Tampereen ammattikorkeakoulu

Moodlen tietoturva

Valtteri Anttila

OPINNÄYTETYÖ
Syyskuu 2020

Tieto- ja viestintätekniikka
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tieto- ja viestintätekniikka
Tietoliikennetekniikka ja tietoverkot

ANTTILA, VALTTERI:
Moodlen tietoturva

Opinnäytetyö 29 sivua, joista liitteitä 3 sivua
Syyskuu 2020

Opinnäytetyössä tutustutaan virtuaalisen oppimisympäristö Moodlen tietoturvaan ja tietoturvaominaisuuksiin. Lisäksi opinnäytetyössä perehdytään tietoturvaan ja sen osa-alueisiin. Opinnäytetyössä esitellään Moodlen tietoturvaan vaikuttavat ominaisuudet sekä esitetään opinnäytetyössä käytettyyn testiympäristöön tehdyt määrittelyt kyseisille ominaisuuksille.

Tietoturvaan perehdyttiin tietoturvan määritelmän sekä sen osa-alueiden kautta. Tämän perehtymisen perusteella luotiin tietoturvavaatimukset opinnäytetyössä käytettyä testiympäristöä varten. Lisäksi arvioitiin, kuinka korkeat tietoturvavaatimukset voidaan asettaa, jotta palvelu pysyy helppokäyttöisenä.

Opinnäytetyössä tutkittiin Moodlen tietoturvaominaisuuksia. Tietoturvaominaisuuksia voidaan kytkeä laajasti käyttöön, mikä parantaa tietoturvaa, mutta samalla hankaloittaa palvelun käytettävyyttä.

Työssä onnistuttiin perehtymään Moodlen tietoturvaominaisuuksiin ja tietoturvaan. Tietoturva-asetusten määrittely onnistui työssä käytettyyn testiympäristöön.

Asiasanat: moodle, tietoturva, virtuaalinen oppimisympäristö

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in ICT Engineering
Telecommunications and Networks

VALTTERI ANTTILA
Security in Moodle

Bachelor's thesis 29 pages, appendices 3 pages
September 2020

This thesis aimed to explore the information security and information security features of the Moodle virtual learning environment. Security features affecting Moodle's information security and specifications of those features are explained in this thesis.

Information security was introduced through its definition and sectors. Based on this introduction, security requirements were created for the test environment used in the thesis. The thesis studied how high information security requirements can be set so that the usability of the service is not significantly affected.

The results show that information security features can be widely enabled, which improves information security but at the same time complicates the usability of the service.

Key words: moodle, information security, virtual learning environment

SISÄLLYS

LYHENTEET JA TERMIT

cron	Ajastettu tehtävä Unix-tietokonejärjestelmissä.
GDPR	General Data Protection Regulation, yleinen tietosuoja-asetus
HTML	Hypertext Markup Language, hypertekstiä kuvaava merkintäkieli.
IP-osoite	Internet Protocol -reititysprotokollan mukainen verkko-osoite
LAMP	Linux, Apache, MySQL ja PHP -pohjainen WWW-palvelin
LDAP	Lightweight Directory Access Protocol, verkkoprotokolla, joka on suunnattu hakemistokäyttöön.
Linux	Linux-ytimeen perustuva käyttöjärjestelmä
MOODLE	Modular Object-Oriented Dynamic Learning Environment. Modulaarinen kohdekeskeinen dynaaminen oppimisympäristö.
SaaS	Software as a Service

1 JOHDANTO

Opinnäytetyön tarkoituksena oli tutustua virtuaalisen oppimisympäristö Moodlen tietoturvaan ja tietoturvaominaisuuksiin ja tutustumisen perusteella määritellä testiympäristöön tietoturva-asetukset. Testiympäristön määrittelyjä on jatkossa tarkoitus hyödyntää verkkokoulutuskäytössä. Lisäksi työssä tutustuttiin tietoturvaan yleisesti sekä erilaisiin tietoturvavaatimuksiin, joita nykyisin vaaditaan verkon kautta käytettäviltä palveluilta.

Moodle on laajalti käytössä oleva virtuaalinen oppimisympäristö, joka on laajasti käytössä niin Suomessa kuin kansainvälisesti. Suomessa Moodle on käytössä muun muassa toisen asteen oppilaitoksissa sekä korkeakouluissa.

Moodle on laaja ohjelmisto, joka sisältää runsaasti erilaisia ominaisuuksia verkkokoulutuksien toteuttamiseen. Tähän perehtyminen sekä tietoturvaominaisuuksien hahmottaminen sekä niiden peilaaminen yleisiin tietoturvavaatimuksiin olivat tämän opinnäytetyön keskeisimmät tavoitteet.

2 TIETOTURVA

Tietoturva tarkoittaa tietojen kokonaisvaltaista suojaamista väärinkäytöksiltä, muuttumiselta sekä katoamiselta. Tietoturva kattaa käsitteenä itse tietojen kuin myös järjestelmien, palveluiden sekä tietoliikenteen suojaamisen. (Helsingin yliopisto 2019.) Tietoturva koostuu perinteisen jaottelun mukaan kolmesta osa-alueesta: tiedon luottamuksellisuudesta, eheydestä ja saatavuudesta (Kyberturvallisuuskeskus 2019).

Tietoturva on tärkeää niin yksilön kuin yhteiskunnan kannalta. Yhteiskunta perustuu suurelta osin sähköiseen tiedon siirtoon ja käsittelyyn, jolloin käytettävien yhteyksien ja laitteiden tulee olla tietoturvallisia. Tämän vuoksi tietoturvallisuus on tietoteknisten sovellusten ja palveluiden perusedellytys. (Pietikäinen 2013.)

Petteri Järvisen (2002, 47) mukaan tietoturva on 20 % tekniikkaa ja 80 % psykologiaa. Tämä tarkoittaa sitä, että teknisesti täysin tietoturvallinen järjestelmä ei takaa kokonaisuudessa tietoturvaa nimeksikään, vaan käyttäjien toimet tietoturvallisuuden saavuttamiseksi ovat teknistä toteutusta keskeisemmässä asemassa.

2.1 Luottamuksellisuus

Tiedon luottamuksellisuudella tarkoitetaan sitä, että tietoon on pääsy vain tarkoitetuilla henkilöillä. Tietoon on pääsy- ja muokkausoikeus vain etukäteen määritellyillä käyttäjiltä, joille kyseinen oikeus on annettu. Luottamuksellisuus edellyttää myös, että käyttöoikeuden saaneet henkilöt käyttävät tietoa vain työtehtäviensä hoitamiseen ja että tarpeetonta tiedon käyttöä ei tapahdu. (Pietikäinen 2013.)

Tiedon luottamuksellisuus varmistetaan salauksella (Järvinen 2002, 22). Salauksen periaatteena on muuttaa tieto sellaiseen muotoon, että vain se, joka tietää salauksen purkutavan, voi käyttää tietoa (Helsingin yliopisto 2015). Luottamuk-

sellisuuteen kuuluu vahvasti myös käyttäjätunnusten ja salasanojen henkilökohtaisuus. Henkilökohtaista käyttäjätunnusta ja salasanaa ei tule luovuttaa toiselle henkilölle käytettäväksi, vaan toiselle käyttäjälle tulisi aina luoda omat henkilökohtaiset tunnukset järjestelmän käyttämiseen. (Helsingin yliopisto 2019.)

2.2 Todennus

Tiedon luottamuksellisuus edellyttää todentamista. Käyttäjän on todennettava olevansa väittämänsä henkilö, jotta hän pääsee käyttämään järjestelmää omilla valtuuksillaan. Samalla myös käyttäjän tulee todentaa käyttävänsä oikeaa järjestelmää. (Turner 2016.)

Käyttäjä voidaan todentaa joko yksi- tai kaksivaiheisesti. Yksivaiheinen todentaminen tarkoittaa perinteistä käyttäjätunnusta ja salasanaa, jolloin käyttäjä tunnistetaan hänen syöttämän käyttäjätunnuksen perusteella ja todennetaan oikean salasanan perusteella. Jos käyttäjä siis tietää nämä molemmat tiedot, on tämä järjestelmän näkökulmasta se kuka tämä väittää olevansa, sillä todennus tehdään vain salasanan perusteella. (Turner 2016; Tietoturvallinen tunnistautuminen 2018.)

Kaksivaiheinen todennus tapahtuu nimen mukaisesti käyttämällä kahta tunnistustapaa käyttäjän tunnustamiseen. Tyypillisesti kaksivaiheisessa tunnistautumisessa käytetään käyttäjätunnuksen ja salasanan lisäksi tekstiviesti- tai mobiilisovellusvarmennusta. Biometrinen tunnistautuminen on myös yleistynyt viime vuosina osana kaksivaiheista tunnistautumista. (Turner 2016; Tietoturvallinen tunnistautuminen 2018.)

