esitellään myös käytännönläheisesti erilaisia tietoturvatyökaluja, kuten ZAP (Zed Attack Proxy), joka on avoimen lähdekoodin työkalu sovellusturvallisuuden testaamiseen, WPScan, joka on WordPress-haavoittuvuuksien skannaukseen tarkoitettu työkalu, sekä KeePass 2, turvallinen salasanojen hallintaohjelma.

Lopputuloksena syntyi tietoturvatoiminnoilla varustettu WordPress-sivusto sekä käytännönläheinen opas, joka toimii hyödyllisenä tukena erityisesti aloitteleville WordPress-sivuston ylläpitäjille.

Kieli
suomi

Sivuja 40

Asiasanat
WordPress, tietoturva, haavoittuvuudet, suojausratkaisut

Karelia
UNIVERSITY OF APPLIED SCIENCES

THESIS
February 2025
Information Technology Education

Tikkarinne 9
80200 JOENSUU
FINLAND
+ 358 13 260 600

Author
Aatu Kärnä

Title
Security of WordPress Websites: Vulnerabilities, Protection Methods, and Cyber Threat Management

Commissioned by
Sisustuspalvelut Minna Nevalainen Oy

Abstract

The thesis focuses on the security of WordPress websites and aims to create a comprehensive and practical security guide. The goal of the guide is to help WordPress site administrators effectively protect their websites against various threats and to guide them in utilizing available security tools and plugins. The thesis thoroughly explores the security solutions offered by different plugins.

A literature review was conducted as part of the thesis, drawing on academic publications, security reports, and WordPress documentation. WordPress and WAMP software were used to test the security solutions, and all steps were carefully documented. The thesis also provides a practical introduction to various security tools, such as ZAP (Zed Attack Proxy), an open-source tool for application security testing, WPScan, a tool for scanning WordPress vulnerabilities, and KeePass 2, a secure password management application.

The outcome of the thesis was a WordPress website equipped with security features, as well as a practical guide that serves as a helpful resource, especially for novice WordPress website administrators.

Language
Finnish

Pages 40

Keywords
WordPress, security, vulnerabilities, protection solutions

Sisältö

1 Opinnäytetyön tausta ja toteutus

1.1 Johdanto

Tämä opinnäytetyö käsittelee maailman suurimman sisällönhallintajärjestelmän, WordPressin, tietoturvakysymyksiä. Tietoturvaratkaisuja tutkitaan eri näkökulmista. Tavoitteena on luoda kattava, selkeä ja käytännönläheinen tietoturvaopas, jonka avulla lukija voi suojata WordPress-sivustonsa asianmukaisesti. Opas soveltuu käyttäjille, jotka eivät ole kovin tietoteknisiä, mutta haluavat ylläpitää omaa WordPress-sivustoa. Tutkimuksen kohteena on myös se, kuinka paljon manuaalista konfigurointia WordPress-palvelimen suojaaminen vaatii, vai riittääkö lisäosien tarjoamat tietoturvaratkaisut sivuston suojaamiseen. Työstä muodostuu myös WordPress-sivusto toimeksiantajalle, johon on toteutettu valmiiksi tarvittavat tietoturvatoimenpiteet. Sivustoon toteutetaan myös muuta sisältöä, mutta tässä opinnäytetyössä keskitytään vain tietoturvaan.

1.2 Tietoperusta

Opinnäytetyössä on toteutettu kattava kirjallisuuskatsaus, joka sisältää erilaisia akateemisia julkaisuja, tietoturvaraportteja ja paljon WordPressiin liittyvää dokumentointia. Tutkimuksessa on pyritty käyttämään mahdollisimman tuoreita ja luotettavia lähteitä, jotta opinnäytetyöllä olisi vahva teoreettinen pohja ja että siinä huomioitaisiin parhaat nykyiset käytännöt ja trendit WordPressin tietoturvassa. Työssä analysoidaan ja vertaillaan myös erilaisia valikoituja haavoittuvuusraportteja. Myös erilaista kirjallisuutta hyödynnetään O'Reillyn for Higher Education -kirjatietokannasta sekä Karelian Tikkarinteen kampuksen kirjaston valikoimasta.

1.3 Tutkimusmenetelmät

Tietoturvaratkaisujen testaamiseen ja toteuttamiseen käytetään WordPressiä sekä WAMP-ohjelmistoa. Kaikki vaiheet myös dokumentoidaan käyttäen esimerkiksi kuvakaappauksia. Työssä esitellään käytännönläheisesti erilaisia työkaluja, lisäosia ja menetelmiä, jotka liittyvät WordPressin tietoturvaan. Tähän sisältyy myös tietoturvatyökalut ZAP ja WPScan, sekä KeePass 2 -salasanojen hallintasovellus. Kaikki sovellukset, lukuun ottamatta WPSCan, asennetaan ja testataan Windows 10 -PC:llä. Työssä hyödynnetään myös Oracle VM VirtualBox -sovellusta, jossa ajetaan Kali Linux -käyttöjärjestelmää. Käytössä on myös Arch Linux -palvelin, jota hyödynnetään tarvittaessa. Tutkimus suoritetaan eettisesti ja tietoturvahyökkäyksiä tehdään vain omalle palvelimelle omassa suljetussa verkossa. Myös eri selaimia hyödynnetään opinnäytetyön aikana, kuten Mozilla Firefoxia ja Microsoft Edgeä. Työssä viitataan usein myös Wingetiin eli Windows Package Manageriin. Se on Microsoftin kehittämä komentorivityökalu, jolla voidaan asentaa, päivittää, poistaa ja hallita ohjelmia. Jos Wingetiä käyttää ensimmäistä kertaa, kysytään käyttöehtojen hyväksymistä. Jatkaakseen on hyväksyttävä käyttöehdot kirjoittamalla kenttään ”y” ja painamalla Enter-näppäintä.

2 Tietoturvan perusteet ja WordPress

WordPressin suuri käyttäjäkunta tekee siitä erittäin hyvän kohteen erilaisille rikollisille toimijoille ja WordPress-sivuston tietoturvan pettämisellä voikin olla hyvin vakavia seurauksia. Hyökkääjä voi pahimmillaan varastaa sivuston käyttäjätietoja, maksutietoja, upottaa sivustolle haittaohjelmia ja takaovia (Kyberturvallisuuskeskus 2016, 3). Eri lähteistä paljastuu jatkuvasti uusia haavoittuvuuksia, joiden avulla hyökkääjä voi jopa ottaa koko sivuston omaan käyttöönsä (Kyberturvallisuuskeskus 2016, 3). Vaikka verkkosivu olisi pienikokoinen ja vähäliikenteinen, voi se silti joutua hyökkäyksen kohteeksi, sillä hakkereita kiinnostaa palvelimien kaappaaminen osaksi bottiverkkoa (Friedman 2014).

Kyberturvallisuuden lähtökohta on se, että suojaudutaan haittaohjelmilta ja erilaisilta tietomurto-yrityksiltä käyttäen mm. tietoturvaohjelmistoja, kuten palomuureja ja virustorjuntaohjelmia (Hänninen 2025, 252). Olipa kyseessä tavallinen roskapostittaja tai huippuluokan hakkeroija, paras puolustuskeino on kouluttautua. Verkkosivuston turvallisuus ei rajoitu pelkästään suojaamiseen ammattimaisilta hyökkääjiltä ja vihamielisiltä kollegoilta, vaan se liittyy myös hyvien päätösten tekemiseen, jotka estävät virheiden kehittymisen suuriksi ja kalliiksi ongelmiksi. (Friedman 2014.)

WordPressissä yleisin roskapostin muoto ovat kommentit. Nämä ovat bottien jättämiä kommentteja julkaisuihisi, ja niiden tarkoituksena on yleensä saada linkki omalle verkkosivulleen lisätäkseen brändin näkyvyyttä hakukoneissa. Roskapostittajat pyrkivät esiintymään aidolta vaikuttavina käyttäjinä jättäessään kommentteja blogeihin. (Friedman 2014.)

WordPressin suosio kattaa jopa 43.5% verkkosivustoista (W3Techs 2025). Suuren suosionsa vuoksi WordPress-sivustot selvästikin houkuttavat rikollisia toimijoita, sillä Sucurin tekemän tutkimuksen mukaan vuonna 2023 saastuneista sisällönhallintajärjestelmällä toteutetuista sivustoista noin 95.5% oli tehty WordPressillä (Sucuri 2024, 5). Tämä korostaa asianmukaisen WordPressin suojaamisen merkitystä.

Vuonna 2024 noin 96% uusista tietoturvaongelmista johtui laajennuksista, noin 4% teemoista ja alle 0.01% WordPress-ytimestä. Ytimestä löytyi 6 matalan tason haavoittuvuutta ja 1 keskitason haavoittuvuus. (Patchstack 2025.) Tämä näyttää myös sen, että ylimääräisten lisäosien ja teemojen asentamista kannattaa välttää tietoturvan näkökulmasta, sekä sen että WordPressin kehitystiimi on omistautunut järjestelmän tietoturvan parantamiseen ja järjestelmän säännölliseen päivittämiseen. WordPressin ytimen tietoturvasta kertoo myöskin se, että useat isot yritykset käyttävät WordPress-sivustoja, kuten Samsung, Sony, eBay ja The New York Times (Friedman 2014).

Tietoturva ei myöskään ole vain tietoteknisten ihmisten vastuulla. Yrityksiltä ja organisaatiolta kyberturvallisuus edellyttää myös henkilöstön koulutusta, tietojen

turvallista käsittelyä ja käyttäjien tietoisuuden lisäämistä tietoturvasta (Hänninen 2025, 252). Lisäksi käyttäjäkoulutus ei ole pelkästään turvallisuusloukkauksien estämistä; se on myös turvallisuustietoisuuden kulttuurin edistämistä. Tietoiset käyttäjät sopeutuvat nopeammin uusiin turvallisuusprotokolliin ja pystyvät tehokkaammin navigoimaan WordPress-hallinnan monimutkaisuuksissa, varmistaen, että sivusto pysyy vahvana mahdollisia uhkia vastaan (Goodchild 2023). WordPressin tietoturvan ylläpito vaatii sitoutumista. Haittaohjelmien torjunta on jatkuva prosessi, koska uusia haittaohjelmia kehitetään ja julkaistaan jatkuvasti. Se vaatii suunnitelmien ja tietojen jatkuvaa päivittämistä. (Hänninen 2025, 274.)

3 HTTPS / SSL

Luvatonta pääsyä arkaluontoisiin tietoihin voidaan estää salaamalla liikenne HTTPS-protokollalla (Hänninen 2025, 259). WordPress-sivuston parhaan tietoturvan takaamiseksi onkin suositeltavaa aina käyttää HTTPS-yhteyttä, sekä asianmukaista SSL-sertifikaattia.

Testiympäristössä voidaan käyttää itse allekirjoitettua sertifikaattia käyttäen esimerkiksi OpenSSL:ää. Se voidaan asentaa Windows 11 -käyttöjärjestelmään syöttämällä komento ”winget install --id=FireDaemon.OpenSSL -e” PowerShell-sovellukseen. Oikeassa ympäristössä kannattaa kuitenkin käyttää luotettavan tahon allekirjoittamaa SSL-sertifikaattia. Se voidaan aktivoida helposti käyttämällä lisäosaa Really Simple Security. Aktivoidakseen SSL-yhteyden, tulee klikata Really Simple Securityn hallintapaneelista ruskeaa ”Activate SSL” -nappia. Sen jälkeen tulee klikata sinistä ”Activate SSL” -nappia. Asennusohjelma opastaa asennuksen loppuun.

Jos sivustolla ilmenee ”Insecure content” -virheitä HTTPS-yhteyden aktivoimisen jälkeen, voidaan siihen käyttää avuksi esimerkiksi SSL Insecure Content Fixer -lisäosaa. Sen asetuksista voidaan valita, kuinka laajalle alueelle lisäosa vaikuttaa. Menemällä ylemmästä vaihtoehdosta alempaan varmistetaan, että sivusto toimii oikein. Esimerkiksi asetus ”Simple” on suorituskyvyn kannalta

kevyin ja vähiten häiriöitä aiheuttava vaihtoehto, kun taas ”Capture All” soveltuu tilanteisiin, joissa muut tasot eivät riitä ongelman korjaamiseen.

