jamk.fi

Arktiset Rakenteet -portaalin dokumentointi ja testaus

Jarkko Pajuniemi

Opinnäytetyö
Maaliskuu 2017
Tekniikan ja liikenteen ala
Insinööri (AMK), tietotekniikan koulutusohjelma

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Pajuniemi, Jarkko	Opinnäytetyö, AMK	Maaliskuu 2017
	Sivumäärä 60	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x**Virhe.**

Työn nimi
Arktiset Rakenteet -portaalin dokumentointi ja testaus

Tutkinto-ohjelma
Insinööri (AMK), tietotekniikan koulutusohjelma

Työn ohjaaja(t)
Häkkinen, Antti
Kotikoski, Sampo

Toimeksiantaja(t)
Arktiset Rakenteet -projekti / JAMK

Tiivistelmä

Opinnäytetyön tehtävänä oli dokumentoida kesällä 2016 toteutetun Arktiset Rakenteet -projektin tietoportaalin sisältö ja siihen käytetyt tekniikat. Lisäksi tavoitteena oli testata ja tarvittaessa parantaa portaalin tietokantaan ja tietoturvaan liittyviä ominaisuuksia.

Arktiset Rakenteet on Tekesin rahoittama projekti, jossa ovat mukana Jyväskylän ammattiorkeakoulu JAMK ja Lappeenrannan teknillinen yliopisto LUT. Projekti toimii osana Tekesin Arktiset Meret -ohjelmaa ja projektin keskeisenä tavoitteena on laajentaa tietämystä eri rakenteiden käyttäytymisestä arktisissa meriolosuhteissa.

Portaalin dokumentointiin sisältyi eri komponenttien, kuten palvelimen, tietokannan ja sisällönhallintajärjestelmän, sisällön ja toiminnan esittäminen. Tämän lisäksi dokumentoitiin myös portaalin hallinnassa tarvittavat elementit: käyttäjien, valikoiden, artikkelien, moduulien ja teeman hallinta sekä käytettävät lisäosat.

Portaalin tietoturvaa kovennettiin ottamalla käyttöön automaattinen varmuuskopiointi, asettamalla sivusto käyttämään tiedonsiirtoon HTTP:n sijasta HTTPS-yhteyttä ja testaamalla sivuston tietoturvaa eri skannereilla. HTTPS-yhteys toteutettiin käyttämällä Let's Encrypt -organisaation tarjoamaa sertifikaattia. Tietoturvaa testattiin käyttäen HTTPS-yhteyden mahdollistavan TLS-protokollan konfiguraatiota testaavaa SSL Labsia, yleisemmin sivuston tietoturvakonfiguraatiota ja -asetuksia testaavaa Mozilla Observatorya, ja lisäksi Joomlan tietoturvan testaamiseen tarkoitettu skanneria Joomscan.

Lopulliseen dokumentaatioon saatiin sisällytettyä sivuston hallintaan liittyvät keskeiset asiat. Tietokanta-osio jäi puolestaan odotettua lyhyemmäksi johtuen Joomlan automaattisesta tietokannan hallinnasta, kun taas tietoturva-osiosta tuli odotettua laajempi.

Avainsanat (asiasanat)
Verkkosivusto, Joomla, tietoturva, HTTPS

Muut tiedot

jamk.fi

Description

Author(s)	Type of publication	Date
Pajuniemi, Jarkko	Bachelor's thesis	March 2017
		Language of publication: Finnish
	Number of pages: 60	Permission for web publication: x

Title of publication

Documentation and testing of Arctic Structures portal

Degree programme

Information Technology

Supervisor(s)

Häkkinen, Antti

Kotikoski, Sampo

Assigned by

Arctic Structures project / JAMK

Abstract

The assignment for the bachelor's thesis was to document the content and techniques used for Arctic Structures information portal created in summer 2016. An additional objective was to test the portal's database and security and improve them if necessary.

Arctic Structures is a project funded by Tekes carried out in co-operation with JAMK University of Applied Sciences and Lappeenranta University of Technology (LUT). The project is a part of Tekes Arctic Seas programme, and the central objective of the project is to expand the knowledge of the behavior of different structures in arctic sea conditions.

The portal's documentation included the presentation of content and operation of various components, such as the server, database and content management system. Additionally, the elements used for the portal's management were documented including the management of users, menus, articles, modules and theme along with applied expansions.

The portal's security was hardened by implementing automatic backups, setting the webpage to use HTTPS for data transfer instead of HTTP and testing the page with various security scanners. HTTPS was applied by using a certificate provided by Let's Encrypt organization. The testing of security was implemented by utilizing SSL Labs for testing TLS protocol's configuration used for enabling HTTPS, Mozilla Observatory for testing webpage's security configuration and settings on a wider scale as well as Joomscan, a scanner used for testing Joomla's security.

The final documentation included essentials for managing the page. However, the part covering webpage's database was shorter than expected due to Joomla's automatic management of the database, whereas the part covering the webpage's security turned out wider than expected at the beginning of the project.

Keywords/tags (subjects)

Webpage, Joomla, security, HTTPS

Miscellaneous

Sisältö

Lyhenteet **5**

1 Johdanto **6**

1.1 Arktiset Rakenteet 6

1.2 Lähtökohdat ja tavoitteet 6

2 Palvelin ja sivusto **7**

2.1 Sisällönhallinta 7

2.2 Palvelin ja komponentit 8

2.3 Etäyhteys palvelimelle 9

3 Tietokanta **10**

3.1 Yleistä tietokannoista 10

3.2 MariaDB 10

3.3 Portaalin tietokanta 11

4 Tietoturva **13**

4.1 Varmuuskopiointi 13

4.1.1 Varmuuskopioinnin toiminta 13

4.1.2 Todennus varmuuskopioinnin toiminnasta 14

4.2 SSL/TLS 19

4.2.1 Yleistä 19

4.2.2 Let’s Encrypt 20

4.2.3 SSL Labs 21

4.2.4 SSL:n käyttöönotto 21

4.2.5 SSL:n toiminnan todennus 25

4.3 Palomuuri 27

4.4 Two Factor Authentication 28

4.5 ReCaptcha 30

4.6 Tietoturvan testaus 32

4.6.1 Mozilla Observatory 32

4.6.2 Tietoturvan testaus Observatorylla 32

4.6.3 Joomscan 37

5 Portaalin hallinta 40

5.1 Hallintapaneeli 40

5.2 Käyttäjät 40

5.3 Valikot 42

5.4 Artikkelit 43

5.5 Moduulit 45

5.6 Teema 46

5.7 Lisäosat 47

5.7.1 Yleistä 47

5.7.2 K2 47

5.7.3 BreezingForms 49

5.7.4 Widgetkit 51

5.7.5 JCE Editor 53

5.7.6 Attachments 54

5.8 Liitännäiset 54

6 Yhteenveto ja pohdinta 56

Lähteet 58

Liitteet 59

Liite 1. Tietokannan taulukot 59

Kuviot

Kuvio 1. SSH-etäyhteys palvelimelle. 9
Kuvio 2. SFTP-etäyhteys palvelimelle. 10
Kuvio 3. K2 extra fields tietokannassa 12
Kuvio 4. Tietokannan koko ja taulukoiden määrä 12
Kuvio 5. Joomlan varmuuskopiointiin käytettävä crontab-skripti 13
Kuvio 6. Tietokannan varmuuskopiointiin käytettävä crontab-skripti 13
Kuvio 7. Vanhojen varmuuskopioiden poistoon käytettävät crontab-skriptit. 14
Kuvio 8. Joomlan varmuuskopiot 14
Kuvio 9. Purettu Joomlan varmuuskopio 15
Kuvio 10. Tietokannan varmuuskopiot 16
Kuvio 11. Tietokannan varmuuskopion sisältöä tekstimuodossa 17
Kuvio 12. Tietokannan varmuuskopion taulukot 18
Kuvio 13. Tietokannan varmuuskopion koko ja taulukoiden määrä 19
Kuvio 14. SSL/TLS-sertifikaattiketju 20
Kuvio 15. Yksityisen avaimen ja CSR:n luominen 22
Kuvio 16. Sertifikaatin onnistunut asennus 22
Kuvio 17. SSL-konfiguraation arvostelu 23
Kuvio 18. Korjatun SSL-konfiguraation arvostelu 24
Kuvio 19. Sertifikaatin uusimiseen käytettävä crontab-skripti 25
Kuvio 20. HTTPS:n toimivuuden todennus 25
Kuvio 21. Lisätietoja sivustosta 26
Kuvio 22. Lisätietoja varmenteesta 27
Kuvio 23. Palomuuri 28
Kuvio 24. Google Authenticatorin käyttöönotto 29
Kuvio 25. Estetty hallintapaneeliin sisäänkirjautuminen 30
Kuvio 26. ReCaptcha 31
Kuvio 27. ReCaptcha-liitännäisen asetukset 32
Kuvio 28. Tietoturvan arvostelu Observatorylla 33
Kuvio 29. CSP:n estämä tarpeellinen sisältö portaalin etusivulla 34
Kuvio 30. Tietoturvan lopullinen arvostelu Observatorylla 37
Kuvio 31. Joomscan-skannauksen aloittaminen 38

Kuvio 32. Skannauksen tulokset....38
Kuvio 33. Skannauksessa löydetyt haavoittuvuudet....39
Kuvio 34. Toisen skannauksen tulokset....39
Kuvio 35. Hallintapaneelin etusivu....40
Kuvio 36. Portaalin käyttäjäryhmät....41
Kuvio 37. Valikoiden hallinta....42
Kuvio 38. Esimerkki valikon nimikkeen luomisesta....43
Kuvio 39. Artikkelien hallinta....44
Kuvio 40. Portaalin artikkelien kategoriat....45
Kuvio 41. Portaalissa käytettäviä moduuleja....46
Kuvio 42. Teemojen hallinta....46
Kuvio 43. Laitteet ja osaaminen....48
Kuvio 44. K2:n hallinta....49
Kuvio 45. Palautekaavake....50
Kuvio 46. BreezingForms-kaavakkeiden hallinta....51
Kuvio 47. Widgetkit-moduulien luonti....52
Kuvio 48. Portaalin Widgetkit-moduulit....53
Kuvio 49. JCE-tekstieditori....53
Kuvio 50. Liitteiden hallinta....54
Kuvio 51. Liitännäisten hallinta....55

Lyhenteet

CA	Certificate Authority
CSP	Content Security Policy
CSR	Certificate Signing Request
DHCP	Dynamic Host Configuration Protocol
EPEL	Extra Packages for Enterprise Linux
HTML	HyperText Markup Language
HPKP	HTTP Public Key Pinning
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ISRG	Internet Security Research Group
MIME	Multipurpose Internet Mail Extensions
PHP	PHP: Hypertext Preprocessor
SQL	Structured Query language
SSL	Secure Sockets Layer
TLS	Transport Layer Security
XSS	Cross-site scripting

1 Johdanto

1.1 Arktiset Rakenteet

Arktiset Rakenteet on Tekesin rahoittama projekti, jonka keskeisenä tavoitteena on laajentaa tietämystä eri rakenteiden käyttäytymisestä arktisissa meriolosuhteissa. Tämän selvittäminen on tärkeää koneiden, laitteiden ja rakenteiden toiminnan ja kestävyyden varmistamisen kannalta. Tekes on myöntänyt projektille 600 000 € rahoituksen ja projektissa ovat mukana Jyväskylän ammattikorkeakoulu JAMK ja Lappeenrannan teknillinen yliopisto LUT. Arktiset Rakenteet toimii osana Tekesin Arktiset Meret -ohjelmaa, jonka tarkoituksena on edesauttaa uusien liiketoimintojen syntymistä merenkulun ekotehokkaissa ratkaisuissa ja merialueiden luonnonvarojen kestävässä hyödyntämisessä. (JAMK mukana arktisten rakenteiden kehityksessä 2015.)

1.2 Lähtökohdat ja tavoitteet

Opinnäytetyössä tarkoitus oli dokumentoida jo tehdyn Arktiset Rakenteet -tietoportaalin sisältö ja toteutus. Tietoportaali luotiin vuonna 2016 touko-lokakuussa työharjoitteluna minun ja toisen JAMK:n opiskelijan, Roozbeh Negahbanin, toimesta. Tietoportaalin tarkoituksena on kerätä Arktiset Rakenteet -projektissa mukana olevat organisaatiot ja niiden laitteisto ja osaaminen samalle sivustolle. Portaaliin kerätään myös projektiin liittyvää ainestoa, kuten artikkeleita ja tutkimustuloksia, sekä julkisesti että projektin sisäisesti näytille. Tietoportaalin dokumentointi sisältää portaalin toteutustavan ja portaaliin toteutetut ratkaisut:

- Palvelin ja siihen asennetut tarvittavat komponentit
- Tietokanta ja sen tyyppi, rakenne ja sisältö
- Moduulit, artikkelit ja lisäosat sekä niiden hallinta
- Portaalin rakenne ja teema
- Tietoturvaratkaisut.

Lisäksi työssä tuli pohtia ja toteuttaa tietokantaan ja tietoturvaan liittyviä ominaisuuksia ja testata niiden toiminta. Portaali on toistaiseksi asennettuna JAMK:n palvelimella ja näkyvissä osoitteessa arctic.labranet.jamk.fi. Portaali siirretään myöhemmin toiselle ja palvelimelle ja toiseen verkko-osoitteeseen.

Työn tavoitteena oli kehittää tietoportaalia ja dokumentoida sen toteutusta seuraavin tavoin:

- Tehdä portaalista tietoturvallisesti vahva ja varmistaa tietoturvallisuus portaalin käyttäjille ja ylläpidolle.
- Dokumentoida portaalin tietokanta ja palvelimelle asennetut komponentit ja muut ratkaisut kattavasti ja selkeästi.
- Dokumentoida portaalin rakenne siten, että portaalin ylläpito onnistuu tulevilta ylläpitäjiltä mahdollisimman helposti.

2 Palvelin ja sivusto

2.1 Sisällönhallinta

Tietoportaalin suunnittelussa tuli pohtia, millä tavalla portaali toteutetaan: vaihtoehtoina olivat joko sivuston itse alusta lähtien ohjelmoiminen tai jonkin sisällönhallintajärjestelmän käyttäminen. Sivuston itse ohjelmoimisessa on etuna se, että sivusto voidaan silloin toteuttaa täysin itse haluamallaan tavalla, eikä vastaan tule mitään mahdollisia sisällönhallintajärjestelmän tuomia rajoitteita. Haittapuolena on taas se, että sivuston luonti on tällä tavalla paljon työläämpää ja vaikeampaa, sillä valmiiden ratkaisujen sijaan tehdään kaikki itse ja tämä vaatii myös enemmän muun muassa ohjelmointi- ja tietokantojen käsittelytaitoja.

Toteutustavaksi valittiin sisällönhallintajärjestelmä, koska sillä pystytään toteuttamaan kaikki sivuston vaatimukset ja sen käyttäminen vähentää työmäärää. Lopputulos on myös todennäköisesti vähintään yhtä hyvä, ellei jopa parempi, sillä sisällönhallintajärjestelmät käyttävät valmiiksi kehitettyjä ja toimiviksi todettuja ratkaisuja.

Näitä voidaan sivustolla soveltaa ja tarvittaessa mukaan voidaan lisätä itse ohjelmoituja komponentteja. Sisällönhallintajärjestelmä valittiin vertailemalla ja testaamalla kolmea yleisintä: Drupal, Joomla ja WordPress.

Kaikki kolme edellä mainittua sisällönhallintajärjestelmää ovat ilmaisia avoimen lähdekoodin ohjelmistoja ja ovat kirjoitettu pääasiassa PHP:lla. Ne kaikki myös käyttävät sivustojen ulkoasun hallintaan teemoja ja valmiita pohjia, sekä käyttävät liitännäisiä, moduuleja ja lisäosia sivuston toimintojen hallintaan. Kyseiset sisällönhallintajärjestelmät myös tukevat MySQL-tietokantaa. Drupal ja Joomla tukevat myös muita tietokannan hallintajärjestelmiä WordPressin tukiessa ainoastaan MySQL:ää. (WordPress vs Joomla vs Drupal – Which One is Better? 2016.)

Suurin eroavaisuus kyseessä olevilla sisällönhallintajärjestelmillä on niiden käyttöliittymä, joka on jokaisella järjestelmällä erilainen. WordPress on näistä helppokäyttöisin ja Drupal teknisesti haastavin vaatien vähintään perustavanlaatuista osaamista yleisimmistä verkko-ohjelmointikielistä, kuten HTML ja PHP, ja Joomla taas sijoittuu käyttöliittymän haastavuudessa näiden välille. (Mening 2016.)

Kaikilla kolmella sisällönhallintajärjestelmällä Arktiset Rakenteet -projektin vaatima tietoportaali on kuitenkin varmasti mahdollista toteuttaa ja lopullinen valinta onkin lähinnä makuasia. Sisällönhallintajärjestelmän valinnassa päädyttiin Joomlaan sen käyttöliittymän selkeyden ja käytettävyyden vuoksi. Joomla oli myös haastavuudessaan sopiva ja sen käytöstä oli tekijöillä jo entuudestaan jonkin verran kokemusta.

2.2 Palvelin ja komponentit

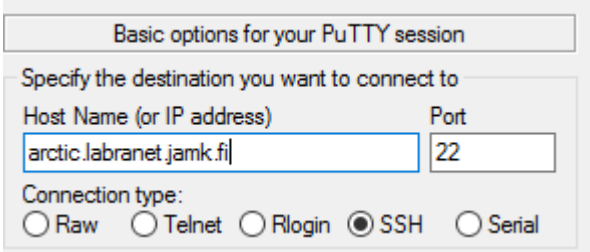
Sivusto on toistaiseksi asennettu JAMK:n palvelimelle, jonka käyttöjärjestelmänä toimii CentOS 7. Lisäksi Joomla vaatii toimiakseen komponentit Apache, PHP ja MySQL. Apache on palvelimelle asennettava ohjelmisto, jolla saadaan jaettua tiedostoja HTTP:n (Hypertext Transfer Protocol) yli. Käytännössä tämä siis tarkoittaa, että Apachella saadaan hallittua palvelimelta verkkosivuja.

Joomla vaatii myös palvelimelle asennettuna PHP-ohjelmointikielen, jota käytetään verkko-ohjelmoinnissa, ja MySQL-tietokannan. Tietokantajärjestelmänä käytetään MySQL:ään pohjautuvaa MariaDB:tä, joka on myös yhteensopiva MySQL:n kanssa ja toimii siten myös Joomlan kanssa. Portaali tulee myös konfiguroida käyttämään

HTTPS:ää (Hypertext Transfer Protocol Secure), joka on salattu versio HTTP:stä, koska portaalissa on käytössä kirjautumissivu. Jos kirjautumiseen käytettäisiin HTTP:tä, olisi kirjautumistiedot mahdollista kaapata selkokielisenä.

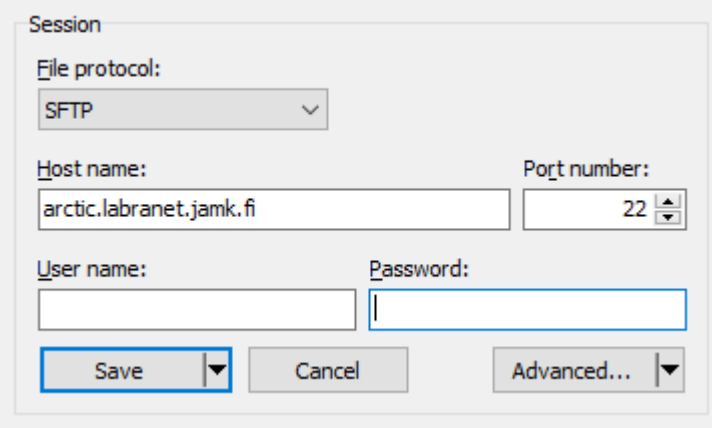
2.3 Etäyhteys palvelimelle

Palvelimelle muodostettiin etäyhteys SSH-protokollalla. SSH mahdollistaa salatun yhteyden internetin kautta käyttäjän ja palvelimen välillä. SSH-yhteys saadaan muodostettua esimerkiksi PuTTY-sovelluksella käyttäen porttia 22 ja kirjautumiseen palvelimelle lisätyn käyttäjän tunnuksia. SSH-yhteyden luominen PuTTY:lla on esitetty kuviossa 1.



Kuvio 1. SSH-etäyhteys palvelimelle.

Tiedostojen siirto esimerkiksi käyttäjän tietokoneelta palvelimelle saadaan toteutettua helposti SFTP (SSH File Transfer Protocol) -protokollalla. SFTP on tiedonsiirtoon käytettävä protokolla, joka käyttää nimensä mukaisesti SSH-istuntoa salaamaan tiedonsiirron. SFTP:tä voidaan käyttää esimerkiksi WinSCP-sovelluksella, kuten kuviossa 2 on esitetty.



Kuvio 2. SFTP-etäyhteys palvelimelle.

3 Tietokanta

3.1 Yleistä tietokannoista

Tietokanta on paikka, jonne on tallennettu tietoa organisoidusti ja järjestelmällisesti. Tietokantoihin voidaan tallentaa tietoa missä tahansa formaatissa, kuten elektronisesti, tulostettuna, graafisena, äänenä, tilastollisesti tai eri yhdistelminä. Tietokannat voidaan jakaa fyysisiin (esimerkiksi paperilla) ja elektronisiin tietokantoihin (esimerkiksi kovalevylle tallennettuna). Tietokanta voi olla yksinkertaisimmillaan esimerkiksi puhelinluettelo, johon puhelinnumerot on jaoteltu nimien mukaan aakkosjärjestykseen, ja monimutkaisempana vaikkapa elektroninen tietokanta, johon on tallennettu tietoa useissa eri formaateissa. (A Primer on Databases and Catalogs n.d.)