2.3 Eheys

Eheys tarkoittaa tietoturvan yhteydessä tiedon säilymistä sellaisena kuin se on tarkoitettu. Tällä tarkoitetaan siis sitä, että tiedot ja järjestelmät ovat luotettavia, oikeita ja ajantasaisia, eivätkä ne ole muutettavissa tai muutu esimerkiksi ohjelmisto- tai laitteistovikojen tai inhimillisen toiminnan vuoksi. Tietojen säännöllinen

päivittäminen ajantasaisiksi sekä varmuuskopioinnista huolehtiminen lisää tiedon eheyttä. (Pietikäinen 2013; Helsingin yliopisto 2019.) Toisaalta tiedon eheys eli luotettavuus vaarantuu, jos tietoa ei päivitetä ajantasaiseksi ja järjestelmään jää vanhentunutta tietoa.

2.4 Saatavuus

Tietoturvaan liittyy oleellisesti tiedon saatavuus. Järjestelmien on toimittava ja tiedon on oltava saatavilla silloin kun tietoa tarvitaan. Verkon kautta käytettävissä palveluissa tiedon saatavuus korostuu, sillä palveluiden on oltava saatavilla ajasta ja paikasta riippumatta. Tätä tarvetta on lisännyt myös sähköisten palveluiden käyttötapojen muutokset koskien käyttöaikoja ja paikkoja, jotka eivät enää noudata vain perinteisiä toimistotyöaikoja. (Pietikäinen 2013.)

Saatavuus takaa järjestelmien ja tiedon toiminnan sekä tiedon saavutettavuuden sitä tarvittaessa. Yleisin riski verkkoon liitetyissä järjestelmissä tiedon saatavuudelle on palvelunestohyökkäys, jossa hyökkääjä estää pääsyn verkossa olevaan järjestelmään ja sen sisältämään tietoon. Saatavuuden varmistamiseksi on tärkeää varmistaa järjestelmän toiminta myös virhetilanteissa esimerkiksi valvomalla järjestelmään tulevaa verkkoliikennettä ja tarvittaessa estää tulevia haitallisia yhteyksiä. (Gil 2018.)

2.5 Tietosuoja

Tietosuoja tarkoittaa jokaiselle kuuluvaa perusoikeutta yksityisyyteen eli yksityiselämän ja henkilötietojen suojaan. Tietosuoja on hyvä huomioida aina tietoturvaa käsiteltäessä, sillä tietoturva on yksi tietosuojan toteuttamiskeino. (Tietosuojavaltuutetun toimisto 2020.) Tietosuoja määrittelee siis osaltaan tietoturvavaatimuksia.

2.5.1 Tietosuoja-asetus

Euroopan Unionin yleinen tietosuoja-asetus asettaa tarkkoja vaatimuksia yrityksille ja organisaatioille. Tietosuoja-asetuksessa asetetut vaatimukset koskevat henkilötietojen keräämistä, säilytystä ja hallinnointia. Tietosuoja-asetuksen vaatimuksia sovelletaan yrityksiin, jotka käsittelevät henkilötietoja Euroopan Unionin alueella, sekä yrityksiin, jotka käsittelevät Euroopan Unionin alueella asuvien henkilöiden henkilötietoja. (Yleinen tietosuoja-asetus 2020.)

Yleisen tietosuoja-asetuksen perusteella henkilötiedoilla tarkoitetaan kaikkia tietoja, joiden perusteella rekisteröity voidaan tunnistaa tai rekisteröity on tunnistettavissa. Henkilötietoihin lukeutuu muun muassa nimi, osoite, IP-osoite, puhelinnumero sekä potilastiedot. (Yleinen tietosuoja-asetus 2020.) Lisäksi henkilötietoihin lukeutuu esimerkiksi virtuaalisen oppimisympäristön tekniset seurantatiedot (lokitiedot), kun käyttäjä opiskelee materiaalia henkilökohtaisella tunnuksellaan. Luonnollisesti myös verkkokurssin suoritustiedot ovat henkilötietoja.

Henkilötietojen käsittelyä koskevat periaatteet on esitetty tietosuoja-asetuksessa. Nämä henkilötietojen käsittelyä koskevat periaatteet tulee huomioida henkilötietoja käsiteltäessä. Lisäksi yhtenä periaatteena on sisäänrakennettu ja oletusarvoinen tietosuoja. Tällä tarkoitetaan esimerkiksi tietojärjestelmiä ja -ratkaisuja suunniteltaessa ja kehittäessä huomioidaan muut tietosuoja-asetuksen henkilötietojen käsittelyä koskevat periaatteet. Näin kehitettävät järjestelmät ovat lähtökohtaisesti jo alusta alkaen suunniteltu täyttämään tietosuojavaatimukset. (Hanninen, Laine, Rantala, Rusi & Varhela 2017, 47–55.)

3 MOODLE

Moodle on avoimeen lähdekoodiin perustuva ilmainen virtuaalinen oppimisympäristö, joka on asennettavissa www-palvelimelle. Moodle mahdollistaa laajan kustomoinnin niin ulkonäöllisesti kuin asetuksien puolesta. (Moodle LMS 2020.) Virtuaalisen oppimisympäristön käyttäjä voi käyttää Moodle-kursseja modernilla verkkoselaimella, eikä käyttäjän tarvitse asentaa ohjelmia verkkokurssien käyttämiseksi. Moodle on saatavana myös mobiilisovelluksena Google Play ja App Store -sovelluskaupoista. (Moodle App 2020.)

Avoimen lähdekoodin toteutuksen vuoksi Moodle on helposti muokattavissa ja kustomoitavissa eri tarpeisiin. Moodle toimii modulaarisesti, jolloin erilaisia moduuleja voidaan ottaa käyttöön tai kytkeä pois käytöstä käyttäjän tarpeiden mukaan. Lisäksi Moodleen on saatavilla laajennuksia ja lisäosia, joilla käyttömahdollisuuksia voi laajentaa. (Moodle Docs 2018.)

Moodle on käytössä alustana kymmenissä tuhansissa verkkokoulutusympäristöissä maailmanlaajuisesti, ja sen käyttäjiin lukeutuu muun muassa suuryrityksiä ja kouluja, kuten Shell, Microsoft ja London School of Economics. Moodle-verkkokoulutusympäristöillä on maailmanlaajuisesti yli 90 miljoonaa loppukäyttäjää koulutus- ja yrityskäytössä. Näin ollen Moodle on maailman laajimmin käytetty verkkokoulutusympäristö. Moodle skaalautuu hyvin eri käyttäjämäärien mukaan, joten se soveltuu käytettäväksi riippumatta organisaation käyttäjämäärästä. (Moodle Docs 2018.) Moodle on myös Suomessa laajasti käytössä toisen asteen oppilaitoksissa, korkeakouluissa sekä yrityksissä.

Moodle-verkkokoulutusympäristö näyttäytyy käyttäjälle SaaS-pilvipalveluna *(Software as a Service*). SaaS-pilvipalvelussa käyttäjä käyttää ohjelmaa internetin välityksellä verkkoselaimen kautta. SaaS-pilvipalvelu mahdollistaa lisäksi tehokkaan ylläpidon, joka vapauttaa palveluntuottajalta resursseja ylläpitotehtävistä. (Leppänen 2013.)

Moodle on kehitetty käyttäen LAMP-arkkitehtuuria, johon sisältyy Linux-käyttöjärjestelmä, Apache-webpalvelin, MySQL-tietokanta sekä PHP-ohjelmointikieli.

Moodle-verkkokoulutusympäristön voi perustaa myös muita vastaavia ratkaisuja käyttäen, mutta LAMP-arkkitehtuuri on yleisin käytössä oleva ratkaisu. (Büchner 2016, 34.)

3.1 Tietoturva-asetukset

Moodlen tietoturvan valvontaa kehitetään ja päivitetään jatkuvasti. Tietoturvan valvonnalla voidaan turvata tietoturvan ja käyttäjien yksityisyyden toteutuminen. Tämä tarkoittaa esimerkiksi yksityisyyden suojaamista tietojen luvattomalta käytöltä, tietojen katoamiselta sekä väärinkäytöksiltä. Moodlen tietoturvaa voi parantaa ottamalla Moodle käyttöön omalla palvelimella, jolloin koko palvelinympäristö ja Moodlen hallinnointi on ylläpitäjän hallinnassa. (Moodle Docs 2018.)

