Webvoter-järjestelmän ja Aalto-yliopiston ylioppilaskunnan edustajistovaaleihin 2011 suunnitellun sähköisen äänestyksen

Auditointiraportti

Kirjoittajat: Antti Pitkänen ja Jyry Suvilehto

Sisällysluettelo

Tiivistelmä

Äänestysjärjestelmää voidaan käyttää edustajistovaaleissa.

Oletukset

Mitään tietoturva-arviointia ei voida tehdä ilman tiettyjä pohjaoletuksia. On käytännössä mahdotonta tehdä järjestelmää, jossa joku järjestelmän kanssa tekemisissä oleva taho ei pystyisi tekemään jotain mitä ei saisi. Useimmiten auditointi kohdistuu lähinnä järjestelmän loppukäyttäjiin ja on mahdollista, joskaan ei helppoa, tehdä järjestelmiä, joiden loppukäyttäjät saavat tehdä vain mitä heidän on mahdollista tehdä.

Vaalivilpistä hyvin suuri osa on vaaliviranomaisten tekemiä. Koska auditointiraportin on tilannut vaalit järjestävä taho, ohjeistettiin auditoijia luottamaan vaaliviranomaisiin ja ylioppilaskunnan työntekijöihin. Ilman tätä implisiittistä järjestäjiin luottamista vaalien tuloksiin ei olisi missään

tapauksessa mahdollista luottaa. Mainitsemme kuitenkin muutaman kohdan, joissa järjestäjien erehtyminen saattaa vaarantaa äänestämisen.

Verifioitavat kohdat

Vaalijärjestelmän käyttöliittymän tietoturva

Kaikki järjestelmän lomaketiedot lähetään oikeaoppisesti HTTP-protokollan POST-pyyntöinä eli mitään salasanoja ei jää näkyviin tai talteen esimerkiksi selaimen osoiteriville tai oletuslokeihin.

Käyttäjän syöte parsitaan/tarkastetaan aina ennen sen käyttämistä ohjelmassa. XSS- tai SQL injection -hyökkäykset eivät ole siis mahdollisia tavalliselta käyttäjältä. Lisäksi äänestäjän suoraan järjestelmälle antama syöte on hyvin rajoitettua.

Käyttöliittymästä pitää ottaa pois käytöstä Javan virhetulosteet, jotka voivat näkyä käyttäjille (tahallisissa) virhetilanteissa ja paljastaa tietoja koko sovelluksesta. JBoss-palvelimen pystyy helposti säätämään niin, ettei näitä virheilmoituksia näytetä tuotannossa olevassa järjestelmässä.

Pääsy vaalijärjestelmään liittyville hallintasivuille on syytä estää kokonaan muilta koneilta kuin itse palvelimelta ja mahdollisesti joltain muulta järjestelmän ylläpitäjän käytössä olevalta koneelta. Hallintasivut sijaitsevat rinnakkain varsinaisen loppukäyttäjän äänestyssivujen kanssa, esimerkiksi `/webvoter/ConfirmVote.jsp` (äänen vahvistaminen) ja `/webvoter/EnterBulkVotes.jsp` (äänien manuaalinen lisääminen järjestelmään).

Vaikka järjestelmä välittääkin itselleen parametrit POST-pyyntöinä, eikä GET-pyyntöinä, hyväksyy se silti GET-pyyntöjä. Lisäksi järjestelmä ei erityisesti tarkista, että sen saama äänestyskäsky on tullut sen itsensä luomalta äänestyssivulta. Tämä avaa mahdollisuuden niinkutsutuille Cross Site Request Forgery, eli CSRF-hyökkäyksille. Hyökkäyksen teko ei ole helppoa, sillä käyttäjän pitää autentikoitua koulun tarjoaman Shibboleth-autentikaatiojärjestelmän kautta päästäkseen äänestämään. Kuitenkin on mahdollista huijata käyttäjä luulemaan, että tämä on menossa jonnekin muualle kuin äänestyssivulle. CSRF-hyökkäystä vastaan on kuitenkin mahdollista suojautua Apachen asetuksia muuttamalla. Kaikkien muiden sivujen kuin äänestyksen etusivun asetuksiin pitää laittaa, että kutsut näille sivuille sallitaan vain, jos HTTP-kutsun Referer-kentässä on vaalipalvelimen osoite.

