Contents

[WordPress 1](#_Toc51241654)

[Asennus 1](#_Toc51241655)

[Tietokannan asentaminen ja luominen 1](#_Toc51241656)

[WordPress asennus 3](#_Toc51241657)

[WordPress käyttöönotto 4](#_Toc51241658)

[WordPressin murtaminen 8](#_Toc51241659)

[WordPress suojaaminen 9](#_Toc51241660)

[Muita tärkeitä WordPress asetuksia 11](#_Toc51241661)

# WordPress

WordPress on sisällönjulkaisujärjestelmä, jolla pystyy helposti tekemään nettisivuja ilman koodausta. Sen avulla saa nopeasti pystyyn esimerkiksi yksinkertaisen nettisivun yritykselle, verkkokaupan tai blogin. Koska WordPress on laajassa käytössä siihen kohdistuu myös paljon tietoturvauhkia.

Tässä ohjeessa käydään läpi WordPressin asennus Debian palvelimelle, perusasetusten tekoa ja tietoturva uhkia.

## Asennus

Ensin asennetaan apache2, PHP ja sen lisäosia. Kiinnitä huomioita välilyönteihin. Lopussa oleva -y tekee sen ettei jokainen asennus kysyy erikseen saadaanko se asentaa.

**apt install apache2 php7.3 libapache2-mod-php7.3 php7.3-common php7.3-mbstring php7.3-xmlrpc php7.3-soap php7.3-gd php7.3-xml php7.3-intl php7.3-mysql php7.3-cli php7.3-ldap php7.3-zip php7.3-curl -y**

## Tietokannan asentaminen ja luominen

Tämän jälkeen asennetaan vielä mariadb

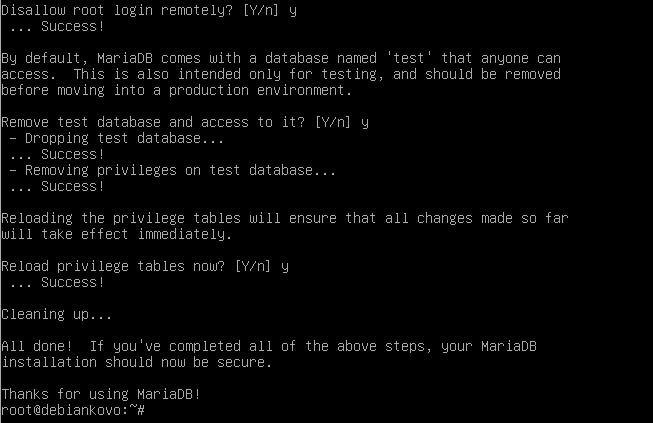
**apt install mariadb-server**

Tämän jälkeen ota mariadb käyttöön.

**mysql\_secure\_installation**

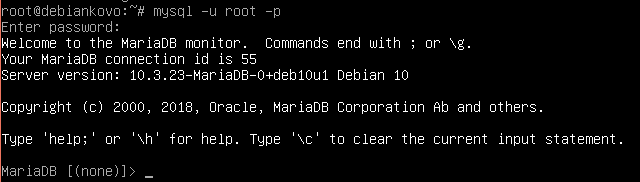
Tämän aikana aseta salasanaksi jokin jonka muistat. Esim: Sala1234

Muihin kohtiin voit vasta y

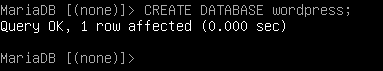


Seuraavaksi muodostetaan yhteys MariaDB ohjelmaan:

**mysql -u root -p**

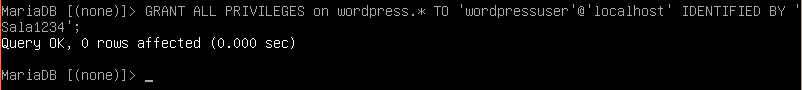
Tämä kysyy salasanaa jonka asetit aikaisemmassa vaiheessa.