Käyttäjätunnuksia voidaan suojata salasanan vaihtopyyntöjen yhteydessä. Salasanan vaihtoviesti lähetetään käyttäjän syöttämään sähköpostiosoitteeseen, jos kyseinen sähköposti on liitetty järjestelmässä olevaan käyttäjätiliin. Käyttäjälle ei kuitenkaan kerrota, onko kyseinen sähköpostiosoite liitetty järjestelmässä olevaan käyttäjätiliin. Näin esimerkiksi vihamielinen taho ei voi selvittää, mitä sähköpostiosoitteita järjestelmään on rekisteröityneenä. (Moodle Docs 2019.) Tämä lisää näin myös sähköpostiosoitteen käyttäjän tietosuojaa, kun vihamielinen taho ei voi päätellä, onko sähköpostiosoite rekisteröityjen käyttäjien joukossa esimerkiksi tietyssä verkkokoulutusympäristössä.

Moodlessa käyttäjät voidaan pakottaa kirjautumaan sisään käyttääkseen järjestelmää. Ilman kirjautumista käyttäjiltä voidaan estää myös koko järjestelmän etusivulle pääsy, jolloin käyttäjä ei pääse käsiksi mihinkään tietoihin ennen kirjautumista. Lisäksi kirjautuminen voidaan vaatia, jotta käyttäjä pääsee tarkastelemaan toisien käyttäjien profiileja järjestelmässä. (Moodle Docs 2019.) Tämä ei vielä kuitenkaan estä ketä tahansa rekisteröitymästä järjestelmään, vaan järjestelmään rekisteröityminen tulee rajata erikseen tarvittaessa.

Käyttäjien käyttäjäprofiilissa oletuksena näkyviä tietoja voidaan piilottaa käyttäjiltä, jolloin kyseisiin kenttiin syötetyt tiedot eivät ole näkyvissä käyttäjän profiili-

sivulla. Seuraavat tiedot ovat piilotettavissa: Kuvaus, kaupunki, maa, web-sivusto, ICQ-numero, Skype ID, Yahoo ID, AIM ID, MSN ID, ensimmäinen käyttöhetki viimeisin käyttöhetki, viimeisin IP-osoite, omat kurssit. (Moodle Docs 2018.)

Moodle-ympäristö voidaan sallia hakukoneiden indeksoitavaksi, jolloin sivusto löytyy paremmin esimerkiksi Google-hakukoneella tehdyissä hauissa. Lisäksi Moodlessa voidaan sallia Googlen hakuohjelmiston pääsy sivustolle, jolloin kaikki järjestelmässä vierastunnuksella luettava sisältö tulee näkyviin Google-hakujen yhteydessä. (Moodle Docs 2019.) Tämä asetus siis mahdollistaa joko sivuston tehokkaamman löytymisen hakukoneiden, varsinkin Googlen, kautta, tai vaihtoehtoisesti heikentää sivuston hakukonenäkyvyyttä niin haluttaessa. Esimerkiksi organisaation sisäiseen käyttöön suunnatusta Moodle-verkkokoulutusympäristöstä on mahdollista kytkeä hakukoneindeksointi pois käytöstä, jolloin sivustolle tulee vähemmän ulkopuolista verkkoliikennettä.

Käyttäjien pääsyn Moodle-ympäristöön voidaan rajata myös IP-osoitteiden perusteella (Moodle Docs 2016). IP-osoitteiden perusteella tehtävällä rajauksella voidaan sallia järjestelmän käyttäminen ainoastaan organisaation sisäverkosta taikka vain tietyistä IP-osoitteista. Myös tiettyjen IP-osoitteiden kieltäminen erikseen on mahdollista, jolloin IP-osoitteita kieltämällä voidaan karsia haitallista verkkoliikennettä.

Cron-ajoilla voidaan tehdä useita ylläpidollisia tehtäviä Moodle-ympäristössä, kuten lähettää ilmoituksia ja poistaa väliaikaisia tiedostoja. Web-selaimen kautta cron-ajoja tehdessä järjestelmän tietoturva vaarantuu, sillä selaimen kautta tehdyissä ajoissa ei ole käyttäjän varmennusta, eli kuka tahansa voi näitä ajoja tehdä. Cron-ajoja tulisi tehdä vain salasanalla suojatun etäyhteyden kautta tai suoraan komentorivillä, jolloin ulkopuolisten väärinkäytösten riski vähenee. (Büchner 2016, 332–333; Moodle Docs 2019.)

3.2 Käyttäjätilit

Käyttäjätilien luominen järjestelmään on mahdollista joko käyttäjän itsensä tai järjestelmän ylläpitäjän toimesta. Järjestelmän ylläpitäjän luomia tunnuksia kutsutaan **manuaalisiksi tunnuksiksi**. Nämä tunnukset toimitetaan automaattisesti sähköpostitse käyttäjälle tunnusten luonnin yhteydessä, kun ylläpitäjä syöttää pakolliseen sähköpostikenttään käyttäjän sähköpostiosoitteen.

Käyttäjä voi luoda itselleen tunnuksen järjestelmään rekisteröitymällä käyttäjäksi. Tällöin käyttäjä itse syöttää omat tietonsa ja valitsee itselleen käyttäjätunnuksen ja salasanan. Käyttäjän itse itselleen luotua tunnusta kutsutaan **itserekisteröidyksi tunnukseksi.** Tämä tunnus käyttäjän tulee erikseen vahvistaa sähköpostiin tulevan vahvistusviestin kautta ennen kuin tunnusta pääsee käyttämään.

Itserekisteröitymisen salliminen mahdollistaa lähtökohtaisesti kenelle tahansa rekisteröitymisen Moodle-ympäristöön. Tämä ei kuitenkaan ole aina toivottu tilanne, jos Moodle-ympäristö on suunnattu vain tietylle käyttäjäryhmälle, esimerkiksi yrityksen työntekijöille tai koulun opiskelijoille. Itserekisteröitymistä voidaan rajata itserekisteröityihin tunnuksiin vain tiettyjä **sallittuja sähköpostitoimialueita**. Tällöin esimerkiksi kaikki yrityksen sähköpostiosoitteen omaavat voivat luoda itselleen tunnuksen, mutta muiden kohdalla järjestelmä hylkää toimialueen, joka ei ole sallittujen osoitteiden listalla.

Itserekisteröityjen ja manuaalisten tilien lisäksi Moodlessa on mahdollista käyttää ulkoisia käyttäjähakemistoja, kuten esimerkiksi LDAP-palvelinta, käyttäjätietojen hakuun ja käyttäjän tunnistamiseen.

3.3 Käyttäjäroolit

Käyttäjäroolit ovat käytännössä käyttöoikeuksia, joilla määritellään mihin toimintoihin ja ominaisuuksiin käyttäjillä on pääsy Moodlessa (Büchner 2016, 53). Kurssitasoiset käyttäjäroolit ovat voimassa vain sillä kurssilla, jolla käyttäjärooli on käyttäjälle annettu. **Opiskelija**-roolilla käyttäjä voi käyttää verkkokurssia ja

suorittaa verkkokurssin arvioitavia tenttejä. **Opettaja**-roolilla käyttäjällä on muokkausoikeus verkkokurssin sisältöön sekä asetuksiin mutta ei pääsyä suorittamaan tenttejä. Rooleja on mahdollista luoda myös itse Moodle-ympäristöön, ja roolien oikeuksia voi tarvittaessa myös muokata.

3.4 Käyttäjän todennus

Moodle tukee useita eri todennusvaihtoehtoja käyttäjien todentamiseen kirjautumisen yhteydessä. Manuaalisten tunnusten ja itserekisteröityjen tunnusten todennuksen ohella on mahdollista käyttää esimerkiksi organisaatiotasoisia LDAP-palvelimen sisältämiä todennustietoja. LDAP-todennusta käytettäessä kirjautumistiedot varmistetaan ulkoiselta palvelimelta, jossa organisaatiotason käyttäjätietoja hallinnoidaan.

Eri todennustapoja voi käyttää myös rinnakkain. Samaan verkkokoulutusympäristöön voi kirjautua käyttäjiä samanaikaisesti sekä manuaalisilla tunnuksilla että esimerkiksi AD-tunnuksilla LDAP-yhteyden välityksellä.

Käyttäjän kirjautumisen yhteydessä Moodle tarkistaa käyttäjän syöttämät kirjautumistiedot eli käyttäjätunnuksen ja salasanan. Jos nämä tiedot ovat oikeita, käyttäjä pääsee kirjautumaan tunnukselleen. Väärällä käyttäjätunnuksella tai salasanalla kirjautuminen ei onnistu, vaan järjestelmä ilmoittaa kirjautumisen epäonnistumisesta.

