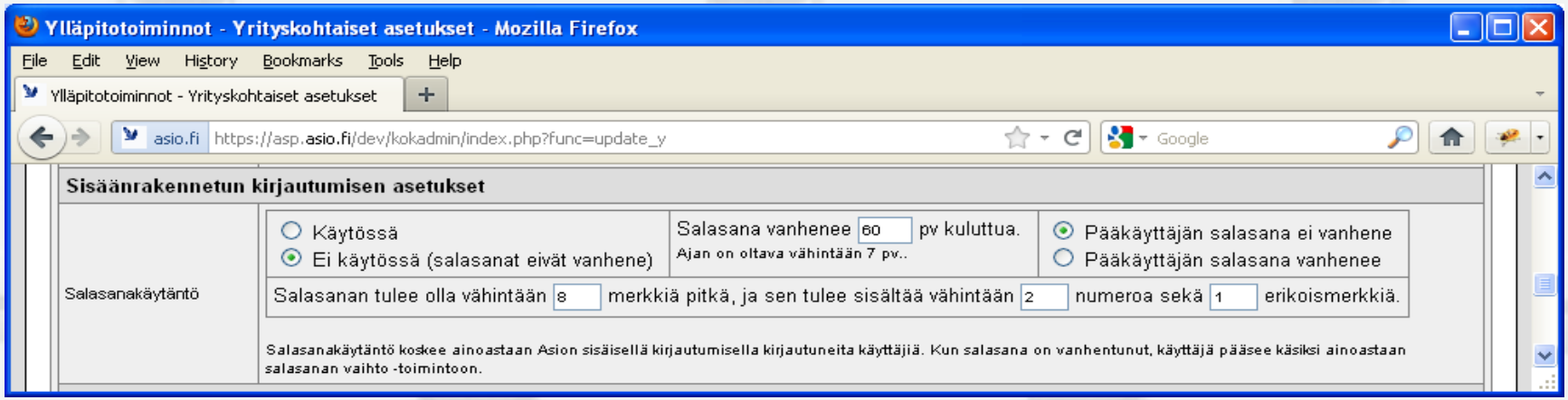
AsioEduERP v12
-
Tietoturvaparannukset

Yhteenveto

- AsioEduERP v12:n tietoturvaa parantavat uudet ominaisuudet:
  - Salasanakäytäntö
  - Kirjautumisviive
  - Käyttäjien aktiivisuuden seuranta
  - Uloskirjautuminen (myös muut kuin Shibboleth)
  - Henkilötunnusten suojaus
- Ajoympäristön turvallisuus
  - Asio-selailupalvelin
  - PHP:n versiopäivitykset
  - Yleisiä huomioita ajoympäristön tietoturvasta

Salasanakäytäntö

- AsioEduERP v12 mahdollistaa pääkäyttäjän määrittelemän salasanapolitiikan sisäisille tunnuksille
- Salasanalle voidaan määritellä maksimi-voimassaoloaika päivinä sekä hyvyysvaatimus (pituus sekä numeroiden/erikoismerkkien määrä)

