Sisältö

1. Johdanto

{URL REDACTED}-verkkosivuston tarkastustilaus vastaanotettiin 22.4.2024 klo 14.00 osoitteesta {REDACTED EMAIL ADDRESS}.

Alla olevat tulokset ovat nykyisen verkkosivuston, näkyvän koodin ja nopeustestityökalujen tutkimustuloksia, joiden avulla saatiin peruskuva verkkosivuston turvallisuudesta ja teknisestä laadusta. Tässä tarkastuksessa ei käytetty aktiivisia skannaustekniikoita.

Tarkastus suoritettiin Lisa-Marie Karvosen toimesta.

Tarkastus tehtiin ISO 19011:2018 -standardin mukaisesti.

2. Riskien yleiskatsaus

Tässä taulukossa on esitetty ongelmien lukumäärä kussakin luokassa. Taulukko on myös koodattu vakavuustasolle, olipa kyseessä KORKEA riski, KESKITASOINEN riski tai MATALA riski.

Riski			
Tyyppi	Korkea	Keskitasoinen	Matala
Tietoturva	11	3	2
Yksityisyys	-	1	1
SEO/Nopeus	-	2	2
Käytettävyys	-	1	1

3. Löydökset

3.1 Perustiedot

Nimipalvelimet	{REDACTED NAMESERVER} {REDACTED NAMESERVER}
Hosting	IP: {REDACTED IP} {REDACTED URL}
Palvelin	Apache
Tietokanta	MySQL/MariaDB
Alusta	WordPress
Teema	{REDACTED THEME NAME AND VERSION} {REDACTED CHILD THEME INFO}

3.2 Turvallisuuslöydökset

Riski	Kohde
Korkea	Vanhemman teeman uusin versio on 3.2.4 ja versio sivustolla on 2.4.8. Vanhempi teema tulisi pitää ajan tasalla. On parasta tehdä pieniä päivityksiä usein, sen sijaan että päivittäisit teeman harvoin, jotta se ei hajoaisi helposti.
Korkea	Palvelimesi vuotaa hakemistotietoja ja tiedostonimiä osoitteesta {URL REDACTED}. Sinun tulee poistaa hakemiston listaus kaikista hakemistoistasi.
Korkea	WordPressin versio näkyy 5.8.9:nä, joka julkaistiin 30. tammikuuta 2024. Nykyinen versio on 6.5.2. On suositeltavaa pitää WordPressin ydinohjelmisto ajan tasalla heti, kun uusia julkaisuja on saatavilla.
Korkea	Palvelimen otsikot eivät suojaa sivustoasi lainkaan. Voit nähdä tulokset täältä: {URL REDACTED}

Korkea	Contact Form 7 -lisäosan versio on 5.4.2 ja uusin versio on 5.9.3. On suositeltavaa pitää kaikki lisäosat ajan tasalla, erityisesti lisäosat, jotka käsittelevät käyttäjän syöttöä (lomakkeiden lisäosat, verkkokauppa ratkaisut jne.).
Korkea	Cookie Law Info -lisäosa on vanhentunut. Asennettu versio on 2.0.6, mutta uusin on 3.2.1. On suositeltavaa pitää kaikki lisäosat ajan tasalla.
Korkea	Js_composer -lisäosa on todennäköisesti vanhentunut. Näyttää siltä, että versio on 6.7.0, kun taas uusin versio on 7.5. Passiivinen havainnointi käytössä.
Korkea	LayerSlider -lisäosa on vanhentunut. Kotisivun HTML-meta-generaattoritunnisteet näyttävät Layerslider 6.11.9:n. LayerSliderin uusin versio on 7.10.1. LayerSlider on maksullinen lisäosa, ja sen lisenssin hankkiminen ja ajan tasalla pitäminen on suositeltavaa.
Korkea	WP-Rocket -lisäosa näyttää olevan versio 3.7.2. Uusin versio on 3.15.10. Tämä tulisi pitää ajan tasalla kuten muutkin lisäosat.
Korkea	Kun WordPress-ydin ja useat lisäosat näyttävät olevan vanhentuneita, on suuri mahdollisuus, että muita lisäosia, joita ei löydetty passiivisen skannauksen avulla, ovat myös vanhentuneita. On suositeltavaa päivittää kaikki lisäosat, ydin ja teemat.
Korkea	Kirjautuminen ei ole suojattu. Yritettäessä käyttäjänimeä 'admin', sivusto kertoo, ettei käyttäjää nimeltä admin ole, ja kehottaa yrittämään sähköpostiosoitetta. Ihanteellisesti WordPress ei tulisi paljastaa mitään, ja parhaissa tapauksissa sen tulisi estää käyttäjä, joka yrittää käyttää ilmeistä käyttäjänimeä, kuten admin. Wordfence on hyvä lisäosa kirjautumisen suojaamiseen ja sillä on myös paljon muita ominaisuuksia.
Keskitasoinen	Koodissa on tietovuotoja. Esimerkiksi Layerslider, revslider, WP-versio, WP Bakery, Redux 4.3.1 jne. Ne kaikki vuotavat versioita, jotka antavat kriittistä tietoa boteille ja hyökkääjille sivustosi haavoittuvuuksista.