Luodaan wordpress niminen tietokanta:



Luodaan uusi käyttäjä ja annetaan sille oikeudet käyttää wordpress nimistä tietokantaa joka sijaitsee localhostissa (eli tällä palvelimella). Käyttäjän salasana on Sala1234

**GRANT ALL PRIVILEGES on wordpress.\* TO 'wordpress\_user'@'localhost' IDENTIFIED BY ‘Sala1234';**

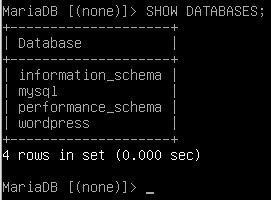


Tämä komento vaaditaan joskus, jotta käyttäjän asetukset tulevat voimaan:

**FLUSH PRIVILEGES;**



Tällä komennolla voit katsoa mitä tietokantoja palvelimella on.



**EXIT** komennolla pääset pois MariaDB ohjelmasta.



Nyt meillä on tietokanta luotuna. Seuraavaksi ladataan ja asennetaan itse WordPress

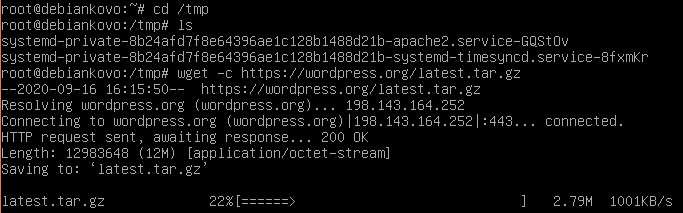
## WordPress asennus

Mennään /tmp hakemistoon ja tänne ladataan WordPressin asennustiedostot wordpressin sivuilta. Wordpressiä ei saa asennettua käyttämällä apt komentoja.

**wget -c https://wordpress.org/latest.tar.gz**

wget on ohjelmalla jolla ladataan tiedostoja netistä.

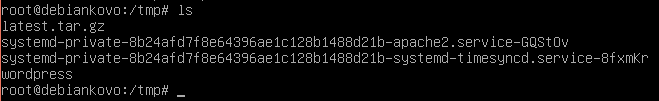
<https://wordpress.org/latest.tar.gz> on osoite josta wordpressin viimeisin asennuspaketti löytyy.



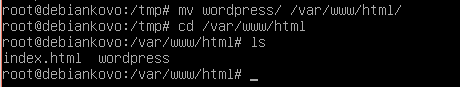
Latauksen jälkeen pakattu kansio puretaan. tar on komento jolla puretaan kansioita linuxissa.



Puretut kansiot tulevat /tmp kansion sisälle wordpress kansioon.

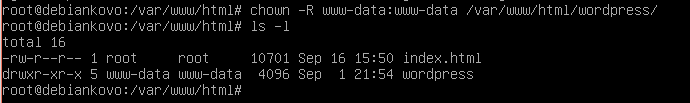


Siirretään wordpress kansio apache2 oletushakemistoon eli /var/www/html kansion sisälle



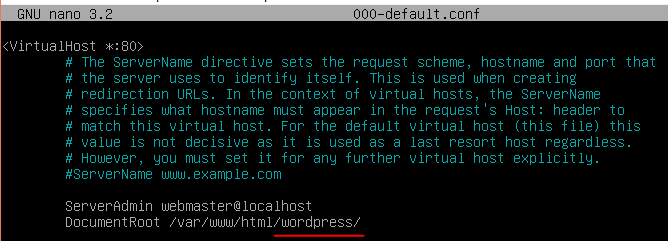
Annetaan oikeudet, jotta apache2 voi käyttää tarvittavia tiedostoja ja kansioita.

**chown -R www-data:www-data /var/www/html/wordpress/**



Muokkaa apache2 oletussivun konfiguraatiota. Tässä sen oletushakemistoksi määritetään /var/www/html/wordpress/ hakemisto johon wordpress siirrettiin.