Myös WordPress- ja Site Address kohtiin tulee päivittää https-alkuosa. Kyseiset asetukset löytyvät valitsemalla hallintapaneelista ensin ”Settings” ja sen jälkeen ”General”. (kuva 1).

Kuva 1. WordPressin asetukset.

4 Lisäosat ja teemat

4.1 Tietoa lisäosista ja teemoista

Koska suurin osa WordPressiin kohdistuvista tietoturvaongelmista johtuu lisäosista ja teemoista (Patchstack 2025), on niiden huolellinen valitseminen erittäin tärkeää. Ylimääräisiä lisäosia kannattaa välttää, jotta tietoturva-aukkojen määrä saadaan minimoitua (Seravo 2024). WordPress-sivustolla kannattaa käyttää vain vakaita lisäosia ja moduuleita (Georgia Technology Authority 2024). Kolmannen osapuolen lisäosia valittaessa kannattaa etsiä sellaisia, joilla on hyvät arvostelut ja luokitukset, suuri latausmäärä sekä monipuoliset käyttömahdollisuudet omalla sivustolla. On hyvä varmistaa myös, että lisäosaa päivitetään säännöllisesti ja että se on yhteensopiva uusimman WordPress-version kanssa (Needham 2022).

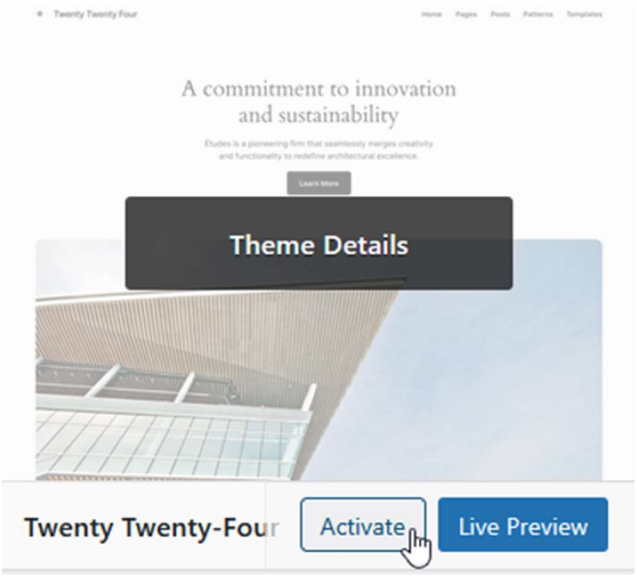
On olemassa myös lisäosia, jotka etsivät haittaohjelmia WordPress-sivustoilta. Lisäosiin pohjautuvat etä- sekä paikalliset skannerit voivat tarjota suojaa matalamman tason uhkia vastaan, sillä keskiverto hakkerin käyttämät työkalut eivät usein ole kovin tehokkaita. (Alkan 2023.)

Yksi vaarallinen lisäosa voi vaikuttaa hyvin monen käyttäjän sivustoon. Vuonna 2022 yleinen tietoturvaan pohjautuva WPGateWay -lisäosa vaaransi yli 280 000 käyttäjän WordPress-sivuston, sillä siinä oli haavoittuvuus, joka mahdollisti ylimääräisen ylläpitotilin luomisen (Pisani 2024).

4.2 Turvallisen teeman valinta

Teemoja voidaan asentaa siirtymällä hallintapaneelin vasemman reunan valikosta kohtaan Appearance ja valitsemalla sen alta Themes. Seuraavaksi aukeaa sivu, jossa on WordPressin omat teemat. Samalta sivulta voidaan etsiä uusia teemoja käyttämällä yläreunasta löytyvää hakukenttää.

Kolmansien osapuolien teemojen tulee käyttää harkiten. Ennen teeman asentamista, tulee tehdä huolellinen tutkimus, onko teema varmasti tietoturvallinen. Helpon tietoturvallisen ratkaisun takaamiseksi voidaan käyttää WordPressin omia teemoja, tässä tapauksessa Twenty Twenty-Four -teemaa. Teema voidaan aktivoida klikkaamalla ”Activate” -nappia. ”Live Preview” -napin klikkaaminen mahdollistaa teeman testaamisen. (kuva 2).



Kuva 2. WordPressin teeman aktivointi ja -tarkastelu.

4.3 Lisäosien asentaminen ja poistaminen

WordPress-sivustoille on oletuksena asennettu Hello Dolly- sekä Akismet Anti-Spam: Spam Protection -lisäosat. Hello Dolly -lisäosa näyttää admin-sivulla satunnaisesti Louis Armstrongin Hello Dolly -kappaleen sanoja. Se voidaan poistaa, sillä se ei tuo tietoturvan kannalta mitään lisäarvoa. Akismet Spam -lisäosa voidaan halutessaan ottaa käyttöön, mutta se vaatii maksullisen lisenssin, jos sitä halutaan käyttää kaupallisesti. Kummatkin lisäosat voidaan poistaa siirtymällä hallintapaneelin vasemman reunan valikosta kohtaan ”Plugins” ja valitsemalla sieltä ”Installed Plugins” -välilehti. Lisäosan poistaminen onnistuu valitsemalla kyseisen lisäosan kohdalta ”Delete” (kuva 3).

Kuva 3. WordPressin lisäosan poistaminen.

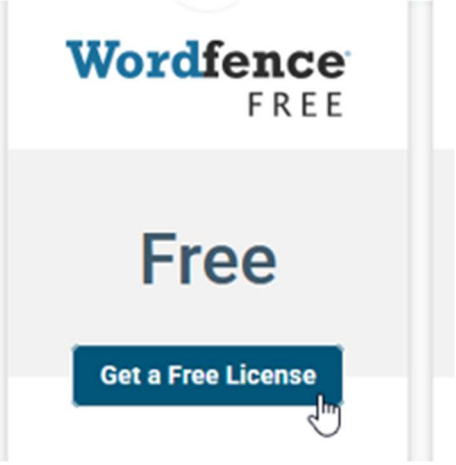
Uusia laajennuksia voidaan asentaa siirtymällä hallintapaneelin vasemman reunan valikosta kohtaan ”Plugins” ja valitsemalla sen alta ”Add New Plugin”. Avautuvalta välilehdeltä voidaan ylhäältä löytyvästä hakukentästä (Search Plugins) etsiä lisäosia. Kun haluttu lisäosa on löytynyt, voidaan se asentaa klikkaamalla ”Install Now” -nappia. Lopuksi lisäosa aktivoidaan klikkaamalla ”Activate”-nappia. (kuva 4).

Kuva 4. WordPressin lisäosia.

4.4 WordFencen asennus

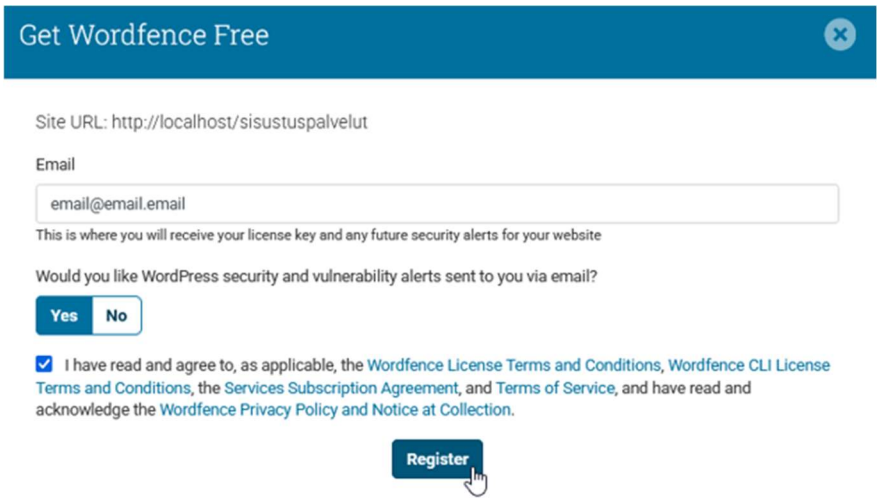
WordFence on hyvin olennainen lisäosa WordPressin tietoturvan ylläpitämisessä, koska se tarjoaa kattavan suojan sivuston tietoturvauhkia vastaan. Tässä osiossa käydään läpi WordFencen asentaminen alusta loppuun. Kun lisäosa on aktivoitu ja WordFencen konfigurointi on aloitettu, tulee ikkuna, josta voidaan edetä klikkaamalla ”GET YOUR WORDFENCE LICENSE” -nappia.

WordFence tarvitsee toimiakseen lisenssin. Maksulliset lisenssit tarjoavat kattavammat toiminnot, mutta myös saatavilla oleva ilmainen lisenssi lisää tietoturvaa huomattavasti. Ilmainen lisenssi voidaan hankkia klikkaamalla ”Get a Free License” -nappia (kuva 5).



Kuva 5. Ilmainen WordFence-lisenssi.

Seuraavaksi tulee klikata ”I’m OK waiting 30 days for protection from new threats” -tekstiä. Tässä vaiheessa asennusta kysytään sähköpostiosoitetta. Kenttään tulee syöttää oikea sähköpostiosoite, sillä sähköpostiin saapuvaa linkkiä tarvitaan asennuksen viimeistelyyn. WordFence myös tarjoaa kuukausittaisen tietoturvaraportin sähköpostitse. On suositeltavaa vastaanottamaan tietoturvaraportit sähköpostiin valitsemalla ”Yes”. Asennusta voidaan jatkaa klikkaamalla lopuksi ”Register”-nappia (kuva 6).



Kuva 6. WordFencen asennusohjelma.

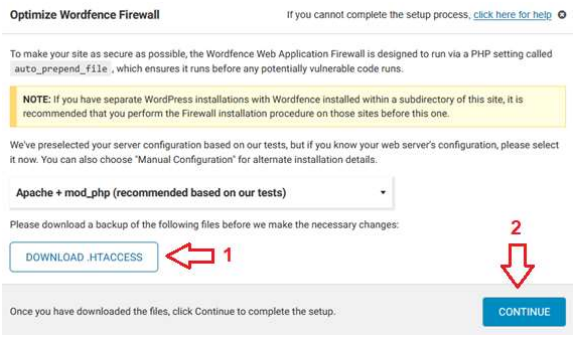
Seuraavaksi tulee ilmoitus, joka kertoo, että lisenssiavain on lähetetty annettuun sähköpostiosoitteeseen. Sähköpostiviestistä löytyy sininen nappi, jossa lukee ”Install My License Automatically”. Sen klikkaaminen asentaa lisenssin automaattisesti, mutta se pitää avata samalla selaimella, jolla asennusta on tehty tähän asti. On suositeltavaa klikata nappia hiiren oikealla näppäimellä ja kopioida linkki. Tämän jälkeen linkki voidaan liittää selaimen osoiteriville (kuva 7).

Kuva 7. WordFencen lähettämä sähköposti.

Kun linkki on avattu, voidaan vielä tarkistaa annettu sähköpostiosoite ja ottaa WordFencen lisenssiavaimen talteen. Lisenssiavain löytyy ”License Key” tekstin alta. Lopuksi tulee klikata vielä ”INSTALL LICENSE” -nappia ja asennus on valmis.

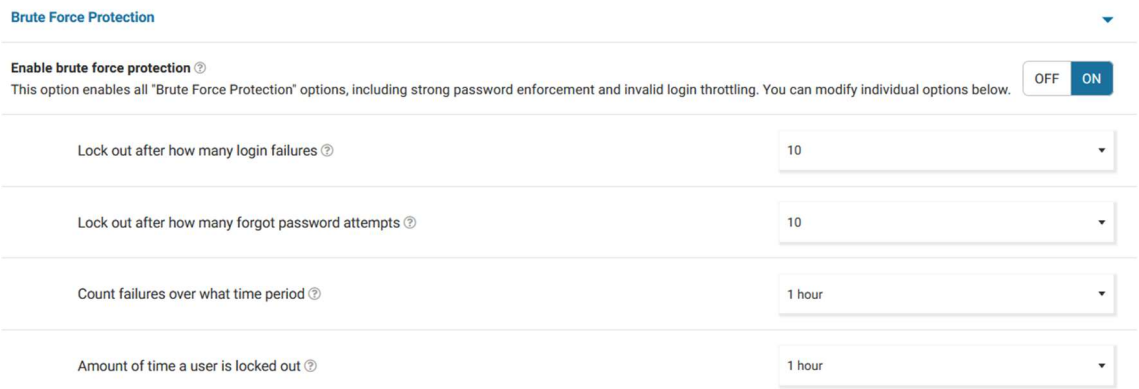
Kun WordFence on toiminnassa, voidaan erilaisia konfigurointeja vielä tehdä. WordFencen palomuuri voidaan optimoida klikkaamalla ”CLICK HERE TO CONFIGURE” -tekstiä sivun yläreunassa olevasta ilmoituksesta. Optimointi voidaan aloittaa myös ”Basic Firewall Options” -valikosta. Seuraavassa näkymässä käyttäjän on pakko ladata ”.HTACCESS” -tiedosto, ennen kuin

”CONTINUE”-nappi toimii. Asennusta voidaan jatkaa klikkaamalla ”DOWNLOAD .HTACCESS” -nappia ja sen jälkeen ”CONTINUE” -nappia (kuva 8).