4 TESTIYMPÄRISTÖN MÄÄRITTELY

Käytännön työnä oli tarkoitus selvittää Moodle-ympäristön tietoturvaominaisuuksia ja sen perusteella määritellä Moodleen verkkokoulutuskäyttöön soveltuvat tietoturva-asetukset. Olennaista työn tekemisessä oli hankkia ajantasaista tietoa Moodlen tietoturva-asetuksista ja niiden mahdollistamista ratkaisuista käyttäjien tietoturvan ja tietosuojan takaamiseksi.

Työssä käytettiin testiympäristöä, johon tietoturvaominaisuudet ja -asetukset määriteltiin. Testiympäristönä käytettiin Moodlen versiota 3.8.3.

4.1 Tietoturvavaatimukset Moodle-ympäristöön

Moodlea verkkokoulutuskäytössä käytettäessä olennaista on mahdollistaa käyttäjien pääsy verkkokoulutusympäristöön ajasta ja paikasta riippumatta, jotta palvelun käyttö käyttäjille on mahdollisimman helppoa ja joustavaa. Olennaista on siis palvelun saatavuus käyttäjille. Tämä tarkoittaa käytännössä, että ylimääräisiä rajoituksia palvelun saatavuuteen ei tulisi olla, vaikka ne voisivat osaltaan parantaa toisia tietoturvan osa-alueita.

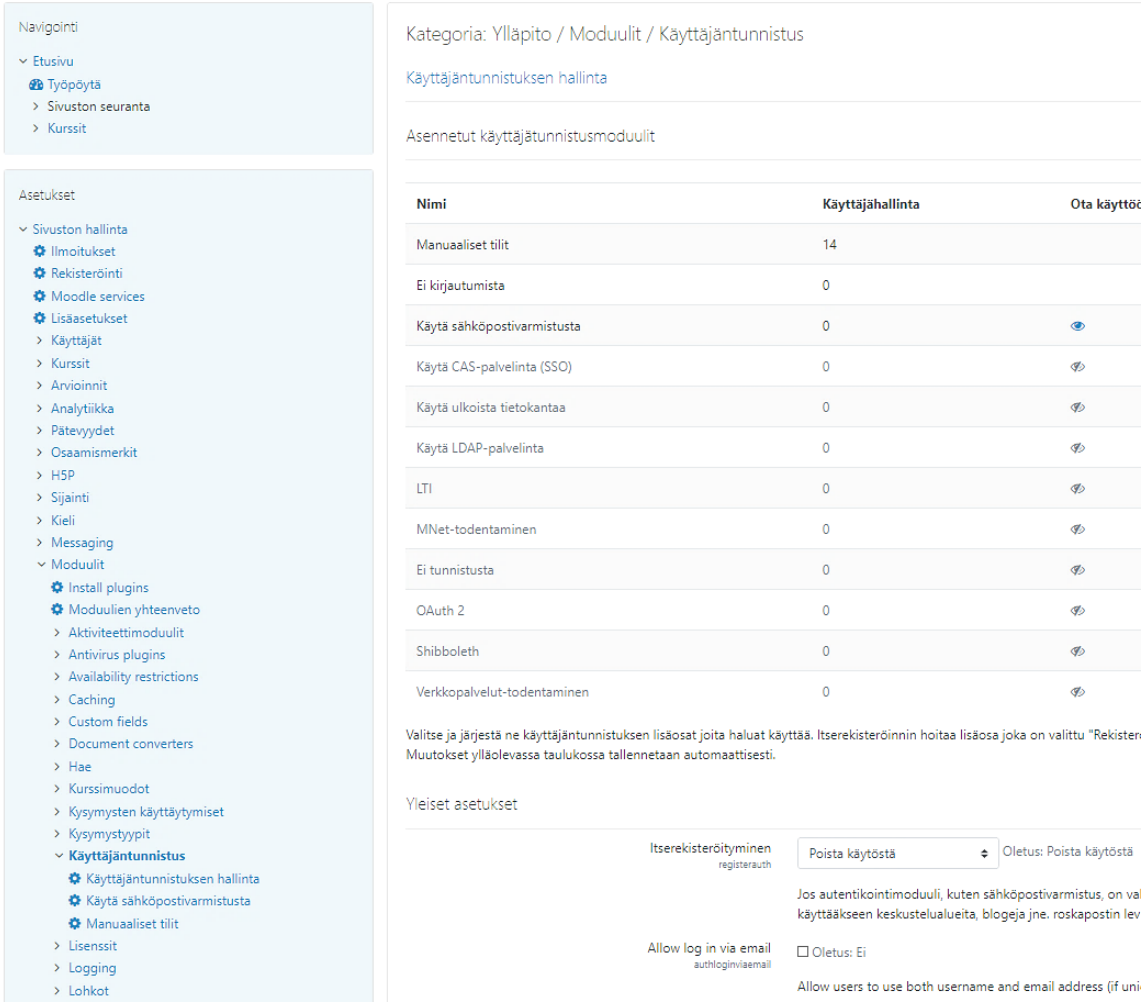
Käyttäjien todentaminen tulee tehdä heikentämättä liikaa palvelun saatavuutta, jonka vuoksi otetaan käyttöön käyttäjätunnus ja salasana käyttäjän tunnistamiseen. Salasanaan asetetaan kahdeksan merkin vähimmäisvaatimus pituudelle sekä yhden merkin vaatimus isoista ja pienistä kirjaimista, numeroista ja erikoismerkeistä.

4.2 Käyttäjäntunnistuksen määrittely

Käyttäjäntunnistus voidaan toteuttaa Moodlessa käyttäjätunnuksella ja salasanalla, joka on lähtökohtaisesti oletustapa tunnistaa rekisteröity käyttäjä. Käyttäjän

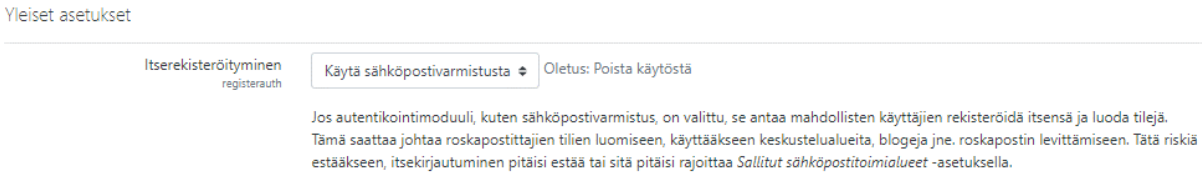
tunnistaminen rekisteröintivaiheessa toteutetaan ottamalla käyttöön itserekisteröityminen, jolloin käyttäjät voivat luoda itselleen käyttäjätunnuksen verkkokoulutuskäyttöä varten.

Itserekisteröityminen otetaan käyttöön ”Asetukset”-valikosta avaamalla ”Sivuston hallinta”, jonka alta avataan ”Moduulit” ja edelleen sen alta ”Käyttäjäntunnistus”. Aukeava asetusvalikko on esitetty alla kuvassa 1.



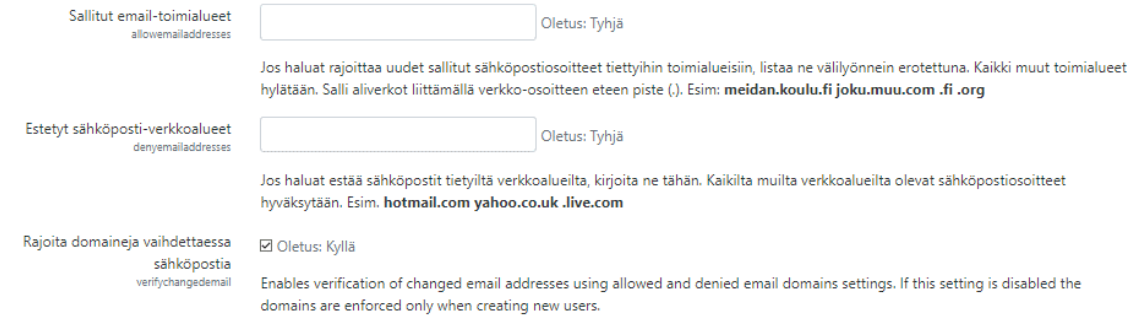
KUVA 1. Käyttäjäntunnistus

Käyttäjäntunnistus-valikosta voidaan ottaa itserekisteröityminen käyttöön tai poistaa se käytöstä. Oletuksena se on poistettu käytöstä, eli valintaruutuun tulee tässä tapauksessa valita kohta ”Käytä sähköpostivarmistusta”. Tämä on esitetty alla kuvassa 2.