**nano /etc/apache2/sites-available/000-default.conf**

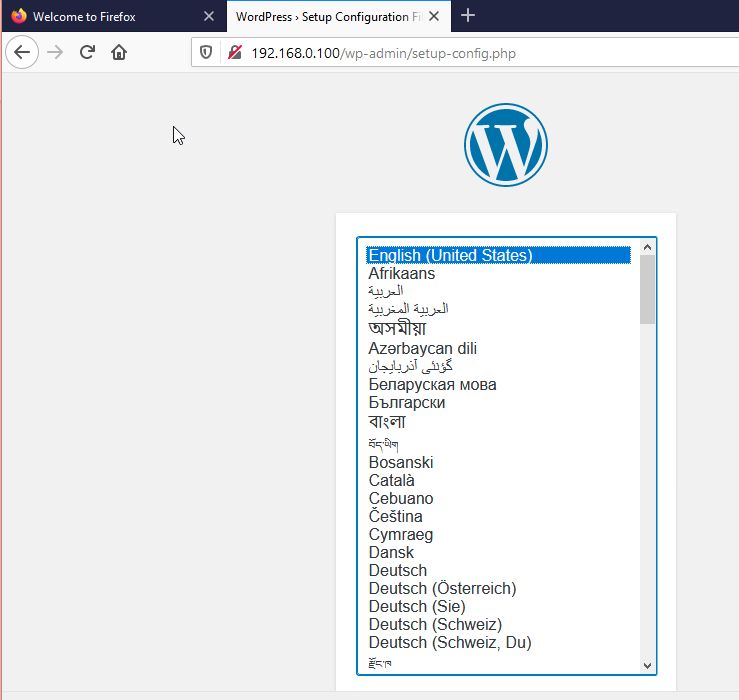


Käynnistä apache2 vielä uudestaan.

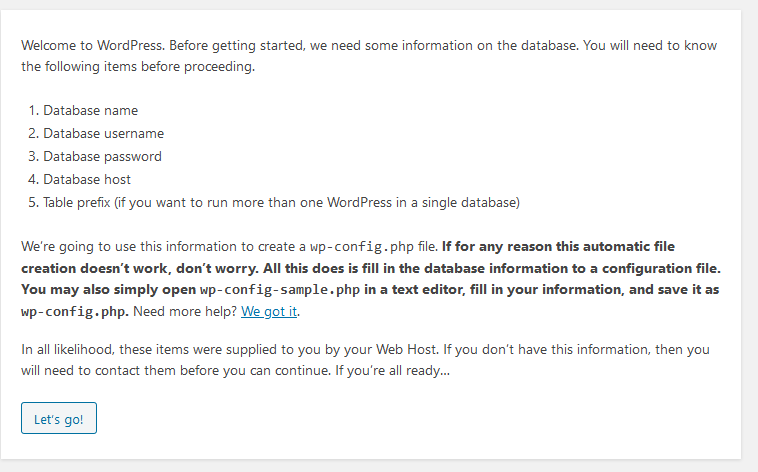
**systemctl restart apache2**

## WordPress käyttöönotto

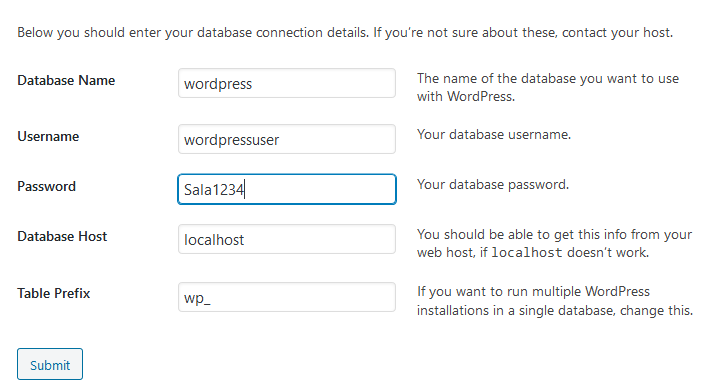
Kaikki on nyt kunnossa palvelimen puolella. Seuraavaksi kirjaudu koneella, jolla on graafinen käyttöliittymä. Avaa palvelimesi IP-osoite selaimessa ja sinulle tulisi avautua seuraavanlainen ruutu. Valitse kieleksi English.