Kuva 8. WordFencen palomuurin optimointi.

Palomuurin optimointi on valmis, kun käyttäjä saa ilmoituksen ”Installation Succesful”. Palomuurin optimointi voidaan päättää klikkaamalla ”CLOSE” -nappia. Kirjautumisyritysten rajoittaminen onnistuu myös WordFencellä. Tämä löytyy ”Brute Force Protection” -kohdan alta. Kirjautumisyritykset voidaan rajoittaa esimerkiksi 10 kertaan tunnissa (kuva 9).



Kuva 9. WordFencen brute force -suojauksen asetukset.

WordPress-sivuston versio voidaan piilottaa ja laittaa koodin ajaminen ”../uploads” -kansiosta pois käytöstä (kuva 10).

Kuva 10. WordFencen asetukset.

On hyvä myös tietää, että oletusasetuksilla WordFence jakaa sivustosta tietoturvaan liittyviä tietoja. Vastapalveluksena käyttäjä saa tietoa muilta käyttäjiltä, joka voi lisätä tietoturvaa. Asetus voidaan ottaa halutessaan pois päältä tai jättää oletusarvoon. Asetus löytyy nimellä ”Participate in the Real-Time Wordfence Security Network” (Osallistu Wordfencen reaaliaikaiseen suojausverkostoon).

5 Kirjautuminen ja tunnistautuminen

5.1 Hyökkääminen kirjautumissivulle

WordPressin oletusasetuksilla kirjautumissivu on julkisesti kaikkien saavutettavissa, sisäänkirjautumisyrityksille ei ole määrärajoitusta, 2FA-autentikaatio ei ole käytössä sekä sivusto vuotaa erilaisia tietoja. Jos näitä asioita ei huomioida, voivat ne altistaa sivuston esimerkiksi brute force -hyökkäyksille. Monet näistä ongelmista voidaan estää muutamalla yksinkertaisella muutoksella ympäristöön. (Martin 2022.) Useimmiten hyökkääjät eivät edes tiedä, mihin sivustoihin he kohdistavat hyökkäyksensä. Ne skannaavat verkkoa, merkitsevät muistiin WordPressiä käyttävät sivustot ja hyökkäävät niitä vastaan. Siksi ennalta-arvaamattomuus auttaa suojaamaan WordPress-sivustot useimmilta hyökkääjiltä. (Friedman 2014.)

5.2 Ohjeet vahvojen salasanojen ylläpitämiseen ja luomiseen

Tässä osiossa käsitellään KeePass 2 -sovelluksen käyttöä. KeePass 2 on salasanojen hallintaan tarkoitettu sovellus, ja sen käyttöä tai vastaavan turvallisen hallintaratkaisun hyödyntämistä suositellaan WordPress-sivustojen käyttäjille

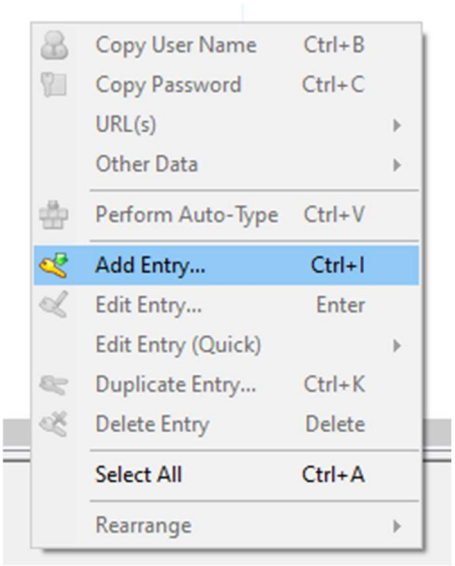
salasanojen turvallista säilyttämistä ja hallintaa varten. Tämä koskee erityisesti järjestelmänvalvojan oikeuksia omaavia käyttäjiä.

WordPressin käyttäjätunnuksia ei myöskään koskaan tule jakaa kenellekään, vaan kaikille sivustoa käyttäville tulee luoda oma käyttäjätili. Heikkojen ja huonosti suojattujen salasanojen käyttäminen johtaa todennäköisesti tilien hakkeroimiseen. (Friedman 2014.)

KeePass 2 -sovellus voidaan asentaa helposti Windows 11 -käyttöjärjestelmään käyttämällä Wingetiä avaamalla PowerShell-sovellus ja ajamalla komento ”winget install -e --id DominikReichl.KeePass”. Jos KeePass halutaan ladata jollekkin muulle käyttöjärjestelmälle, löytyy vaihtoehdot osoitteesta ”https://keepass.info/download.html”.

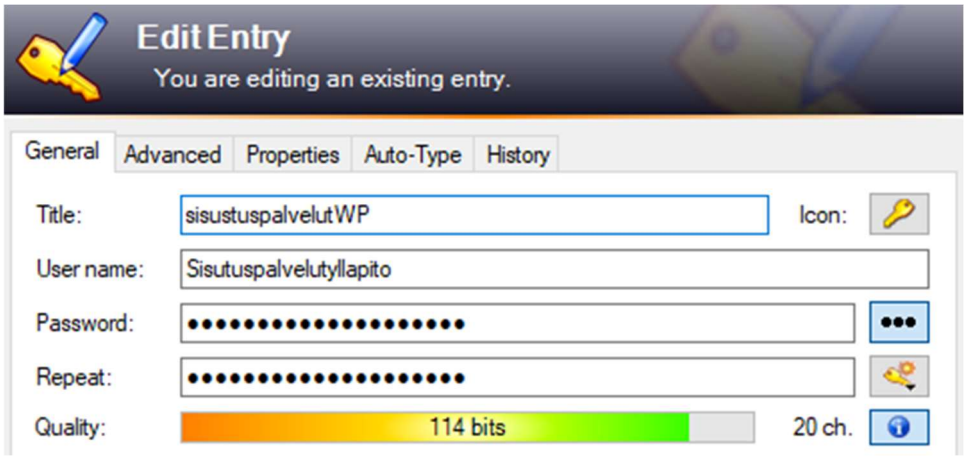
Kun KeePass 2 on asennettu, voidaan uusi Master Key luoda valitsemalla ylävalikosta ensin File ja sen jälkeen New. Tämä toimii ns. ”salasanatietokantana”. Aukeavaan ”Master password” kenttään tulee syöttää vahva salasana. Salasana tulee pitää tallessa.

Tässä vaiheessa WordPress-tunnuksia varten voidaan luoda uusi merkintä (entry) klikkaamalla oikeaa hiiren näppäintä ja valitsemalla ”Add Entry” (kuva 11).



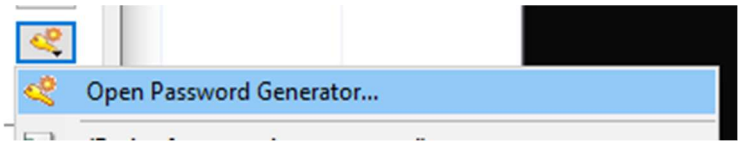
Kuva 11. Add Entry -vaihtoehto.

Seuraavaksi voidaan syöttää nimi tunnuksille, WordPress-sivuston käyttäjätunnus ja salasana (kuva 12).



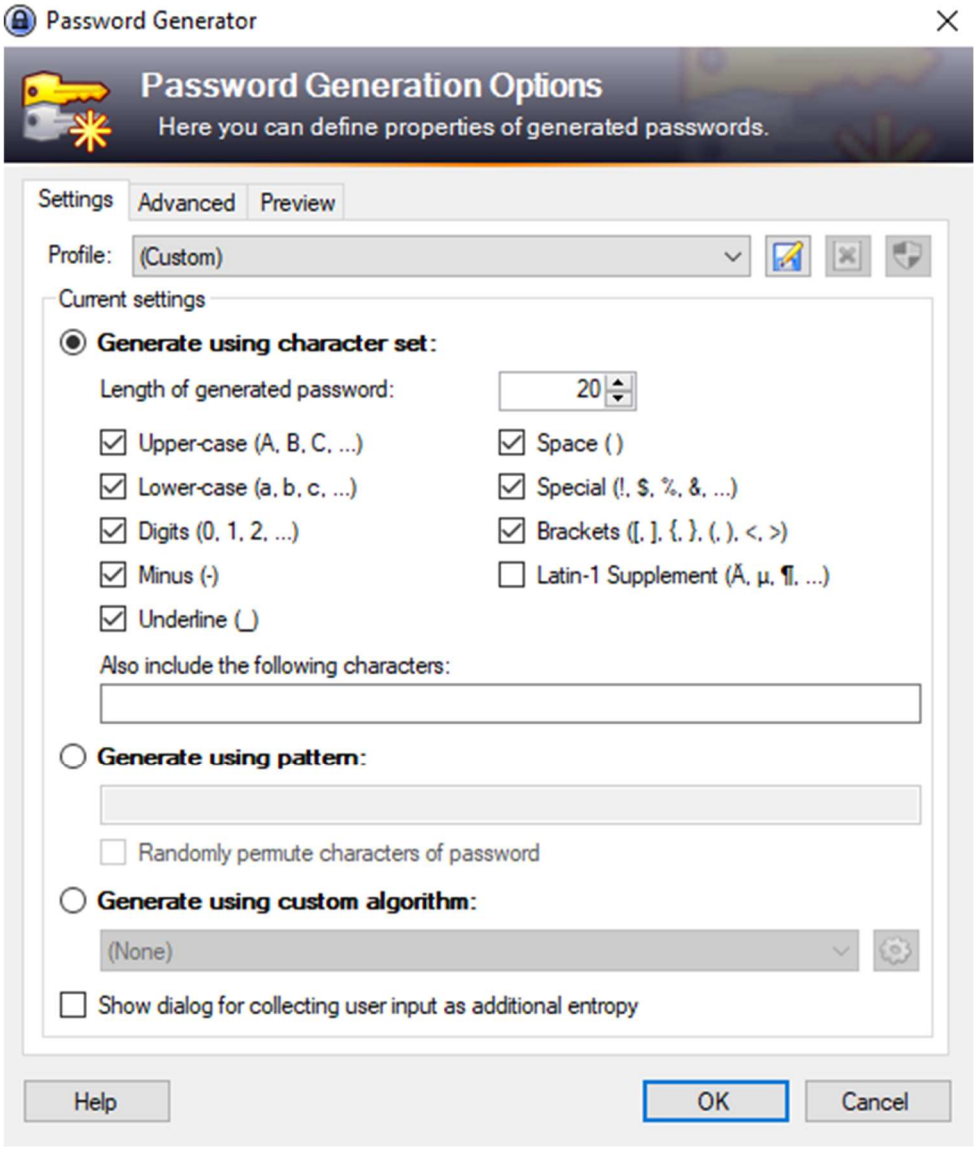
Kuva 12. Edit Entry -näkymä.

Salasana voidaan myös luoda KeePassilla klikkaamalla ”Open Password Generator...” (kuva 13).