SQL (Structured Query language) on ohjelmointikieli, jota käytetään tietokantojen hallintaan. SQL-tietokantojen sisältämää tietoa voidaan esimerkiksi lisätä, poistaa, päivittää, hakea ja järjestellä eri kriteerien mukaan. Eri ominaisuuksilla varustettuja SQL-tietokantajärjestelmiä on useita erilaisia, ja niitä ovat esimerkiksi MySQL, PostgreSQL, SQLite ja MariaDB. (SQL (Structured Query Language) n.d.)

3.2 MariaDB

MariaDB on MySQL:ään pohjautuva tietokantatyyppi, jonka on luonut ryhmä suurimmaksi osaksi entisiä MySQL:n työntekijöitä. MariaDB:tä johtaa ja rahoittaa MySQL:n

perustajajäsen Michael Widenius. MariaDB:n tavoite on korvata MySQL suuremmalla määrällä toimintoja ja paremmalla suorituskyvyllä. (Bartholomew n.d.)

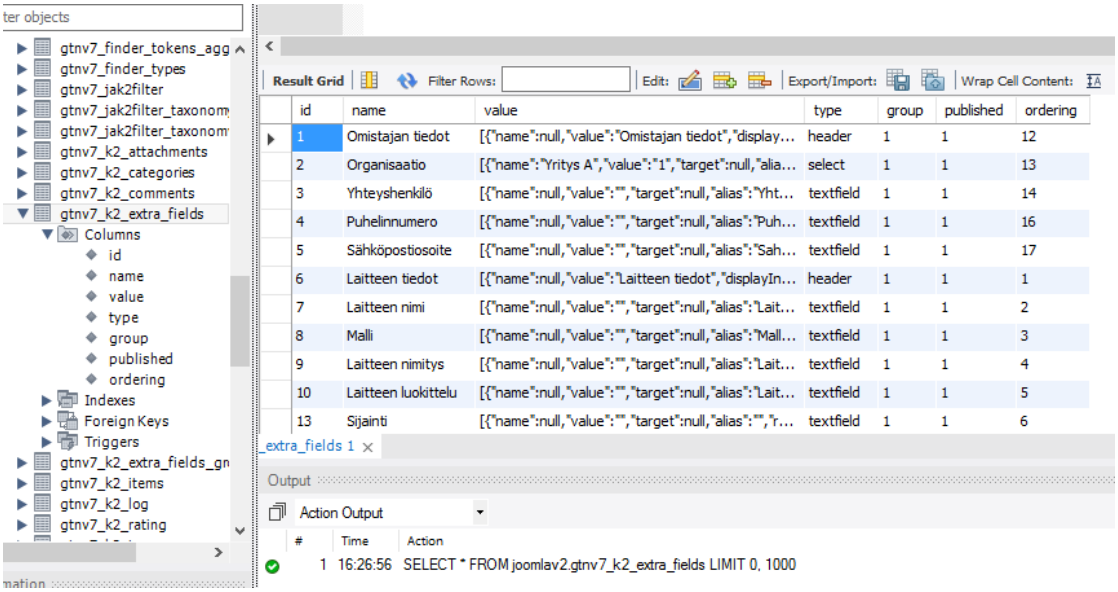
Portaalin tietokantajärjestelmäksi valittiin MariaDB. MariaDB:n etuja MySQL:ään verrattuna ovat muun muassa useamman tietokantamoottorin tukeminen, suurempi määrä toimintoja sekä nopeampi bugien korjaus ja toimintojen kehittäminen. MariaDB on myös täysin takaisinpäin yhteensopiva MySQL:n kanssa. (Patra 2015.)

3.3 Portaalin tietokanta

Joomla hallitsee tietokantaa automaattisesti: ainoastaan Joomlaa asennettaessa tarvitsee palvelimelle asentaa myös haluttu Joomlan tukema tietokantatyyppi. Tietokantaa ei siis välttämättä tarvitse hallita suorasti ollenkaan Joomla-pohjaisella verkkosivustolla, mutta tietokantaa ja sen rakennetta voidaan kuitenkin tutkia esimerkiksi MySQL Workbench -ohjelmalla. Arktiset Rakenteet -portaalissa tietokantaa ei tarvinnut hallita suoraan missään vaiheessa, sillä kaikki tietokantaan liittyvät asiat saatiin toteutettua K2-lisäosan menetelmillä.

Portaalin tietokannan nimi on ”joomlav2”. Tietokanta on jaettu taulukoihin siten, että jokaisesta sivuston eri osiosta, josta tarvitsee tallentaa tietoa tietokantaan, on luotu oma taulukko. Liitteessä 1 on esitetty tietokannan taulukot. Kaikki taulukot ovat Joomlan automaattisesti generoimia.

Kuviossa 3 on näkyvillä esimerkki taulukon sisällöstä. Kyseisessä taulukossa on esitettynä osa K2 extra fields -kentistä, jotka ovat sivustolla näkyvillä jokaisella laitesivulla.



Kuvio 3. K2 extra fields tietokannassa

Kuviossa 4 on vielä nähtävillä tietokannan taulukoiden kokonaismäärä ja arvioitu tietokannan koko. Tämä on myöskin saatu esille käyttäen MySQL Workbenchiä.

Kuvio 4. Tietokannan koko ja taulukoiden määrä

4 Tietoturva

4.1 Varmuuskopiointi

4.1.1 Varmuuskopioinnin toiminta

Joomlan varmuuskopiointi suoritetaan crontab-skriptillä, jolla kopioidaan hakemisto */var/www/html/* joka lauantai klo 02:15 hakemistoon */backup/v2*. Skripti ajetaan tuohon kellonaikaan, koska silloin palvelimella on oletettavasti vähän liikennettä. Varmuuskopiot tallennetaan gzip-tiedostomuodossa ja nimetään automaattisesti päivämäärän ja kellonajan mukaan. Kuviossa 5 on kuvattu kyseinen Joomlan varmuuskopiointiin käytettävä skripti.

```
#Joomla Backup
15 2 * * 6 root tar -czf /backup/v2/joomla-`date
 +\%Y\%m\%d\%H\%M\%S`.tar.gz /var/www/html/
```

Kuvio 5. Joomlan varmuuskopiointiin käytettävä crontab-skripti

Sivuston tietokannasta luodaan varmuuskopio myöskin crontab-skriptillä, joka kopioi tietokannan hakemistoon */backup/v2-mysql* lauantaisin klo 02:30. Myös tietokannan varmuuskopiot tallennetaan gzip-tiedostomuodossa ja nimetään automaattisesti päivämäärän ja kellonajan mukaan. Skripti hakee tietokannan tunnukset hakemistossa */etc/my.cnf.d/* olevasta tiedostosta *client.cnf*, jossa tunnukset ovat luettavissa vain root-käyttäjälle. Kuviossa 6 on kuvattu kyseinen tietokannan varmuuskopiointiin käytettävä skripti.

```
#db Backup
30 2 * * 6 root mysqldump --defaults-file="/etc/my.cnf.d/client.cnf" joomlav2
| gzip > /backup/v2-mysql/v2db-`date +\%Y\%m\%d\%H\%M\%S`.sql.gz
```

Kuvio 6. Tietokannan varmuuskopiointiin käytettävä crontab-skripti

Sekä Joomlan että tietokannan varmuuskopioista säilytetään palvelimella 14 uusinta. Crontab-skripti poistaa lauantaisin vanhat Joomlan varmuuskopiot klo 02:45 ja vanhat tietokannan varmuuskopiot klo 03:00. Kuviossa 7 on kuvattu vanhojen Joomlan ja tietokannan varmuuskopioiden poistoon käytettävät skriptit.

```
#delete old files
45 2 * * 6 root ls -d -1tr /backup/v2/* | head
 -n -14 | xargs -d '\n' rm -f
0 3 * * 6 root ls -d -1tr /backup/v2-mysql/* |
 head -n -14 | xargs -d '\n' rm -f
```

Kuvio 7. Vanhojen varmuuskopioiden poistoon käytettävät crontab-skriptit.

4.1.2 Todennus varmuuskopioinnin toiminnasta

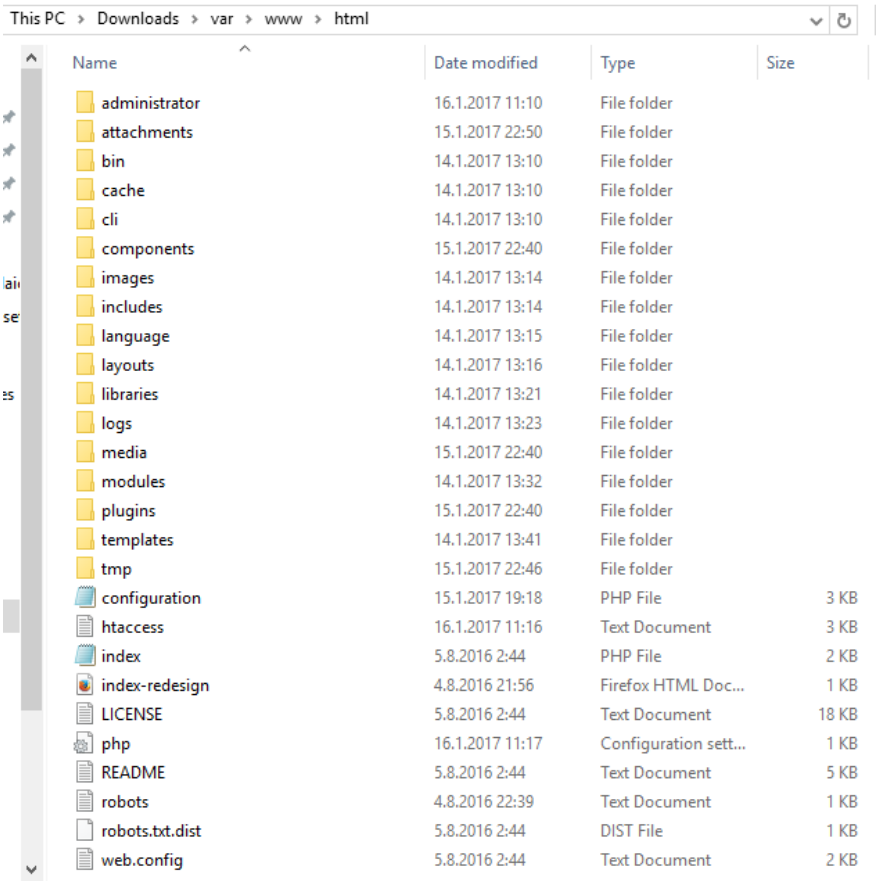
Kuviossa 8 on esitetty Joomlan varmuuskopiot. Kuviosta nähdään, että varmuuskopiot menevät hakemistoon */backup/v2*, varmuuskopioita tehdään viikoittain klo 02:15 ja varmuuskopioista säilytetään 14 uusinta. Vanhimmat varmuuskopiot eivät kuulu samaan viikoittaiseen rytmiin, vaan ne on otettu vanhemmalla varmuuskopioinnin asetuksella.

/backup/v2

Name	Size	Changed	Rights	Owner
..		10.11.2016 12:56:25	rwxr-xr-x	root
joomla-20161129021501.tar.gz	51 260 KB	29.11.2016 2:15:07	rw-r--r--	root
joomla-20161130021501.tar.gz	51 260 KB	30.11.2016 2:15:07	rw-r--r--	root
joomla-20161201021501.tar.gz	51 260 KB	1.12.2016 2:15:23	rw-r--r--	root
joomla-20161202021501.tar.gz	51 260 KB	2.12.2016 2:15:35	rw-r--r--	root
joomla-20161203021501.tar.gz	51 260 KB	3.12.2016 2:15:21	rw-r--r--	root
joomla-20161204021501.tar.gz	51 260 KB	4.12.2016 2:15:12	rw-r--r--	root
joomla-20161205021501.tar.gz	51 260 KB	5.12.2016 2:15:06	rw-r--r--	root
joomla-20161210021501.tar.gz	51 259 KB	10.12.2016 2:15:07	rw-r--r--	root
joomla-20161217021501.tar.gz	51 259 KB	17.12.2016 2:15:31	rw-r--r--	root
joomla-20161224021501.tar.gz	51 259 KB	24.12.2016 2:15:41	rw-r--r--	root
joomla-20161231021501.tar.gz	51 259 KB	31.12.2016 2:15:39	rw-r--r--	root
joomla-20170107021501.tar.gz	51 259 KB	7.1.2017 2:15:39	rw-r--r--	root
joomla-20170114021501.tar.gz	51 193 KB	14.1.2017 2:15:09	rw-r--r--	root
joomla-20170121021501.tar.gz	53 943 KB	21.1.2017 2:15:31	rw-r--r--	root

Kuvio 8. Joomlan varmuuskopiot

Joomlan varmuuskopion sisältö purettuna on */var/www/html*-hakemisto, jossa sijaitsee Joomlan tiedostot ja kansiot. Kuviossa 9 on esitetty puretun Joomlan varmuuskopion sisältö. Varmuuskopio voidaan palauttaa yksinkertaisesti poistamalla palvelimelta *html*-kansio ja korvaamalla se halutun varmuuskopion *html*-kansiolla ja asettamalla kansiolle ja sen alikansioille ja tiedostoille omistajaksi *apache*.



Kuvio 9. Purettu Joomlan varmuuskopio

Kuviossa 10 on esitetty tietokannan varmuuskopiot. Kuviosta nähdään, että tietokannan varmuuskopiointi toimii vastaavalla tavalla kuin Joomlan varmuuskopiointi.

/backup/v2-mysql

Name	Size	Changed	Rights	Owner
..		10.11.2016 12:56:25	rwxr-xr-x	root
v2db-20161129023001.sql.gz	224 KB	29.11.2016 2:30:01	rw-r--r--	root
v2db-20161130023001.sql.gz	224 KB	30.11.2016 2:30:01	rw-r--r--	root
v2db-20161201023001.sql.gz	224 KB	1.12.2016 2:30:02	rw-r--r--	root
v2db-20161202023001.sql.gz	224 KB	2.12.2016 2:30:02	rw-r--r--	root
v2db-20161203023001.sql.gz	224 KB	3.12.2016 2:30:01	rw-r--r--	root
v2db-20161204023001.sql.gz	224 KB	4.12.2016 2:30:01	rw-r--r--	root
v2db-20161205023001.sql.gz	224 KB	5.12.2016 2:30:01	rw-r--r--	root
v2db-20161210023001.sql.gz	224 KB	10.12.2016 2:30:01	rw-r--r--	root
v2db-20161217023001.sql.gz	225 KB	17.12.2016 2:30:01	rw-r--r--	root
v2db-20161224023001.sql.gz	268 KB	24.12.2016 2:30:01	rw-r--r--	root
v2db-20161231023001.sql.gz	224 KB	31.12.2016 2:30:01	rw-r--r--	root
v2db-20170107023002.sql.gz	224 KB	7.1.2017 2:30:02	rw-r--r--	root
v2db-20170114023001.sql.gz	226 KB	14.1.2017 2:30:02	rw-r--r--	root
v2db-20170121023001.sql.gz	229 KB	21.1.2017 2:30:01	rw-r--r--	root

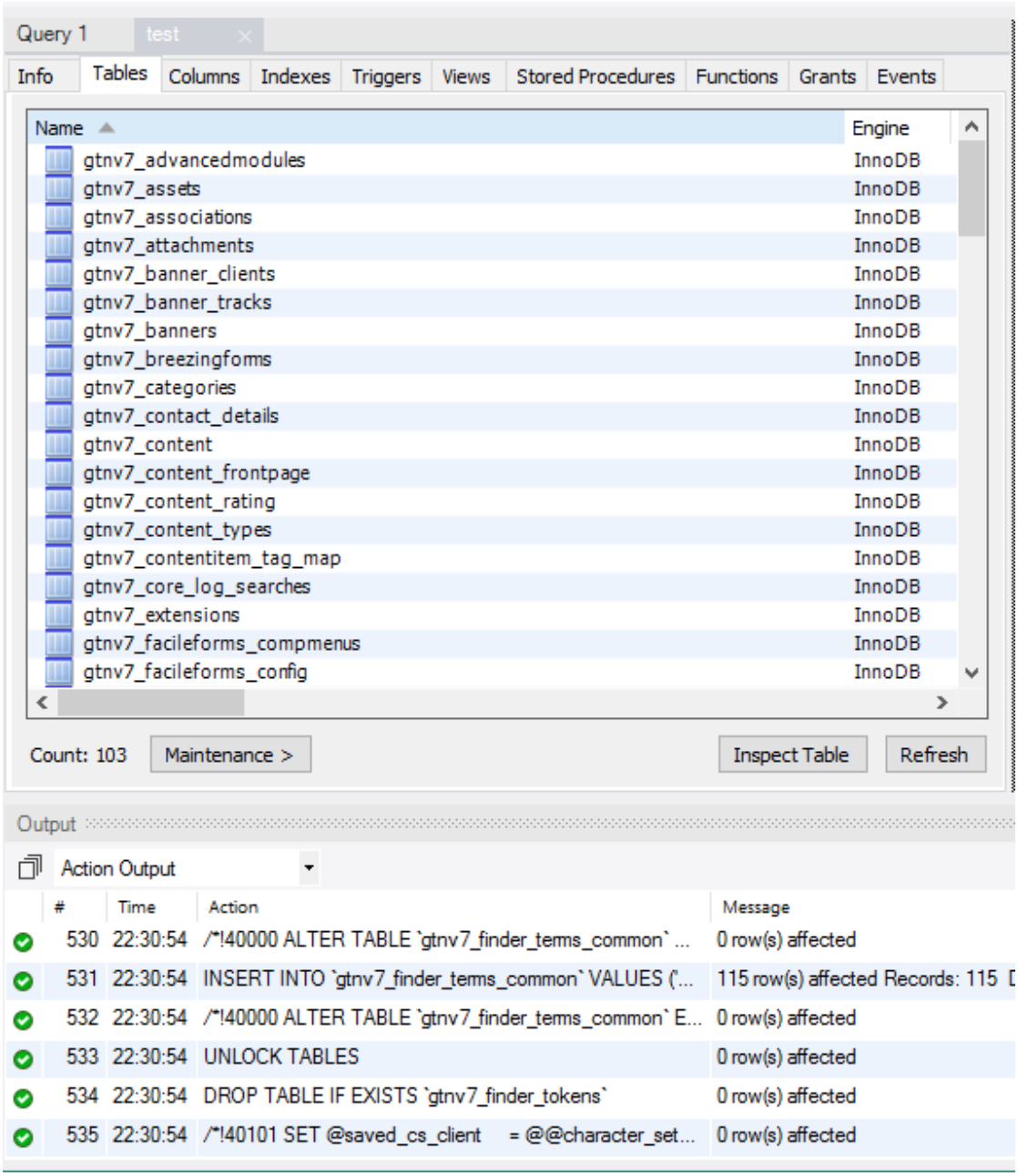
Kuvio 10. Tietokannan varmuuskopiot

Tietokannan varmuuskopio on purettuna .sql-tiedosto, joka sisältää komennot, joilla saadaan luotua tietokannan sisältö. Tiedoston sisältämät komennot ovat tekstimuodossa, joten ne on mahdollista saada näkyville esimerkiksi Notepad-ohjelmalla. Kuvissa 11 on esitetty osa .sql-tiedoston sisältöä Notepad++-ohjelmalla, jolla saadaan tiedoston sisältö näkyville siistimmässä muodossa.

```
-- MySQL dump 10.14  Distrib 5.5.47-MariaDB, for Linux (x86_64)
--
-- Host: localhost    Database: joomlav2
-- ------------------------------------------------------
-- Server version   5.5.47-MariaDB

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `gtnv7_advancedmodules`
--

DROP TABLE IF EXISTS `gtnv7_advancedmodules`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `gtnv7_advancedmodules` (
  `moduleid` int(11) unsigned NOT NULL DEFAULT '0',
  `asset_id` int(10) unsigned NOT NULL DEFAULT '0',
  `mirror_id` int(10) NOT NULL DEFAULT '0',
  `params` text NOT NULL,
  PRIMARY KEY (`moduleid`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
/*!40101 SET character_set_client = @saved_cs_client */;
```

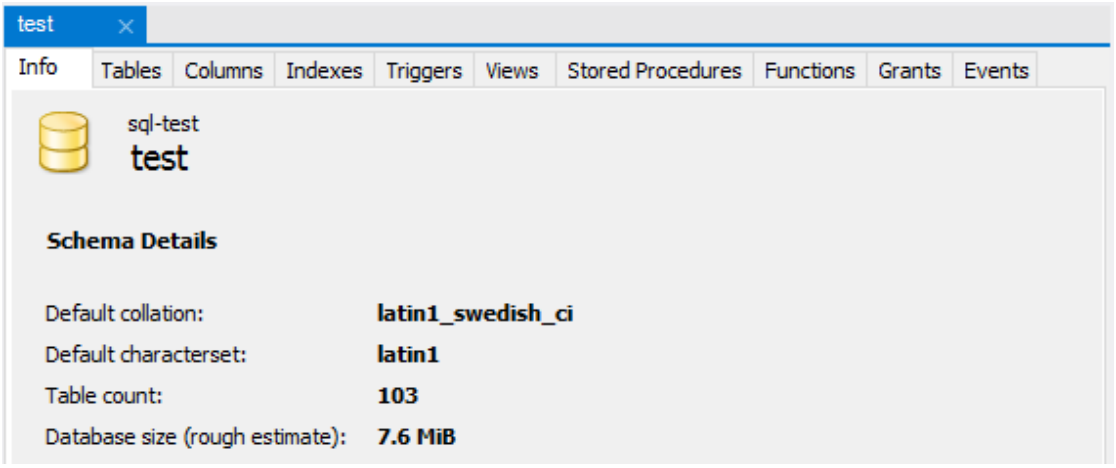
Kuvio 11. Tietokannan varmuuskopion sisältöä tekstimuodossa

Jos tiedoston komennot halutaan suorittaa, tarvitaan siihen SQL-tietokantaa käyttävä palvelin. Palvelimeen voidaan yhdistää esimerkiksi SQL Workbench -ohjelmalla, jolla voidaan suorittaa kyseiset komennot. Kuviossa 12 on esitetty osa SQL Workbenchin luomista taulukoista. Taulukoita voidaan verrata liitteeseen 1, jossa on esitetty kaikki tietokannan taulukot.