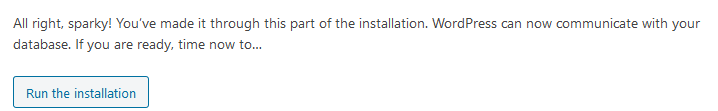
Seuraavaksi määritetään mitä tietokantaa WordPress käyttää. Nämä määritettiin oppaan alussa.



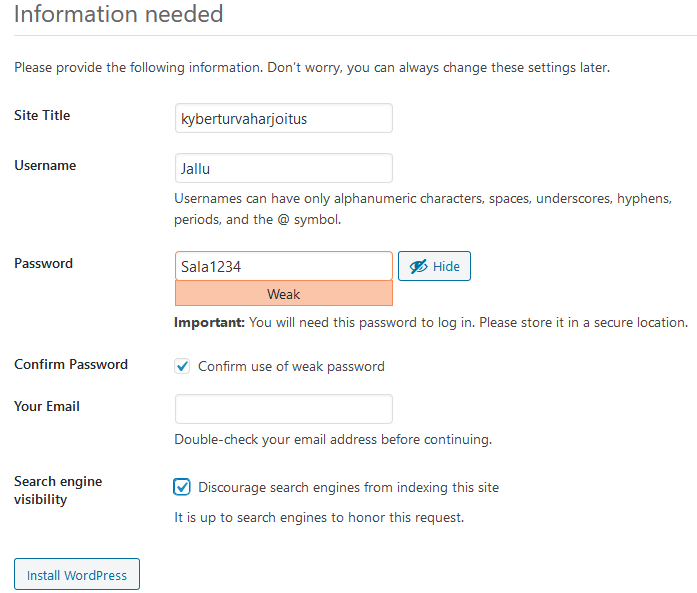
Tässä ohjeessa tehtiin wordpress niminen tietokanta. Tietokannan käyttäjän nimi on wordpressuser ja sen salasana Sala1234. Tietokanta sijaitsee palvelimessa itsessään, joten host voi olla localhost.



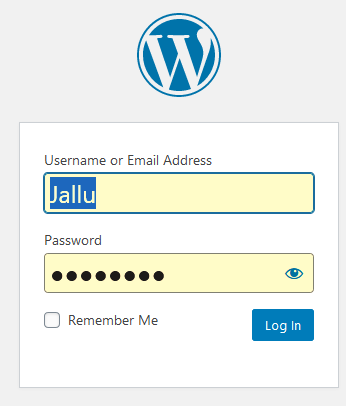
Ajetaan asennus loppuun.



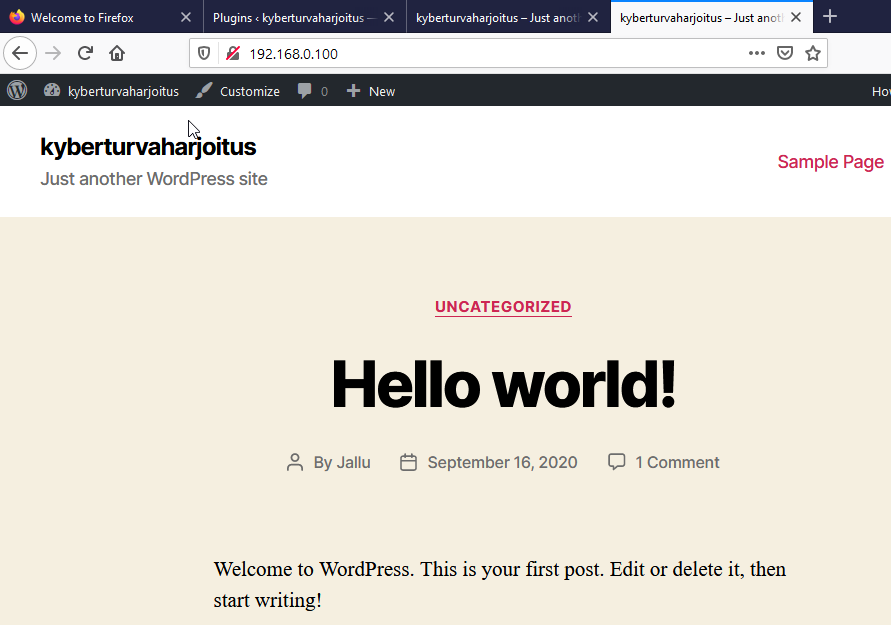
Joudut antamaan sivustolle nimen ja käyttäjätilin sekä salasanan. Joudut myös antamaan sähköpostiosoitteen. Käytä vaikka koulun @edu.hyria.fi tiliä.