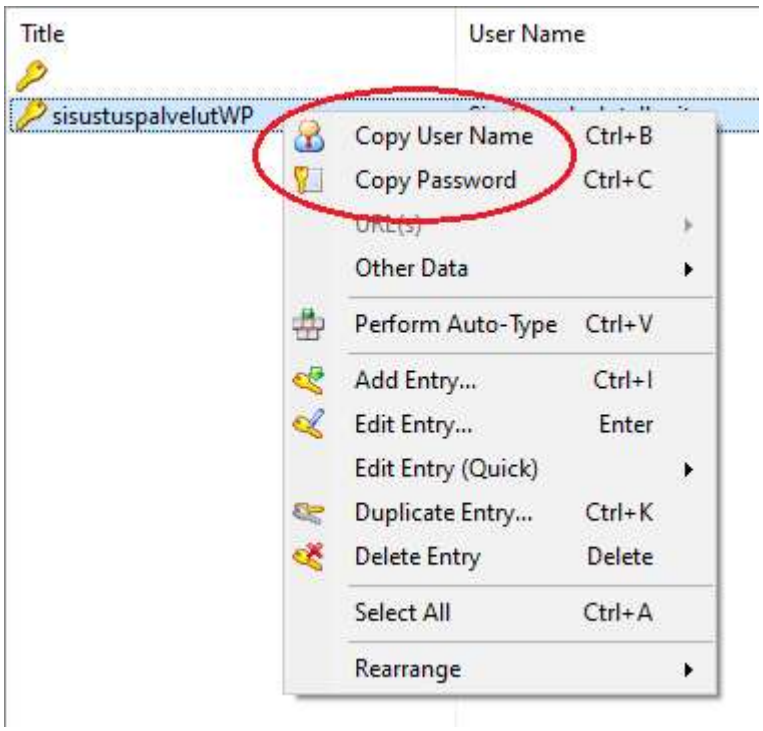
Kuva 13. Uuden salasanan luominen.

Koska WordPress tukee laajaa valikoimaa erilaisia merkkejä salasanoissa, voidaan hyödyntää esimerkiksi kuvan osoittamia asetuksia salasanan muodostamisessa. Tunnukset on luotu, kun ”OK” -nappia on klikattu kaikista auki olevista valikoista (kuva 14).



Kuva 14. Password Generator -näkymä.

WordPress-sivustolle kirjautuessa tunnukset voidaan kopioida klikkaamalla tunnusten nimeä oikealla hiiren painikkeella ja valitsemalla aukeavasta valikosta ”Copy User Name” kopioidakseen käyttäjänimen ja ”Copy Password” kopioidakseen salasanan. Tiedot pysyvät leikepöydällä (clipboardilla) 10 sekuntia, eli ne täytyy liittää WordPress-sivuston kirjautumiskenttiin sen aikana (kuva 15).

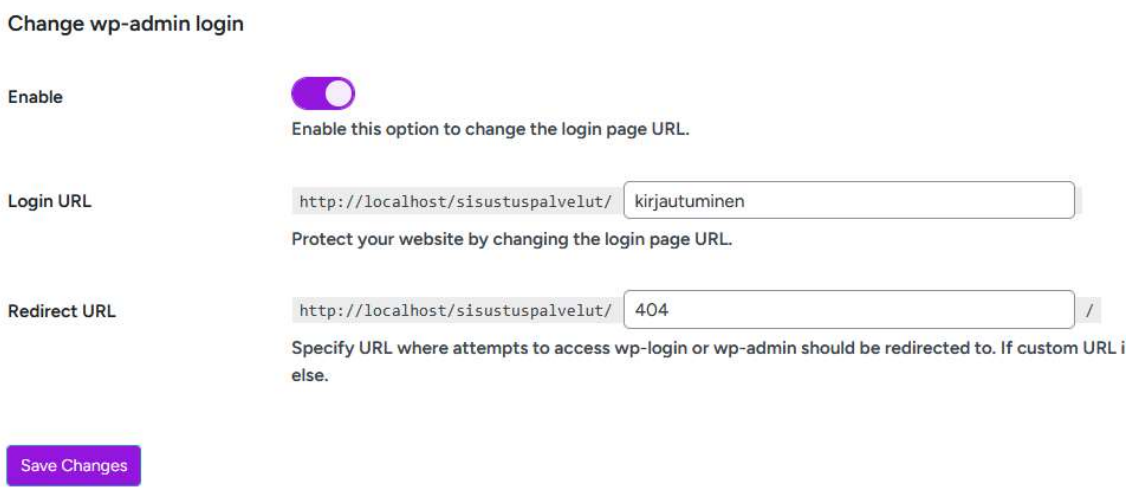


Kuva 15. Käyttäjätunnuksen ja salasanan kopioiminen.

5.3 Kirjautumissivun suojaaminen

All-In-One Login -lisäosalla voidaan vaihtaa ”../wp-admin” ja ”../wp-login” -osoitteet yksilöllisiksi, mikä vaikeuttaa bottien löytämistä kirjautumissivulle. Kun All-In-One Login -lisäosa on asennettu, sen hallintapaneeliin pääsee siirtymällä hallintapaneelin vasemman reunan valikosta kohtaan ”AIO Login” ja valitsemalla sieltä ”Login Protection”. Kirjautumissivun yksilöinnin ja uudelleenohjauksen asetuksiin pääsee klikkaamalla ”Change wp-admin login” -välilehdeltä ”Enable” -valinnan päälle.

Ylempään kenttään voidaan syöttää uusi kirjautumissivun osoite ja alempaan osoite, johon ohjataan henkilöt, jotka koittavat oletuskirjautumissivua (../wp-admin). Näistä ylempi on olennaisin. Alempaan kenttään voidaan kirjoittaa esimerkiksi ”404” (kuva 16).



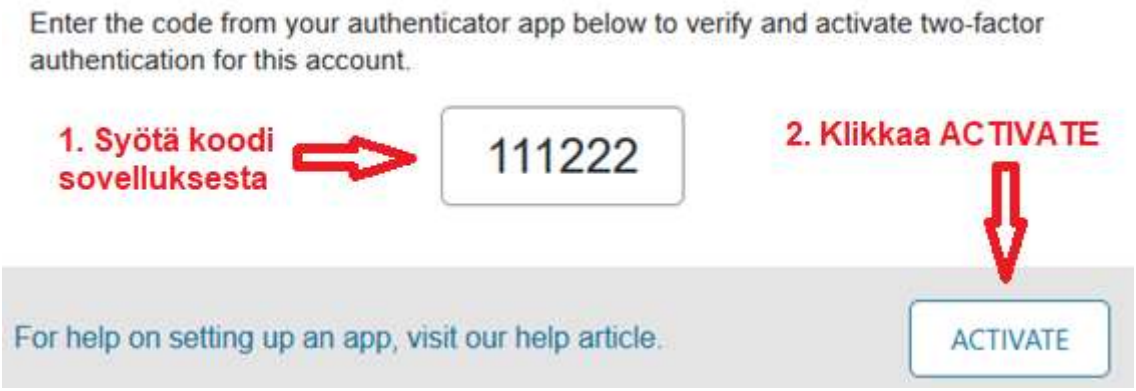
Kuva 16. All-In-One Login -lisäosan Logic Protection -välilehti.

Haitallista liikennettä voidaan torjua aktivoimalla ilmainen Google reCAPTCHA -palvelu. Se perustuu CAPTCHA-järjestelmään, joka on Turingin testi ihmisten ja bottien erottamiseksi toisistaan. Google reCAPTCHA on helppo ihmisille, mutta vaikea automatisoidulle ohjelmistolle, mikä tekee siitä tehokkaan tavan estää haitallista liikennettä ja samalla säilyttää käyttäjäystävällisyys. (Google 2025.) Palvelu voidaan ottaa käyttöön AIO Loginin ”Security”-välilehdeltä.

5.4 Kaksivaiheinen todennus

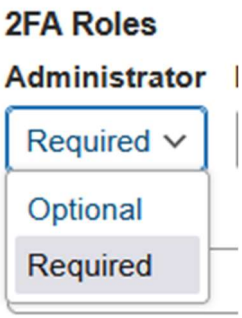
Kaksivaiheinen todennus (2FA) vaatii käyttäjää antamaan kaksi erillistä tunnistetta, jotta käyttäjä voi päästä järjestelmään (Hänninen 2025, 259).
Toiminto voidaan ottaa käyttöön siirtymällä hallintapaneelin vasemman reunan valikosta kohtaan ”Wordfence” ja valitsemalla sieltä ”Login Security”.

Vasemmalla näkyy QR-koodi, joka voidaan skannata älypuhelimella käyttäen esim. Google Authenticator -sovellusta. Oikealla näkyy palautusavaimia, joilla voidaan palauttaa tili tapauksissa, joissa käyttäjällä ei ole enää pääsyä autentikaattoriin. Nämä avaimet kannattaa ottaa talteen. Kun QR-koodi on skannattu, tulee autentikaatio-sovelluksessa näkyvä koodi syöttää alla olevaan kenttään ja klikata ”ACTIVATE” -nappia (kuva 17).



Kuva 17. WordFencen kaksivaiheisen tunnistautumisen aktivointi.

Lisäksi Login Securityn ”Settings” -välilehdeltä 2FA-kirjautuminen kannattaa laittaa pakolliseksi vähintään ylläpitotileille. Tämä voidaan tehdä valitsemalla 2FA Roles -kohdassa Administrator-riviltä avattavasta valikosta vaihtoehto ”Required”. (kuva 18).



Kuva 18. WordFence 2FA Roles.

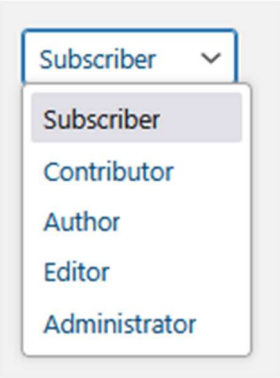
Samalta välilehdeltä kannattaa myös ottaa XML-RPC yhteys pois käytöstä valitsemalla vaihtoehto ”Disable XML-RPC authentication”. XML-RPC on WordPressin ja muiden järjestelmien välistä viestintää mahdollistava tekniikka, joka on ollut oletuksena käytössä versiosta 3.5 lähtien mobiilisovelluksen yhteensopivuuden vuoksi (Needham 2022).

5.5 Käyttäjien hallinta, suojaaminen ja oikeudet

Käyttäjiä voidaan tarkastella siirtymällä hallintapaneelin vasemman reunan valikosta kohtaan ”Users” ja valitsemalla sieltä ”All Users”. Uusia käyttäjiä voidaan

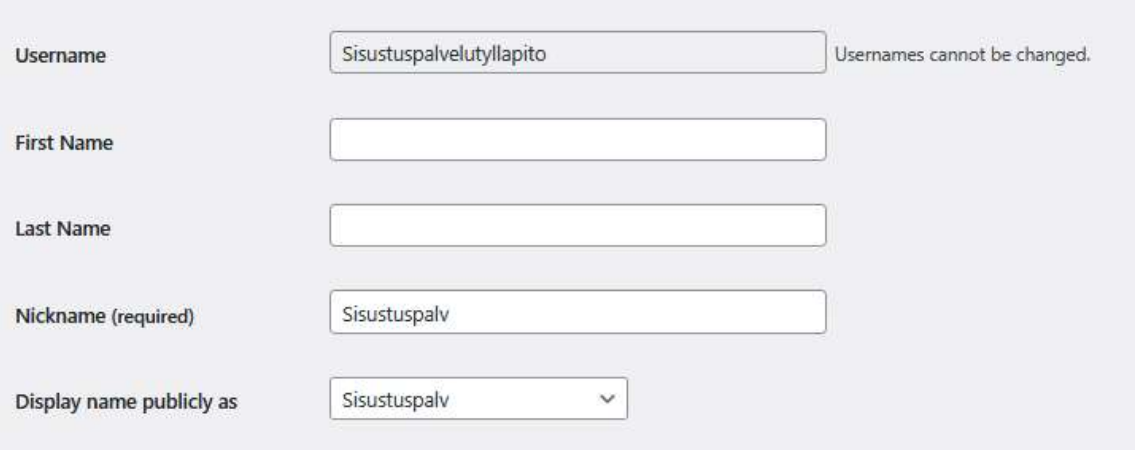
lisätä valitsemalla ”Users”-valikosta ”Add New User”. Käyttäjiä luodessa voidaan hyödyntää WordPressin vakio-oikeuksia.