Kuvio 12. Tietokannan varmuuskopion taulukot

Kuviossa 13 on esitetty vielä tietokannan taulukoiden kokonaismäärä ja arvioitu tietokannan koko. Kuviota voidaan verrata kuvioon 4, jossa on esitetty samaiset tiedot portaalin tietokannasta, ja huomataan tietojen olevan molemmissa samat.



Kuvio 13. Tietokannan varmuuskopion koko ja taulukoiden määrä

4.2 SSL/TLS

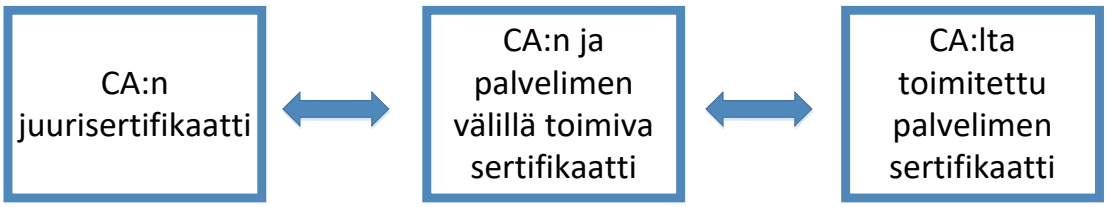
4.2.1 Yleistä

SSL (Secure Sockets Layer) ja TLS (Transport Layer Security) ovat protokollia, joita käytetään salatun ja tietoturvallisen linkin luomiseen palvelimen ja käyttäjän välille. Tyypillisesti palvelin on esimerkiksi verkkosivusto tai sähköpostipalvelin, ja käyttäjä on selain tai sähköpostin käyttäjä. SSL/TLS-protokollilla saadaan korvattua verkkosivustoilla tiedonsiirtoon käytettävä HTTP HTTPS:llä, joka salaa tiedon ennen sen siirtämistä. HTTPS:n käyttö on tärkeää esimerkiksi kirjautumissivulla, koska muuten kirjautumistieto voidaan kaapata selkokielisenä. (What Is SSL (Secure Sockets Layer) and What Are SSL Certificates? 2016.)

SSL ja TLS ovat saman protokollan eri versioita: SSL-versio 3.0:n jälkeen protokolla nimettiin uudelleen, ja uudeksi versioksi tuli SSL 4.0:n sijaan TLS 1.0. Protokollan uusin valmis versio on TLS 1.2. Vaikka protokollan nimi onkin nykyään TLS, kutsutaan sitä silti vielä yleisesti SSL:ksi ja protokollassa käytettäviä sertifikaatteja TLS-sertifikaattien sijaan SSL-sertifikaateiksi. (Mt.)

SSL/TLS toimii käyttämällä sertifikaatteja, jotka vaativat avainparin: julkisen ja yksityisen avaimen. Avaimia käytetään yhdessä salatun yhteyden luomisessa. Sertifikaatin hankkimiseksi on lähetettävä CSR (Certificate Signing Request) jollekin SSL-sertifikaattien tarjoajalle eli CA:lle (Certificate Authority). Tällä tavoin saadaan luotua

julkinen ja yksityinen avain omalle palvelimelle ja lähetettyä CA:lle julkinen avain, joka sisältyy CSR:iin. CA käyttää CSR:iin sisältyvää tietoa luodakseen tietorakenteen, joka täsmää yksityiseen avaimeen luovuttamatta kuitenkaan sitä CA:lle. CA ei koskaan näe yksityistä avainta. CA:n luovuttaman SSL-sertifikaatin lisäksi omalle palvelimelle asennetaan toinen sertifikaatti, joka sitoo CA:lta saadun sertifikaatin CA:n juurisertifikaattiin toimimalla niiden välillä. CA:n juurisertifikaatti ja palvelimella oleva sertifikaatti eivät ole siis suoreen kytköksissä toisiinsa. (Mt.) Kuviossa 14 on kuvattu SSL/TLS:n käyttämä sertifikaattiketju.



Kuvio 14. SSL/TLS-sertifikaattiketju

Yhteydenmuodostus selaimen ja SSL-suojatun verkkosivun välillä toimii suorittamalla ”SSL-kättely” selaimen luodessa yhteyden palvelimelle. Käyttäjälle kättely on täysin näkymätön eikä vaadi mitään toimia. Kättely käyttää kolmea eri avainta: julkista, yksityistä ja istuntoavainta. Kaikki julkisella avaimella salatut tiedot voidaan purkaa yksityisellä avaimella ja päinvastoin. Koska avainten purkaminen ja salaaminen vievät paljon prosessorin tehoja, käytetään julkista ja yksityistä avainta vain SSL-kättelyssä, jossa luodaan symmetrinen istuntoavain. Yhteyden luomisen jälkeen istuntoavainta käytetään kaikkeen salaukseen ja sen purkamiseen. (Mt.)

4.2.2 Let’s Encrypt

SSL-sertifikaatteja on mahdollista hankkia eri tarjoajilta, kuten DigiCert, Comodo ja GlobalSign. Sertifikaatit ovat yleensä maksullisia ja ne ovat voimassa tietyn määräajan. Let’s Encrypt on Internet Security Research Group:n (ISRG) luoma ilmainen, automaattinen ja vapaa CA, jonka tarkoituksena on parantaa internetin tietoturvallisuutta ja yksityisyyden kunnioittamista. Portaalissa käytetään Let’s Encyptin tarjoamia sertifikaatteja. (About Let’s Encrypt 2016.)

4.2.3 SSL Labs

SSL Labs on sivusto, jossa voidaan testata eri sivustojen SSL-konfiguraation tietoturvaa. SSL Labs on epäkaupallinen tutkimus, johon sisältyy SSL:iin liittyviä asiakirjoja, työkaluja ja ajatuksia. SSL Labs:n tarkoituksena on ymmärtää ja parantaa SSL:iä sekä myös kehittyä paikaksi, jossa SSL:stä voidaan keskustella ja sitä voidaan kehittää. SSL Labs -sivustolle voidaan syöttää testattavan sivuston osoite ja SSL Labs antaa sen SSL-konfiguraatiosta arvosanan sekä tarvittaessa parannusehdotuksia SSL-tietoturvan parantamiseksi. (Ristić n.d.)

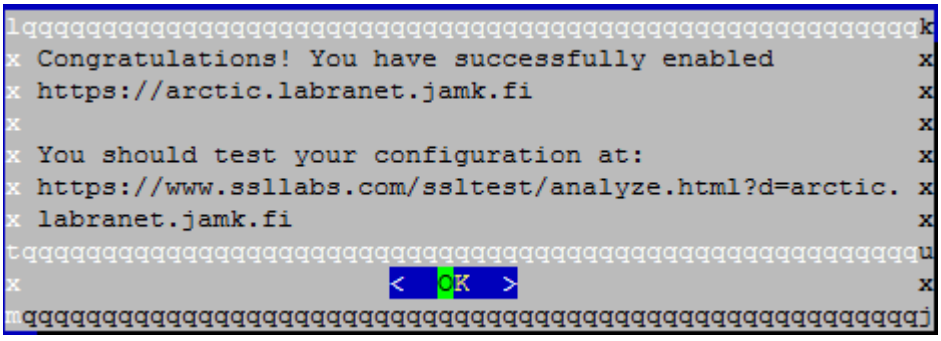
4.2.4 SSL:n käyttöönotto

SSL vaatii toimiakseen OpenSSL- ja mod_ssl-komponentit, jotka saadaan asennettua komennolla *yum install openssl mod_ssl*. OpenSSL sisältää SSL:n toimintaan tarvittavat työkalut, ja mod_ssl on Apachen käyttöliittymä OpenSSL:iin. OpenSSL:n avulla luodaan yksityinen avain ja CSR. Kuviossa 15 on esitetty tarvittavat komennot. Kuviossa ovat myös näkyvillä kentät, jotka tulee täyttää CSR:ia luodessa. Avain ja CSR tulee vielä siirtää niille asianmukaiseen hakemistoon */etc/pki/tls/private*, mikä onnistuu komennoilla *cp ca.key /etc/pki/tls/private/ca.key* ja *cp ca.csr /etc/pki/tls/private/ca.csr.*

```
[root@arctic ~]# openssl genrsa -out ca.key 2048
Generating RSA private key, 2048 bit long modulus
.....................................+++
.....................................................+++
e is 65537 (0x10001)
[root@arctic ~]# openssl req -new -key ca.key -out ca.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:FI
State or Province Name (full name) []:
Locality Name (eg, city) [Default City]Jyväskylä
Organization Name (eg, company) [Default Company Ltd]:Arktiset Rakenteet
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:arctic.labranet.jamk.fi
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@arctic ~]#
```

Kuvio 15. Yksityisen avaimen ja CSR:n luominen

Let’s Encryptin sertifikaatti saadaan hankittua Certbotilla, joka on automaattisesti toimiva sertifikaattien hankinta- ja asennusohjelma. Certbot haetaan EPEL-pakettivarastosta (Extra Packages for Enterprise Linux). Certbot saadaan asennettua komennolla *yum install python-certbot-apache* ja käynnistettyä komennolla *certbot --apache.* Certbot hankkii ja asentaa Let’s Encryptin tarjoaman sertifikaatin automaattisesti. Onnistuneen sertifikaatin asennuksen lopuksi näkyy kuvion 16 esittämä ruutu. Ruudussa on myös osoite SSL Labs -sivustolle, missä voidaan testata ja arvioida SSL:n konfiguraation tietoturvaa.



Kuvio 16. Sertifikaatin onnistunut asennus

Klikkaamalla edellisen kuvion linkkiä saadaan testattua SSL:n konfiguraatiota SSL Labs -sivustolla. Kuviossa 17 on näkyvillä sivuston antama arvostelu konfiguraation tietoturvallisuudelle kokonaisuudessaan ja eri osa-alueittain. Arvosteluun on myös merkitty konfiguraatiossa olevat merkittävät puutteet.

Kuvio 17. SSL-konfiguraation arvostelu

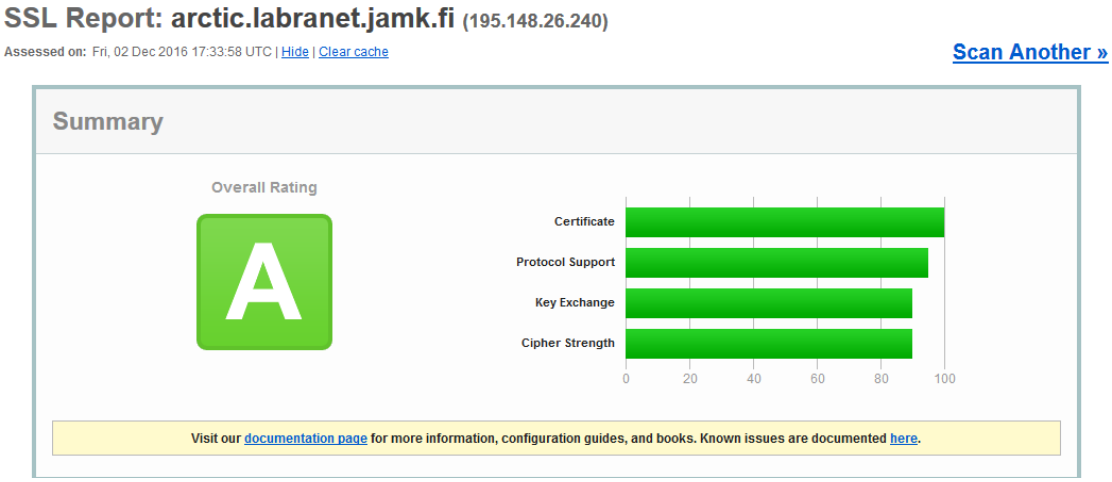
Puutteet konfiguraatiossa ovat siis RC4-salauksen ja ”forward secrecyn” tukemisessa, ja kokonaisarvioksi on luokiteltu B. RC4-salaus on tietoturvallisesti heikko, ja se kannattaa poistaa palvelimelta kokonaan käytöstä. Forward secrecy on salausjärjestelmän ominaisuus, jolla estetään aiemmin salattujen viestien tietoturvan vaarantuminen murretun salausavaimen johdosta.

Forward secrecy otetaan käyttöön asettamalla palvelin ottamaan käyttöön turvallisimmat ja nopeimmat avaimenvaihtoprotokollat sen mukaan, mitä palvelimelle yhteyttä ottava asiakas tukee. Forward secrecyn tukeminen ja RC4:n käytöstä poistaminen saadaan toimimaan lisäämällä palvelimen SSL-konfiguraatiotiedostoon */etc/httpd/conf.d/ssl.conf* seuraavat rivit:

SSLHonorCipherOrder on

SSLCipherSuite "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384 EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH EDH+aRSA RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS !RC4"

Nyt voidaan testata SSL:n konfiguraatiota uudestaan. Kuviosta 18 huomataan, että kokonaisarvio on nyt nostettu A:han, eikä siihen ole merkitty mitään merkittäviä puutteita.



Kuvio 18. Korjatun SSL-konfiguraation arvostelu

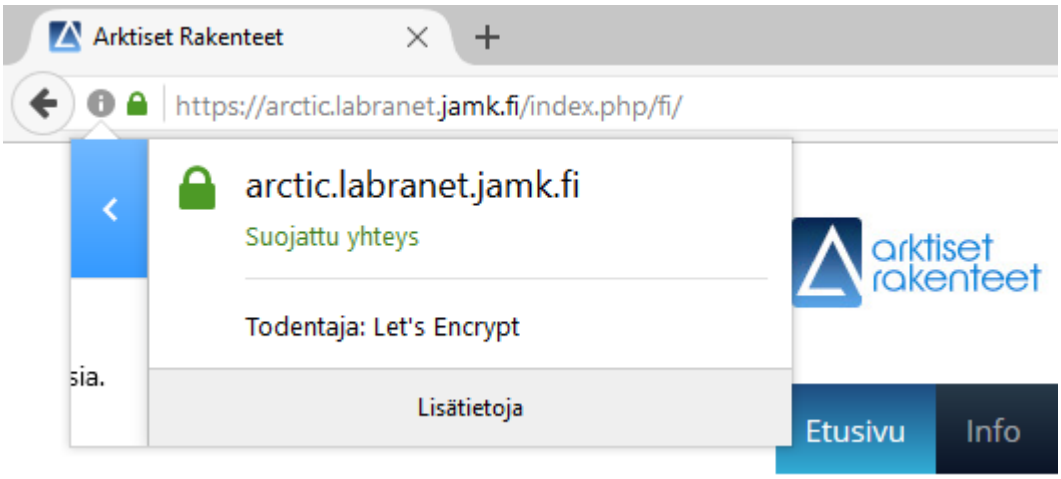
Let's Encrypt:n sertifikaatti on voimassa vain 90 päivää, joten sertifikaatin uusiminen kannattaa tehdä automaattisesti. Komennolla *certbot renew --dry-run* saadaan uusittua nykyinen sertifikaatti. Sertifikaatti voidaan uusia automaattisesti crontab-skriptillä. Kuviossa 19 on esitetty kyseinen crontab-skripti. Skripti on mahdollista ajaa säännöllisesti ja usein, sillä sertifikaatti uusitaan vain, kun sen viimeinen voimassaolopäivämäärä on lähellä. Skripti ajetaan kahdesti päivässä: klo 05:37 ja klo 09:37 hiljaa siten, ettei siitä tule muuta tulostetta käyttäjälle kuin mahdolliset virheet.

```
#Certificate renew
37 5,19 * * * root certbot renew --quiet
```

Kuvio 19. Sertifikaatin uusimiseen käytettävä crontab-skripti

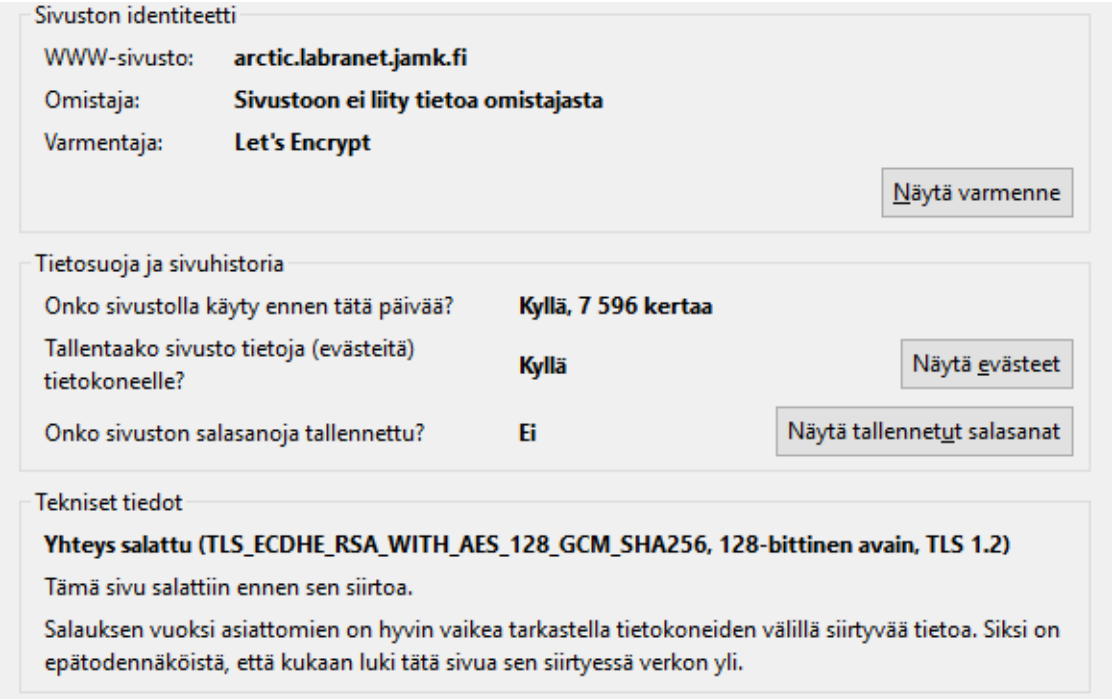
4.2.5 SSL:n toiminnan todennus

Toimiva HTTPS-yhteys voidaan todentaa Mozilla Firefox -selaimella sivustolla ollessa ikkunan vasemmasta yläreunasta osoiterivin vieressä olevasta vihreästä lukosta, jotka on esitetty kuviossa 20. Lukkoa klikkaamalla saadaan näkyville lisätietoja SSL:n toimivuudesta.



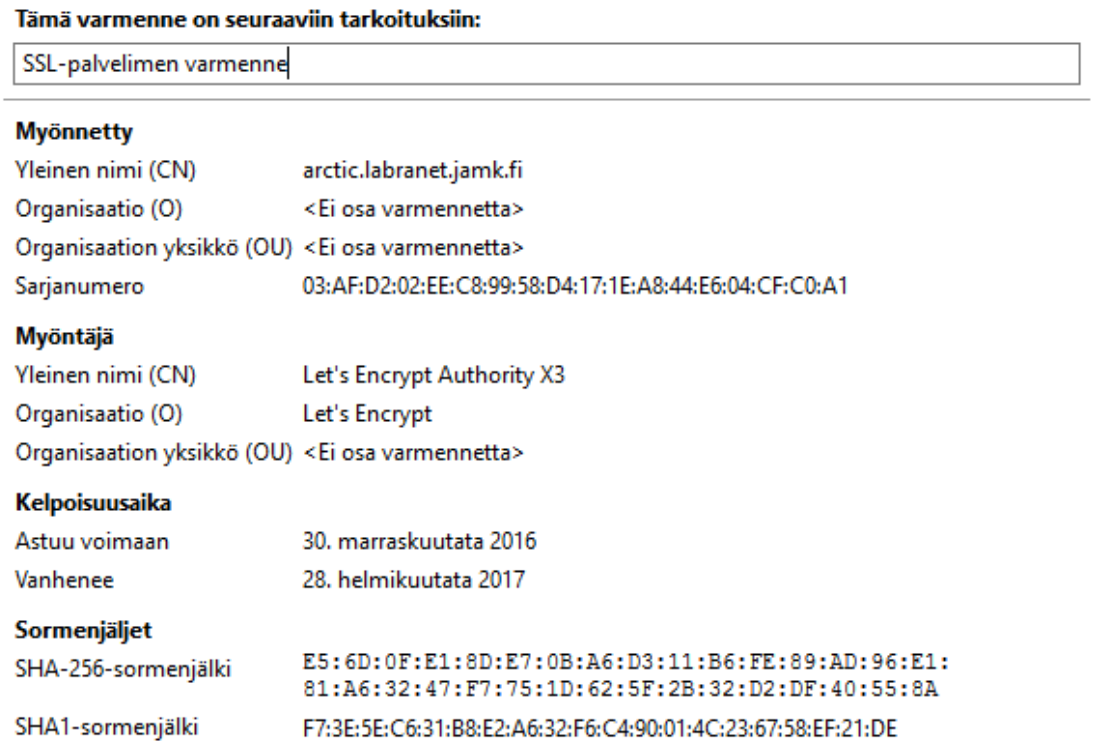
Kuvio 20. HTTPS:n toimivuuden todennus

Klikkaamalla *Lisätietoja* saadaan näkyville kuvion 21 esittämä ikkuna. Ikkunassa näkyy lisätietoja sivustosta, sen tietosuojasta ja salauksesta.