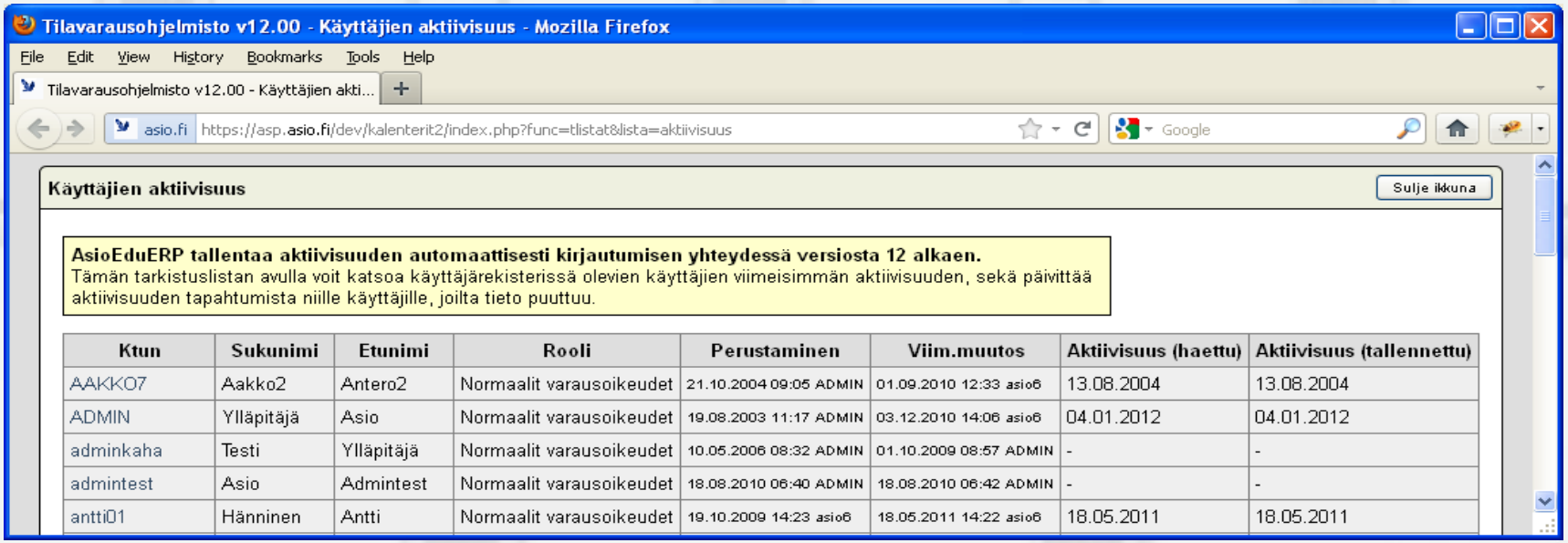


Kirjautumisviive

- Kirjautumisviive ehkäisee salasanojen arvailemista brute force -tekniikalla, ja se aktivoituu kolmen samalla tunnuksella tehdyn epäonnistuneen kirjautumisen jälkeen:
  - Kolmas epäonnistunut kirjautuminen aiheuttaa 2 sekunnin viiveen
  - Jokainen epäonnistunut kirjautuminen tuplaa viiveen
    - Max. viive on 24 sekuntia
  - Viive nollautuu onnistuneen kirjautumisen jälkeen
- Yritykset kirjataan loki_p -tauluun:
  - ohjelma = “asio_auth_lib”
  - id1 = “login_failure”
  - Id2 = kirjautumisyrityksen numero
  - ktun = kirjautumisessa käytetty käyttäjätunnus
  - pvm, klo = viimeisimmän kirjautumisyrityksen aika
  - ip = yrittäjän IP-osoite

Käyttäjien aktiivisuuden seuranta

- AsioEduERP v12 kirjaa käyttäjätunnukseen viimeisimmän sisäänkirjautumishetken aktiivisuus -tiedoksi
- Tarkoituksena on ehkäistä vanhojen tunnusten jääminen “lojumaan” rekisteriin
- Käyttäjien aktiivisuutta voi seurata käyttöoikeuksien hallinnan sekä erillisen tarkistuslistan kautta