Administrator-roolilla on laajin hallintaoikeus yksittäisellä sivustolla. Kyseessä on käytännössä täysi kontrolli verkkosivuston toiminnasta. Editor-rooli tarjoaa valtuudet hallita kaikkea sisältöä ilman pääsyä järjestelmän asetuksiin. Editorilla on oikeus muokata ja julkaista myös muiden käyttäjien tuottamaa sisältöä. Author-rooli rajoittuu käyttäjän itse tuottaman sisällön hallintaan. Author voi julkaista, muokata ja poistaa vain omia artikkeleitaan, mutta ei voi vaikuttaa muiden käyttäjien tuotantoon. Contributor-rooli antaa käyttäjälle mahdollisuuden kirjoittaa ja tallentaa omia artikkeleitaan, mutta ei julkaista niitä. Näin ollen kontributori tarvitsee editorin tai ylläpitäjän hyväksynnän ennen sisällön julkaisemista. Subscriber-rooli on kaikkein rajoitetuin, koska sillä ei ole sisällöntuotanto-oikeuksia lainkaan. Se on hyödyllinen esimerkiksi silloin, kun käyttäjien tulee pystyä kirjautumaan sisään saadakseen pääsyn tiettyyn sisältöön ilman muokkausoikeuksia. (Nair 2023.) (kuva 19).



Kuva 19. WordPressin vakio-oikeudet käyttäjille.

Ylläpitotileille on suositeltavaa aina määrittää nimimerkki ja käyttää sitä julkisesti. Tämä vaikeuttaa ylläpitotilin oikean kirjautumisnimen selvittämistä (kuva 20).



Kuva 20. WordPressin asetukset.

On tärkeää myös varmistaa, että kaikilla, joilla on pääsy WordPress-sivuston hallintapaneeliin, on vain ne käyttöoikeudet, joita heidän tehtävänsä edellyttävät. On hyvä luoda itselleen kaksi tiliä, joista toinen on järjestelmänvalvojan tasoinen tili, jossa on vaikeasti arvattava käyttäjänimi, ja toinen editorin tasoinen tili sisällön julkaisemista varten. On suositeltavaa käyttää pääasiallisesti editoritiliä kirjautumiseen, ja turvautua järjestelmänvalvojan tiliin vain, kun se on välttämätöntä. (Friedman 2014.)

Remove Dashboard Access on kevyt WordPress-lisäosa, jonka tarkoituksena on rajoittaa pääsyä sivuston hallintapaneeliin. Se mahdollistaa hallintapaneelin käytön estämisen käyttäjäroolien tai -oikeuksien perusteella. Käyttäjät, joilla ei ole määriteltyä oikeutta, ohjataan automaattisesti käyttäjän määrittelemään URL-osoitteeseen. Lisäosa tukee roolikohtaista tai kyvykkyyteen (capability) perustuvaa rajoittamista, ja se tarjoaa vaihtoehtoja esimerkiksi vain ylläpitäjien tai myös sisällöntuottajien pääsyn sallimiseen. (TrustedLogin 2025.) Lisäksi hallintapaneelin käyttöä voidaan entisestään turvata rajoittamalla sen saavutettavuutta vain tietyistä IP-osoitteista. Tämä toimii kuin vieraslista juhlissa, sillä kaikki muut estetään ja vain valtuutetut käyttäjät pääsevät sisään. (Nair 2023.)

6 Palvelinympäristön ja palveluntarjoajan rooli tietoturvassa

Pilvipalveluita käytettäessä kannattaa olla tarkkana, koska näitä palveluja käyttäessä osa tietoturvan vastuusta siirtyy toiselle taholle (ENISA 2009, 5). Hosting-palveluntarjoaja voi kuitenkin auttaa asiakasta tarjoamalla joko proaktiivista tai reaktiivista tukea sivuston tietoturvaan (Tajalizadehkhoob 2018, 1). Palveluntarjoajan käyttämät pilvipalvelinympäristöt voivat myös tarjota tukea hyökkäysten estämiseksi, sillä pilvipalvelinympäristössä voidaan nopeasti lisätä suojauskapasiteettia esimerkiksi DDoS-hyökkäyksen aikana (ENISA 2009, 4).

Laitteiston kehittyessä yhä useampi verkkosivusto voi sijaita yhdellä palvelimella. Tätä ratkaisua kutsutaan yleisesti jaetuksi hostingiksi (Shared Web Hosting), ja sillä on useita etuja, kuten edullinen hinta ja palvelinten tehon maksimaalinen hyödyntäminen (Arshad. Jalili. 2013, 1). Jos kuitenkin jaettujen palvelimien verkkosivustojen välillä ei ole kunnollista eristystä, antaa se hyökkääjille useita mahdollisuuksia hyödyntää erilaisia haavoittuvuuksia (Arshad. Jalili. 2013, 2). On suositeltavaa valita palveluntarjoaja, joka eristää sivustosi resurssit muista sivustoista, koska se tarjoaa perustason tietoturvaa (Needham 2022). On olemassa hosting-palveluntarjoajia, jotka ovat menneet konkurssiin jouduttuaan tietoturvaongelmiin. Kannattaa valita luotettava toimittaja ja maksaa hieman enemmän laadusta, sillä pitkällä aikavälillä laadukkaan hosting-palvelun valitseminen voi tulla halvemmaksi. (WordPress 2021.)

Euroopan Unionin alueella toimivien hosting-yhtiöiden tulee myös huomioida erilaisia lakiteknisiä seikkoja. Euroopan yleinen tietosuoja-asetus GDPR:n 33. artikla edellyttää, että ylläpitäjä ilmoittaa henkilötietojen tietoturvaloukkauksista valvontaviranomaiselle viipymättä ja viimeistään 72 tunnin kuluessa, mikäli riskit henkilöiden oikeuksille ovat koholla (GDPR 2016/679, EU 33 artikla). Suomessa on voimassa myös kansallinen tietosuojalaki (Tietosuojalaki 1050/2018), joka toimii GDPR:n rinnalla.

7 Tietoturvatestaukset

7.1 Haavoittuvuudet ja niiden löytäminen

Vaikka WordPressin ydin onkin tunnettu turvallisena, kuitenkin WordPress-sivustoja koitetaan murtaa useilla eri keinoilla, erityisesti laajennusten ja teemojen kautta. WPScanin raportista ilmenee, että vuonna 2023 WordPressin ekosysteemistä löydettiin noin 5271 haavoittuvuutta (WPScan 2024). Toisen raportin mukaan seuraavana vuonna löydettiin 7966 haavoittuvuutta (Patchstack 2025).

Kolme yleisintä haavoittuvuustyyppiä vuonna 2024 WordPress-ekosysteemissä olivat Cross-Site Scripting (XSS), Broken Access Control ja Cross Site Request Forgery (Patchstack 2025). Yhteensä nämä kolme kattaa jo noin 73,2 % haavoittuvuustyypeistä ja pelkästään XSS-hyökkäykset muodostivat noin 47,7 % kaikista uusista WordPressiin liittyvistä haavoittuvuuksista (Patchstack 2025).

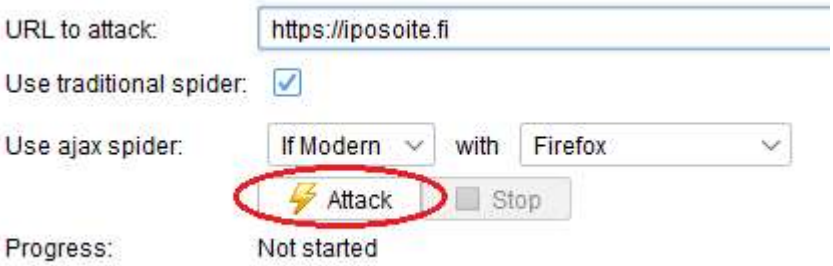
XSS-hyökkäyksessä hyökkääjä syöttää haitallisia skriptejä verkkosivuille, joita muut käyttäjät tarkastelevat. Tämä voi johtaa esimerkiksi käyttäjäistuntojen kaappaamiseen, sivuston vääristymiseen tai haittaohjelmien levittämiseen vierailijoille. (W3Schools, 2025.)

Hyvä tapa testata oman sivuston tietoturvaa on tehdä siihen tietoturvahyökkäys. Tietoturvatestauksen ja haavoittuvuuksien etsinnän tulee tapahtua eettisesti. Löydettyjä haavoittuvuuksia ei pidä hyödyntää ongelman todentamiseksi. Suomessa Traficomin Kyberturvallisuuskeskus ylläpitää kanavaa, johon voi ilmoittaa haavoittuvuuksia luottamuksellisesti. (Kyberturvallisuuskeskus 2023.) Tässä oppaassa käytyjen tunkeutumistestaustyökalujen lisäksi on useita muitakin vaihtoehtoja tarjolla, kuten Burp Suite ja Nikto.

7.2 Zed Attack Proxy

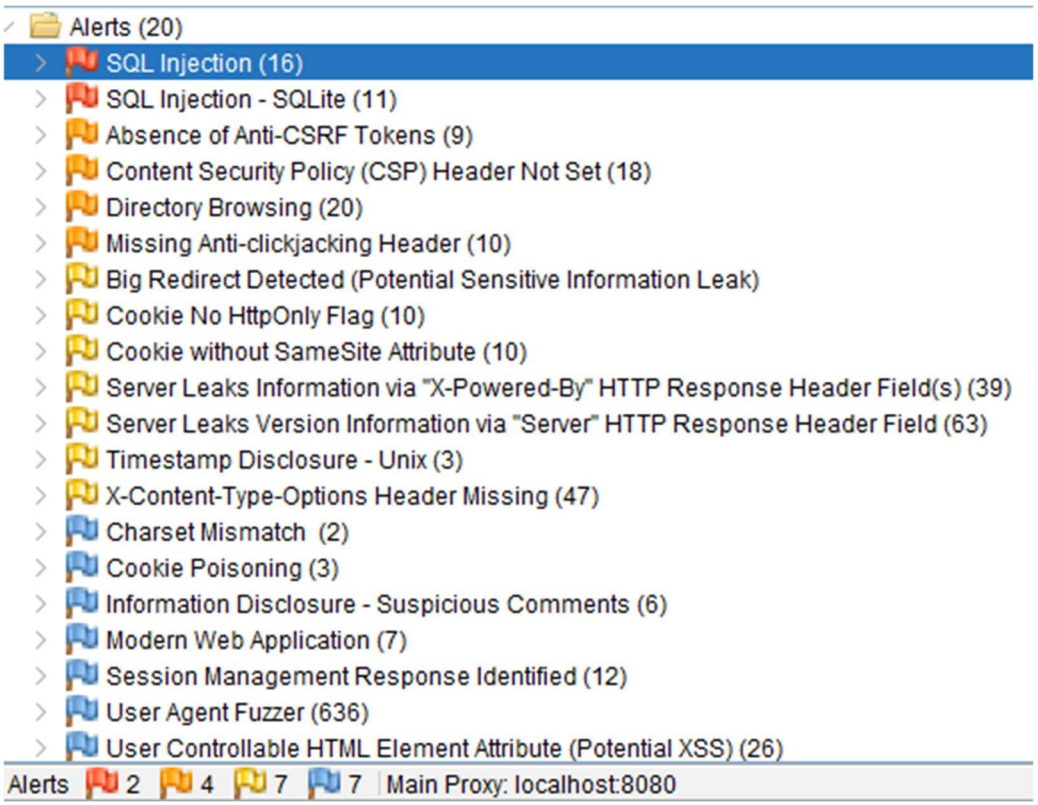
Tässä osiossa demonstroidaan WordPress-sivuston tunkeutumistestaamista käyttäen Zed Attack Proxy -sovellusta. Sovellus on saatavilla Linuxille sekä Windowsille. Esimerkeissä ajetaan ZAP-sovellusta Windows 10 -käyttöjärjestelmällä. ZAP voidaan asentaa Windows 11 -käyttöjärjestelmään syöttämällä komento ”winget install --id=ZAP.ZAP -e” PowerShell-sovellukseen.

Kun ZAP on asennettu, voidaan automaattinen hyökkäys suorittaa klikkaamalla ”Automated Scan” -nappia. Seuraavaksi ei tarvitse kuin syöttää sivuston URL ja klikata ”Attack”, niin ZAP suorittaa hyökkäyksen (kuva 21).



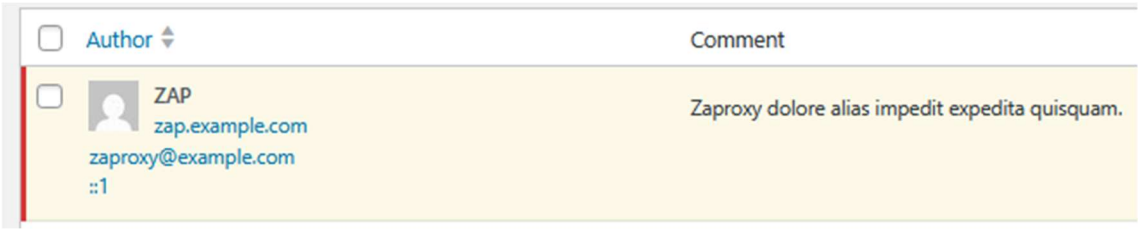
Kuva 21. Zed Attack Proxy -sovelluksen Automated Scan -näkymä.