	Tämäntyyppinen vuoto on yleistä käytettäessä valmiita teemoja ja lisäosia, mutta sivustollasi on vielä enemmän vuotoja kuin tavallisesti.
Keskitasoinen	Joitakin muita löydettyjä lisäosia olivat massive-elements-for-wpbakery ja mpc-massive. Näiden lisäosien versioita ei voitu määrittää, mutta nämä ovat lisäosia, jotka löytyivät passiivisen skannauksen tuloksena, mikä tarkoittaa, että hallintapaneelissa on todennäköisesti paljon enemmän lisäosia. Lisäksi revslider on vanhentunut. Sivustosi todennäköisesti ei tarvitse kahta eri liukusäädin-lisäosaa. On suositeltavaa poistaa niin monta lisäosaa kuin mahdollista, jotta hyökkäyspinta-ala pienenee. Mitä enemmän lisäosia, sitä enemmän aluetta bottien käyttöön.
Keskitasoinen	Saattaisit harkita WP-cronin asettamista sisäiseen suoritukseen. Tällä hetkellä sitä voidaan suorittaa ulkoisesti osoitteessa {URL REDACTED}. Tämä parantaisi suorituskykyä.

Matala	Teidän robots.txt sallii kaikkien sisältöjen indeksoinnin. On suositeltavaa estää tiettyjen kansioiden, kuten wp-admin, indeksointipääsy. Yoast SEO auttaisi tässä, mutta esimerkki olisi:
	
	`User-agent: *`
	`Disallow: /wp-admin/`
	`Disallow: /wp-login.php`

Matala	Saattaisit haluta estää pääsyn XML-RPC:hen osoitteessa {URL REDACTED}, jos et käytä mitään etäjulkaisutoimintoja. Tämä tiukentaa turvallisuutta. Lisätietoja löydät osoitteesta: https://www.hostinger.com/tutorials/xmlrpc-wordpress. Toinen tehokas tapa estää se on Cloudflaren kautta.

3.3 Yksityisyyslöydökset

Riski	Kohde
Keskitasoinen	Sivusto käyttää Google Fontsia. Google Fonts ei ole täysin GDPR-yhteensopiva. Ratkaisu on itse isännöidä fontteja lataamalla ne palvelimellesi ja päivittämällä teeman koodi. Tämä auttaisi myös verkkosivuston nopeutta ja vähentäisi sivuston viiveiden riskiä.
Matala	Mahdollinen tietovuoto. Sivustosi kartta (sitemap) saattaa vuotaa käyttäjänimiä ja nimiä osoitteessa: {URL REDACTED}. On hyvä idea sulkea pois automaattinen käyttäjänimien luetteloiminen.