Kuvio 21. Lisätietoja sivustosta

Klikkaamalla *Näytä varmenne* saadaan näkyville lisätietoja sivuston SSL:n toiminnasta. Ikkunassa näkyy lisätietoja sivustosta, sertifikaatin myöntäjästä, sertifikaatin voimassaoloajasta ja sivuston kryptografisesta tiivistämisestä, kuten kuviosta 22 voidaan huomata.



Kuvio 22. Lisätietoja varmenteesta

4.3 Palomuuri

Palvelimelle on asetettu palomuuri internetiin kiinni olevaan *ens192*-rajapintaan. Palomuuri on asetettu sallimaan DHCP-liikenteen (Dynamic Host Configuration Protocol) IP-osoitteen hakemista varten, HTTP- ja HTTPS-liikenteen tiedonsiirtoon sivuston ja käyttäjän välillä (vaikka sivusto käyttää kaikkeen tiedonsiirtoon HTTPS:ää, tulee HTTP myös sallia, jotta HTTP-pyynnöt voidaan ohjata HTTPS:ään) ja SSH-liikenteen (Secure Shell) etäyhteyden muodostamiseksi palvelimelle. Kuviossa 23 on todennettu palomuurin asetukset ja että palomuuri on toiminnassa.

```
[root@arctic ~]# firewall-cmd --zone=public --list-all
public
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: dhcpv6-client http https ssh
  ports: 8000/tcp 10000/tcp
  protocols:
  masquerade: no
  forward-ports:
  sourceports:
  icmp-blocks:
  rich rules:

[root@arctic ~]# firewall-cmd --state
running
[root@arctic ~]#
```

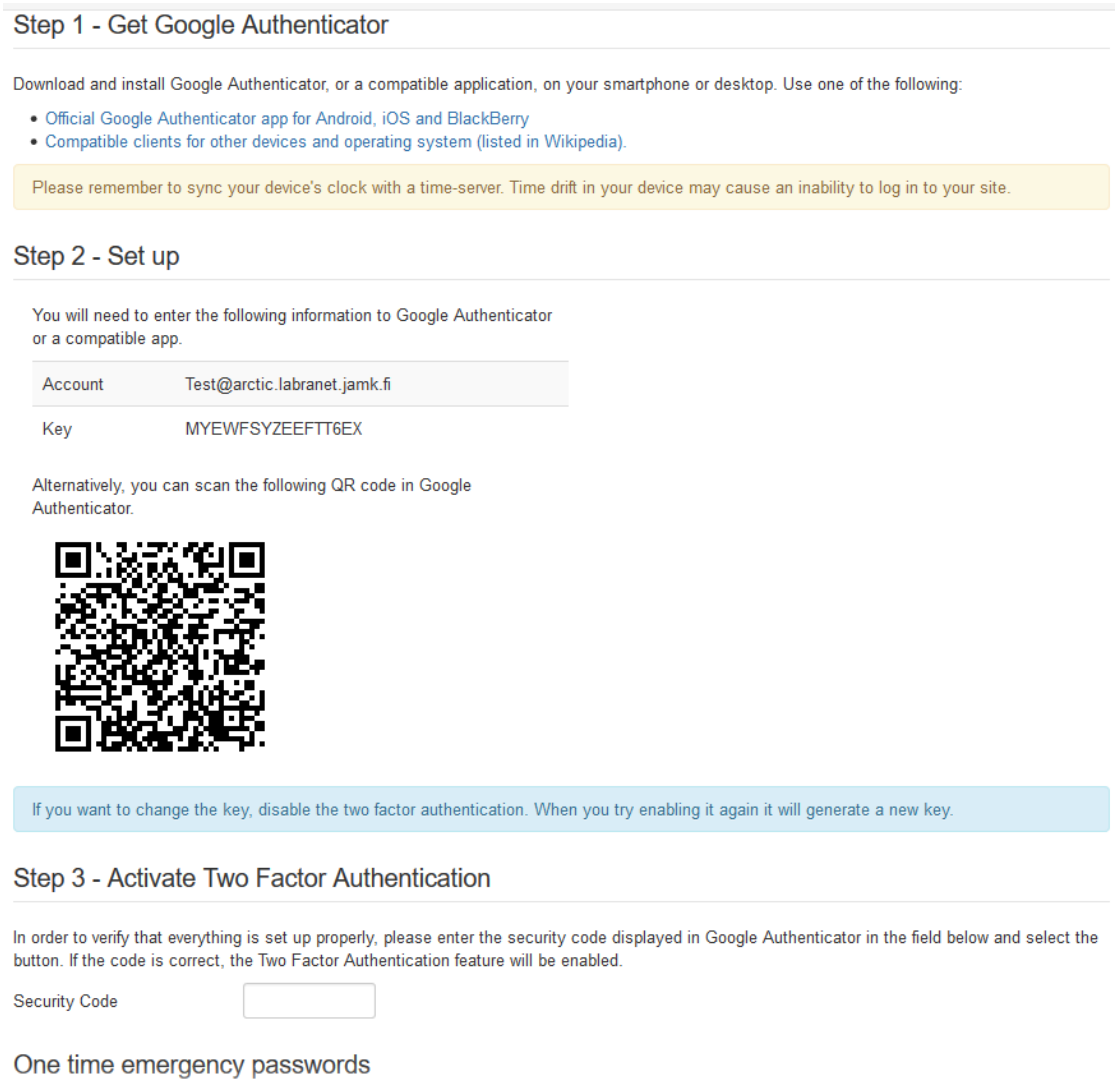
Kuvio 23. Palomuuri

4.4 Two Factor Authentication

Portaalin hallintapaneeliin sisäänkirjautumisessa on käytössä Two Factor Authentication, jota käytetään Google Authenticatorilla. Vaihtoehtoisesti on myös mahdollista ottaa käyttöön YubiKey, joka on USB-laitteella toimiva käyttäjän todennus. Google Authenticator toimii siten, että hallintapaneeliin kirjautuessa tulee syöttää käyttäjänimen tai salasanan lisäksi 30 sekunnin välein vaihtuva tunnusluku. Tunnusluku on näkyvillä halutulle laitteelle asennetussa Google Authenticator -sovelluksessa, joka on linkitetty portaalin käyttäjään. Jos käyttöön halutaan ottaa YubiKey, tulee siinä kirjautuessa sisään käyttäjätunnuksen ja salasanan syöttämisen lisäksi asettaa YubiKey-laite tietokoneen USB-porttiin. Two Factor Authenticator lisää kirjautumisen turvallisuutta, sillä vaikka sivustolle hyökkääjä olisi saanut ylläpitäjän tunnukset haltuunsa, tarvitsee hänen vielä saada oikein tunnusluku, joka vaihtuu 30 sekunnin välein.

Google Authenticator otetaan käyttöön sallimalla Two Factor Authentication - Google Authenticator -liitännäinen. Liitännäisen voi ottaa käyttöön sivuston julkisessa tai hallintapaneeliin kirjautumisessa tai molemmissa. Portaalissa liitännäinen on käytössä vain hallintapaneeliin kirjautuessa. Google Authenticator otetaan käyttöön käyttäjälle hallintapaneelin yläosasta välilehdeltä *Users > Manage*, valitsemalla käyttäjä, menemällä *Two Factor Authentication* -välilehteen ja valitsemalla Google

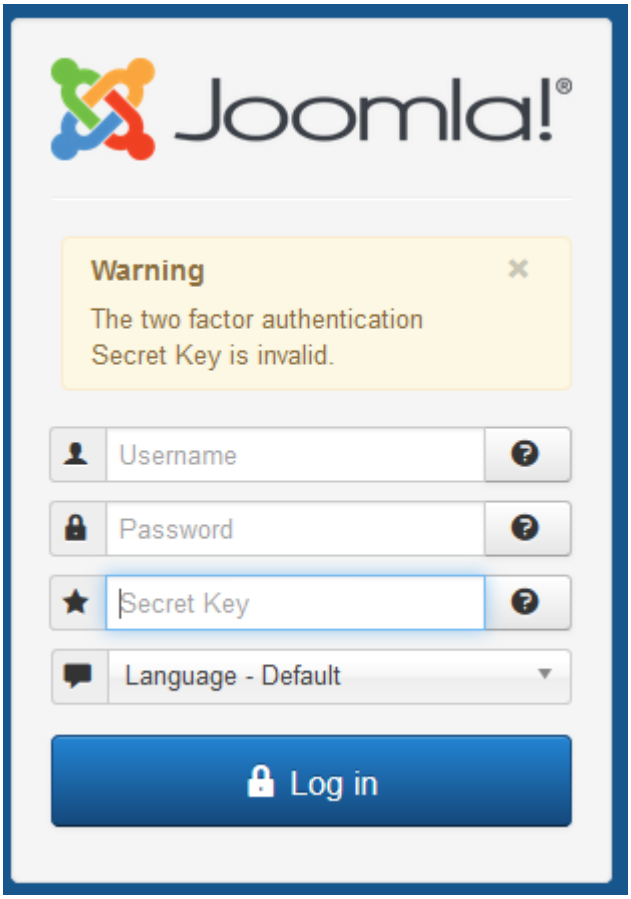
Authenticator. Kuviossa 24 on esitetty *Two Method Authentication* -välilehden askeleet Google Authenticatorin käyttöönottoon.



Kuvio 24. Google Authenticatorin käyttöönotto

Kuvion mukaisesti asennetaan Google Authenticator halutulle laitteelle ja joko syötetään kyseiseen sovellukseen askeleen 2 käyttäjä ja avain tai skannataan laitteella QR-koodi. Google Authenticator -laitteelle tulee sitten 30 sekunnin välein vaihtuva tunnusluku, joka syötetään askeleen 3 Security Code -kenttään ja tallennetaan sivu. Google Authenticator on nyt otettu käyttöön valitulle käyttäjälle ja kirjautumisen yhteydessä tulee nyt aina syöttää 30 sekunnin välein vaihtuva tunnusluku. Google Aut-

henticatorin käyttöönoton yhteydessä luodaan myös muutamia kertakäyttöisiä salasanoja, jotka tuhotaan käytön jälkeen. Ne voidaan tallentaa, jolloin niitä on mahdollista käyttää, jos pääsy Google Authenticator -laitteelle on jostain syystä estynyt. Kuviossa 25 on vielä esitetty todennus siitä, ettei hallintapaneelin voi kirjautua ilman Google Authenticator -tunnuslukua, jos sellainen on käyttäjälle asetettu.

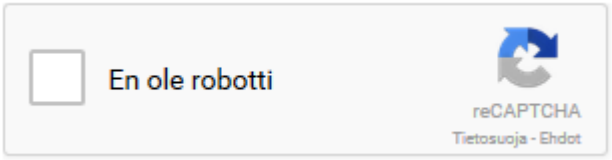


Kuvio 25. Estetty hallintapaneeliin sisäänkirjautuminen

4.5 ReCaptcha

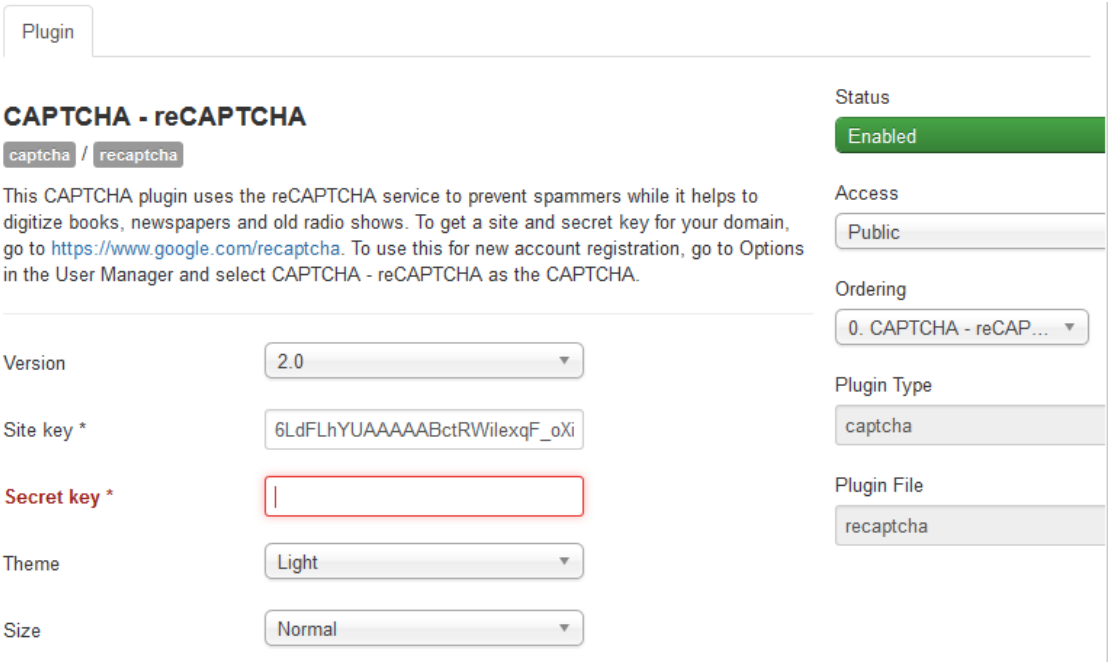
ReCaptcha on Googlen palvelu, jonka tavoitteena on varmistaa palvelun käyttäjän olevan ihminen. Tällä voidaan estää esimerkiksi botteja lähettämästä roskapostia tai muuta ei-toivottua sisältöä. Portaalissa reCaptcha on käytössä kaavakkeissa ja sen ta-

voitteena on estää mahdollisia roskapostittajia täyttämästä automatisoidusti kaavakkeita. Kuviossa 26 on näkyvillä portaalissa käytettävä reCaptcha ja sivun 50 kuviossa 45 on näkyvillä reCaptcha liitettynä kaavakkeeseen.



Kuvio 26. ReCaptcha

ReCaptcha otetaan käyttöön sallimalla CAPTCHA – reCAPTCHA -liitännäinen ja rekisteröimällä haluttu toimialue osoitteeseen https://www.google.com/recaptcha. Kun toimialue on rekisteröity, saadaan kaksi avainta: Site Key, joka on sivuston ja käyttäjän välillä toimiva avain ja Secret Key, joka on sivuston ja Googlen välillä toimiva avain. Secret Key tulee pitää salassa ulkopuolisilta osapuolilta. Avaimet sitten syötetään Site Key -ja Secret Key -kenttiin. ReCaptcha on nyt mahdollista liittää haluttuun kohtaan sivustoa. Kuviossa on esitetty reCaptcha-liitännäisen asetukset. Secret Key on poistettu kuviosta.



Kuvio 27. ReCaptcha-liitännäisen asetukset

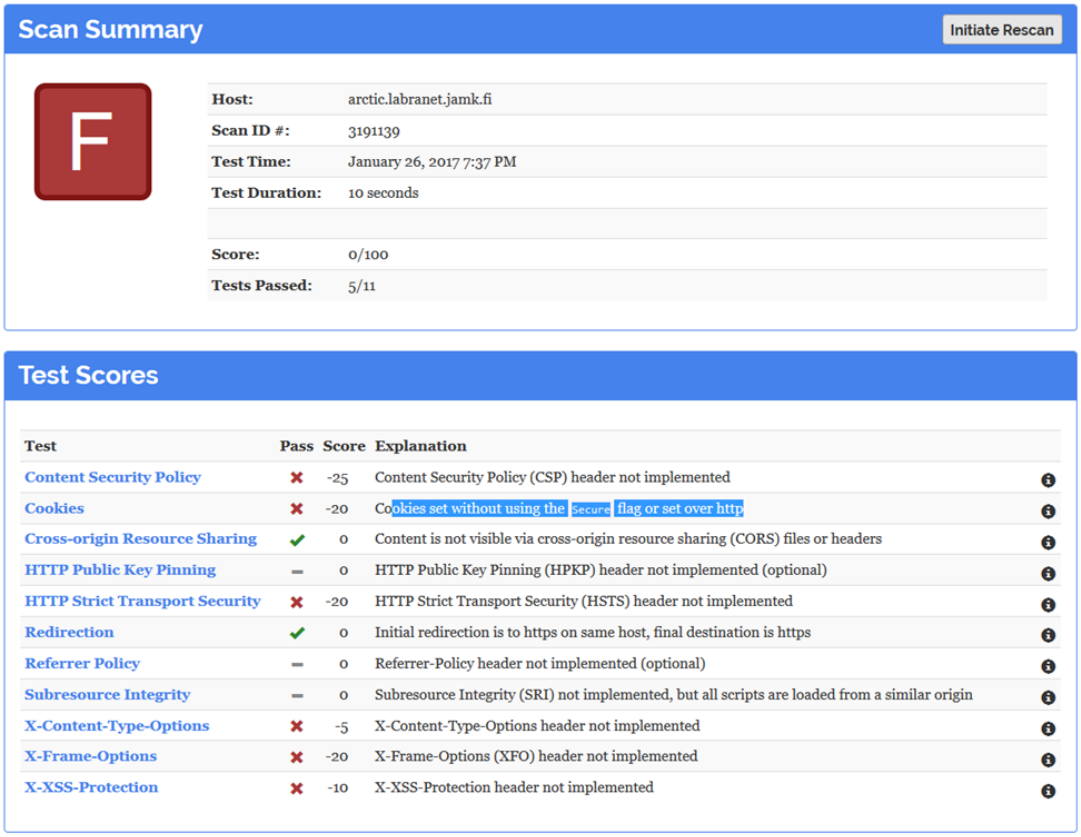
4.6 Tietoturvan testaus

4.6.1 Mozilla Observatory

Mozilla Observatory on ilmainen palvelu, jolla voidaan testata verkkosivuja ylläpitävien palvelinten tietoturvakonfiguraatioita ja -asetuksia. Sivusto on ottanut inspiraatioita aikaisemminkin käytetystä SSL/TLS-konfiguraatiota testaavasta SSL Labs -sivustosta, mutta Observatorylla testataan laajemmalla skaalalla verkon eri tietoturvamekanismeja. Observatory testaa ovatko kyseiset teknologiat yleensä käytössä sivustolla ja onko niiden toteutus tehty oikein. (Constantin 2016.)

4.6.2 Tietoturvan testaus Observatorylla

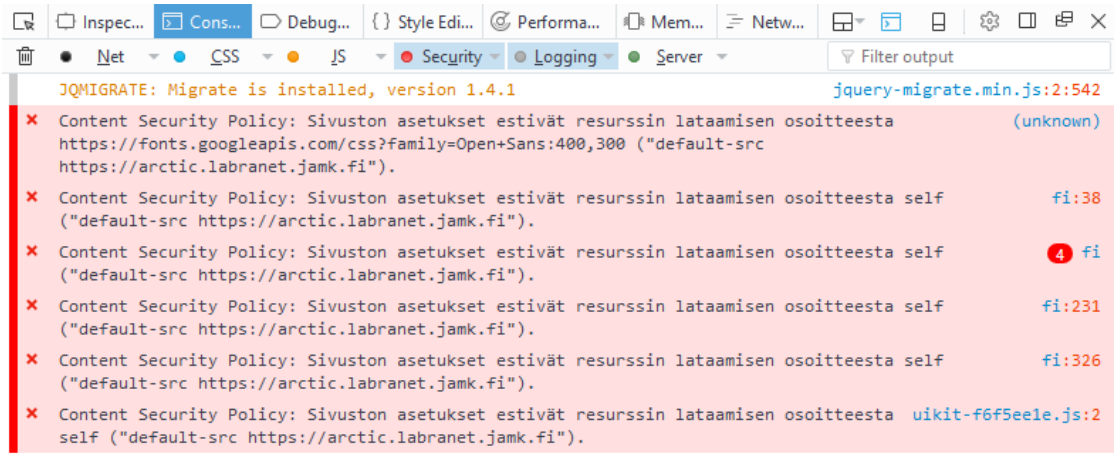
Arktiset Rakenteet -portaalin ensimmäinen testaus Mozilla Observatorylla ei antanut hyvää tulosta: palvelun 11 suorittamasta testistä vain 5 meni läpi ja kokonaisuudessaan testi hylättiin arvosanalla F. Kuviossa 28 on esitetty ensimmäisen testin antamat tulokset.



Kuvio 28. Tietoturvan arvostelu Observatorylla

Content Security Policy (CSP) on HTTP-kehys, joka antaa sivuston operaattoreille tarkan hallinnan mistä sivuston resurssit voidaan ladata. CSP on paras XSS-haavoittuvuuksien (cross-site scripting) estämiseen käytettävä metodi. CSP otetaan käyttöön lisäämällä rivi *Header set Content-Security-Policy "default-src 'self';"* HTTP-konfiguraatiotiedostoon */etc/httpd/conf/httpd.conf.* Nyt XSP sallii sisällön lataamisen vain sivustosta itsestään. (Web Security 2017.)