ZAP käyttää oletuksena Microsoft Edge -selainta hyödykseen hyökkäyksessä. Edge saattaa avautua ja sammua monta kertaa skannauksen aikana ja se voi näyttäytyä ”ruudun vilkkumisena”. Hyökkäyksen etenemistä voidaan seurata ruudulle ilmestyvästä palkista. Kun hyökkäys on suoritettu, ilmestyy sovellukseen lista löydetyistä haavoittuvuuksista (kuva 22).



Kuva 22. Lista Zed Attack Proxyn löytämistä haavoittuvuuksista.

On myös hyvä huomioida, että ZAP jättää erilaisia jälkiä skannauksen aikana, kuten blogipostauksia ja -kommentteja. Ne voidaan poistaa, tai mikäli sivustosta on otettu varmuuskopio ennen tietoturvatestausta, voidaan sivuston aiempi tila palauttaa sen avulla. (kuva 23).



Kuva 23. Zed Attack Proxyn jättämä kommentti.

7.3 WPScan

WPScan löytyy oletuksena Kali Linux -käyttöjärjestelmästä. Se voidaan kuitenkin asentaa myös Windows-käyttöjärjestelmille käyttäen Ruby Gem -paketinhallintajärjestelmää komennolla ”gem install wpscan”, jos Ruby Gem on asennettu. Tässä esimerkissä käytetään kuitenkin Kali Linux -käyttöjärjestelmää.

Täyden raportin saamiseksi tarvitaan API-token, jonka saa ilmaiseksi rekisteröitymällä osoitteessa ”https://wpscan.com/register”. Kirjautunut käyttäjä voi katsoa API-tokeninsa osoitteesta ”https://wpscan.com/profile/”.

Ennen hyökkäysten suorittamista, WPScan kannattaa aina ensimmäiseksi päivittää komennolla ”Wpscan –update”. WPScanissa voidaan suorittaa useita hyökkäyksiä. Tässä esimerkissä skannataan haavoittuvien teemojen varalta suorittamalla komento ”wpscan --url https://iposoite/sisustuspalvelut/ -e vt --api-token MINUNTOKEN” (kuva 24).

Kuva 24. WPScan-tietoturvahyökkäys aloitettu.

Mikäli tarkoituksena on testata lisäosien haavoittuvuuksia, voidaan aiemmassa komennossa vaihtaa parametriksi vp (vulnerable plugins) vt:n (vulnerable themes) sijaan. Useita komentoja voidaan suorittaa samanaikaisesti erottamalla ne toisistaan pilkulla, esimerkiksi: vt, vp. Oletuksena skannauksen lopputuloksen tiedot tulevat samaan ikkunaan, jossa komento on ajettu. Tulokset voidaan tallentaa tekstitiedostoon lisäämällä komentoon parametri --output sekä tiedoston nimi ja tiedostomuoto. Esimerkiksi komennossa ”Wpscan --url https://esimerkki.fi --output tulokset.txt” skannauksen tulokset ohjataan tallennettavaksi tiedostoon nimeltä ”tulokset.txt”.

8 Tietoturvan ylläpito ja jatkuvuus

8.1 Tietoa ylläpitämisestä

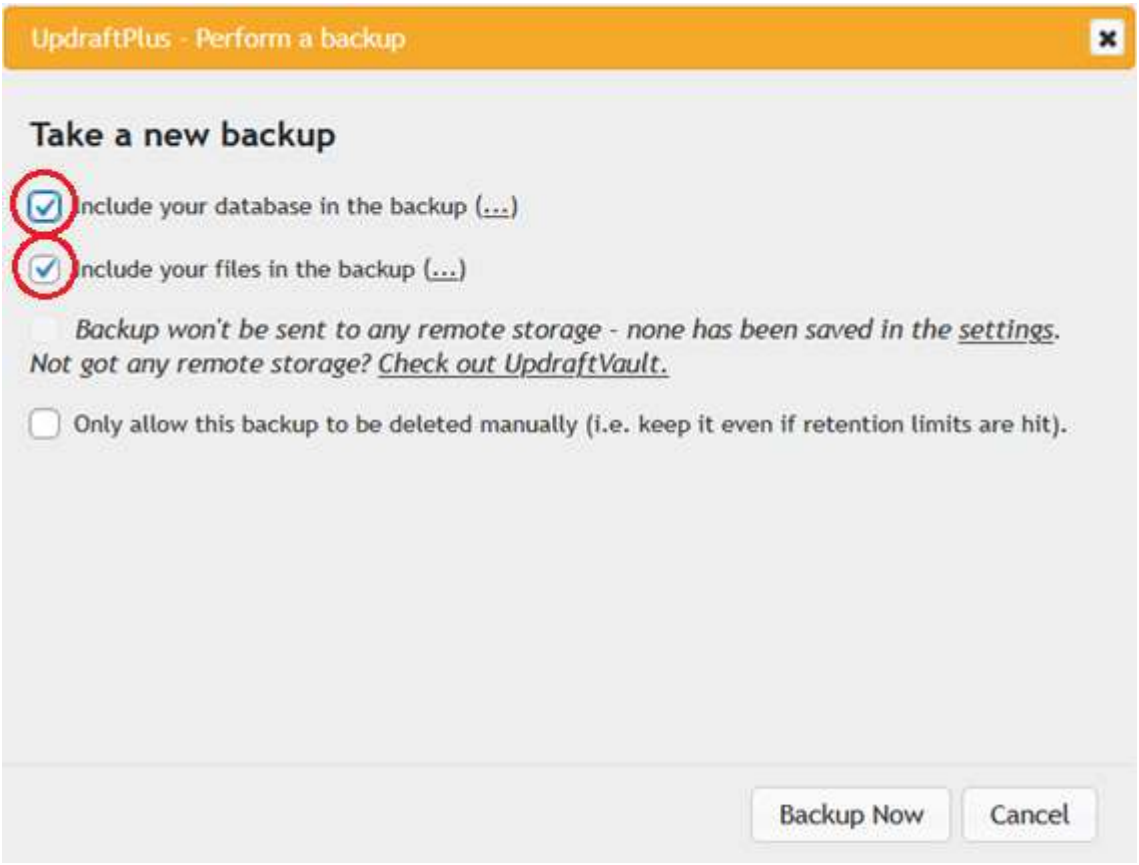
Kaikkien järjestelmien osien päivitykset on tehtävä uusimpien tietoturvaohjeistusten mukaisesti. Georgian osavaltion teknologiaviranomaisen julkaiseman standardin mukaan kaikki käyttäjätilit tulee käydä aika ajoin läpi ja varmistaa, että entiset työntekijät tai yhteistyökumppanit eivät säily käyttöoikeuksiaan järjestelmään. Ulkopuolisen tekemä turvallisuusauditointi tulisi tehdä vähintään kahden vuoden välein kaikille verkkosivustoille. Erityisen arkaluontoisia tietoja käsittelevät sivustot on syytä auditoida vielä useammin. Auditoinneissa tulee tunnistaa mahdolliset tietoturvahaavoittuvuudet, tarvittavat toimenpiteet avoimien ongelmien korjaamiseksi sekä aikataulu toimenpiteiden toteuttamiselle. (Georgia Technology Authority 2024.)

WordPress-sivustoa täytyy ylläpitää myös lakiteknisistä syistä. GDPR:n 32. artikla velvoittaa WordPress-sivuston ylläpitävää tahoa tekemään asianmukaiset tekniset ja organisatoriset toimenpiteet henkilötietojen käsittelyn turvaamiseksi. Lain tekstissä mainitaan, että on kyettävä takaamaan käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus. Lisäksi on Pystyttävä palauttamaan tiedot nopeasti mahdollisessa vikatilanteessa, sekä säännöllisesti testattava ja arvioitava suojatoimien tehokkuus (GDPR 2016/679, EU 32 artikla).

8.2 Varmuuskopiot

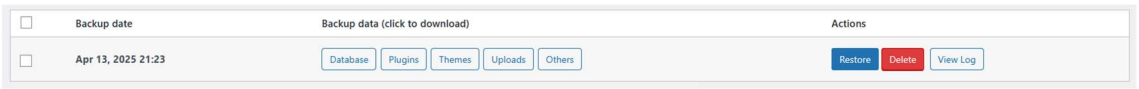
Varmuuskopiointi on hyvin keskeinen osa jatkuvuuden hallintaa. On huolehdittava säännöllisistä varmuuskopioista koko sivustosta, mukaan lukien tietokanta ja tiedostot. Parhaiden käytäntöjen mukaan varmistukset tulee tallentaa turvalliseen sijaintiin, joka on fyysisesti erillään tuotantopalvelimesta (Georgia Technology Authority 2024).

UpdraftPlus on ilmainen lisäosa, joka mahdollistaa varmuuskopioiden tekemisen WordPress-sivustoista. Kun UpdraftPlus on asennettu, voidaan varmuuskopio luoda klikkaamalla sen omasta hallintapaneelista sinistä ”Backup now” -nappia. Tämän jälkeen ohjelma kysyy, mitä varmuuskopioidaan. Kaksi ylintä vaihtoehtoa on syytä valita, jotta sekä tiedostot että tietokanta tulevat varmuuskopioon (kuva 25).



Kuva 25. Varmuuskopion tekeminen UpdraftPlussalla.

Varmuuskopion luonnin edistymistä voidaan seurata sinisestä palkista. Kun varmuuskopio on tehty, on tarjolla eri vaihtoehtoja. Klikkaamalla ”Others”, aukeaa lisää vaihtoehtoja. Aukeavalta näkymältä voidaan ladata varmuuskopio käyttäjän tietokoneelle klikkaamalla ”Download to your computer”. (kuva 26).

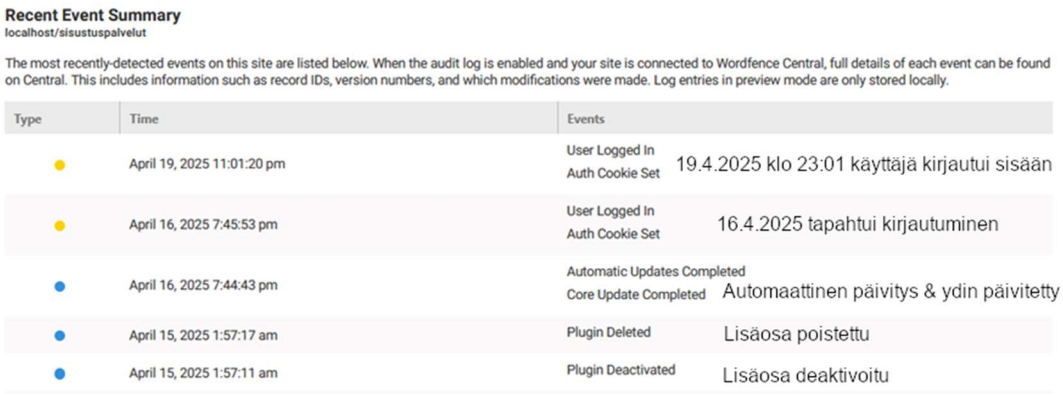


Kuva 26. Vaihtoehdot varmuuskopioinnin jälkeen.