Mikäli äänestystä varten tarjotaan pystypäätteitä, on syytä pitää huolta pystypäätteiden selaimien tietoturvasta. Moderneihin selaimiin on mahdollista asentaa selainlisäosia, jotka voivat muokata selaimella ladattuja sivuja ja/tai sillä lähetettyjä tietoja. Tällainen lisäosa on nopea tehdä ja se voi esimerkiksi saada ehdokkaan A näyttämään ehdokkaalta B äänestyslistoissa. Lisäosan asentaminen on yleensä nopeaa ja lisäosa on oletusarvoisesti huomaamaton.

Vaalijärjestelmän palvelimen tietoturva

Vaalijärjestelmässä applikaatiopalvelimena käytettävä JBoss pitää päivittää uusimpaan versioon, joka on yleisesti saatavissa. JBoss julkaisi 16.8.2011 Final-version 6.x -kehityspolusta (http://www.jboss.org/jbossas/downloads, 6.1.0.final), ja kyseisen julkaisun pitäisi sisältää kaikki tietoturvapäivitykset 6.x versioissa ja olla riittävän turvallinen sekä toimiva sovelluksen kanssa. Ehdotamme siihen siirtymistä, sillä juuri julkaistu 7.0 -versio sisältää todennäköisemmin haavoittuvuuksia ja vaatisi joka tapauksessa kattavan testauksen äänestysjärjestelmän kanssa. 6.x -versio on jo havaittu äänestysjärjestelmän kanssa yhteensopivaksi.

Vaalijärjestelmä tullaan ajamaan virtuaalikoneella ylioppilaskunnan palvelimella. Virtuaalipalvelinta ajetaan isäntäkoneessa, joka sijaitsee AYY:n pääkonesalissa. Virtuaalipalvelimen isäntäkoneella tulee noudattaa alan olemassaolevia käytänteitä, eli isäntäkoneella ei tule ajaa mitään tarpeetonta. Lisäksi isäntäpalvelimeen kirjautuminen on mahdollista vain tietyiltä hallintakoneilta.
Suora pääkäyttäjänä kirjautuminen tulee estää. Vaalien ajaksi tulee tallentaa isäntäpalvelimen ulkopuolelle lokitieto etäkirjautumisista ja käyttöoikeuksien nostamisisista isäntäkoneella. Unixeissa käytetty sudo-ohjelma voidaan konfiguroida tallentamaan lokitietoja etäkoneelle. Tämän etäkoneen pitää sijaita jossain muualla kuin samalla virtuaalikoneisännällä. Lisäksi sudo-ohjelman voi konfiguroida lähettämään sähköpostia aina kun jonkun käyttöoikeuksia nostetaan. Parasta olisi laittaa molemmat päälle sekä isäntä-, että virtuaalikoneeseen vaalien ajaksi ja välttää ylläpitotoimia isäntäkoneella vaalien aikana.

Virtuaalipalvelimella ei ajeta vaaliohjelmiston lisäksi muita palveluja ja vaaliohjelmiston tarvitsemista palveluista vain www-palvelun annetaan vastaanottaa yhteyksiä koneen ulkopuolelta. Tietokantaohjelmiston ei tarvitse hyväksyä yhteyksiä koneen ulkopuolelta, koska www-palvelu ja tietokanta sijaitsevat samalla koneella.

Mikäli vaalijärjestelmän tai sen isäntäpalvelimeen asetuksiin on tarpeen tehdä muutoksia kesken vaalien, on vähintään yhden, mielellään tietotekniikkataitoisen vaalilautakunnan jäsenen oltava läsnä valvomassa toimenpiteitä.

Suositeltavampaa olisi ajaa vaaliohjelmistoa omalla koneellaan, joka on lukittu erilleen muista palvelinsalin koneista. Virtuaalipalvelimessa on se huono puoli, että virtuaalipalvelinta ajavan koneen ylläpitäjä pääsee käsiksi virtuaalipalvelimen muistiin ja virtuaaliseen kovalevyyn. Näistä molempia on mahdollista (joskaan ei helppoa) lukea tai muokata. Tällainen muokkaus voi vaarantaa joko vaalien eheyden siten, että joku muokkaa tietokannassa olevia tietoja tai luotettavuuden siten, että joku seuraa kuka äänesti ja ketä.