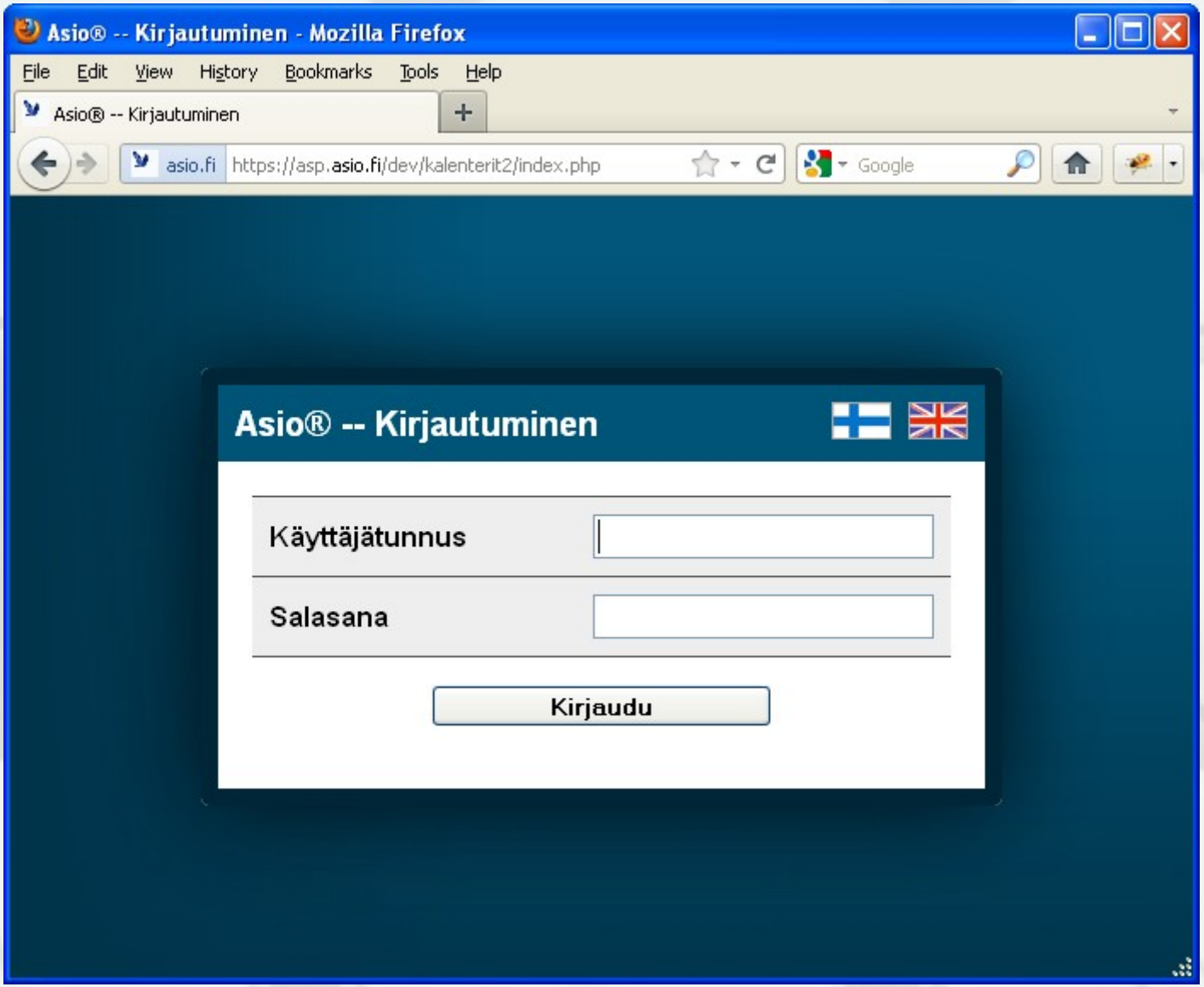


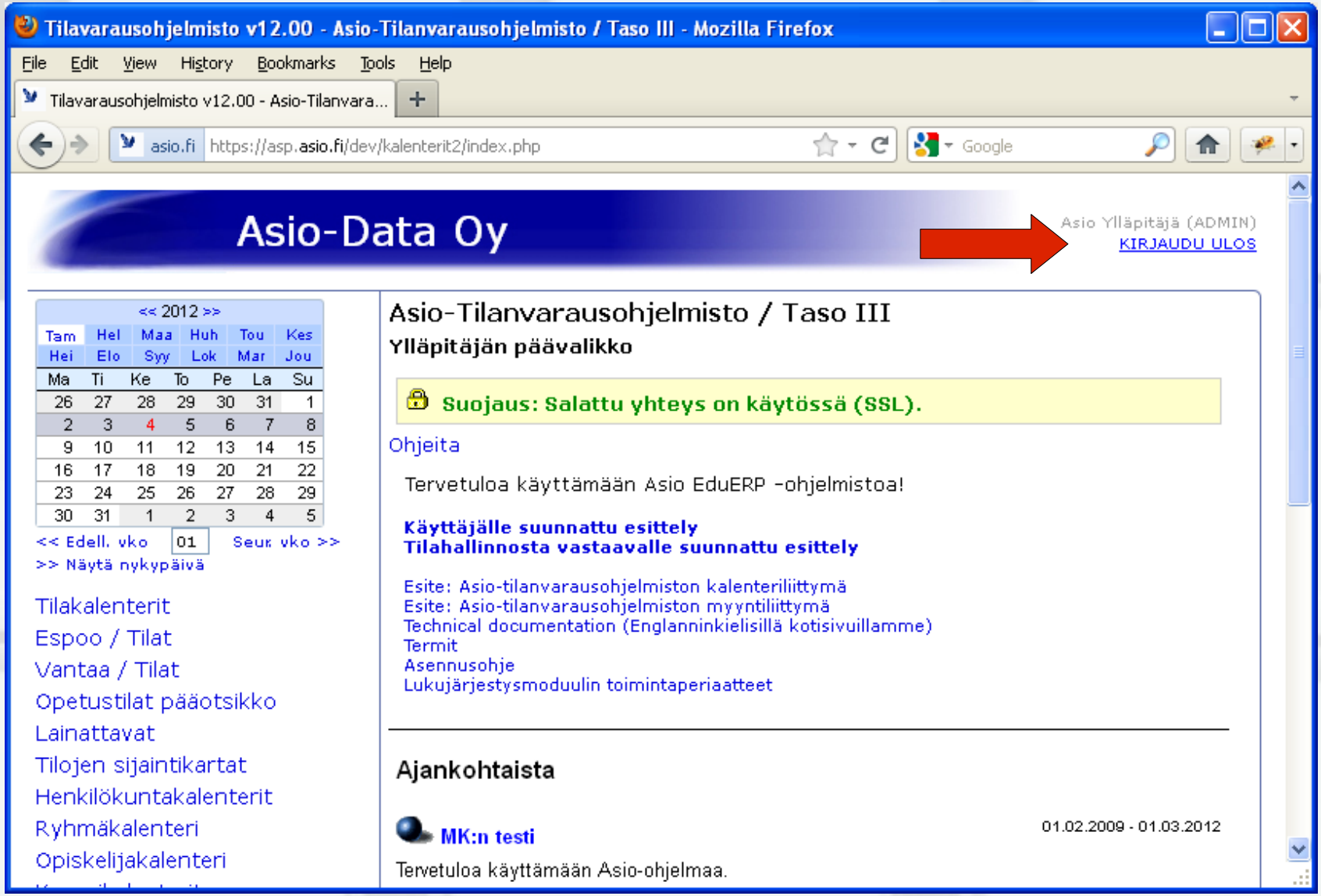
Ktun	Sukunimi	Etunimi	Rooli	Perustaminen	Viim.muutos	Aktiivisuus (haettu)	Aktiivisuus (tallennettu)
AAKKO7	Aakko2	Antero2	Normaalit varausoikeudet	21.10.2004 09:05 ADMIN	01.09.2010 12:33 asio6	13.08.2004	13.08.2004
ADMIN	Ylläpitäjä	Asio	Normaalit varausoikeudet	19.08.2003 11:17 ADMIN	03.12.2010 14:06 asio6	04.01.2012	04.01.2012
adminkaha	Testi	Ylläpitäjä	Normaalit varausoikeudet	10.05.2006 08:32 ADMIN	01.10.2009 08:57 ADMIN	-	-
admintest	Asio	Admintest	Normaalit varausoikeudet	18.08.2010 06:40 ADMIN	18.08.2010 06:42 ADMIN	-	-
antti01	Hänninen	Antti	Normaalit varausoikeudet	19.10.2009 14:23 asio6	18.05.2011 14:22 asio6	18.05.2011	18.05.2011

Uloskirjautuminen

- AsioEduERP v12 mahdollistaa aikaisemmin käytetyn HTTP Basic -kirjautumismenetelmän korvaamisen uudella istuntopohjaisella menetelmällä
- Uusi menetelmä mahdollistaa uloskirjautumisen myös muille kuin Shibbolethia käyttäville organisaatioille
- Uusi menettely ei ole oletuksena päällä, vaan se on otettava käyttöön erikseen Asio-järjestelmän pääkonfiguraatiosta server_settings.php

```
$auth_method = "asio_v12";
```


Asio® -- Kirjautuminen - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Asio® -- Kirjautuminen
asio.fi https://asp.asio.fi/dev/kalenterit2/index.php