KUVA 2. Itserekisteröityminen

Järjestelmä varoittaa asetuksen valinnan jälkeen, että sähköpostivarmennuksen käyttöön ottaminen saattaa johtaa roskapostittajien tileihin, jonka vuoksi järjestelmä suosittelee rajaamaan itserekisteröitymistä sallituilla sähköpostitoimialueilla. Sallitut sähköpostitoimialueet syötetään samalla käyttäjäntunnistus-asetussivulla olevaan ”Sallitut email-toimialueet”-kenttään muodossa ”toimialue.com”, eli sähköpostiosoitteen @-merkin jälkeinen osa syötetään kenttään. Useita toimialueita syötettäessä erottimena käytetään välilyöntiä. Tämä valikon osa on kuvattu kuvassa 3. Samalla periaatteella voi erikseen estää tietyt toimialueet ”Estetyt sähköposti-verkkoalueet”-kenttää käyttämällä.

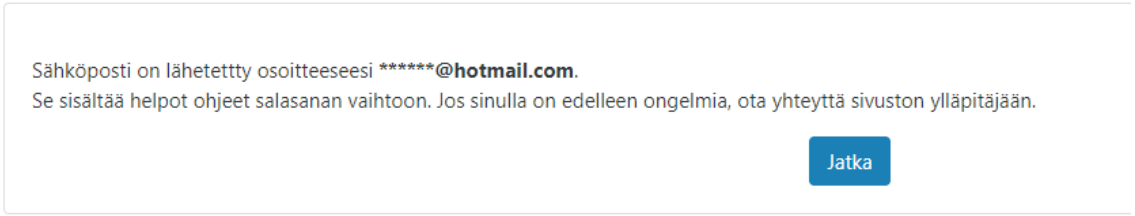


KUVA 3. Sallitut sähköpostitoimialueet

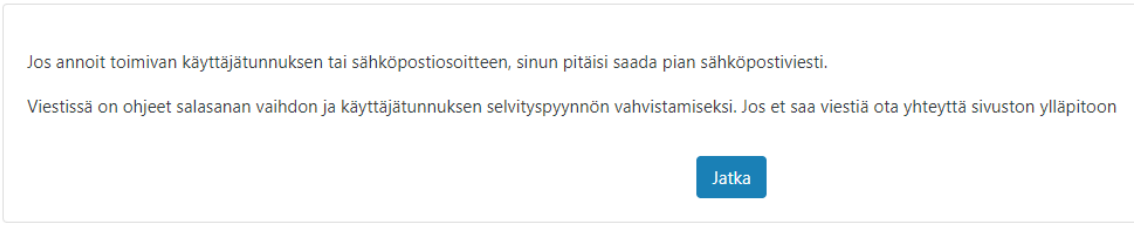
4.3 Tietoturva-asetusten määrittely

Tietoturva-asetusten määrittely tapahtuu ”Asetukset”-valikon kohdasta ”Sivuston hallinta”, josta valitaan ”Tietoturva” ja sen alta vielä ”Sivuston käyttöehdot”. Aukeavalla sivulla voidaan määrittää keskeisimmät tietoturvaan liittyvät asetukset. Tässä kappaleessa käsitellään asetuksien nimityksiä englanniksi yhtenäisyyden vuoksi, sillä Moodlen suomennoksesta puuttuu valtaosa näiden asetuksien käännöksistä. Kaikki tietoturva-asetukset (*Site security settings*) on kuvattu Liitteessä 1.

Käyttäjätunnuksia suojataan vihamielisiltä kalasteluyrityksiltä salaamalla käyttäjänimet ja sähköpostiosoitteet salasanan vaihtopyyntöjen yhteydessä. Tämä asetus ”*Protect usernames*” on oletuksena päällä. Alla kuvat 4 ja 5, joissa näkyy tämän asetuksen vaikutus salasanan vaihtopyynnön yhteydessä pyytäjälle näytettävästä viestistä.



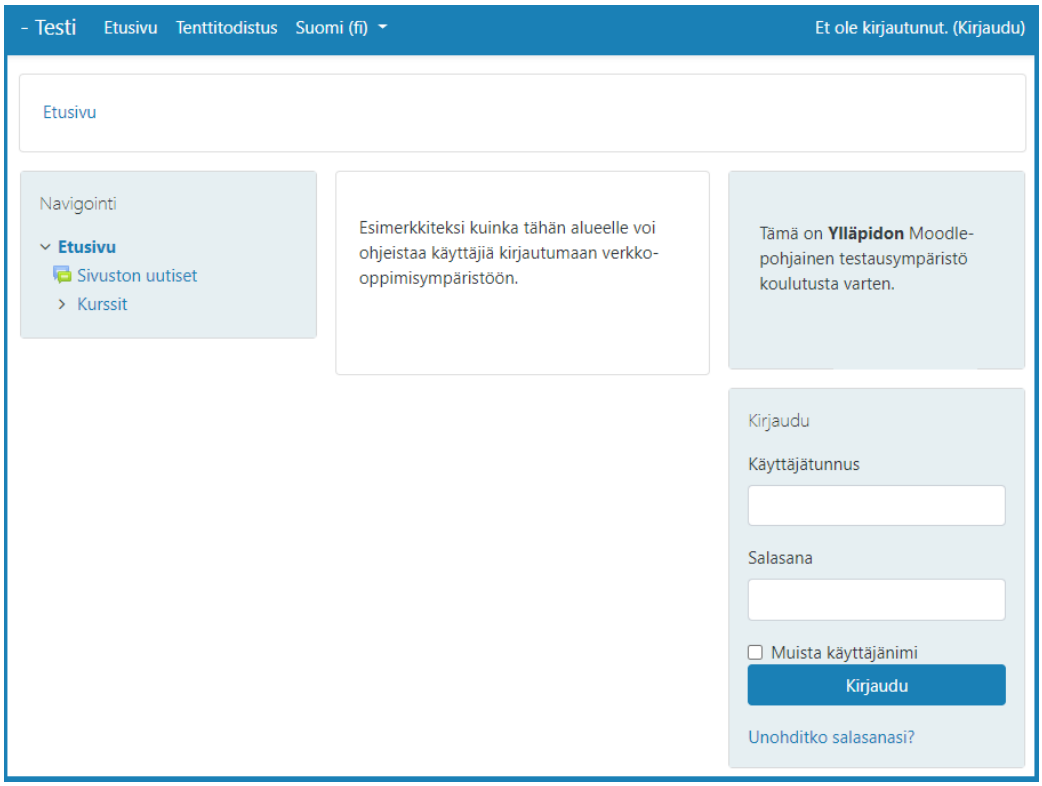
KUVA 4. Sähköpostiosoite näkyvissä



KUVA 5. Sähköpostiosoite suojattu

Kuvassa 4 näkyy, kuinka salasanan vaihtoa pyytävälle näytetään tunnuksen olemassaolo, toisin kuin kuvassa 5 jossa ei kerrota onko kyseisellä sähköpostiosoitteella rekisteröity tunnusta. Tämä sama toistuu myös, jos salasanaa halutaan palauttaa käyttäjätunnuksen perusteella sähköpostiosoitteen sijasta.

Käyttäjä voidaan pakottaa kirjautumaan sisään järjestelmään ennen varsinaisen etusivun näyttämistä. Tämä ei kuitenkaan tämän projektin osalta ole tarkoituksenmukaista, sillä järjestelmän etusivu on hyvä olla näkyvissä käyttäjien ohjeistamiseksi. Etusivu on esillä kuvassa 6.



KUVA 6. Moodle-ympäristön etusivu

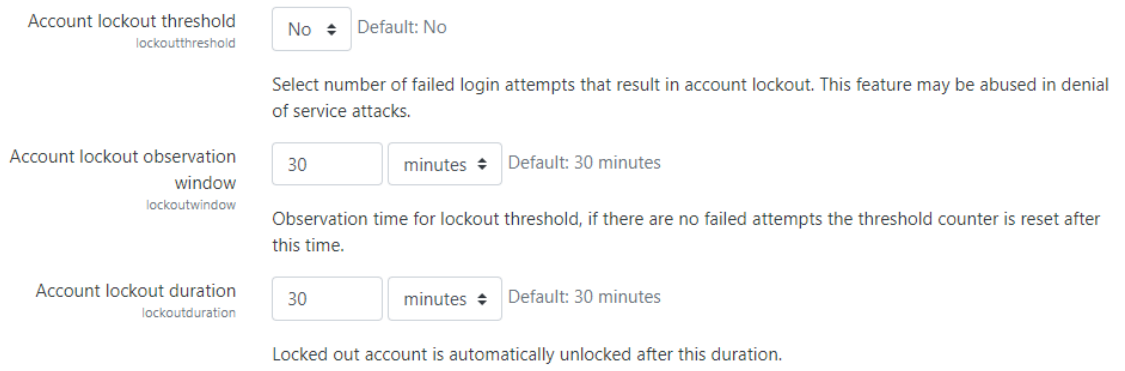
Käyttäjäprofiilit voidaan piilottaa kirjautumattomilta käyttäjiltä käyttäjätietojen suojaamiseksi. Tämä tapahtuu asetuksella ”*Force users to log in for profiles*”, joka on oletuksena käytössä.