Vaalijärjestelmän laskentaosan vaalipäivälle suunniteltu suojaus

Paraskaan suojaus ei auta jos järjestelmään päästään fyysisesti käsiksi. Vaalijärjestelmän laskentaosan fyysinen suojaus on enimmäkseen kulunvalvontaa.

Vaalijärjestelmän laskentaosa ollaan sijoittamassa vaalipäivänä ylioppilaskunnan pääkonesaliin. Kustannussyistä järjestelmä ei ole tilassa yksin vaan siellä on myös muita ylioppilaskunnan IT-infrastruktuuria. Tästä syystä tilaan on pääsy myös joillakin ylioppilaskunnan työntekijöillä, jotka eivät ole vaalien järjestäjiä.

Kyseisiltä käyttäjiltä voitaisiin poistaa pääsyoikeus ao. tilaan, mutta tätä ei ole katsottu mielekkääksi. Samassa tilassa oleva ylioppilaskunnan IT-infrastruktuuri sisältää mm. reitittimiä, joita ilman vaalijärjestelmä on hyödytön ja vian sattuessa vaalit jouduttaisiin uusimaan, koska äänestysjärjestelmään ei saada yhteyttä.

Kompromissiratkaisuna palvelimelle voidaan järjestää nauhoittava videovalvonta. Mikäli videovalvonnassa ei näy muita kuin mahdollisia valvottuja käyntejä koneella, voidaan olettaa että vaalijärjestelmään ei ole fyysisesti kajottu. Tämä videovalvonta täydentää elektronista kulunvalvontaa.

Mikäli tilassa ei ole käyty eikä virtuaalikoneeseen ole kirjauduttu eikä virtuaalikoneen isäntäkoneessa ole eskaloitu oikeuksia pääkäyttäjätasolle, voidaan luottaa riittävällä varmuudella siihen, että järjestelmää ei ole muutettu.

Äänestäjän henkilöllisyyden varmistaminen

Äänestäjän henkilöllisyys varmennetaan käyttämällä yliopiston tarjoamaa Shibboleth-tunnistautumista. Shibboleth-tunnistautumisesta saadaan opiskelijan opiskelijanumero. Opiskelijanumeroa etsitään kantaan syötetyistä henkilötiedoista. Opiskelijanumeron puuttuminen kannasta estää äänestystapahtumaa tapahtumasta.

Äänestäjän henkilöllisyyden varmistaminen ja äänestäjien äänestysoikeuden tarkastaminen toimivat halutusti olettaen, että äänioikeutettujen eli ylioppilaskunnan jäsenien opiskelijanumerot on ajettu kantaan oikein. Koska ylioppilaskunta on laillisesti velvoitettu pitämään kirjaa opiskelijoistaan, on tieto läsnäolevista opiskelijoista olettaenkin saatavissa.

AYY:n säännöistä §2

> Ylioppilaskunnan jäseniä ovat kaikki yliopiston opiskelijat, jotka on otettu opiskelijoiksi alempaan ja ylempään korkeakoulututkintoon johtaviin opintoihin lukuun ottamatta tilauskoulutukseen osallistuvia opiskelijoita. Ylioppilaskunnan hallitus voi hyväksyä jäseniksi myös muita yliopiston opiskelijoita.

Ylioppilaskunnan jäsenten on siis sääntöjen mukaisesti oltava yliopiston opiskelijoita ja yliopiston opiskelijoilla on oltava opiskelijanumero.

Yliopiston opiskelijoilla on oletusarvoisesti käyttöoikeus yliopiston järjestelmiin ja siten mahdollisuus käyttää äänioikeuttaan. Aalto-yliopiston tietojärjestelmien käyttöpolitiikan §3 rajaa opiskelijoiden käyttäjäkohtaiset käyttäjätunnukset yksittäisen henkilön käyttöön ja kieltää käyttämästä toisten henkilöiden tunnuksia. Vaaleja järjestettäessä tämä täytyy tiedostaa, koska vaaleissa on tarkoitus estää tietyllä tietoturvatasolla toisen henkilön nimissä äänestäminen.