Kuitenkin nyt CSP estää myös sivustolle tarpeellisen sisällön lataamisen. CSP:n sisällön lataamisen estämiset voidaan nähdä esimerkiksi Mozilla Firefox -selaimella klikkaamalla Inspect Element ja siirtymällä Console-välilehteen. Kuviossa 29 on esitetty CSP:n estot portaalin etusivulta.



Kuvio 29. CSP:n estämä tarpeellinen sisältö portaalin etusivulla

CSP:n *Default-src* -kohtaan lisätään kaikkien muiden kohtien oletustoiminta, jos ne jätetään tyhjäksi. Portaalin CSP-otsikossa on käytössä myös kohdat *script-src* ja *style-src*: *script-src* -kohdassa määritetään mistä lähteistä sallitaan skriptejä suoritettavaksi ja *style-src* -kohdassa määritetään mistä lähteistä sallitaan tyylitaulukot. Alla on esitetty uusi HTTP-konfiguraatiotiedoston CSP-otsikko. (Content Security Policy Reference 2016.)

> *Header set Content-Security-Policy: "default-src 'self' https://platform.twitter.com https://cdn.syndication.twimg.com https://syndication.twitter.com https://pbs.twimg.com https://www.google.com/recaptcha/ data:; script-src 'self' https://platform.twitter.com https://cdn.syndication.twimg.com https://syndication.twitter.com https://www.google.com/recaptcha/ https://www.gstatic.com/recaptcha/ 'unsafe-eval' 'unsafe-inline'; style-src 'self' https://platform.twitter.com 'unsafe-inline' https://fonts.googleapis.com"*

Ulkoisista lähteistä ladattu sisältö saadaan sallittua lisäämällä kyseiset lähteet CSP-otsikkoon. Otsikkoon lisätyt ulkoiset lähteet ovat tarpeellisia Twitterin, reCaptchan ja joidenkin fonttien toimintaan. Lisäksi sallittiin resurssien lataaminen data-järjestelmän kautta arvolla *data:*. *Script-src* ja *style-src* -kohtiin lisättiin vielä arvo *'unsafe-inline'*, jolla sallitaan avoimien lähde-elementtien lataaminen, ja *script-src* -kohtaan arvo *'unsafe-eval'*, jolla sallitaan dynaaminen koodin määritys, kuten JavaScript. Kyseisten *”unsafe”*-arvojen käyttäminen *script-src*:ssä on tietoturvallisesti epäluotettavaa,

mutta CSP:n käyttäminen ilman näitä arvoja on teknisesti hankalaa ja uudet lisäykset sivustolle tulisivat olla huomioituna CSP:ssä toimiakseen. (Mt.)

Cookies, eli evästeet ovat palvelimen tallentamaa tietoa sivuston käyttäjän laitteelle. Evästeet tulee luoda siten, että niihin pääsy on mahdollisimman rajoitettua. Siten saadaan minimoitua XSS-haavoittuvuuksien aiheuttama vahinko evästeiden sisältäessä yleensä arkaluontoista tietoa. Tämä saadaan toteutettua lisäämällä HttpOnly- ja Secure -liput HTTP-vastausotsikkoon. Se onnistuu lisäämällä rivi *Header edit Set-Cookie ^(.*)$ $1;HttpOnly;Secure* HTTP-konfiguraatiotiedostoon */etc/httpd/conf/httpd.conf*. (Web Security 2017)

Cross-origin Resource Sharing on HTTP-otsikko, jolla voidaan määrittää mille ulkopuolisille lähteille on sallittua päästä käsiksi sivuston tietoihin sen toimialueella skriptien kautta. Cross-origin Resource Sharing ei ole käytössä sivustolla, joten muutoksia ei tarvitse tehdä. (Mt.)

HTTP Public Key Pinning (HPKP) ohjaa sivustoa käyttävää selainta yhdistämään sivuston tiettyyn CA:n juuri- tai välittäjäsertifikaattiin tai loppukäyttäjän julkiseen avaimeen. Tämä estää CA:ta luovuttamasta luvattomia sertifikaatteja toimialueille, joilla olisi jo SSL/TLS-luottosuhde selaimien kanssa. Näillä väärennetyillä sertifikaateilla voi olla mahdollista, että hyökkääjä pystyy esiintymään uhrin sivustona ja saaden näin haltuunsa käyttäjätietoja ja muuta arkaluonteista tietoa. HPKP ei ole kuitenkaan suositeltavaa ottaa käyttöön muissa kuin vahvimman tietoturvan vaativimmilla sivustoilla. Syynä tähän on pieni riski edellä mainittuun hyökkäykseen ja HPKP:n käyttöön ottamisen vaativuus, sillä väärin asetettu HPKP saattaa poistaa sivustolta pääsyn internetiin. HPKP:ta ei otettu käyttöön Arktiset Rakenteet -tietoportaaliin. (Mt.)

HTTP Strict Transport Security (HSTS) on HTTP-otsikko, joka ohjaa sivuston käyttäjät käyttämään HTTPS:ää vaikka valittuna olisikin HTTP. Kaikki selaimen pyynnöt myöskin muutetaan HTTPS:ksi. HSTS myös pakottaa selaimet käsittelemään SSL/TLS- ja sertifikaatti-aiheisia virheilmoituksia vakavammin estämällä selainten käyttäjiä ohittamasta virhesivua. HSTS saadaan käyttöön lisäämällä rivi *Header always set Strict-Transport-Security "max-age=63072000; includeSubdomains;"* HTTP-konfiguraatiotiedostoon */etc/httpd/conf/httpd.conf.* Maksimiajaksi asetettiin kaksi vuotta ja se on aika, kuinka pitkään palvelimen tulee tukea HTTPS:ää maksimiajan asettamisesta lähtien. HSTS-

konfiguraatioon lisättiin myös lapsitoimialueet, mikä tarkoittaa että myös lapsitoimialueiden tulee tukea HTTPS:ää. (Mt.)

Redirectionillä varmistetaan, että jos sivustolle yritetään muodostaa HTTP-yhteys, kaikki yritykset uudelleenohjataan HTTPS-muotoon ja samaan resurssiin, mihin yhteyttä yritettiin muodostaa. HTTP-uudelleenohjaus toimi sivustolla jo ennestään, joten siihen ei tarvinnut tehdä muutoksia. (Mt.)

Referrer Policylla voidaan hallita, miten sivustolla olevista linkeistä nähdään niiden alkuperäosoite. Kun käyttäjä klikkaa sivustolla olevaa linkkiä, lähetetään linkin päässä olevalle sivustolle HTTP Referer -otsikko, josta nähdään linkin alkuperäosoite. Referrer Policylla voidaan estää tämän otsikon lähettäminen. Arktiset Rakenteet -portaalissa ei ole tarvetta piilottaa linkkien alkuperää, joten Referrer Policya ei otettu käyttöön. (Mt.)

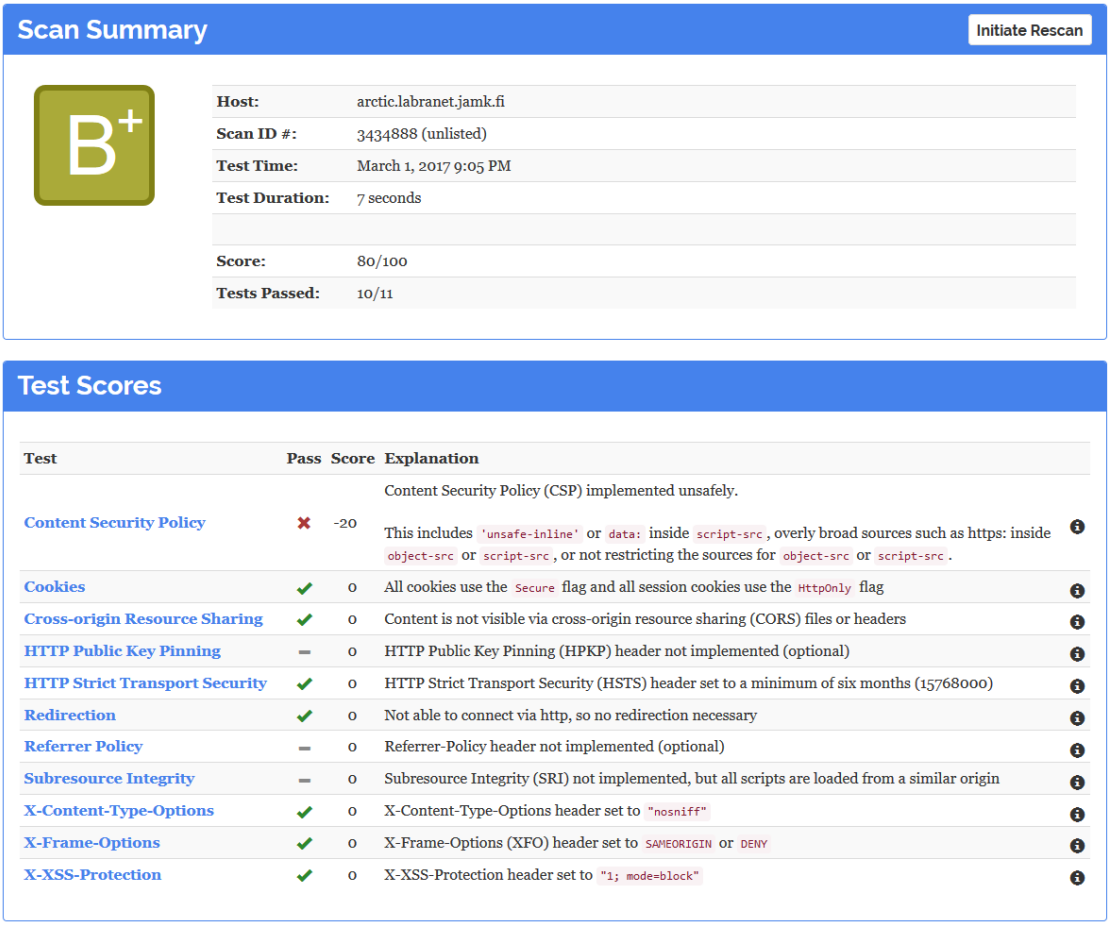
Subresource Integrity on W3C-standardi, joka suojaa CDN-verkoissa sijaitsevien JavaScript-kirjastojen sisältöä muuttavilta hyökkääjiltä. Hyökkäyksen tarkoituksena on luoda haavoittuvuuksia kaikille sivustoille, jotka käyttävät tätä kirjastoa. Tällaisia kirjastoja ei ole portaalissa käytössä, joten Subresource Integritya ei ole tarvetta ottaa käyttöön. (Mt.)

X-Content-Type-Options on Internet Explorerin, Google Chromen ja Mozilla Firefoxin tukema otsikko, joka kertoo selaimelle olematta lataamasta skriptejä ja tyylitaulukkoja ellei palvelin osoita olevansa oikeaa MIME-tyyppiä (Multipurpose Internet Mail Extensions). Ilman tätä otsikkoa edellä mainitut selaimet saattavat virheellisesti havaita tiedostoja skripteinä tai tyylitaulukkoina johtaen XSS-hyökkäykseen. X-Content-Type-Options otetaan käyttöön lisäämällä rivi *Header set X-Content-Type-Options nosniff* HTTP-konfiguraatiotiedostoon */etc/httpd/conf/httpd.conf.* (Mt.)

X-Frame-Options on HTTP-otsikko, joka sallii sivustojen hallita sivuston kehystämistä iframe-elementtiin. Tämä estää haitallisia sivustoja suorittamasta ns. clickjacking-hyökkäystä. Clickjacking on käyttäjän huijaamista klikkaamaan linkkejä, jotka näyttävät olevansa jollakin sivustolla, mutta kuuluvatkin jollekin toiselle osapuolelle. X-Frame-Options otetaan käyttöön lisäämällä rivi *Header always append X-Frame-Options SAMEORIGIN* HTTP-konfiguraatiotiedostoon */etc/httpd/conf/httpd.conf*. (Mt.)

X-XSS-Protection on toiminto Internet Explorer- ja Google Chrome -selaimissa, mikä lopettaa sivuston lataamisen, jos XSS-hyökkäys havaitaan. X-XSS-Protection otetaan käyttöön lisäämällä rivi *Header set X-XSS-Protection "1; mode=block"* HTTP-konfiguraatiotiedostoon */etc/httpd/conf/httpd.conf*. (Mt.)

Kun edellä mainitut kohdat on saatu tehtyä, voidaan suorittaa Observatoryn testi uudestaan. Tällä kertaa palvelun 11:sta testistä 10 meni läpi, poikkeuksena CSP *'unsafe-inline'*- ja *'unsafe-eval'*-arvojen olemisen CSP-otsikossa *script-src* -kohdassa takia. Testin lopulliseksi arvosanaksi tuli B+. Kuviossa 30 on esitetty kyseiset testin tulokset.



Kuvio 30. Tietoturvan lopullinen arvostelu Observatorylla

4.6.3 Joomscan

Joomscan on avoimen lähdekoodin projekti, joka on tarkoitettu haavoittuvuuksien etsimiseen ja analysoimiseen Joomla-sisällönhallintajärjestelmässä. Joomscan vertaa

tunnettuja mahdollisia Joomlan haavoittuvuuksia haluttuun Joomla-pohjaiseen sivustoon. Joomscan antaa lisätietoa haavoittuvuuksista ja niiden paikkaamisesta haavoittuvuuksia löydettäessä. (Category:OWASP Joomla Vulnerability Scanner Project 2016.)

Joomscania käytetään asentamalla se halutulle tietokoneelle ja sitten skannaamalla sillä haluttu sivusto. Kuviossa 31 on esitetty skannauksen aloittaminen komennolla, jossa skannaus on kohdistettu Arktiset Rakenteet -portaaliin ja tulokset tallennetaan skannauksen jälkeen tekstitiedostoon.

```
B:\Lataukset\joomscan-master>joomscan.pl -u https://arctic.labranet.jamk.fi -ot
output.txt

  ..|''||   '|| '||'  '|'      |      .|'''.|  '||''|.
.|'     ||   '|. '|.  .'      |||     ||..  '   ||   ||
||      ||    ||  ||  |      |  ||     ''|||.   ||...|'
'|.     ||    ||| |||     .''''|.  .    '||  ||
 ''|...|'      |   |     .|.  .||. |'....|'  .||.


===============================================================
OWASP Joomla! Vulnerability Scanner v0.0.4
(c) Aung Khant, aungkhant]at[yehg.net
YGN Ethical Hacker Group, Myanmar, http://yehg.net/lab
Update by: Web-Center, http://web-center.si (2011)
===============================================================
```

Kuvio 31. Joomscan-skannauksen aloittaminen

Skannauksen lopuksi löydettiin kaksi haavoittuvuutta 150:stä mahdollisesta haavoittuvuudesta, joihin portaalia verrattiin. Kuviossa 32 on esitetty skannauksen tulokset.

```
[!] Vulnerable Point(s) - 2 in 150 found entries
```

Kuvio 32. Skannauksen tulokset

Skannauksessa löydetyt haavoittuvuudet olivat *htaccess.txt* -tiedoston ja sivuston hallintapaneelin heikossa tietoturvassa. Kuviossa 33 on esitetty skannauksessa löydetyt haavoittuvuudet.

```
# 1
Info -> Generic: htaccess.txt has not been renamed.
Versions Affected: Any
Check: /htaccess.txt
Exploit: Generic defenses implemented in .htaccess are not available, so exploiting is more lil
Vulnerable? Yes

# 2
Info -> Generic: Unprotected Administrator directory
Versions Affected: Any
Check: /administrator/
Exploit: The default /administrator directory is detected. Attackers can bruteforce administrat
Vulnerable? Yes
```

Kuvio 33. Skannauksessa löydetyt haavoittuvuudet

Tiedoston htaccess.txt haavoittuvuus saatiin paikattua uudelleennimeämällä se .htaccess-tiedostoksi. Hallintapaneelin haavoittuvuus oli siinä, että sisäänkirjautumiseen käytettiin oletusosoitetta *arctic.labranet.jamk.fi/administrator/.* Joomlassa ei oletuksena ole mahdollista vaihtaa tätä osoitetta, mutta osoitteen vaihto onnistuu AdminExile-liitännäisellä. AdminExilella hallintapaneelin kirjautumisosoite voidaan vaihtaa muotoon *[sivuston osoite]/administrator/index.php?[haluttu merkkijono].* AdminExilella saatiin käyttöön myös brute force -hyökkäyksien torjunta hallintapaneelin kirjautumissivun etsimiseen. Tämä tehtiin asettamalla väärään kirjautumissivuun yhdistämisyritysten määrä samasta osoitteesta viiteen, jonka jälkeen kirjautumissivulle pääsy on estetty viisi minuuttia. Kuviossa 34 on esitetty tulokset toisesta skannauskerrasta, mistä nähdään ensimmäisellä skannauskerralla löydettyjen haavoittuvuuksien olevan nyt paikattu.

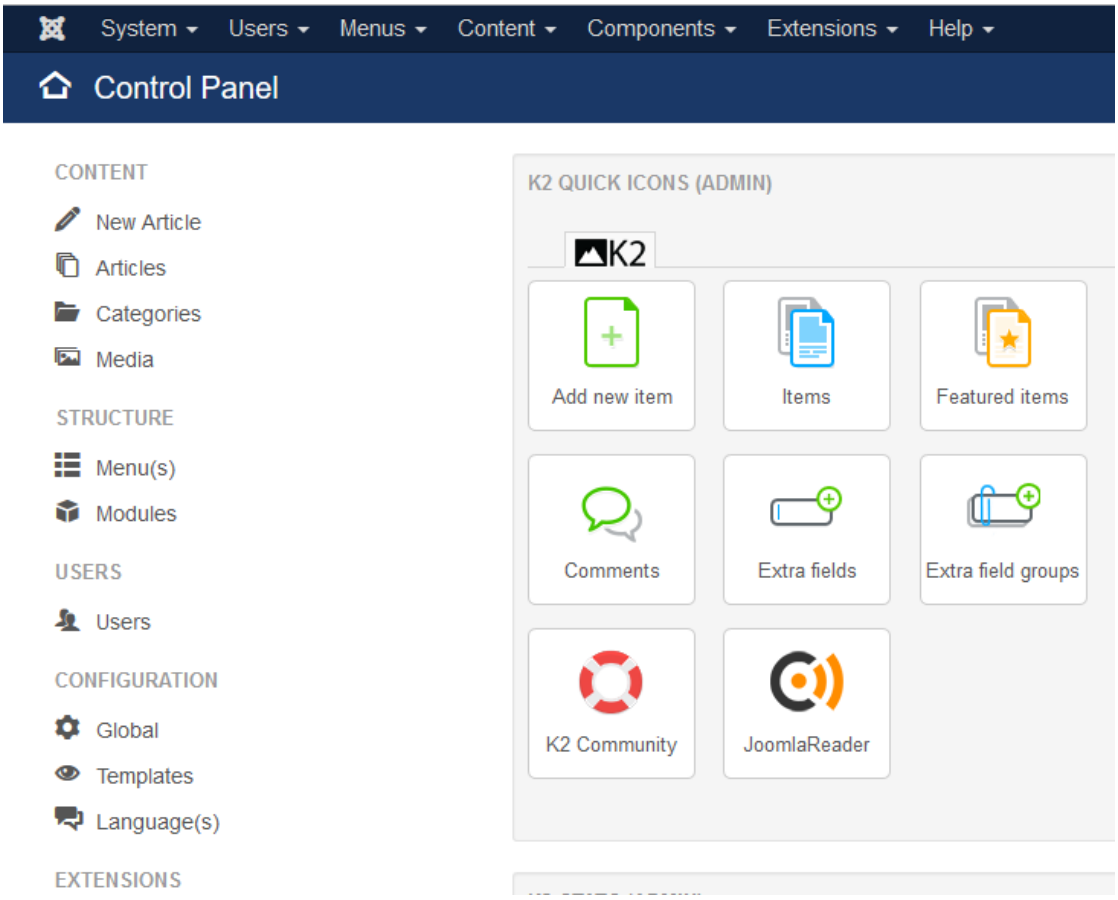
```
[!] Vulnerable Point(s) - 0 in 144 found entries
```

Kuvio 34. Toisen skannauksen tulokset

5 Portaalin hallinta

5.1 Hallintapaneeli

Sivuston hallinta toteutetaan *super users* -ryhmän käyttäjien toimesta hallintapaneelissa. Hallintapaneelista voidaan mm. hallinnoida artikkeleita, moduuleita, lisäosia, liitännäisiä, teemaa ja sivuston asetuksia. Hallintapaneelin on pääsy vain *super users* -käyttäjillä. Kuviossa 35 on esitetty osa hallintapaneelin etusivusta.