Käyttäjiltä on oletuksena estetty *EMBED*- ja *OBJECT*-merkinnät HTML-tekstinsyötön yhteydessä (asetus ”*Allow EMBED and OBJECT tags*”). *EMBED*- ja *OBJECT*-merkintöjä käyttämällä käyttäjä voi lisätä mediatiedostoja alueille, joille tällä on muokkausoikeus, esimerkiksi käyttäjäprofiilinsa tietoihin. Tässä tapauksessa tämän käyttöönotolle ei ole tarvetta, jonka vuoksi asetus tulee ehdottomasti pitää estettynä.

Asetuksella ”*Enable trusted content*” voidaan sallia tietyille käyttäjille mahdollisuus syöttää skriptejä, komentoja taikka upotettuja objekteja. Oletuksena näiden syöttäminen on estetty käyttäjiltä Moodlen tarkistaessa käyttäjien tekstisyötteen. Tällekään toiminnallisuudelle ei tässä tapauksessa ole tarvetta, joten asetus pidetään estettynä.

Cron-ajot voidaan rajata tehtäväksi vain komentorivin kautta asetuksella ”*Cron execution via command line only*”. Tämä asetus on oletuksena käytössä eli cron-ajot on tehtävä Linuxin komentorivin kautta. Koska cron-ajojen tekemiselle selaimen kautta ei ole erikseen tarvetta, jätetään tämä asetus oletustilaan eli cron-ajot rajataan komentoriville.

Käyttäjätunnukset voidaan lukita tietyn epäonnistuneen kirjautumismäärän jälkeen määritellyksi ajaksi asetuksella ”*Account lockout threshold*”. Jos esimerkiksi 30 minuutin sisällä käyttäjätunnukselle tulee kolme perättäistä epäonnistunutta kirjautumisyritystä, käyttäjätunnus voidaan lukita 30 minuutiksi, jonka aikana käyttäjätunnukselle ei pääse kirjautumaan. Lukitusaikaa voi säätää asetuksella ”*Account lockout duration*” ja epäonnistuneiden kirjautumiskertojen tarkkailuaikaa voidaan säätää asetuksella ”*Account lockout observation window*”. Kaikki nämä asetuskohdat ovat näkyvissä alla kuvassa 7.



KUVA 7. Käyttäjätunnuksen lukitus

Käyttäjätunnuksen lukitus siis rajoittaa käyttäjätunnukselle kirjautumista epäonnistuneiden kirjautumisyritysten jälkeen. Kuitenkin palvelun saatavuus asetettiin

tärkeäksi kriteeriksi, jonka vuoksi asetusta ei oteta käyttöön palvelun saatavuuden parantamiseksi käyttäjille.

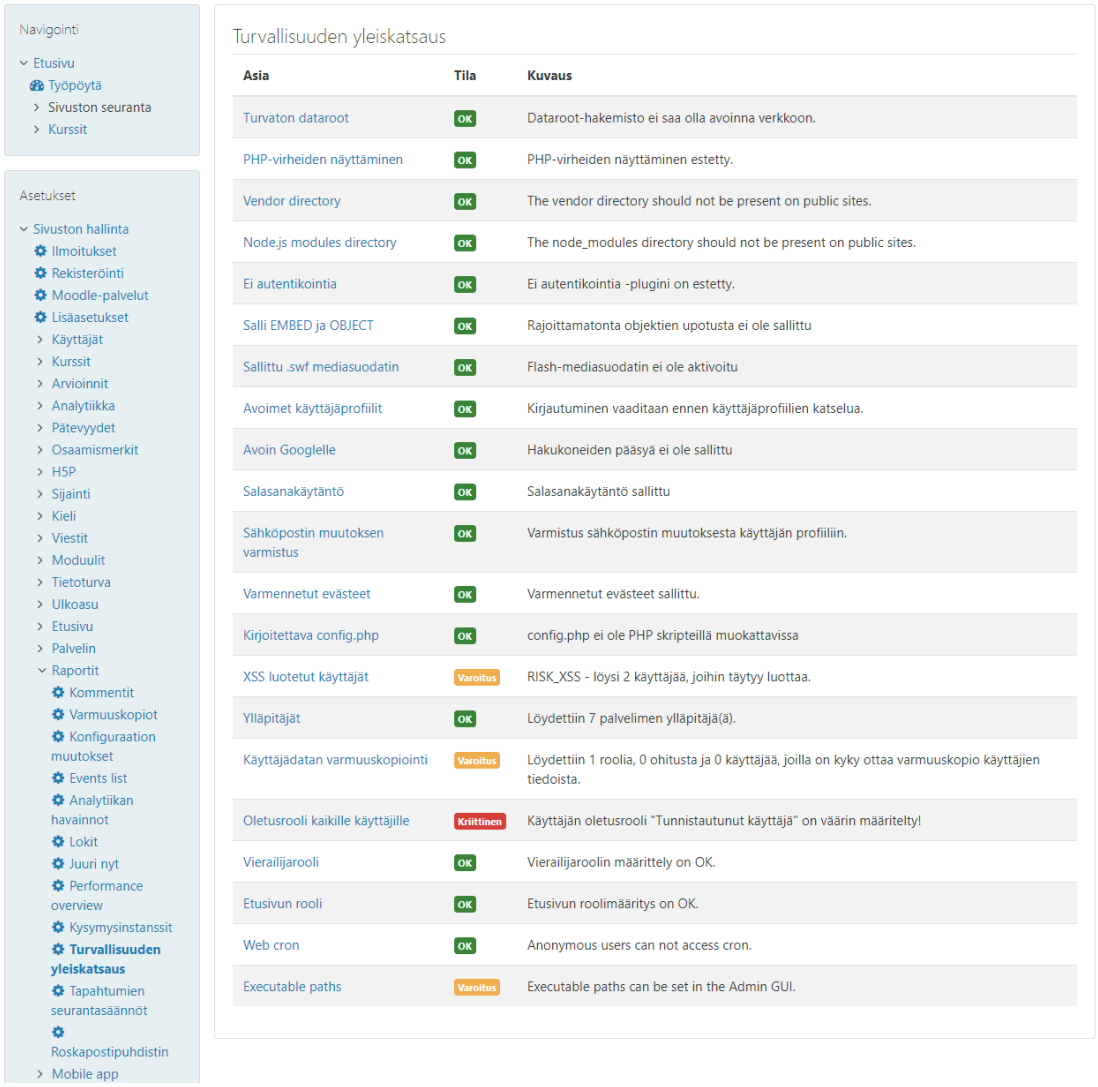
Salasanalle voidaan asettaa vaatimuksia käyttämällä ”*Password policy*”-asetusta. Salasanaan voidaan määrittää minimimäärät salasanan pituudelle, numeroille, pienille ja isoille kirjaimille sekä erikoismerkeille. Myös salasanassa esiintyviä samoja peräkkäisiä merkkejä voidaan haluttaessa rajoittaa sekä asettaa rajoitus, kuinka usein käyttäjä voi käyttää samaa salasanaa. Oletuksena salasanan minimipituus on 8 merkkiä sekä vaatimus vähintään yhdelle isolle tai pienelle kirjaimelle, numerolle ja erikoismerkille. Nämä oletusasetukset ovat riittävät tämän työn tarpeisiin, eikä toisaalta ole syytä lähteä heikentämään salasanavaatimuksia, varsinkin kun käyttäjätunnuksen lukitus on poistettu käytöstä.

4.4 Käyttäjäroolien määrittely

Kurssitasoiset käyttäjäroolit määritellään Moodlessa ”Asetukset”-valikon kohdasta ”Sivuston hallinta”, josta valitaan ”Käyttäjät” ja sen alta vielä ”Oikeudet”. Aukeavalla sivulla on linkki ”Määritä roolit”, josta päästään muokkaamaan käyttäjärooleja. Kyseisellä sivulla voidaan luoda uusia tai poistaa ylimääräisiä käyttäjärooleja, sekä muokata roolikohtaisia oikeuksia valitsemalla se käyttäjärooli, jota halutaan muokata. Käyttäjäroolit on Moodlessa oletuksena asetettu verkkokoulutuskäyttöön hyvin sopiviksi, eli niihin ei tässä kohtaa ole tarpeen lähteä tekemään muutoksia.