Google
Asio® -- Kirjautuminen
Käyttäjätunnus
Salasana
Kirjaudu


Tilavarausohjelmisto v12.00 - Asio-Tilanvarausohjelmisto / Taso III - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Tilavarausohjelmisto v12.00 - Asio-Tilanvara...
asio.fi https://asp.asio.fi/dev/kalenterit2/index.php
Google
Asio-Data Oy
Asio Ylläpitäjä (ADMIN)
KIRJAUDU ULOS
<< 2012 >>
Tam Hel Maa Huh Tou Kes
Hei Elo Syy Lok Mar Jou
Ma Ti Ke To Pe La Su
26 27 28 29 30 31 1
2 3 4 5 6 7 8
9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29
30 31 1 2 3 4 5
<< Edell. vko 01 Seur. vko >>
>> Näytä nykypäivä
Tilakalenterit
Espoo / Tilat
Vantaa / Tilat
Opetustilat pääotsikko
Lainattavat
Tilojen sijaintikartat
Henkilökuntakalenterit
Ryhmäkalenteri
Opiskelijakalenteri
Asio-Tilanvarausohjelmisto / Taso III
Ylläpitäjän päävalikko
Suojaus: Salattu yhteys on käytössä (SSL).
Ohjeita
Tervetuloa käyttämään Asio EduERP -ohjelmistoa!
Käyttäjälle suunnattu esittely
Tilahallinnosta vastaavalle suunnattu esittely
Esite: Asio-tilanvarausohjelmiston kalenteriliittymä
Esite: Asio-tilanvarausohjelmiston myyntiliittymä
Technical documentation (Englanninkielisillä kotisivuillamme)
Termit
Asennusohje
Lukujärjestysmoduulin toimintaperiaatteet
Ajankohtaista
MK:n testi
01.02.2009 - 01.03.2012
Tervetuloa käyttämään Asio-ohjelmaa.