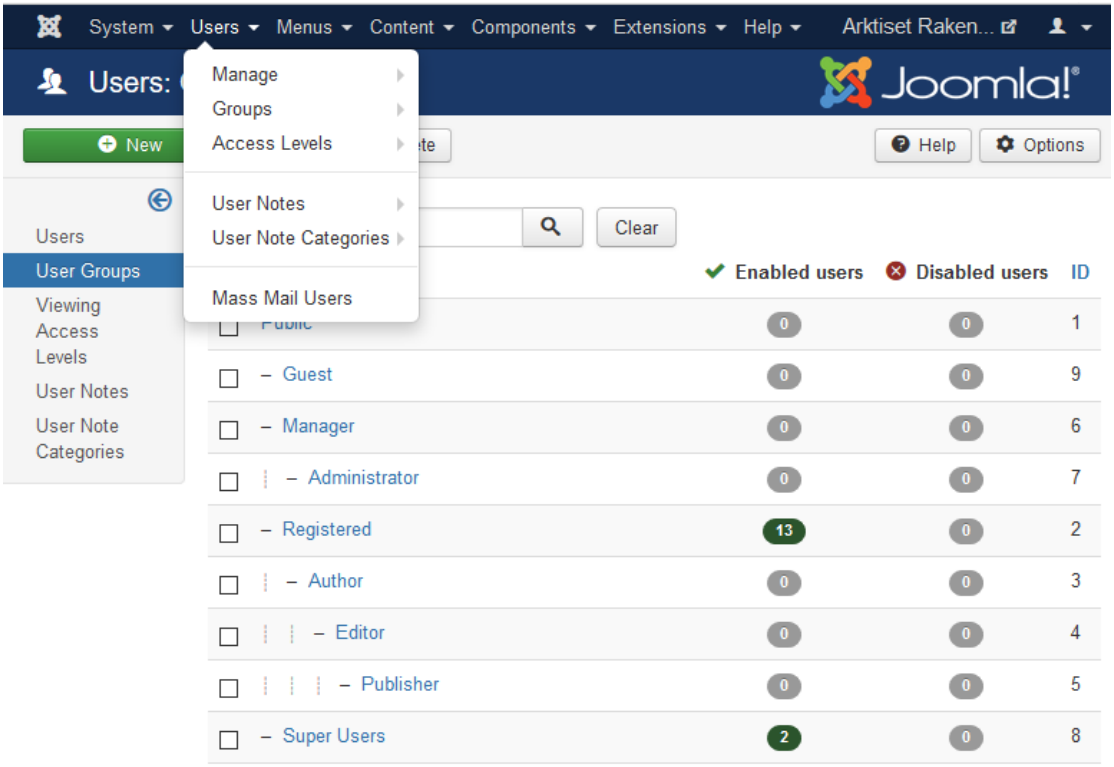
Kuvio 35. Hallintapaneelin etusivu

5.2 Käyttäjät

Portaalin käyttäjähierarkia on toteutettu siten, että käyttäjät ovat jaettu kolmeen ryhmään: *super users*, *registered* ja *public*. Käyttäjäryhmään *super users* kuuluvat

portaalin hallintapaneeliin oikeudet omaavat käyttäjät. Ryhmään kuuluvat sivuston sisällön julkaisemisesta ja kaikesta hallinnasta vastaavat käyttäjät. *Registered*-käyttäjäryhmään kuuluvat muut käyttäjätunnuksen omaavat käyttäjät. He voivat julkaista sivustolla artikkeleita, jotka ovat näkyvillä vain muille käyttäjätunnuksen omaaville käyttäjille. Kuitenkin vain *super users* -käyttäjäryhmään kuuluva käyttäjä voi julkaista niitä yleisesti näkyville. *Public*-käyttäjäryhmään kuuluvat kaikki käyttäjätunnuksettomat sivustolla kävijät, jotka näkevät vain yleisesti näkyvillä olevaa sisältöä.

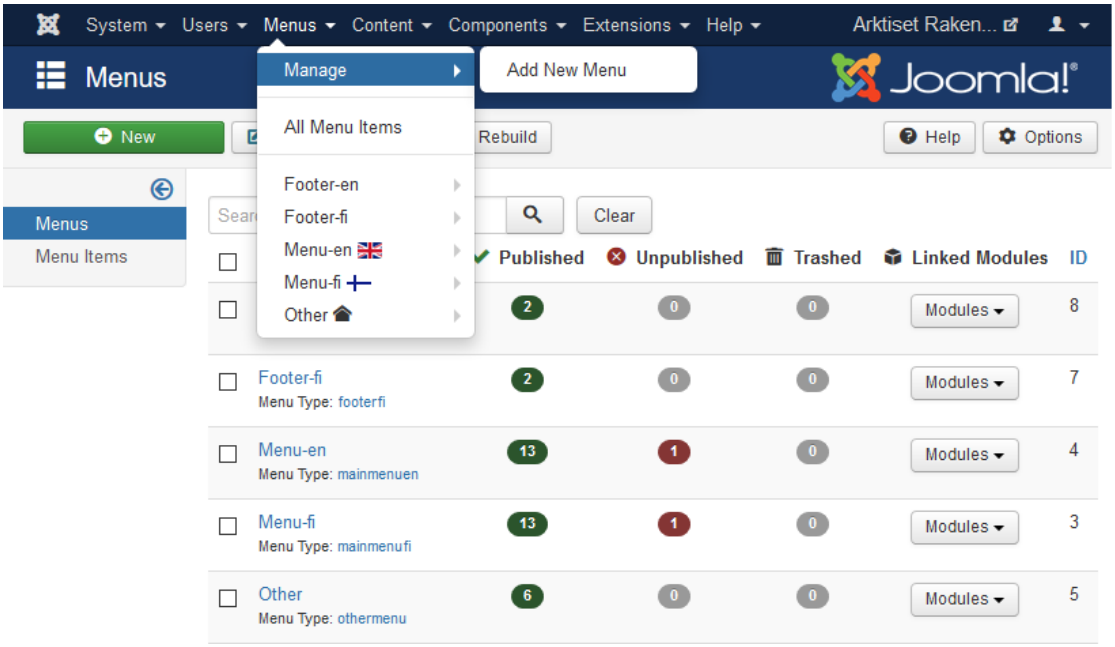
Käyttäjien hallintaan pääsee hallintapaneelin yläosasta välilehdestä *Users*, kuten kuviossa 36 on esitetty. Kuviossa on esitetty kaikki Joomlassa oletuksena olevat käyttäjäryhmät, vaikkakin portaalissa niistä ei ole käytössä kuin *public, registered* ja *super users*.



Kuvio 36. Portaalin käyttäjäryhmät

5.3 Valikot

Valikoilla voidaan hallita portaalin sisältöä järjestämällä se eri osioihin. Eri valikoiden kautta voidaan sitten esittää siihen sopivaa sisältöä. Valikoiden hallinta tapahtuu hallintapaneelin välilehdestä *Menus.* Kuviossa 37 on esitetty osio valikoiden hallintavälilehdestä.

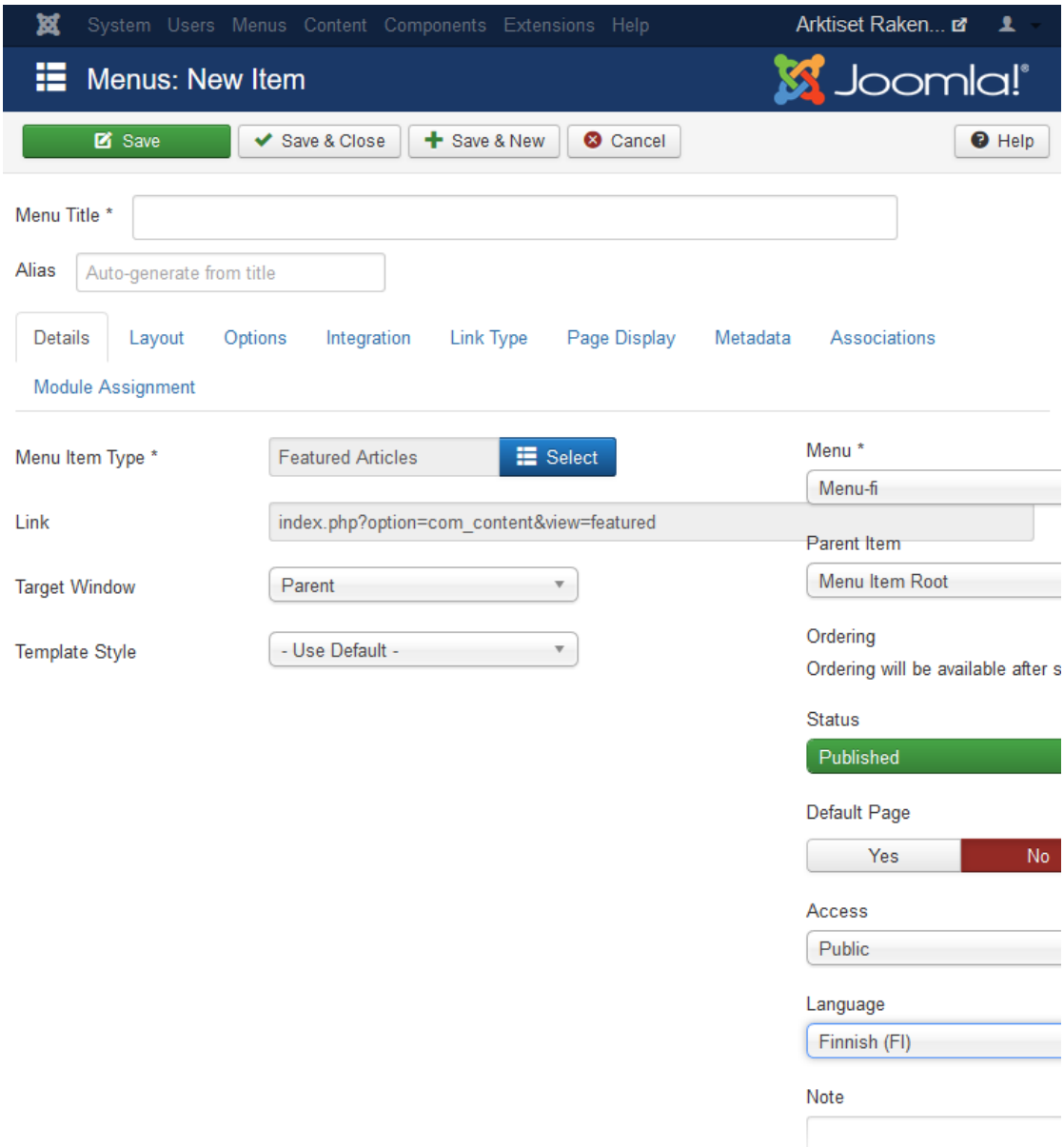


Kuvio 37. Valikoiden hallinta

Portaalissa käytettyjä valikkoja ovat *footer* (englannin- ja suomenkieliset valikot), *menu* (englannin- ja suomenkieliset valikot) ja *other*. *Footer*-valikot sisältävät portaalin alalaidassa olevan sisällön, joka näkyy joka sivulla. Näistä englanninkielinen valikko sisältää englanninkielisen sisällön ja suomenkielinen suomenkielisen. *Menu*-valikot sisältävät sivuston yläpalkin välilehdet ja ne on jaettu samalla tavalla englanniksi ja suomeksi. *Other*-valikko sisältää kaiken muun sisällön.

Valikoiden sisältöä hallitaan erilaisilla nimikkeillä. Nimikkeillä voidaan liittää esimerkiksi moduuli tai yksi tai useampi artikkeli sivulle valitsemalla nimikkeelle tyyppi. Kuviossa 38 on esimerkki nimikkeen luomisesta. Kuviossa ollaan *Details*-välilehdellä, josta voidaan mm. nimetä nimike, asettaa nimikkeen tyyppi, valita minkä valikon ja mahdollisesti myös toisen nimikkeen alaisuudessa toimii, valita kenelle julkaisu näkyy

ja valita kieli. Muilta välilehdeltä voidaan tehdä vielä lisää muutoksia nimikkeen asetuksiin ja näkyvyyteen.

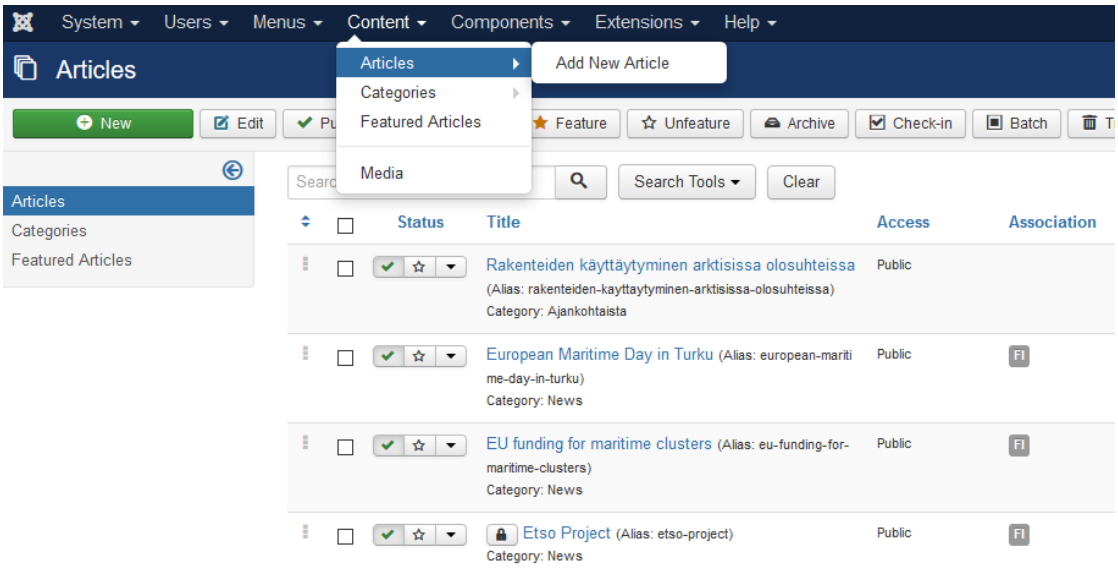


Kuvio 38. Esimerkki valikon nimikkeen luomisesta

5.4 Artikkelit

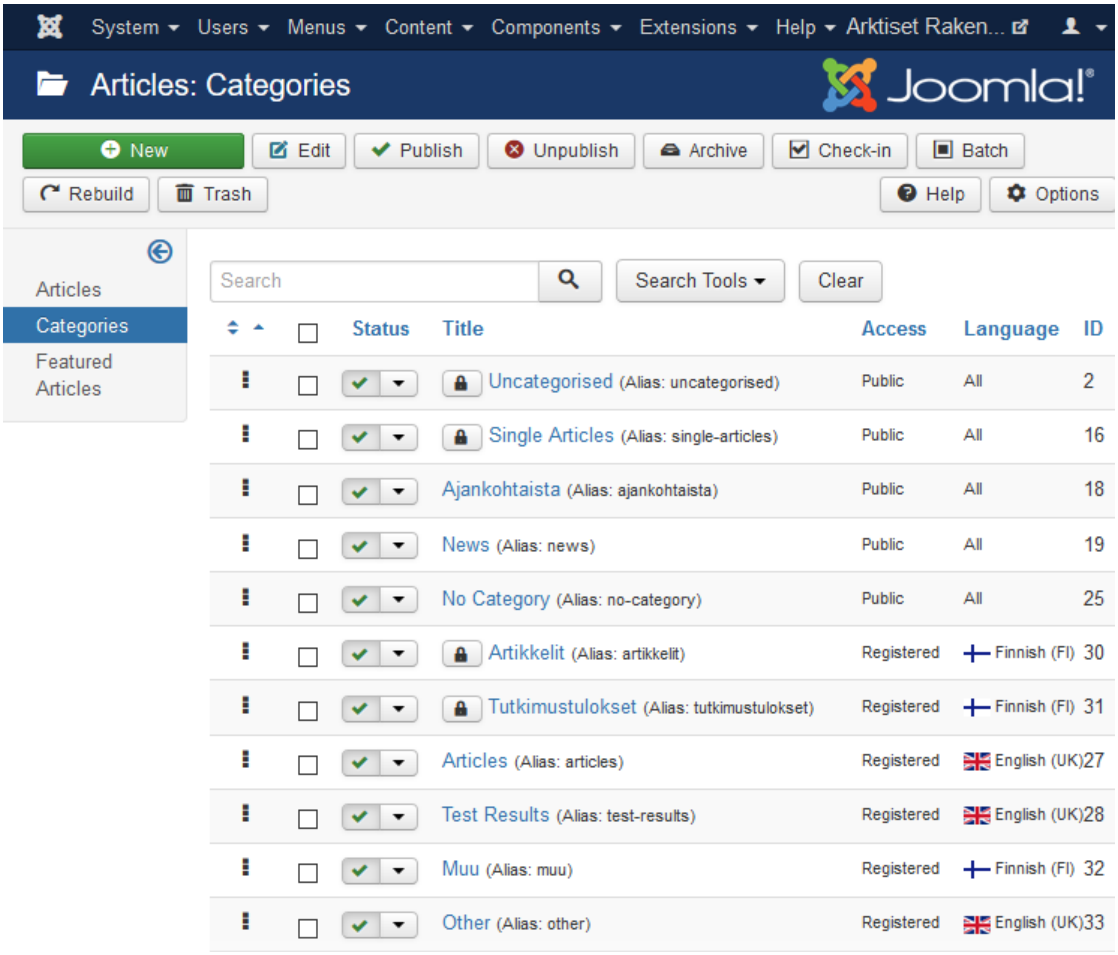
Artikkeleita käytetään sisällön esittämiseen portaalissa. Artikkeleissa on useimmiten kirjoitettua sisältöä, kuten uutisia, mutta niitä voidaan käyttää muunkinlaisen sisällön esittämiseen. Artikkelien hallinta tapahtuu välilehdestä *Content > Articles.* Valikosta

voidaan poistaa, lisätä ja muokata artikkeleja ja kategorioita. Kategorioilla voidaan jakaa artikkeleita ryhmiin, joita voidaan käyttää esimerkiksi usean artikkelin liittämiseen yhdelle sivulle. Kuviossa 39 on esitetty osio artikkelien hallintavälilehdestä.



Kuvio 39. Artikkelien hallinta

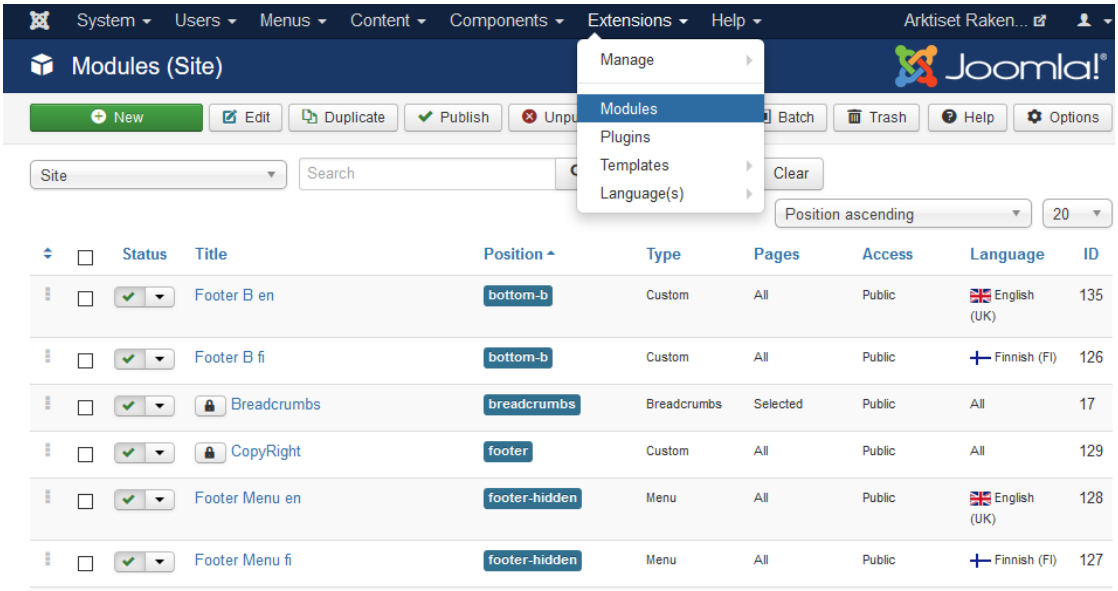
Yleisesti näkyvillä olevat artikkelit ja ainoastaan rekisteröityjen käyttäjien näkyvillä olevat artikkelit erotetaan niille omilla kategorioilla. Lisäksi vain rekisteröityjen käyttäjien näkyvillä olevat artikkelit merkitään *featured*-täpällä ja täppä tulee käyttöön automaattisesti itse sivustolla luoduissa artikkeleissa (ei hallintapaneelissa). Tällä tavoin saadaan rekisteröityjen käyttäjien luomat artikkelit näkymään rekisteröidyille käyttäjille ilman *super user* -käyttäjän oikeuksia. Kuviossa 40 on esitetty portaalin kategoriat. Kuviosta voidaan nähdä yleisesti näkyvillä ja vain rekisteröidyille käyttäjille näkyvillä olevat kategoriat.



Kuvio 40. Portaalin artikkelien kategoriat

5.5 Moduulit

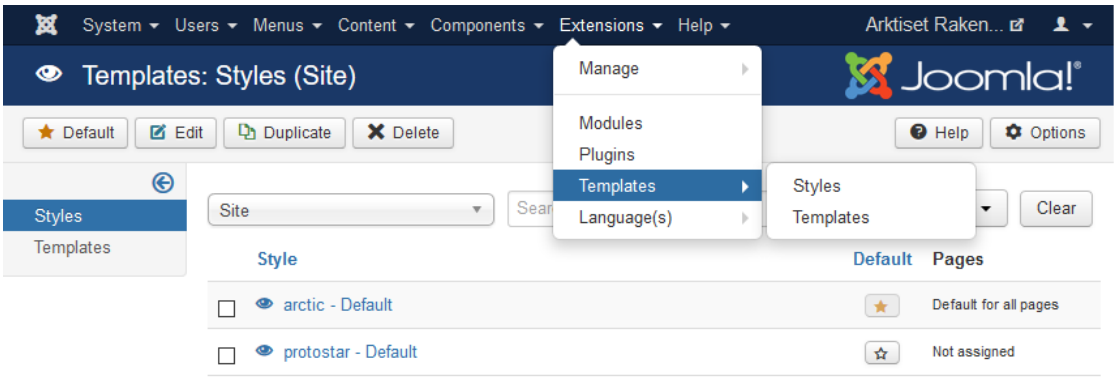
Moduulien kautta saadaan sivustolla näkymään kaikenlaista sisältöä. Moduulien hallintaan pääsee välilehdeltä *Extensions* > *Modules*. Moduuleja on monia erityyppisiä ja niitä voi saada vielä lisää esimerkiksi lisäosien kautta tai luomalla itse. Kuviossa 41 on esitetty muutama portaalissa käytettävä moduuli. Moduuleille tulee valita sijainti, jossa määritetään missä kohdassa sivua moduuli sijaitsee. Käytössä olevat sijainnit määritetään käytettävässä teemassa.