4.5 Turvallisuuden yleiskatsaus

Turvallisuuden yleiskatsaus -raportilla voi nopeasti tarkistaa Moodle-ympäristön kriittisten turvallisuusasetusten tilanteen. Näkymä löytyy asetuksista ”Sivuston hallinta”-kohdan alta ”Raportit”-kohdasta. Turvallisuuden yleiskatsaus -näkymä on esitetty alla kuvassa 8.



KUVA 8. Turvallisuuden yleiskatsaus

Turvallisuuden yleiskatsaus -näkymä listaa Moodlen keskeisimpien turva-asetusten tilan ja antaa selkeän varoituksen, jos asetuksissa on muutettavaa. Tällä näkymällä on järkevää tarkistaa asetusten tilanne säännöllisesti, jolloin ylläpitäjä pysyy paremmin perillä Moodlen asetusten tilasta.

5 POHDINTA

Opinnäytetyötä tehdessä tuli huomattua, että valittu aihe olikin odotettua laajempi. Moodle on laaja järjestelmä, jossa on laajalti erilaisia tietoturvaan eri tavoin vaikuttavia toimintoja. Tämän lisäksi järjestelmän tietoturvaan vaikuttaa se palvelinratkaisu, jolle järjestelmä on asennettu. Tähän palvelinratkaisun tietoturvaan ei tässä työssä juurikaan voitu paneutua, vaikka toki sen merkitys tuli esille usein lähdemateriaalissa, sillä tämän opinnäytetyön tavoitteena oli puhtaasti Moodlen tietoturvaominaisuuksien selvittäminen.

Opinnäytetyön tavoite perehtyä Moodlen tietoturvaan toteutui pääkohdiltaan. Moodlen tietoturva-asetukset sekä -ominaisuudet saatiin selvitettyä, jonka lisäksi perehdyttiin tietoturvan teoriaan sekä tietoturvaan läheisesti liittyvään tietosuojaan. Nämä tietoturva-asetukset ja ominaisuudet saatiin myös määriteltyä testiympäristöön.

Paljon jäi kuitenkin vielä selvitettävää, josta toki osa olikin rajattu tämän työn ulkopuolelle. Moodleen on viime vuosina tuotu paljon tietosuojaan liittyviä toimintoja, pääasiassa yleisen tietosuoja-asetuksen vaikutuksesta. Näiden toimintaa ja merkitystä voisi selvittää jatkossa.

LÄHTEET

Büchner, A. 2016. Moodle 3 Administration. 3. painos. Birmingham: Packt Publishing Ltd.

Data Group & Fujitsu. 2018. Tietoturvallinen tunnistautuminen. Luettu 13.5.2020. https://www.datagroup.fi/fi/asiakkaille/blogi/tietoturvallinen-tunnistautuminen

Euroopan Unioni. 2020. Yleinen tietosuoja-asetus. Luettu 15.4.2020. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm

Gil, A. 2018. Data Security – Confidentiality, Integrity & Availability. Luettu 14.5.2020. https://www.kvausa.com/data-security-confidentiality-integrity-and-availability/

Hanninen, M., Laine, E., Rantala, K., Rusi, M. & Varhela, M. 2017. Henkilötietojen käsittely – EU-tietosuoja-asetuksen vaatimukset. 1. painos. Vantaa: Kauppakamari.

Helsingin yliopisto. 2015. Yleistä salausmenetelmistä. Luettu 15.4.2020. https://helpdesk.it.helsinki.fi/ohjeet/tietoturva-ja-pilvipalvelut/tietoturva/yleista-salausmenetelmista

Helsingin yliopisto. 2019. Opiskelijan digitaidot. Luettu 16.4.2020. https://blogs.helsinki.fi/opiskelijan-digitaidot/4-tietoturva/

Järvinen, P. 2002. Tietoturva & Yksityisyys. 2. painos. Jyväskylä: Docendo Finland Oy.

Kyberturvallisuuskeskus. 2019. Tietoturva. Luettu 16.4.2020. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Leppänen, M. 2013. Pilvipalvelut ja tietoturva. Tietotekniikan koulutusohjelma. Tampereen ammattikorkeakoulu. Opinnäytetyö.

Moodle Docs. 2016. IP blocker. Luettu 18.5.2020. https://docs.moodle.org/38/en/IP_blocker

Moodle Docs. 2018. About Moodle. Luettu 7.5.2020. https://docs.moodle.org/38/en/About_Moodle#Extensive_resources_available

Moodle Docs. 2018. Privacy. Luettu 1.6.2020

https://docs.moodle.org/38/en/Privacy

Moodle Docs. 2019. Site security settings. Luettu 14.5.2020. https://docs.moodle.org/38/en/Site_security_settings

Moodle Pty Ltd. 2020. Moodle App. Luettu 2.3.2020. https://moodle.com/app/

Moodle Pty Ltd. 2020. Moodle LMS. Luettu 2.3.2020. https://moodle.com/lms/
Pietikäinen, S. 2013. Tietoturvallisuus – mitä se on?. Luettu 12.5.2020. https://www.vahtiohje.fi/web/guest/691

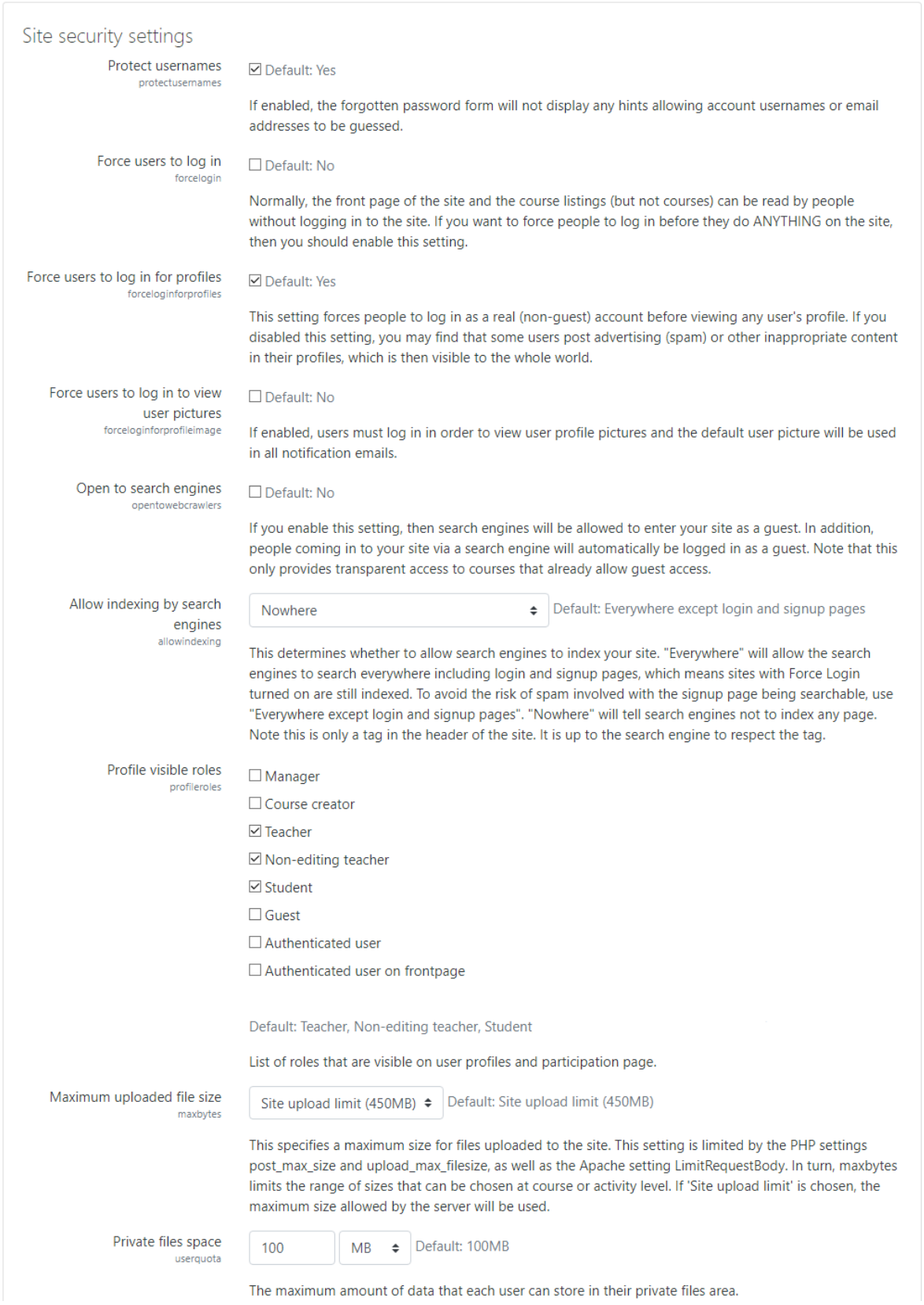
Tietosuojavaltuutetun toimisto. 2020. Mikä on henkilötieto. Luettu 11.5.2020 https://tietosuoja.fi/mika-on-henkilotieto

Tietosuojavaltuutetun toimisto. 2020. Tietosuoja. Luettu 11.5.2020. https://tietosuoja.fi/tietosuoja

Turner, D. 2016. Digital Authentication - the basics. Luettu 13.5.2020. https://www.cryptomathic.com/news-events/blog/digital-authentication-the-basics

LIITTEET

Liite 1. Site security settings



Site security settings

Protect usernames
protectusernames
☑ Default: Yes
If enabled, the forgotten password form will not display any hints allowing account usernames or email addresses to be guessed.