3.4 SEO/nopeuslöydökset

Riski	Kohde
Keskitasoinen	GTMetrix antoi sivustollesi testituloksen F (testaus Kanadasta). Latausaika oli 6.2 sekuntia.
Keskitasoinen	Sivustosi sai Pingdomilta (testaus Saksasta) nopeustestin tuloksen B, mikä on OK, mutta sitä voitaisiin parantaa. Sivun koko oli edelleen 2,5 MB ja siinä oli 88 pyyntöä, joista 15 oli ulkopuolisilta hallitsemattomilta verkkotunnuksilta, ja hitain niistä oli Google Fonts. On suositeltavaa tarjota mahdollisimman paljon sisältöä omasta verkkotunnuksestasi nopeuden ja turvallisuuden vuoksi.
Matala	Teemasi lataa paljon erilaisia fontteja sekä Google Fontsista että myös teeman hakemistosta. Tämä voitaisiin siivota, jotta sivusto toimisi nopeammin.
Matala	Välimuistin käyttöä voitaisiin optimoida. Sinulla on CDN käytössä, mutta saatat haluta harkita Cloudflaren DDoS-suojan ja nopeuden parannusten lisäetuja.

3.5 Käytettävyystulokset

Riski	Kohde
Keskitasoinen	Verkkosivuston valikot eivät tarjoa riittävästi kontrastia taustan kanssa. Punainen hover-valikossa heikentää kontrastia entisestään.
Matala	Sivuston logo on epäselvä korkearesoluutioisissa laitteissa, ja vieritettäessä elementit ovat valkoisen taustan päällä, mikä antaa sivustolle nykivän ilmeen. Kaikki nämä visuaaliset havainnot ovat tietysti makuasia, mutta sisältö, joka on keskitetty ja sitten vasemmalle tasattu ja sitten taas keskitetty, voi olla hyvin hämmentävää käyttäjille. Joissakin elementeissä on liian vähän tilaa, kun taas toisten välissä on liikaa tilaa, mikä vaikeuttaa käytettävyyttä useimmille käyttäjille. Kontrastiongelmat tarkoittavat, että sivusto ei ole saavutettavissa kävijöille, joilla on näköongelmia, esimerkiksi. On suositeltavaa yksinkertaistaa elementtejä ja antaa niille tilaa sekä hillitä joitain värejä, jotta sivustolle saadaan yhtenäisempi ilme. Esimerkki tästä on nähtävissä Liitteessä 2 alla.

3.6 Muita löydöksiä

Riski	Kohde
Ei	Verkkosivustosi kaatui testauksen aikana. Todennäköisesti isäntä esti testaus-IP-osoitteemme, koska sivusto toimi matkapuhelinverkosta ja osoitteesta: {URL REDACTED} Tämä on hyvä asia. Se tarkoittaa, että hostaus on ainakin hieman proaktiivinen, jos joku suorittaa skannauksia verkkosivustoosi. Emme käyttäneet mitään aktiivista skannausta tai penetraatiotestausta sivustollasi, mutta jopa passiiviset skannaukset voivat varoittaa WAF:ää mahdollisista ongelmista.
Ei	Sivustollasi ei näytä tallennettavan muita evästeitä kuin Cookie Law -lisäosan evästeet, mikä on hyvä asia. Testasimme myös CookieBot-skannerilla varmuuden vuoksi, ja näyttää hyvältä. Liitteenä on kuvankaappaus, Liite 1 alla.

3.7 Liitteet

Liite 1: CookieBot-skannerin tulokset osoittavat, että sivusto on matalan riskin.
{ IMAGE REMOVED }

Liite 2: Esimerkki etusivusta, kun se muuttuu sekavaksi pääkohdan alueella.
{ IMAGE REMOVED }

Liite 3: GTMetrix-tuloksia voitaisiin parantaa, mutta testaus tehtiin Kanadasta, joten se vaikuttaa nopeuteen luonnollisesti.
{ IMAGE REMOVED }

4. Yhteenveto ja Lisätietoja

Toivomme, että löydät tämän tarkastustiedon hyödylliseksi verkkosivustosi turvaamisessa. Jos sinulla on kysyttävää tästä tarkastuksesta tai sen löydöksistä, tai haluat meidän hoitavan nämä asiat puolestasi, älä epäröi ottaa meihin yhteyttä alla olevilla yhteystiedoilla.

Lisa-Marie Karvonen
Website Security Specialist

050 3139531
lisa@wpensure.com