Kuvio 41. Portaalissa käytettäviä moduuleja

5.6 Teema

Sivustolla käytettävä arctic-teema on Arktiset Rakenteet -portaalia varten luotu teema. Teemaa pääsee hallitsemaan välilehdeltä *Extensions* > *Templates.* Kuviossa 42 on esitetty teemojen hallintavalikko.



Kuvio 42. Teemojen hallinta

Styles-valikosta voidaan tehdä ulkoasumuutoksia teemaan. Sieltä voidaan muuttaa halutun sivuston kohdan värejä tai muokata moduulien ja valikkojen tyylejä ja miten ne näkyvät eri laitteilla (erilliset tietokone-, tablet- ja puhelintilat), sekä monia muita

muutoksia. *Templates*-valikosta voidaan muokata, luoda ja poistaa teeman tiedostoja ja kansioita. Lisäksi voidaan luoda ns. override-tiedostoja, joilla voidaan muuttaa portaaliin käyttämiä tiedostoja poistamatta alkuperäisiä. Override-tiedosto on kopio sivustolla olevasta tiedostosta ja se syrjäyttää alkuperäisen tiedoston käytöstä. Muutokset tiedostoihin kannattaakin tehdä override-tiedostoilla, koska silloin alkuperäinen tiedosto pysyy tallessa ja se on mahdollista palauttaa käyttöön tulevaisuudessa.

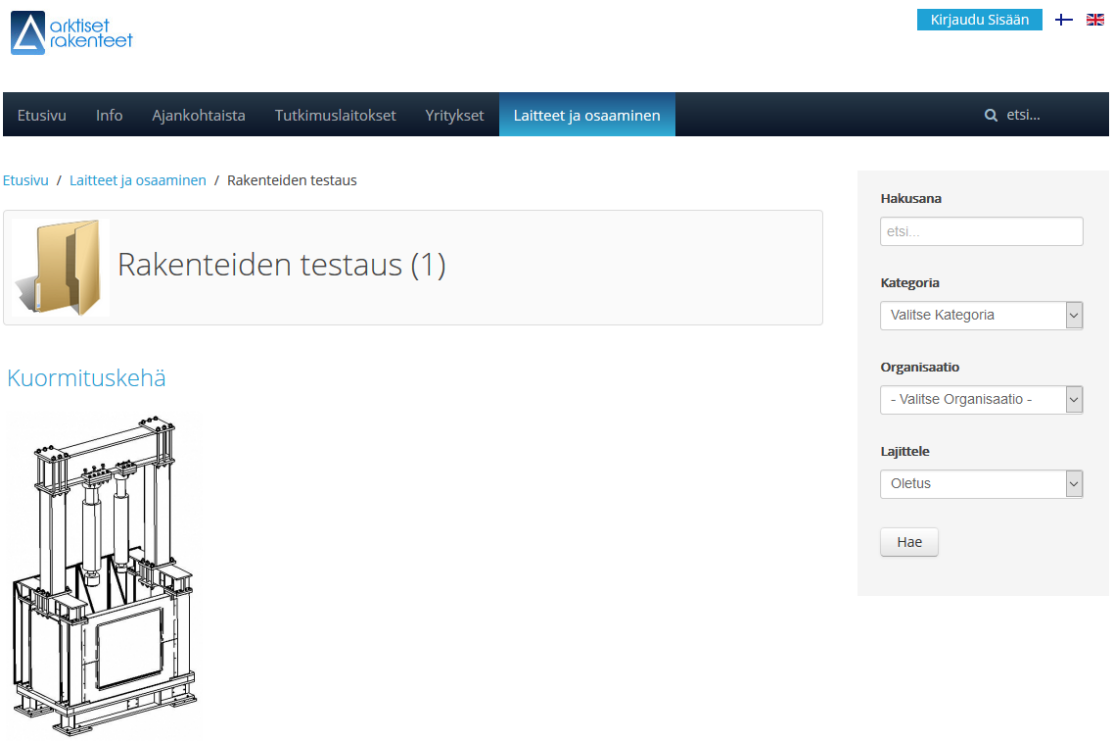
5.7 Lisäosat

5.7.1 Yleistä

Lisäosilla voidaan lisätä uusia toimintoja sivuille käyttäen valmiita ratkaisuja. Lisäosat voivat olla maksullisia tai ilmaisia. Lisäosien hallintaan pääsee välilehdeltä *Extensions*, josta voidaan asentaa, poistaa ja päivittää lisäosien lisäksi myös sivustolle asennettuja liitännäisiä, teemoja ja kieliä. Asennettujen lisäosien toimintoja voidaan hallita *Components*-välilehdeltä.

5.7.2 K2

K2 on lisäosa, jolla saadaan toteutettua portaalin tutkimuslaitokset-, yritykset- sekä laitteet ja osaaminen -välilehtien sisältö. Lisäosalla saadaan toteutettua sivustolle myös haku, jolla pystytään hakemaan edellä mainittujen välilehtien sisältöä. Kuviossa 43 on esitetty portaalin laitteet ja osaaminen -välilehti rakenteiden testaus -kategoriassa. Välilehdessä on myös toteutettu edellä mainittu haku. Haussa voidaan etsiä laitteita haluamalla hakusanalla ja rajata hakua laitteen kategorian tai organisaation mukaan, sekä lajitella hakutuloksia eri tavoin. Sivuston ylälaidassa on vielä yleinen haku, jolla voidaan hakea hakusanalla yleisesti kaikkea sivustolta.

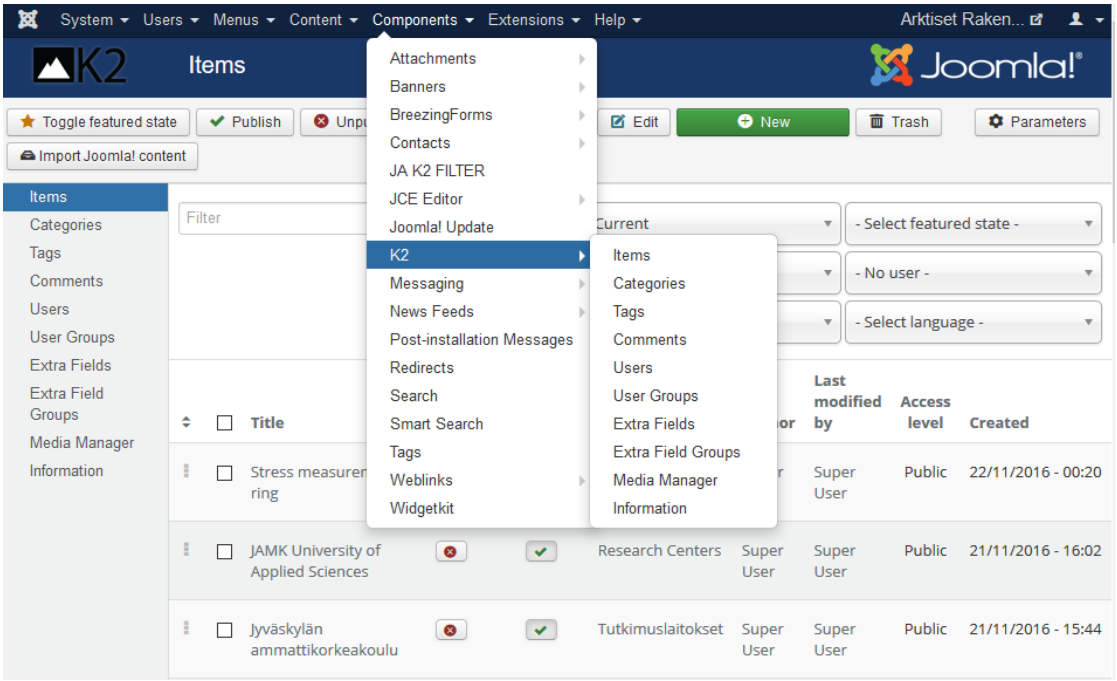


Kuvio 43. Laitteet ja osaaminen

K2:n hallinta toteutetaan portaalissa erilaisilla valikoilla ja niiden sisältämillä nimikkeillä ja kentillä. Alla on esitetty ja selitetty kyseiset K2:n komponentit:

- *Items*-valikossa hallitaan portaalin laitteita, yrityksiä ja tutkimuslaitoksia. Jokainen items-valikon nimike on käytännössä oma sivustolla näkyvä artikkelinsa.
- *Categories*-valikossa jaotellaan *items*-valikon sisältö eri kategorioihin: laitteet ja sen alikategoriat, yritykset ja tutkimuslaitokset.
- *Extra Fields* -valikossa hallitaan kenttiä, joita täytetään jokaiselle *items*-valikon nimikkeelle; esimerkiksi yritykselle täytettäviä kenttiä olisivat yrityksen nimi, osoite, verkkosivu, jne.
- *Extra Fields Groups* -valikossa yhdistetään kategoriat niihin sopivilla *Extra Fields* -kentillä.

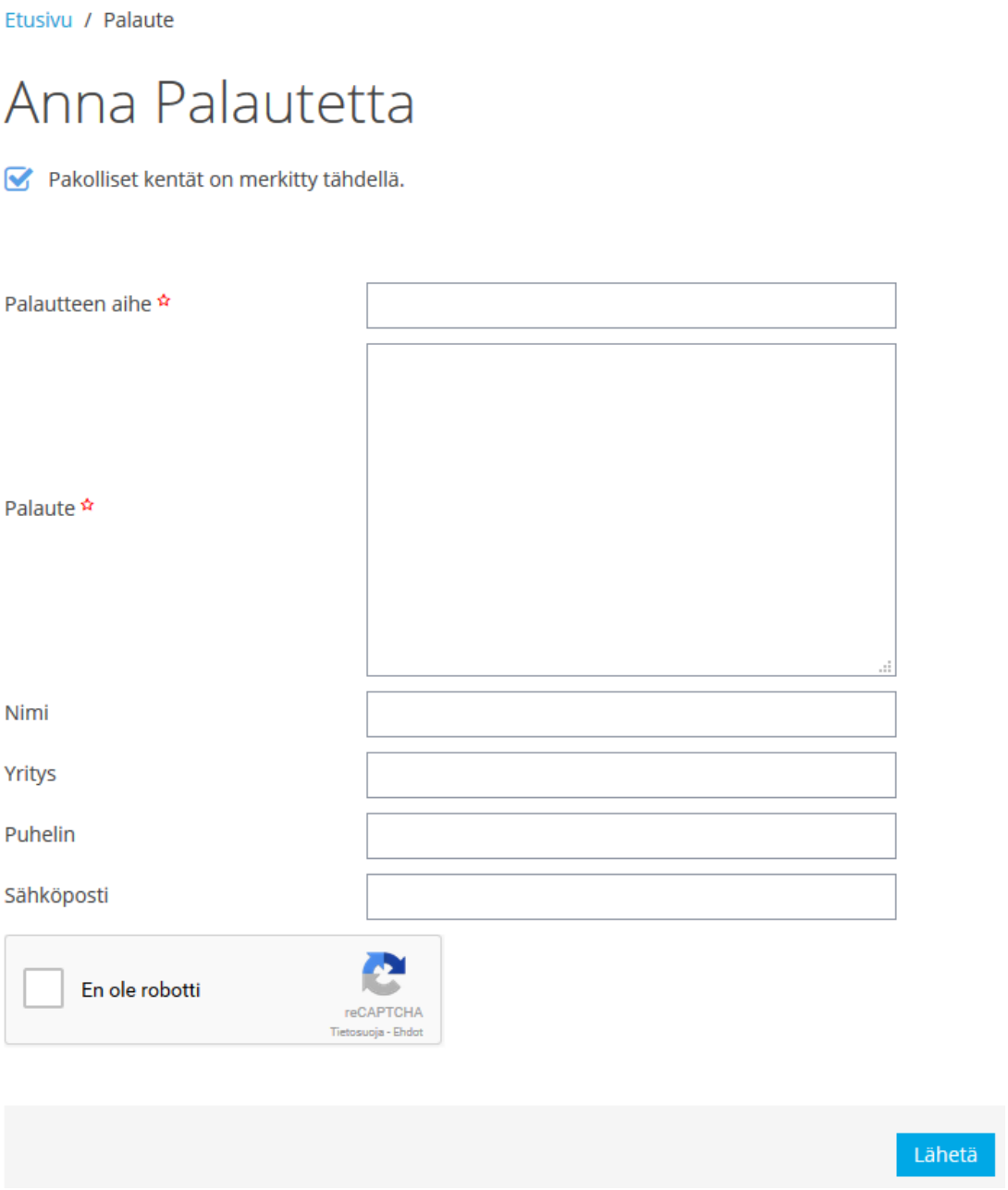
K2:n hallintaan pääsee välilehdeltä *Components > K2*. K2:n hallintasivu on esitetty kuviossa 44.



Kuvio 44. K2:n hallinta

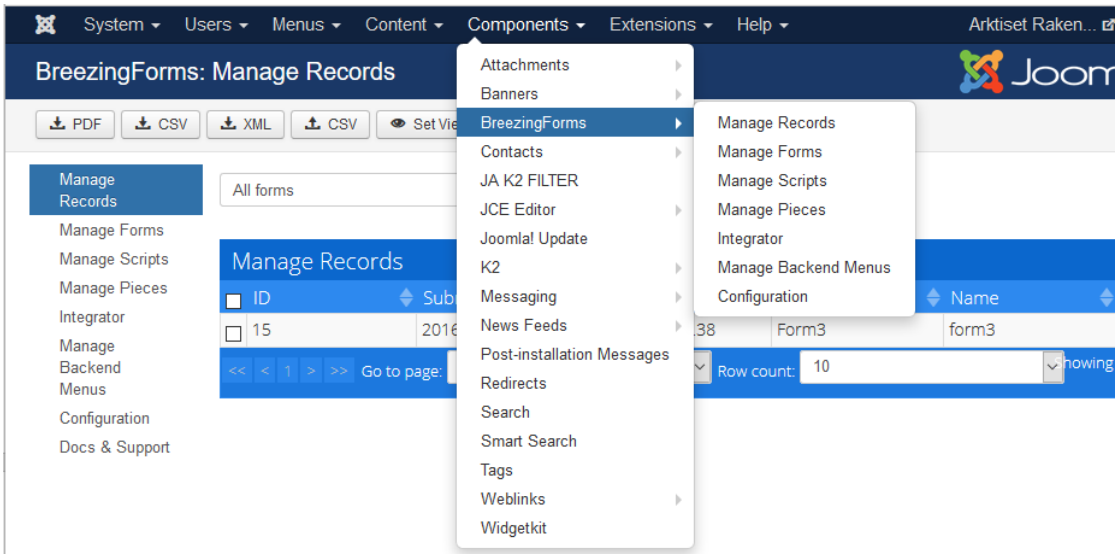
5.7.3 BreezingForms

BreezingForms on lisäosa, jolla saadaan luotua ja hallittua portaalissa käytettäviä kaavakkeita. BreezingForms-kaavaketta käytetään julkisesti sivustolla palautekaavakkeessa sekä tiedonkeruussa Arktiset Rakenteet -projektissa mukana olevien organisaatioiden laitteistosta. Esimerkkinä kaavakkeista on kuviossa 45 esitetty edellä mainittu sivustolla käytössä oleva palautekaavake.



Kuvio 45. Palautekaavake

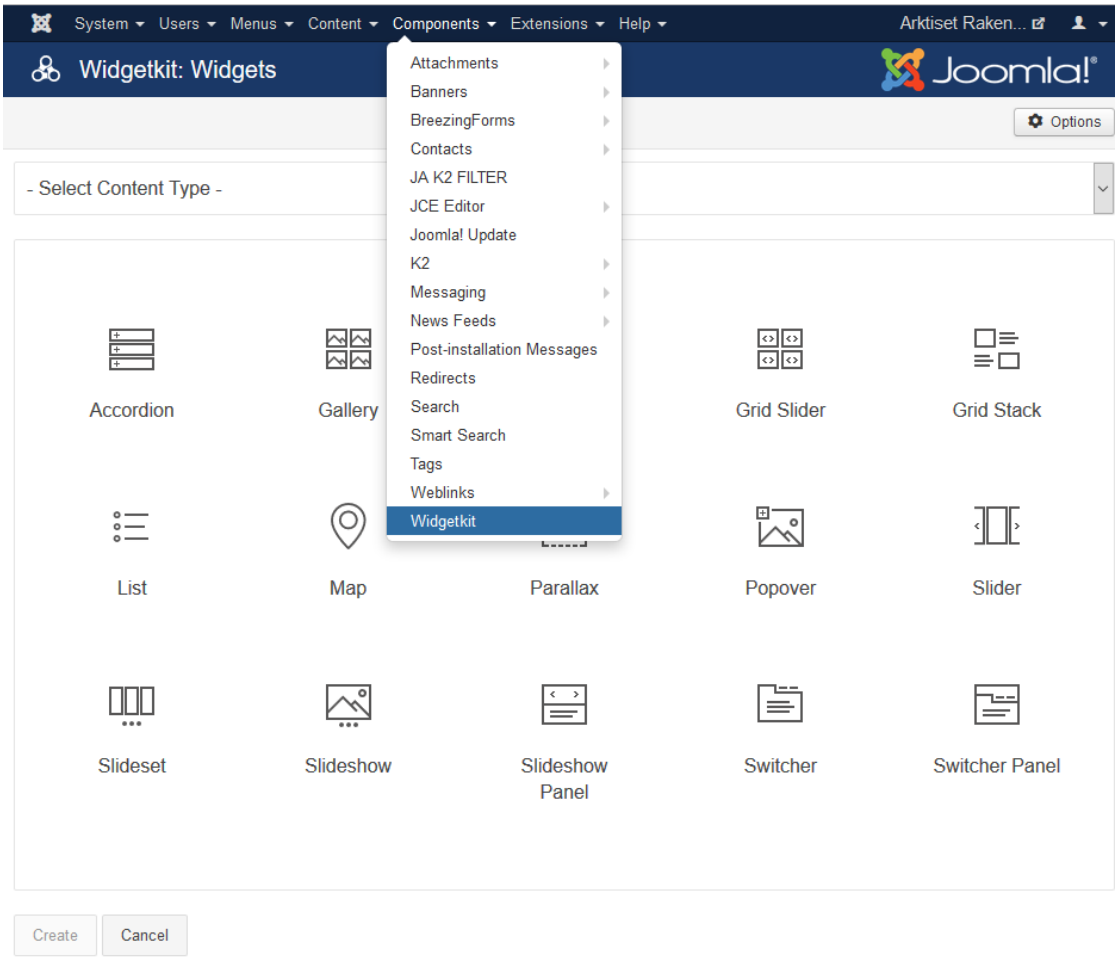
BreezingFormsin hallintaan pääsee välilehdeltä *Components* > *BreezingForms*. *Manage Records* -välilehdelle päivittyvät täytetyt kaavakkeet ja ne voidaan joko ladata tai niitä voidaan selata suoraan hallintapaneelista. Kuviossa 46 on esitetty BreezingForms-kaavakkeiden hallintasivu.



Kuvio 46. BreezingForms-kaavakkeiden hallinta

5.7.4 Widgetkit

Widgetkit on lisäosa, jolla pystyy tekemään omia moduuleja. Widgetkitin hallintaan pääsee välilehdeltä *Components > Widgetkit.* Painamalla *New*-painiketta pääsee moduulin luontiin. Kuviossa 47 on esitetty Widgetkit-moduulin luontisivu.

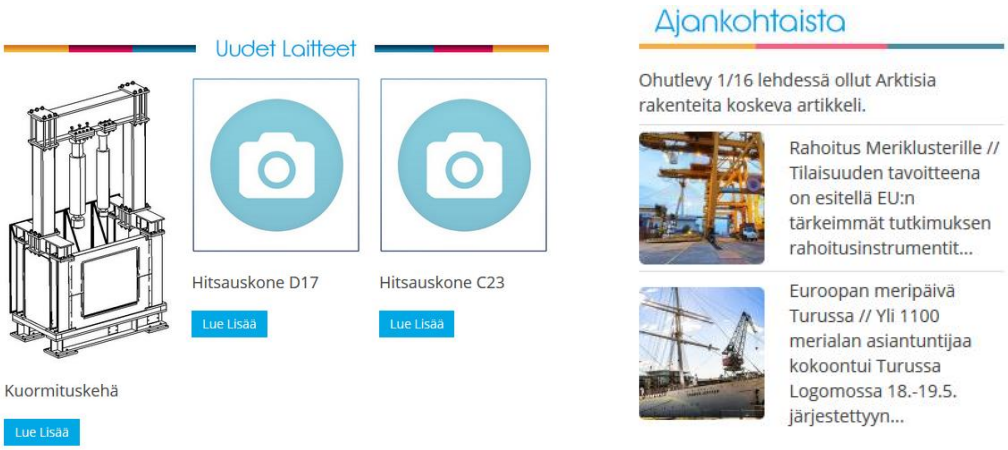


Kuvio 47. Widgetkit-moduulien luonti

Kuten kuvasta huomataan, voidaan Widgetkitillä luoda monenlaisia moduuleja. *Select Content Type* -kentästä valitaan moduulin tyyppi, joka on normaalisti Joomla tai K2-lisäosaan liittyviä moduuleja tehtäessä K2. Lisäksi tyypiksi on mahdollista valita esimerkiksi RSS-uutis- tai Twitter-syöte. Tyypinvalintakentän alapuolelta valitaan vielä vaihtoehdoista moduulille ulkoasurakenne, minkä jälkeen voidaan luoda moduuli. Painamalla *Create* päästään vielä asetussivulle, jonka sisältö riippuu edellisistä valinnoista, missä päästään säätämään moduulin sisältöä ja tarkempia ulkoasuasetuksia.