Force users to log in
forcelogin
☐ Default: No
Normally, the front page of the site and the course listings (but not courses) can be read by people without logging in to the site. If you want to force people to log in before they do ANYTHING on the site, then you should enable this setting.

Force users to log in for profiles
forceloginforprofiles
☑ Default: Yes
This setting forces people to log in as a real (non-guest) account before viewing any user's profile. If you disabled this setting, you may find that some users post advertising (spam) or other inappropriate content in their profiles, which is then visible to the whole world.

Force users to log in to view user pictures
forceloginforprofileimage
☐ Default: No
If enabled, users must log in in order to view user profile pictures and the default user picture will be used in all notification emails.

Open to search engines
opentowebcrawlers
☐ Default: No
If you enable this setting, then search engines will be allowed to enter your site as a guest. In addition, people coming in to your site via a search engine will automatically be logged in as a guest. Note that this only provides transparent access to courses that already allow guest access.

Allow indexing by search engines
allowindexing
Nowhere ⇕ Default: Everywhere except login and signup pages
This determines whether to allow search engines to index your site. "Everywhere" will allow the search engines to search everywhere including login and signup pages, which means sites with Force Login turned on are still indexed. To avoid the risk of spam involved with the signup page being searchable, use "Everywhere except login and signup pages". "Nowhere" will tell search engines not to index any page. Note this is only a tag in the header of the site. It is up to the search engine to respect the tag.

Profile visible roles
profileroles
☐ Manager
☐ Course creator
☑ Teacher
☑ Non-editing teacher
☑ Student
☐ Guest
☐ Authenticated user
☐ Authenticated user on frontpage
Default: Teacher, Non-editing teacher, Student
List of roles that are visible on user profiles and participation page.

Maximum uploaded file size
maxbytes
Site upload limit (450MB) ⇕ Default: Site upload limit (450MB)
This specifies a maximum size for files uploaded to the site. This setting is limited by the PHP settings post_max_size and upload_max_filesize, as well as the Apache setting LimitRequestBody. In turn, maxbytes limits the range of sizes that can be chosen at course or activity level. If 'Site upload limit' is chosen, the maximum size allowed by the server will be used.

Private files space
userquota
100 MB ⇕ Default: 100MB
The maximum amount of data that each user can store in their private files area.

Allow EMBED and OBJECT tags
allowobjectembed

☐ Default: No

As a default security measure, normal users are not allowed to embed multimedia (like Flash) within texts using explicit EMBED and OBJECT tags in their HTML (although it can still be done safely using the mediaplugins filter). If you wish to allow these tags then enable this option.

Enable trusted content
enabletrusttext

☐ Default: No

By default Moodle will always thoroughly clean text that comes from users to remove any possible bad scripts, media etc that could be a security risk. The Trusted Content system is a way of giving particular users that you trust the ability to include these advanced features in their content without interference. To enable this system, you need to first enable this setting, and then grant the Trusted Content permission to a specific Moodle role. Texts created or uploaded by such users will be marked as trusted and will not be cleaned before display.

Maximum time to edit posts
maxeditingtime

30 minutes ⇕ Default: 30 minutes

This specifies the amount of time people have to re-edit forum postings, glossary comments etc. Usually 30 minutes is a good value.

Allow extended characters in usernames
extendedusernamechars

☐ Default: No

Enable this setting to allow students to use any characters in their usernames (note this does not affect their actual names). The default is "false" which restricts usernames to be alphanumeric lowercase characters, underscore (_), hyphen (-), period (.) or at symbol (@).

Keep tag name casing
keeptagnamecase

☑ Default: Yes

Check this if you want tag names to keep the original casing as entered by users who created them

Profiles for enrolled users only
profilesforenrolledusersonly

☑ Default: Yes

To prevent misuse by spammers, profile descriptions of users who are not yet enrolled in any course are hidden. New users must enrol in at least one course before they can add a profile description.

Cron execution via command line only
cronclionly

☑ Default: Yes

Running the cron from a web browser can expose privileged information to anonymous users. Thus it is recommended to only run the cron from the command line or set a cron password for remote access.

Cron password for remote access
cronremotepassword

Click to enter text 🖉 👁

This means that the cron.php script cannot be run from a web browser without supplying the password using the following form of URL:

```
https://site.example.com/admin/cron.php?password=opensesame
```

If this is left empty, no password is required.

Allow 'Run now' for scheduled tasks
tool_task | enablerunnow

☑ Default: Yes

Allows administrators to run a single scheduled task immediately, rather than waiting for it to run as scheduled. The feature requires 'Path to PHP CLI' (pathtophp) to be set in System paths. The task runs on the web server, so you may wish to disable this feature to avoid potential performance issues.

Account lockout threshold
lockoutthreshold

No ⇕ Default: No

Select number of failed login attempts that result in account lockout. This feature may be abused in denial of service attacks.

Account lockout observation window
lockoutwindow

30 minutes ⇕ Default: 30 minutes

Observation time for lockout threshold, if there are no failed attempts the threshold counter is reset after this time.

Account lockout duration
lockoutduration

30 minutes ⇕ Default: 30 minutes

Locked out account is automatically unlocked after this duration.

Password policy
passwordpolicy
☑ Default: Yes

If enabled, user passwords will be checked against the password policy as specified in the settings below. Enabling the password policy will not affect existing users until they decide to, or are required to, change their password.

Password length
minpasswordlength
8 Default: 8

Passwords must be at least these many characters long.

Digits
minpasswordddigits
1 Default: 1

Passwords must have at least these many digits.

Lowercase letters
minpasswordlower
1 Default: 1

Passwords must have at least these many lower case letters.

Uppercase letters
minpasswordupper
1 Default: 1

Passwords must have at least these many upper case letters.

Non-alphanumeric characters
minpasswordnonalphanum
1 Default: 1

Passwords must have at least these many non-alphanumeric characters.

Consecutive identical characters
maxconsecutiveidentchars
0 Default: 0

Passwords must not have more than this number of consecutive identical characters. Use 0 to disable this check.

Password rotation limit
passwordreuselimit
0 Default: 0

Number of times a user must change their password before they are allowed to reuse a password. Hashes of previously used passwords are stored in local database table. This feature might not be compatible with some external authentication plugins.

Maximum time to validate password reset request
pwresettime
30 minutes Default: 30 minutes

This specifies the amount of time people have to validate a password reset request before it expires. Usually 30 minutes is a good value.

Log out after password change
passwordchangelogout
☐ Default: No

If enabled, when a password is changed, all browser sessions are terminated, apart from the one in which the new password is specified. (This setting does not affect password changes via bulk user upload.)

Remove web service access tokens after password change
passwordchangetokendeletion
☐ Default: No

If enabled, when a password is changed, all the user web service access tokens are deleted.

User created token duration
tokenduration
12 weeks Default: 12 weeks

Length of time for which a web services token created by a user (for example via the mobile app) is valid.

Group enrolment key policy
groupenrolmentkeypolicy
☐ Default: Yes

If enabled, group enrolment keys will be checked against the password policy as specified in the settings above.

Disable user profile images
disableuserimages
☐ Default: No

Disable the ability for users to change user profile images.

Email change confirmation
emailchangeconfirmation
☑ Default: Yes

Require an email confirmation step when users change their email address in their profile.

Remember username
rememberusername
optional Default: optional

Enable if you want to store permanent cookies with usernames during user login. Permanent cookies may be considered a privacy issue if used without consent.

Strict validation of required fields
strictformsrequired
☐ Default: No

If enabled, users are prevented from entering a space or line break only in required fields in forms.

Save changes