8.3 Tietoturvalokit

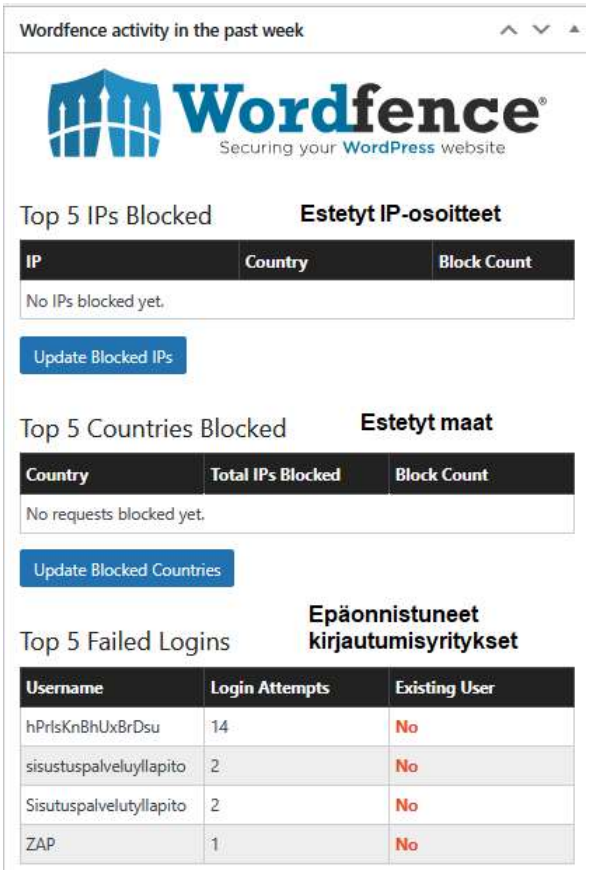
WP-sivuston ylläpitäjän on tärkeää myös monitoroida sivustoansa, eli säännöllisesti seurata sen toimintaa, suorituskykyä ja turvallisuuden tilaa. Voidaan esimerkiksi tarkastella lokeja tai tiedostoja, sillä hyökkäyksen tapahtuessa hyökkääjä jättää aina jälkiä (WordPress 2024).

Viimeaikaisia tapahtumia voidaan seurata WordFencen ”Audit Log” -välilehdeltä löytyvästä ”Recent Event Summary” -näkymästä. Tapahtumatiedot voivat auttaa seuraamaan, milloin ja kuka on ollut aktiivinen sivustolla. (kuva 27).



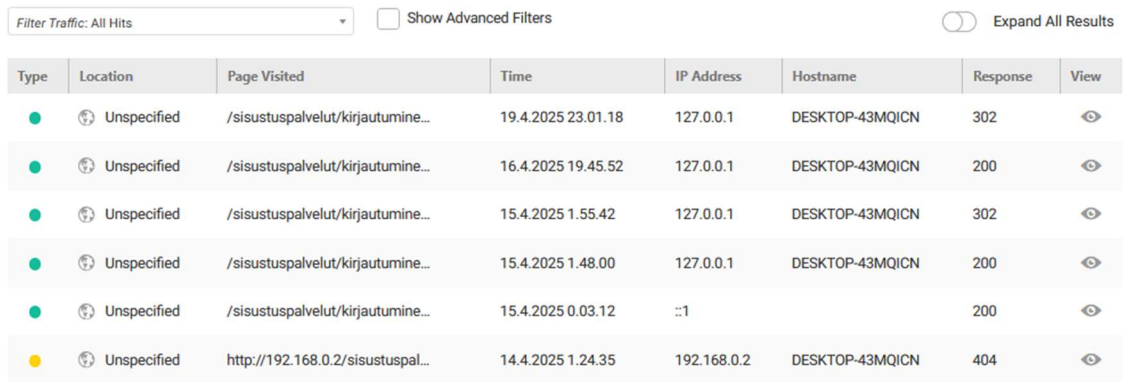
Kuva 27. WordFencen Recent Event Summary -näkymä.

WordFence tarjoaa myös viimeisen viikon katsauksen ”Wordfence activity the past week” -näkymässä. Tämä paneeli antaa nopean yleiskatsauksen sivuston mahdollisista uhkista ja tietoturvan tilasta. (kuva 28).



Kuva 28. WordFencen viikon tapahtumat.

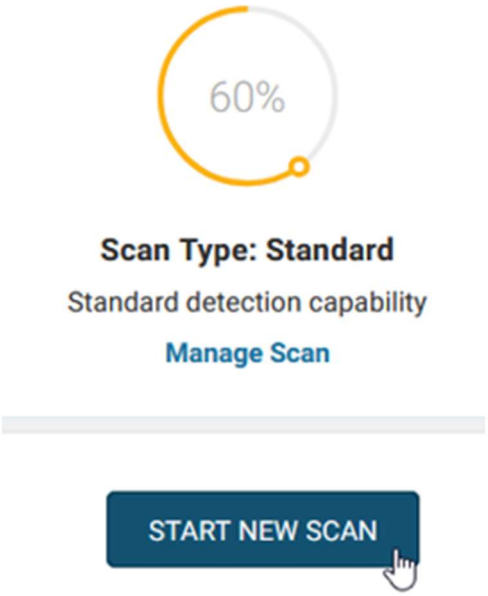
”Live Traffic” -välilehdeltä voidaan seurata toimintaa reaaliajassa. Tämän lokin avulla voidaan tunnistaa mahdollisia ongelmia, kuten väärin muotoiltuja pyyntöjä tai toistuvia epäonnistuneita kirjautumisia. (kuva 29).



Kuva 29. WordFencen Live Traffic -välilehti.

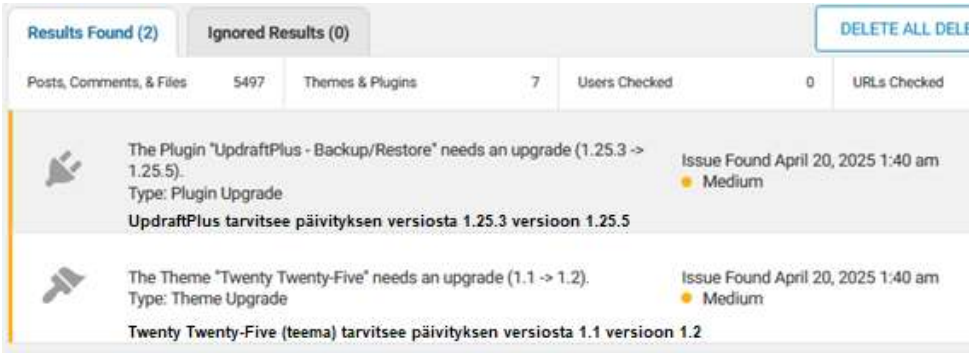
8.4 Tietoturvaskannaus

WordFence tarjoaa työkaluja, joilla voidaan tarkastaa WordPress-sivusto virusten ja mahdollisten haavoittuvuuksien varalta. Prosessi voidaan aloittaa siirtymällä hallintapaneelin vasemman reunan valikosta kohtaan ”WordFence” ja valitsemalla sieltä ”Scan”. ”START NEW SCAN” -napin klikkaaminen aloittaa tarkistuksen (kuva 30).



Kuva 30. WordFencen tietoturvaskannauksen aloittaminen.

Etenemistä voidaan seurata avautuvasta seurantapalkista. Tarkistus on valmis, kun näkymälle ilmestyy ”Scan Complete” -teksti. Tämän jälkeen tuloksia voidaan tarkastella avautuvalta näkymältä (kuva 31).

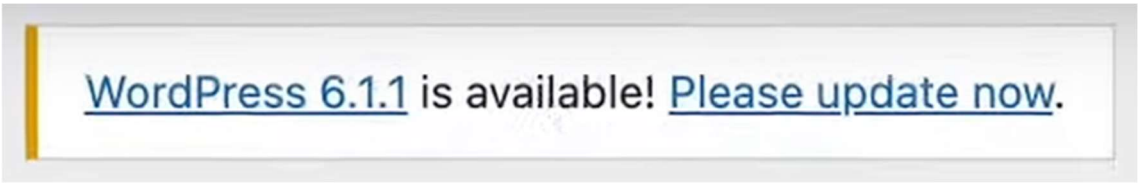


Kuva 31. Tietoturvaskannauksen tulokset.

8.5 Päivittäminen

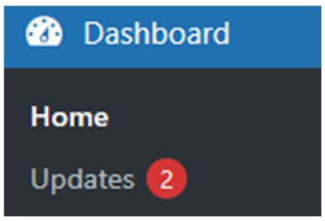
Huolimattomasti ylläpidetty sivusto on altis hyökkäyksille ja voi tulla sivuston omistajalle kalliiksi esimerkiksi maineen korjaamisen vuoksi (Kyberturvallisuuskeskus 2016, 5). Voidaan havaita, että suurin osa WordPress-sivustoista käyttää viimeisimpiä ydinversioita, sillä noin 87.4 % WordPress-sivustoista käyttää uusinta pääversiota 6.x, ja vain pieni osa (noin 0,3 %) käytti versiota 3.x. Kuitenkin noin 12.4% sivustoista käyttää versioita 4-5. (W3Techs 2025.) Voidaan siis todeta, että vanhentuneen WordPress-ytimen käyttäminen ei ole kovinkaan yleistä.

WordPress-sivuston ylläpidossa tulisi huolehtia säännöllisistä päivityksistä. Päivittämisen pystyy hoitamaan usealla eri tavalla, myös automaattisesti, jos käytössä on WordPressin versio 3.7 tai uudempi (WordPress 2024). WordPress-sivuston päivityksen yhteydessä saattaa kuitenkin ilmetä ongelmia, jotka voivat jopa rikkoa sivuston. Siksi onkin suositeltavaa tehdä päivitys manuaalisesti ja olla paikan päällä, jotta mahdollisiin ongelmatilanteisiin voidaan reagoida nopeasti ja tehokkaasti. Automaattiset päivitykset voidaan aktivoida klikkaamalla välilehdeltä ”Enable auto-updates”. Kun WordPressin ytimeen on tarjolla päivityksiä, tulee admin-paneeliin ilmoitus, josta klikkaammalla ”Please update now.” -tekstiä voidaan ladata uusimmat päivitykset (kuva 32).



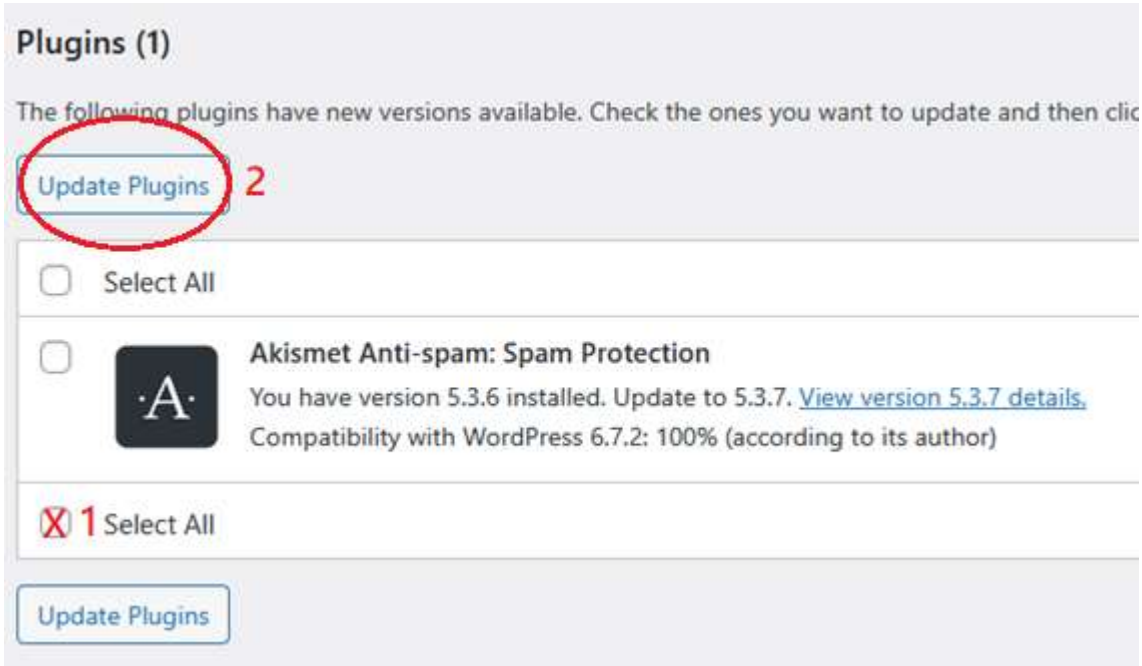
Kuva 32. Ilmoitus WordPress version 6.1.1 päivityksestä.

Päivitykset voidaan tarkistaa siirtymällä hallintapaneelin vasemman reunan valikosta kohtaan ”Dashboard” ja valitsemalla sieltä ”Updates”. ”Updates” -tekstin vieressä näkyy punainen ympyrä, jos päivityksiä on tarjolla (kuva 33).