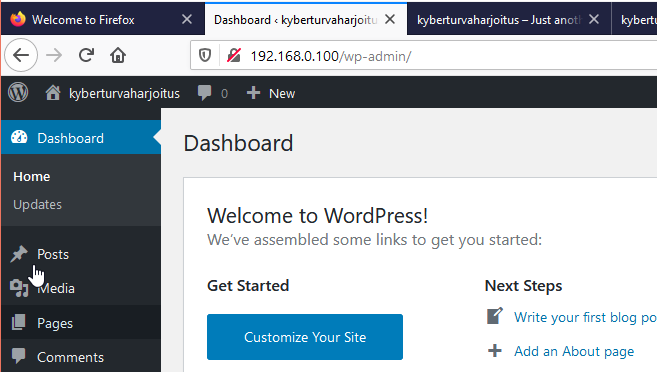
Vihdoin voidaan kirjautua sisään WordPress alustalle äskeisessä kohdassa tehdyillä tunnuksilla.



Nähdään, että meillä on jo yksinkertainen sivusto olemassa.



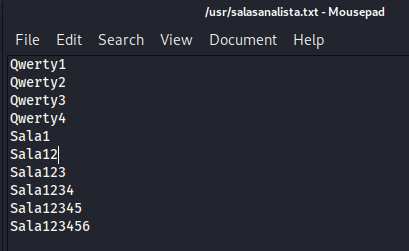
Osoitteesta palvelimesiip/wp-admin/ pääset hallitsemaan sivustoasi kuten alla olevassa kuvassa.



## WordPressin murtaminen

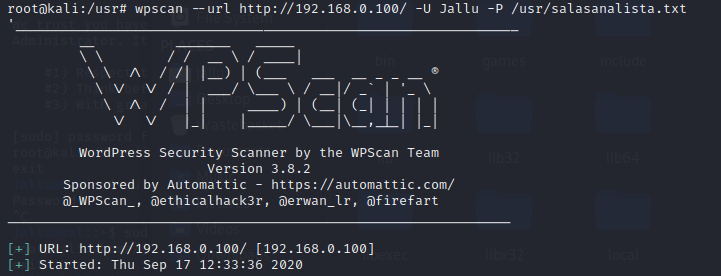
Kalista löytyy wpscan niminen paketti jolla voidaan skannata WordPress sivustojen haavoittuvuuksia. Se on samankaltainen kuin aiemmin käytetty nikto.

Aluksi luodaan salasanalista /usr/ hakemistoon nimeltään salasanalista.txt

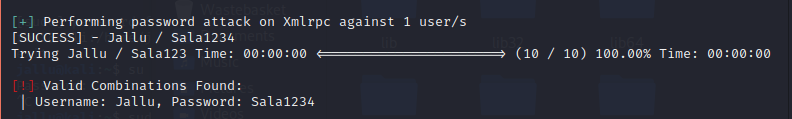


Tällä komennolla skannattaa kyseinen IP-osoite käyttäjänimellä Jallu ja salasanalistalla salasanalista.txt.

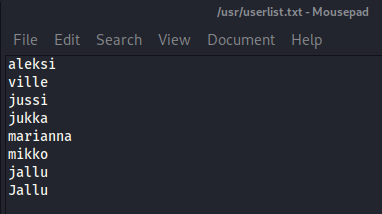
**wpscan –url http://192.168.0.100/ -U Jallu -P /usr/salasanalista.txt**



wpscan löysi oikean salasanan Jallu käyttäjälle. Nyt kun salasana on tiedossa voitaisiin WordPress sivustolle kirjautua.