Widgetkit-moduuleja päästään käyttämään moduulien hallintavalikosta luomalla uusi moduuli, asettamalla sen tyypiksi Widgetkit ja valitsemalla haluttu Widgetkit-moduuli. Sivustolla käytettäviä Widgetkitillä luotuja moduuleja ovat etusivulla olevat

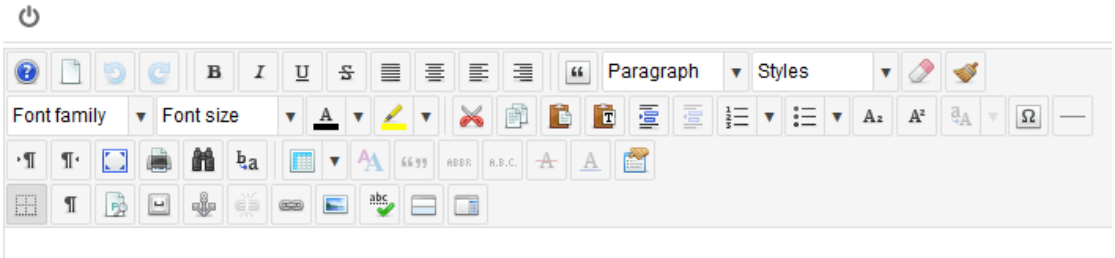
Ajankohtaista- ja *Uudet Laitteet* -valikot, jotka on esitettynä kuviossa 48. Moduuleihin päivittyvät automaattisesti linkit uusimpiin uutisartikkeleihin ja lisättyihin laitteisiin.



Kuvio 48. Portaalin Widgetkit-moduulit

5.7.5 JCE Editor

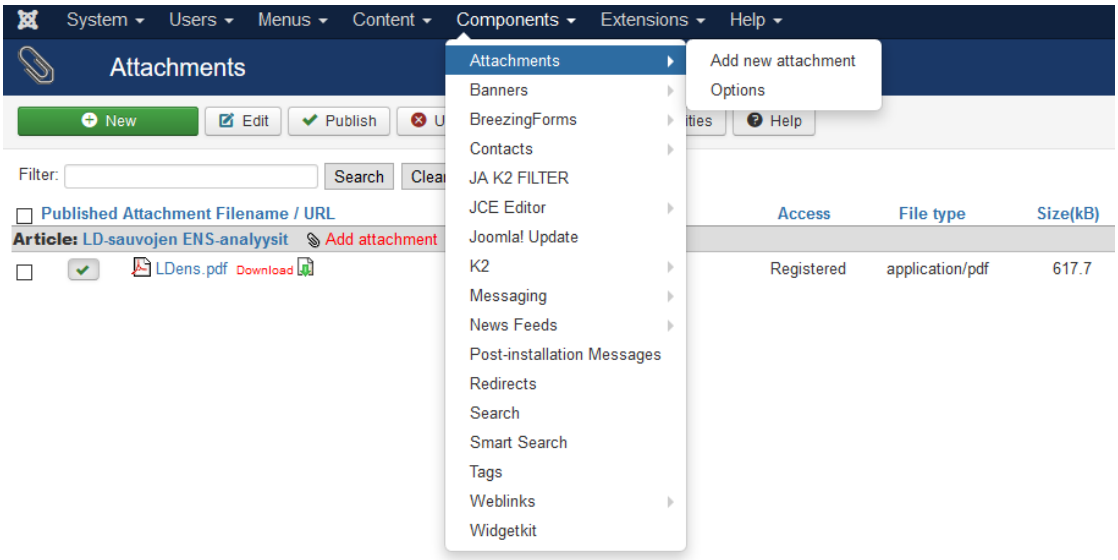
Portaalin käyttäjille on asetettu oletustekstieditoriksi JCE. JCE-tekstieditorilla voidaan suorittaa helposti tekstinkäsittelyn perusominaisuudet, joita ei ole Joomlassa oletuksena käytössä, kuten fontin tyylin ja koon muokkaus ja rivinvaihdot. Lisäksi editori pystyy muuntamaan Word-dokumentteja sivustolle sopivaan muotoon maalaamalla ja kopioimalla koko dokumentti ja liittämällä sen editoriin. JCE:n asetuksia voidaan hienosäätää välilehdeltä *Components > JCE Editor*, missä voidaan esimerkiksi antaa eri käyttäjäryhmille eri oikeuksia JCE-editorin eri elementteihin. Kuviossa 49 on esitetty JCE-tekstieditori.



Kuvio 49. JCE-tekstieditori

5.7.6 Attachments

Attachments-lisäosa tuo ominaisuuden, jolla artikkeleihin voidaan lisätä liitteitä. Tällä ominaisuudella mahdollistetaan, että portaalin ylläpitoon kuulumattomat rekisteröityneet käyttäjät voivat jakaa tiedostoja vain muiden rekisteröityjen käyttäjien kesken julkaistuissa artikkeleissa. Liitteiden hallintaan pääsee välilehdeltä *Components > Attachments*, missä voidaan hallita kaikkia liitteitä ja niiden asetuksia. Kuviossa 50 on esitetty liitteiden hallintasivu. Lisäksi välilehdeltä *System > Global Configuration > Media* voidaan valita tuetut tiedostotyypit liitteille.

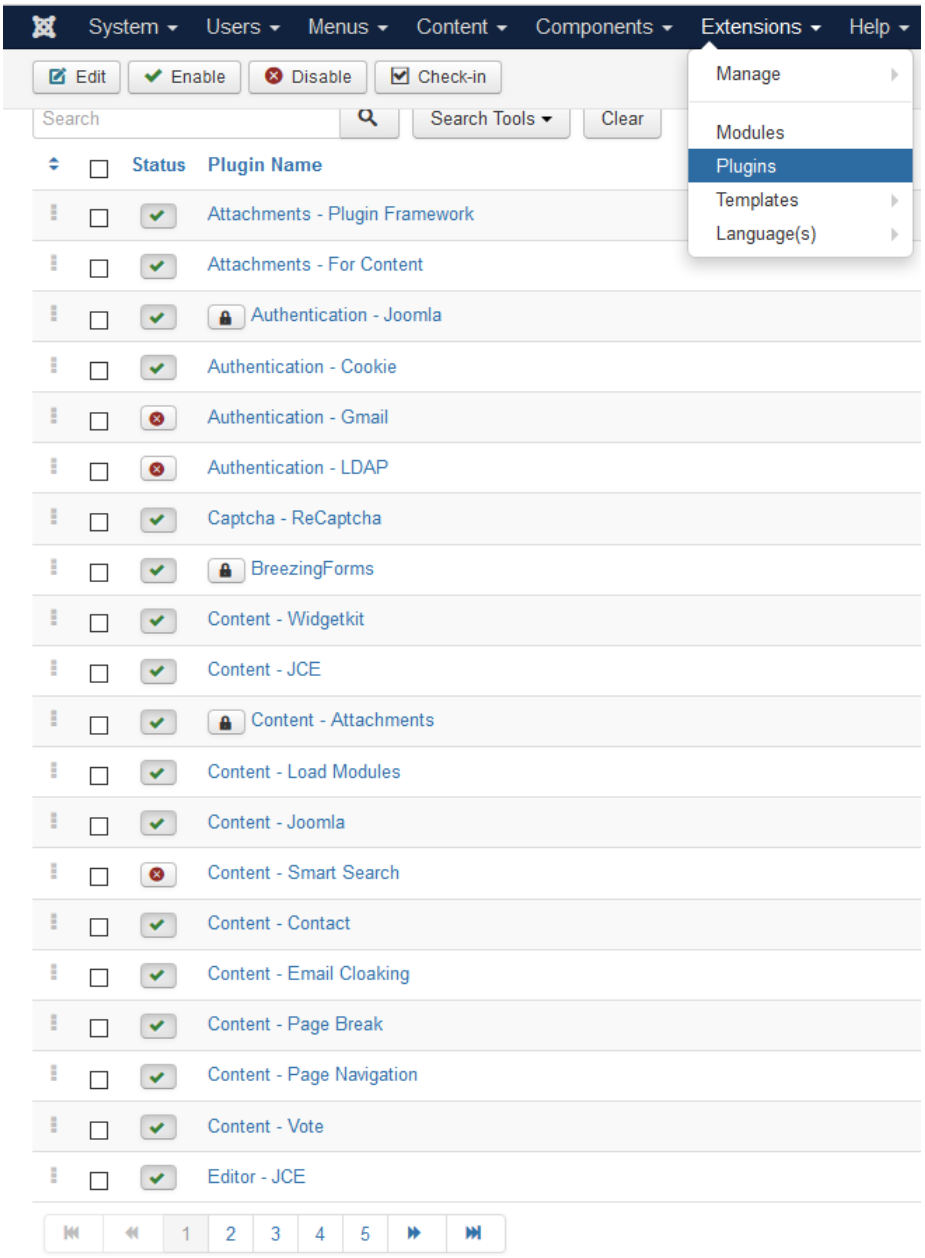


Kuvio 50. Liitteiden hallinta

5.8 Liitännäiset

Liitännäiset ovat sivustolle asennettuja ohjelmia, mutta eivät ole yhtä laajoja kuin lisäosat. Liitännäiset sisältävät yleensä yhden tai muutaman sivustolla käytettävän toiminnon ja niitä asennetaan sivustolle yleensä joko lisäosan mukana tai sellaisenaan. Liitännäisten hallintaan pääsee välilehdeltä *Extensions > Plugins*. Kuviossa 51 on esitetty liitännäisten hallintasivu ja kuten kuviosta nähdään, on liitännäisiä asennettuna sivustolle liikaa, että niitä kannattaisi analysoida yksitellen. Esimerkkeinä sivustolla käytettävistä liitännäisistä voidaan mainita kuitenkin vaikkapa System - AdminExile,

jota käytetään hallintapaneelin kirjautumissivun piilottamiseen, Captcha – Re-Captcha, jota käytetään brute force -hyökkäysten estoon sisäänkirjautumisessa ja Button – Page Break, jolla saadaan käyttöön artikkelin muokkauksessa nappi, jolla luodaan artikkeliin sivunvaihto.



Kuvio 51. Liitännäisten hallinta

6 Yhteenveto ja pohdinta

Opinnäytetyön tavoitteena oli dokumentoida portaalin tietokanta, portaalille asennetut komponentit ja portaalin rakenne tulevia ylläpitäjiä ajatellen, sekä koventaa ja testata portaalin tietokantaa ja tietoturvaa.

Portaalin sisällön dokumentoinniksi muodostui tietokantaa lukuun ottamatta kahdeksi luvuksi, joista ensimmäisen (luku 2) sisältö rakentui käsittelemään sisällönhallintaa ja palvelinta. Luvussa käsiteltiin käytössä olevaa sisällönhallintajärjestelmää Joomla, sekä verrattiin sitä muihin suosittuihin sisällönhallintajärjestelmiin ja dokumentoitiin mitä muita komponentteja portaalin toimintaan tarvittiin palvelimelle asennettuna.

Dokumentoinnin toisessa luvussa (luku 5) käsiteltiin taas Joomlan sisältämiä komponentteja ja niiden hallintaa hallintapaneelissa. Luvussa pyrittiin käsittelemään kyseisten komponenttien hallintaa selittämällä niiden käyttötarkoitukset ja esittää lyhyesti niiden toiminta ja sijainti hallintapaneelissa. Sisällön dokumentoinnin molemmat luvut koostuivat lähes kokonaan jo aikaisemmin pohdituista ja toteutetuista asioista ja luvut sisälsivät vain niiden dokumentoinnin.

Tietokannan dokumentoinnista ja käsittelystä muodostui lopulta oma lukunsa. Kaikki portaalissa oleva tietokantaa käyttävä sisältö pystyttiin toteuttamaan K2-lisäosan avulla siten, että tietokannan käsittely toteutetaan Joomlassa automaattisesti. Kaikki portaalin tietokannan taulukot ovat siis Joomlan automaattisesti generoimia. Ainoa tietokantaa käsittelevä asia olikin tietokantatyypin valinta, jossa päädyttiin MariaDB:hen. Luku käsittelikin lopulta vain tietokannan teoriaa, valintaa ja dokumentaatiota.

Tietoturva-osiossa tuli taas odotettua laajempi sen sisältäessä Joomlan ja tietokannan varmuuskopioinnin, salatun tiedonsiirron HTTPS:llä, palomuurin palvelimelle, Two Factor Authentication -lisätunnistautumisen ylläpitäjille, reCaptcha-tunnistautumisen ja tietoturvan testauksen Mozilla Observatorylla ja Joomscanilla. Tietoturva-osio saatiin kehitettyä muuten suunnitellusti, mutta XSS-hyökkäysten estoon käytettävän CSP:n käyttöönotto aiheutti tilanteen, jossa oli valittava helpommin muutettavan sivuston ja luotettavamman tietoturvan väliltä. Lisäksi varmuuskopiointi tulisi

suorittaa erilliseen kohteeseen, sillä nyt jos portaalia hallinnoivalle palvelimelle sattuu jotain, on vaarana menettää varmuuskopiot.

Lähteet

A Primer on Databases and Catalogs. N.d. Alkeiskirja tietokannoista Online Library Learning Center -sivustolla. Viitattu 5.12.2016. http://www.usg.edu/galileo/skills/unit04/primer04_01.phtml.

About Let's Encrypt. N.d. Info-sivu Let's Encrypt -sivustolla. Viitattu 29.11.2016. https://letsencrypt.org/about/.

Bartholomew, D. MariaDB vs. MySQL. N.d. Admin-magazine. Viitattu 5.12.2016. http://www.admin-magazine.com/Articles/MariaDB-vs.-MySQL.

Category:OWASP Joomla Vulnerability Scanner Project. 2016. Joomscan-projekti tietosivu OWASP-sivustolla. Viitattu 14.2.2017. https://www.owasp.org/index.php/Category:OWASP_Joomla_Vulnerability_Scanner_Project.

Constantin, L. 2016. Mozilla launches free website security scanning service. PCWorld. Viitattu 26.1.2017. http://www.pcworld.com/article/3112335/security/mozilla-launches-free-website-security-scanning-service.html.

Content Security Policy Reference. 2016. CSP-ohje. Viitattu 1.3.2017. https://content-security-policy.com/.

JAMK mukana arktisten rakenteiden kehityksessä. 2015. Uutinen JAMK:n sivustolla. Viitattu 8.12.2016. https://www.jamk.fi/fi/Uutiset/Ajankohtaista-JAMKissa/jamk-mukana-arktisten-rakenteiden-kehityksessa/.

Mening, R. 2016. WordPress vs Joomla vs Drupal? WebsiteSetup. Viitattu 6.11.2016. http://websitesetup.org/cms-comparison-wordpress-vs-joomla-drupal/.

Patra, C. 2015. MariaDB vs MySQL on Amazon's AWS RDS. CloudAcademy. Viitattu 6.12.2016. http://cloudacademy.com/blog/mariadb-vs-mysql-aws-rds/.

Ristić, I. N.d. About SSL Labs. Viitattu 12.12.2016. https://www.ssllabs.com/index.html.

SQL (Structured Query Language). N.d. Artikkeli NTC Hosting -sivustolla. Viitattu 6.12.2016. https://www.ntchosting.com/encyclopedia/databases/structured-query-language/.

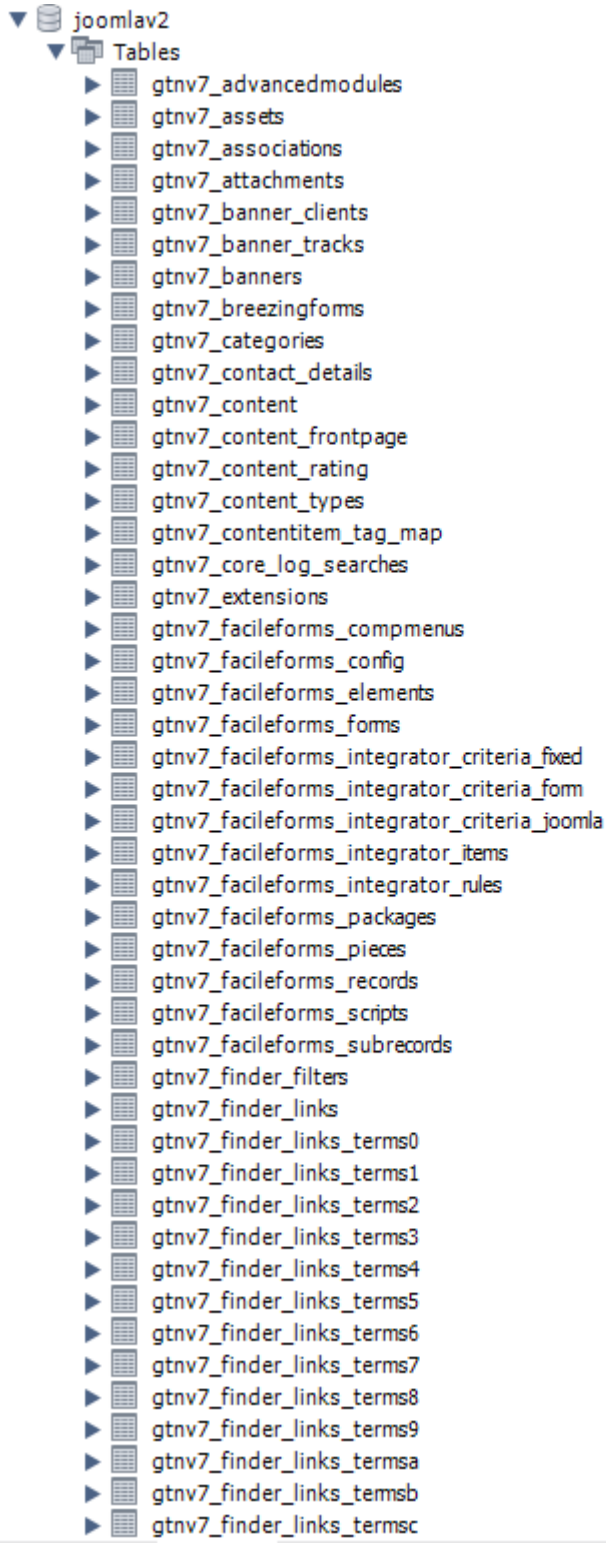
Web Security. 2017. Mozillan verkon tietoturvaa käsittelevä wiki-sivu. Viitattu 26.1.2017. https://wiki.mozilla.org/Security/Guidelines/Web_Security.

What Is SSL (Secure Sockets Layer) and What Are SSL Certificates? 2016. Artikkeli Digicer-sivustolla. Viitattu 19.11.2016 https://www.digicert.com/ssl.htm.

WordPress vs Joomla vs Drupal – Which One is Better? 2016. Artikkeli WPBeginner-sivustolla. Viitattu 6.11.2016. http://www.wpbeginner.com/opinion/wordpress-vs-joomla-vs-drupal-which-one-is-better/.

Liitteet

Liite 1. Tietokannan taulukot



- gtnv7_finder_links_termsd
- gtnv7_finder_links_termse
- gtnv7_finder_links_termsf
- gtnv7_finder_taxonomy
- gtnv7_finder_taxonomy_map
- gtnv7_finder_terms
- gtnv7_finder_terms_common
- gtnv7_finder_tokens
- gtnv7_finder_tokens_aggregate
- gtnv7_finder_types
- gtnv7_jak2filter
- gtnv7_jak2filter_taxonomy
- gtnv7_jak2filter_taxonomy_map
- gtnv7_k2_attachments
- gtnv7_k2_categories
- gtnv7_k2_comments
- gtnv7_k2_extra_fields
- gtnv7_k2_extra_fields_groups
- gtnv7_k2_items
- gtnv7_k2_log
- gtnv7_k2_rating
- gtnv7_k2_tags
- gtnv7_k2_tags_xref
- gtnv7_k2_user_groups
- gtnv7_k2_users
- gtnv7_languages
- gtnv7_menu
- gtnv7_menu_types
- gtnv7_messages
- gtnv7_messages_cfg
- gtnv7_modules
- gtnv7_modules_menu
- gtnv7_newsfeeds
- gtnv7_overrider
- gtnv7_postinstall_messages
- gtnv7_redirect_links
- gtnv7_schemas
- gtnv7_session
- gtnv7_tags
- gtnv7_template_styles
- gtnv7_ucm_base
- gtnv7_ucm_content
- gtnv7_ucm_history
- gtnv7_update_sites
- gtnv7_update_sites_extensions
- gtnv7_updates
- gtnv7_user_keys
- gtnv7_user_notes
- gtnv7_user_profiles
- gtnv7_user_usergroup_map
- gtnv7_usergroups
- gtnv7_users
- gtnv7_utf8_conversion
- gtnv7_viewlevels
- gtnv7_weblinks
- gtnv7_wf_profiles
- gtnv7_widgetkit