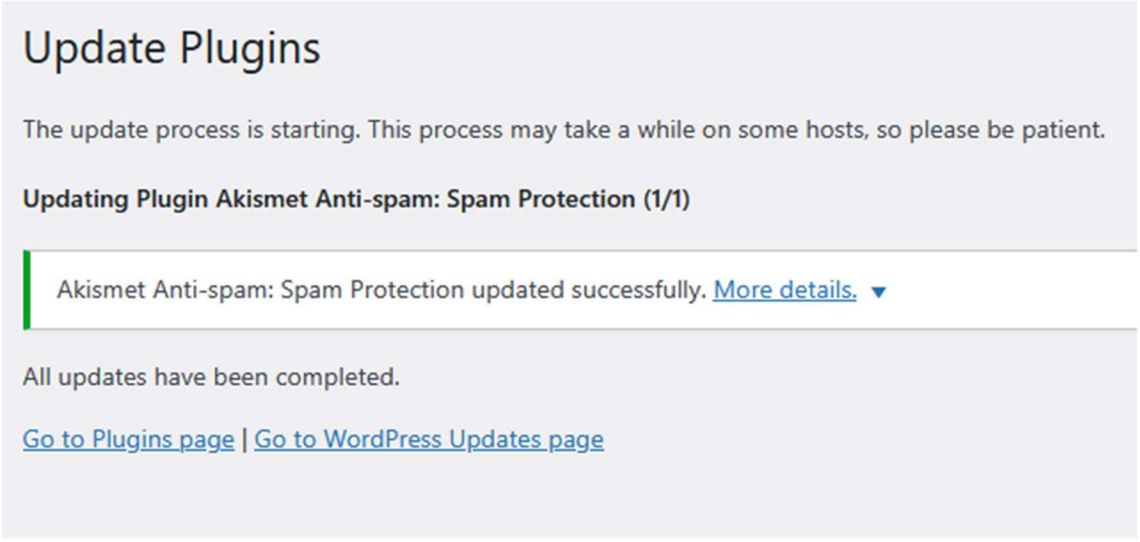
Kuva 33. 2 uutta päivitystä tarjolla.

Updates välilehdeltä löytyy myös tieto siitä, jos sivustolla on jo uusin WordPressin versio. Esimerkiksi jos sivusto käyttää jo uusinta WordPressin versiota, lukee välilehdellä ”You have the latest version of WordPress.”. Samalta välilehdeltä voidaan myös päivittää teemat sekä lisäosat. Päivittääkseen lisäosat tai teemat, tulee etsiä kohta ”Plugins” (lisäosat) tai ”Themes” (teemat), laittaa rasti valintaruutuun ”Select All” (valitse kaikki) ja klikata ”Update Plugins” (päivitä lisäosat) tai ”Update Themes” (päivitä teemat). Nämä toimenpiteet päivittävät kaikki lisäosat tai teemat (kuva 34).



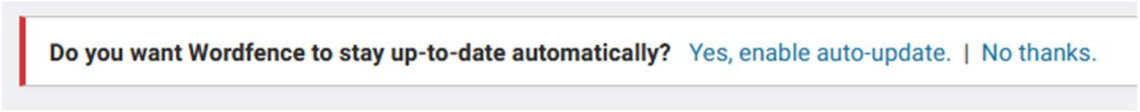
Kuva 34. WordPressin lisäosien päivittäminen.

Päivitys on onnistunut, jos välilehdelle ilmestyy teksti ”All updates have been completed”. Myös vihreä väri kertoo onnistuneesta päivityksestä (kuva 35).



Kuva 35. Onnistunut päivitys.

Lisäosat ja teemat voivat myös antaa omia ilmoituksia päivityksistä admin-paneeliin, joita voidaan käyttää hyödyksi (kuva 36).



Kuva 36. WordFencen ilmoitus automaattisista päivityksistä.

9 Tulokset

Opinnäytetyössä toteutettiin sekä teoreettinen kirjallisuuskatsaus että toiminnallinen osuus. Toiminnallisessa osuudessa keskityttiin erilaisten tietoturvaratkaisujen implementointiin WordPress-sivustolle ja siinä hyödynnettiin automatisoituja testityökaluja, kuten OWASP ZAP ja WPScan, joilla kartoitettiin sivuston haavoittuvuuksia. Työssä käsiteltiin myös laajasti ylläpitoon, jatkuvuuteen ja palvelinympäristöihin liittyviä keskeisiä asioita. Työmenetelminä käytettiin kokeellista testausta ja järjestelmällistä dokumentointia. Kaikki asennus- ja päivitysvaiheet tallennettiin kuvakaappauksin ja mahdollisten ongelmien ratkaisut kirjattiin selkeästi.

Tietoturvaa parantamaan otettiin käyttöön neljä lisäosaa, jotka yhdessä kattoivat keskeiset tietoturvan osa-alueet. Erityisen keskeiseksi osoittautui WordFence-lisäosa, jonka tarjoamat suojaustoiminnot ovat merkittävä lisä WordPressin perusturvallisuuteen. Havaittiin, että vaikka WordPressin ydin on sinänsä turvallinen, se edellyttää lisäkonfigurointia tai ulkopuolisten lisäosien tukea tietoturvan varmistamiseksi.

Työn tuloksena syntyi tietoturvaopas sekä WordPress-sivusto toimeksiantajan tarpeisiin. Sivustolle on toteutettu konkreettiset tietoturvatoimenpiteet, jotka vähentävät merkittävästi tietomurtojen riskiä ja tukevat yrityksen luotettavaa brändikuvaa. Toimeksiantajalle toimitettu kokonaisuus sisältää valmiit turvallisuuskonfiguraatiot, minkä ansiosta yrityksen ei tarvitse itse aloittaa tietoturvatyötä alusta.

10 Pohdinta

Opinnäytetyön toteutus onnistui kokonaisuutena hyvin, ja sen tulokset vastaavat asetettuja tavoitteita. Kirjallisuuskatsaus tarjosi vahvan perustan käytännön työn toteutukselle, ja valitut työmenetelmät kuten automatisoidut testityökalut ja järjestelmällinen dokumentointi osoittautuivat toimiviksi.

WordPressin tietoturva rakentuu vahvasti kolmansien osapuolten lisäosien varaan, mikä herättää kysymyksiä ulkoistetun tietoturvan riskeistä. Esimerkiksi lisäosan sisältämä uusi hyökkäyspinta voi itsessään muodostaa uhan, ellei sen luotettavuutta arvioida kriittisesti. Tämä havainnollistaa tarvetta jatkuvaan seuranta- ja päivitystyöhön. Tietoturva ei ole kertaluonteinen toimenpide, vaan jatkuva prosessi.

Myös taloudelliset näkökulmat nousivat esiin. Kehittyneempien suojausominaisuuksien hyödyntäminen, kuten WordFencen maksulliset lisenssit, saattavat muodostaa merkittävän kuluerän pienelle yritykselle. Tämän vuoksi tietoturvan budjetointi ja lisäosien valinta vaativat tarkkaa harkintaa.

Yksi keskeinen havainto on, että merkittävä osa WordPress-sivustoihin kohdistuvista hyökkäyksistä on automatisoituja bottien toteuttamia yrityksiä, joiden tavoitteena on löytää helposti haavoittuvia kohteita. Tämän vuoksi jo perustason tietoturvatoimenpiteet voivat tehokkaasti torjua suuren osan näistä hyökkäyksistä.

Ammatillisesti työ tarjosi tekijälleen syvällistä oppia WordPressin rakenteesta, tietoturvan osa-alueista sekä projektityöskentelystä toimeksiantajan kanssa. Prosessin aikana karttunut osaaminen on helposti siirrettävissä myös muihin verkkopalveluiden kehitys- ja suojaustehtäviin.

Tulevaisuudessa aihetta voisi laajentaa tutkimalla eri sisällönhallintajärjestelmien tietoturvaa vertailevasti tai tarkastelemalla lisäosien eettisiä ja teknisiä riskejä syvemmin. WordPress-sivustojen tietoturva on tärkeä osa nykyaikaista liiketoimintaa, ja sen merkitys korostuu entisestään digitalisoituvassa yhteiskunnassa.

Lähteet

Arshad, S. Jalili, R. 2013. A Comprehensive Approach to Abusing Locality in Shared Web Hosting Servers. https://www.researchgate.net/publication/261199704_A_Comprehensive_Approach_to_Abusing_Locality_in_Shared_Web_Hosting_Servers. 25.04.2025.

Alkan, C. 2023. Malware Madness 1/2: Why everything you know about your WordPress Malware Scanner is wrong. https://snicco.io/blog/wordpress-malware-scanner. 30.03.2025.

ENISA 2009. Cloud computing: benefits, risks and recommendations for information security. https://www.enisa.europa.eu/sites/default/files/all_files/ENISA%20-%20Cloud%20Computing%20-%20final.pdf. 24.03.2025.

Friedman, J. 2014. WordPress Security. Berkeley: Peachpit Press. O'Reilly.

GDPR (2016/679, EU).

Georgia Technology Authority 2019. Digital Security Standard (SS-19-002). https://gta-psg.georgia.gov/psg/digital-security-standard-ss-19-002. 24.03.2025.

Goodchild, P. 2023. The Role of User Education in WordPress Security. https://getshieldsecurity.com/blog/role-user-education-wordpress-security. 30.03.2025.

Google. 2025. What is reCAPTCHA?. https://support.google.com/recaptcha/answer/6080904. 20.05.2025.

Hänninen, P. 2025. Tietotekniikka. Tampere: Tammertekniikka.

Kyberturvallisuuskeskus 2016. Verkkosivujesi pimeä puoli: ohjeita sisällönhallintajärjestelmien kyberuhkien torjumiseksi. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Sisallonhallintajarjestelmien_kyberuhkia.pdf. 24.03.2025.

Kyberturvallisuuskeskus 2023. Haavoittuvuudet - miten niistä ilmoitetaan oikein. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuudet-miten-niista-ilmoitetaan-oikein. 24.03.2025.

Martin, B. 2022. The Case for 2FA by Default for WordPress. https://blog.sucuri.net/2022/04/the-case-for-2fa-by-default-for-wordpress. 24.03.2025.

Needham, T. 2022. WordPress VIP's Website Security Best Practices. https://wpvip.com/blog/wordpress-security-best-practices/. 30.03.2025.

Nair, S. 2023. 4 Ways to Restrict Admin Access On Your WordPress Site. https://www.malcare.com/blog/restrict-admin-access-on-wordpress/. 18.05.2025.

Patchstack 2025. State of WordPress Security in 2025. https://patchstack.com/whitepaper/state-of-wordpress-security-in-2025/. 24.03.2025.

Pisani, N. 2024. 18 WordPress Security Statistics for 2024. https://wcanvas.com/blog/18-wordpress-security-statistics-for-2023. 30.03.2025.

Seravo 2024. Tarpeettomat, kielletyt ja haitalliset lisäosat. https://help.seravo.fi/article/314-tarpeettomat-kielletyt-ja-haitalliset-lisaosat. 24.03.2025.

Sucuri 2022. 2021 Website Threat Research Report. https://sucuri.net/reports/2021-hacked-website-report. 24.03.2025.
Sucuri 2024. 2023 Hacked Website & Malware Threat Report. https://sucuri.net/wp-content/uploads/2024/06/2023-Hacked-Website-Malware-Threat-Report.pdf. 25.03.2025.
Tajalizadehkhoob, S. 2018. The Role of Hosting Providers in Web Security: Understanding and Improving Security Incentives and Performance via Analysis of Large-scale Incident Data. https://repository.tudelft.nl/file/File_3357b179-c422-4244-ab4f-fc85af089840?preview=1. 24.03.2025.
Tietosuojalaki 1050/2018.
TrustedLogin. 2025. https://wordpress.org/plugins/remove-dashboard-access-for-non-admins. 18.05.2025.
W3Schools. 2025. Cyber Security Web Application Attacks. https://www.w3schools.com/cybersecurity/cybersecurity_web_applications_attacks.php. 24.03.2025.
W3Techs 2025. Usage Statistics and Market Share of WordPress. https://w3techs.com/technologies/details/cm-wordpress. 24.03.2025.
WordPress. 2024. Hardening WordPress. https://developer.wordpress.org/advanced-administration/security/hardening. 25.03.2025.
WordPress. 2025. How to choose the right hosting for your WordPress website. https://learn.wordpress.org/tutorial/how-to-choose-the-right-hosting-for-your-wordpress-website. 26.04.2025.
WPScan. 2024. WPScan 2024 Website Threat Report. https://wpscan.com/2024-website-threat-report/. 25.03.2025.