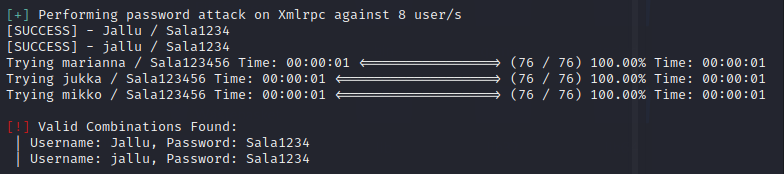
skannaus voidaan myös tehdä käyttämällä käyttäjälistaa. Tässä tehdään sellainen /usr/ hakemistoon.



Melkein sama komento kuin aiemmin, mutta Jallu tilalla on /usr/userlist.txt hakemisto, jossa on käyttäjälista.



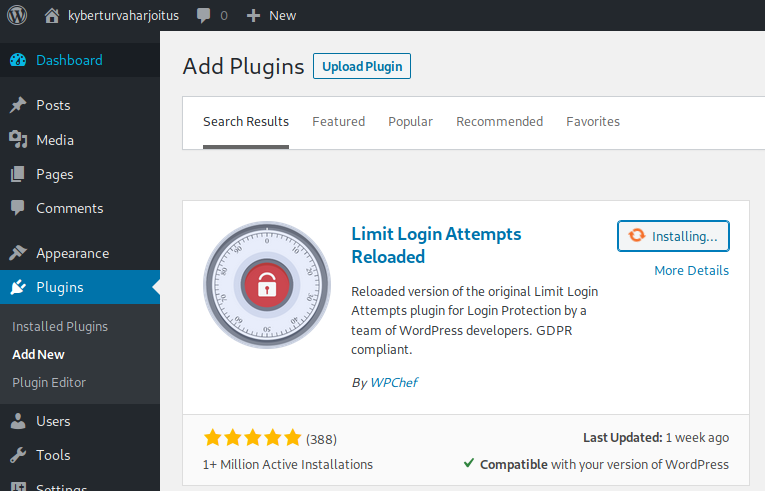
Skannaus käy läpi kaikki tiedostossa olevat käyttäjänimet ja kokeilee jokaista salasanaa niihin.



## WordPress suojaaminen

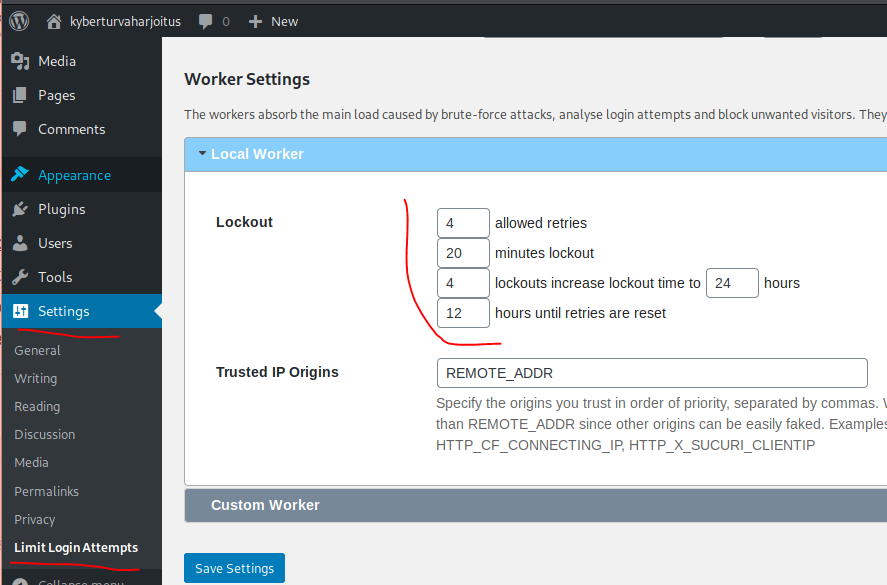
WordPressiin löytyy lisäosia eli plugineita. Niitä on valtava määrä ja tässä käytetään yhtä niistä joka tekee saman asian kuin linuxin fail2ban paketti.