Henkilötunnusten suojaus

- Henkilörekisterin henkilötunnukset on suojattu AsioEduERP:n versiossa 12 aiempaa paremmin
- Henkilötunnus näkyy henkilörekisterin kautta vain, jos käyttäjä on pääkäyttäjä tai käyttöoikeuteen on ruksattu päälle lyhytkurssiohjelmiston henkilörekisterin ylläpito
- Aikaisemmin henkilötunnustieto on ollut ongelmallinen organisaatioissa, joissa on käytössä sekä tilavarausjärjestelmä että lyhytkurssiohjelmisto

Ajoympäristön turvallisuus - Selailupalvelin

- AsioEduERP v12 mahdollistaa erillisen selailupalvelimen käytön edustapalvelimena
  - Pilottina Liikuntakeskus Pajulahti (syksy 2011)
  - Mahdollistaa tuotanto-Asion pitämisen sisäverkossa
  - Alentaa selailukäytön aiheuttamaa kuormaa tuotanto-Asio-palvelimelta
- Selailupalvelin käyttää tuotanto-Asion tietokantaa vain luku -tyyppisen tietokantayhteyden yli
- Selailupalvelimelle ei voi kirjautua, joten AsioEduERP:n toiminnoista vain erikseen selailukäyttöön sallitut ovat käytettävissä selailupalvelimelta
- Konfigurointiohjeet saatavilla pyydettäessä Asio-Datalta

Ajoympäristön turvallisuus – PHP:n versiopäivitykset

- Tuki PHP:n versioille 5.2 ja sitä vanhemmille on päättynyt myös tietoturvapäivitysten osalta
- PHP 5.2 sisältää useita haavoittuvuuksia, joihin ei ole saatavilla korjauksia
- AsioEduERP tukee PHP:n versiota 5.3 alkaen versiosta 11.20
- Kannattaa päivittää sekä AsioEduERP että PHP!

Huomioita ajoympäristön tietoturvasta

- Käytä aina HTTPS -yhteyksiä
  - HTTP-yhteyttä tulisi käyttää vain sisäverkossa
- WWW-selaimen salasanan muistamistoiminnosta:
  - Useat selaimet tallentavat salasanat plaintext-muodossa
  - Käytä toimintoa vain turvallisilta päätelaitteilta käsin!
- Älä tee Asion ohjelmatiedostoista varmuuskopioita muulle tiedostopäätteelle kuin .php
- Apache-käyttäjän oikeudet Linux-ympäristössä:
  - Älä koskaan aja root-tunnuksella!
  - Tarkista että kirjoitusoikeus on vain polkuihin:

```
kokvar/tilakuvat/
asiakas/tilakuvat/
lyhytkurssi/kurssitiedostot/
```

Huomioita ajoympäristön tietoturvasta

- Viimeaikojen hyökkäykset ovat kohdentuneet erityisesti yleisiin avoimen lähdekoodin PHP-sovelluksiin, kuten julkaisujärjestelmiin, keskustelufoorumisovelluksiin ja verkkokauppasovelluksiin.
- PHP-ajoympäristö on yhteinen kaikille sovelluksille - huolehdi siis kaikkien Asio-palvelimella olevien PHP-sovellusten tietoturvapäivityksistä!
- phpMyAdmin on ollut hyökkääjien lempikohteita, joten suojaa se huolellisesti:
  - Suojaa aina IP-osoiterajauksella .htaccess -tiedostolla
  - Asenna kansioon jonka nimi ei ole helposti arvattavissa
- Älä jätä varmuuskopio-tietokantadumppeja lojumaan Asio-palvelimelle

Kiitokset!