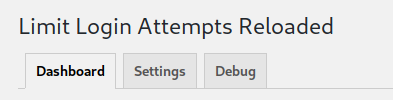
Avaa WordPressin hallintapaneeli > Plugins > Add new > Search > limit login attempts reloaded > Asenna se.



Avaa Settings > Limit Login Attempts > Settings

Kuten kuvasta näkyy, lisäosa on valmiiksi tehnyt asetuksia. Voit itse muokata näitä.

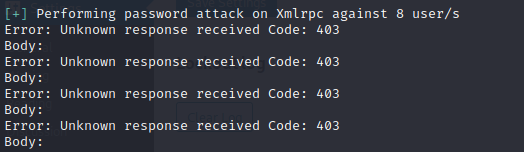




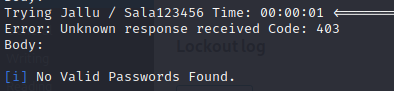
Mennään takaisin kaliin ja yritetään murtautua WordPress sivustolle samalla tavalla kuin ennenkin.



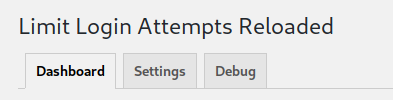
Skannin aikana tulee erroria koska bännit ovat jo tulleet.



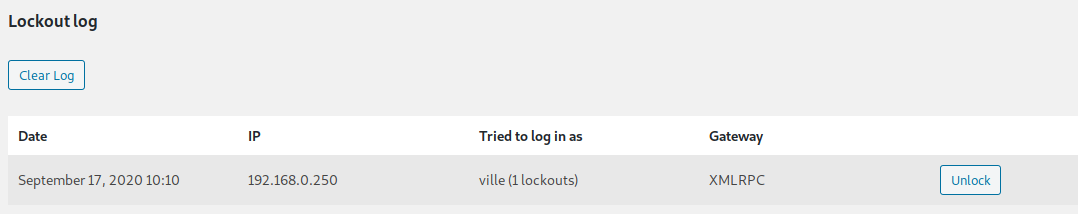
Ei löydetty oikeaa salasanaa sen takia.



Palaa WordPressin hallintapaneeliin > Limit Login Attempts > Dashboard ja näet lokista mistä murtautumisyritys tuli ja kenelle käyttäjälle.

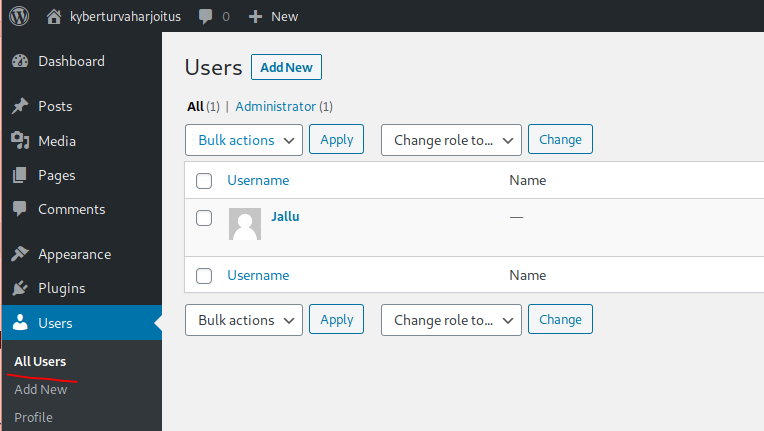


Ville sai bännit IP-osoitteesta 192.168.0.250.



## Muita tärkeitä WordPress asetuksia

WordPress Users kohdasta voi löytyy potentiaalisia ongelmia jos siellä on käyttäjiä joita siellä ei pitäisi olla.



Site Health kohta antaa yleistä tietoa onko WordPress sivustolla kaikki OK.