Tilanne on analoginen paperivaalien kanssa tapauksessa, jossa yksi identtisistä kaksosista käy äänestämässä kaksosparista kummankin puolesta käyttäen toisen kaksosen henkilöllisyystodistusta. Tämä on väärinkäyttöä, jota ei voida havaita. Väärinkäytön estämiseksi se on säädetty rangaistavaksi rikoslaissa (14. luku, §3 Vilpillinen äänestäminen). Analogisesti

AYY:n vaalien tapauksessa toisen henkilön käyttäjätunnuksen käyttäminen on rangaistava teko.

Henkilöllisyyden varmentamisessa ongelman muodostavat henkilöt, joiden Aalto-yliopiston käyttäjätunnus on syystä tai toisesta suljettu, vaikka nämä ovatkin ylioppilaskunnan jäseniä eli siten äänioikeutettuja. Vanhentunut salasana ei ole ongelma. Vaikka äänestys on sähköinen, voi tunnuksen käydä avaamassa esimerkiksi vaalipäivänä yliopiston kampuksilla. Tämä ei aiheuta kohtuutonta vaivaa ja paperivaaleissa kaikkien pitäisi käydä kyseisillä kampuksilla.

Väärinkäytön tai sen epäilyn takia suljettu tunnus sen sijaan on ongelma. Äänestäjän riita kolmatta osapuolta eli tunnistuspalvelua tarjoavaa yliopistoa vastaan ei mitenkään poista tai heikennä tämän äänioikeutta. Jo tämän takia on tarpeen järjestää mahdollisuus uurnavaaliin sähköisen äänestämisen lisäksi.

Äänestysjärjestelmä ei tarjoa reaaliajassa tietoa jo äänestäneistä henkilöistä niin turvallisesti ja varmasti, että uurnavaali ja sähköinen vaali voisivat olla auki yhtä aikaa. Lisäksi järjestelmään ei ole helppo merkitä yhden henkilön äänestäneen merkitsemättä mitä hän äänesti. Riskinä on, että henkilö voisi äänestää kaksi kertaa, äänestämällä nopeasti peräkkäin uurnaan ja sähköisesti.

Äänestäjien ja äänien yhdistämättömyys keskenään

Järjestelmä on suunniteltu siten, että äänestäjän ja tämän antaman äänen yhteyttä ei tallenneta järjestelmään. Testikäytössä järjestelmä kuitenkin tallettaa logiin tiedon siitä, kuka äänestää ja ketä. Tämä luo tietyn riskin siitä, että tuotantokäyttöjärjestelmä unohdetaan konfiguroida siten, että tätä logia ei luoda. Suosittelemme kommentoimaan testikäyttöloggauksen pois tiedostosta VoteBean.java riveiltä 138-139.

Järjestelmän ylläpitäjä voi PostgreSQL:ssä tehdä nk. audittitauluja, joihin tallennetaan kaikki muutokset johonkin toiseen tauluun muutoshetkineen. Audittitaulu luodaan asettamalla niin kutsuttu tietokantatriggeri, joka ajetaan aina kun tiettyyn tauluun tehdään muutos. Triggeri ajaa koodinpätkän, joka voi esimerkiksi tallentaa tarkan kellonajan ajohetkellä.

Mikäli tällainen taulu tehdään ehdokkaat-taulun ääniin, annetut äänet voidaan yhdistää äänestäjiin. Tämä on mahdollista, koska järjestelmä on suunniteltu siten, äänioikeuden käyttötietoa seuraava ehdokkaan äänien lisäys yhdellä on varmasti saman käyttäjän.

Mikäli luotamme järjestelmän ylläpitäjään, ei tämä ole ongelma. Mikäli järjestelmän ylläpitäjään ei haluta luottaa tässä, on syytä toisen henkilön valvoessa poistaa kaikki tietokantataulun candidate.votes käyttäjän määrittämät triggerit.

Dokumentaation (http://www.postgresql.org/docs/8.4/static/sql-altertable.html) mukaan ajettavan kutsun pitäisi olla muotoa: “ALTER TABLE candidate.votes DISABLE TRIGGER USER;”. Emme kuitenkaan ole testanneet kutsua. On syytä huomata, että kaikkia triggereitä ei pidä poistaa käytöstä, koska järjestelmän toiminta perustuu osittain automaattisiin triggereihin. Siksi on syytä poistaa vain käyttäjän määrittelemät triggerit.

Äänioikeutta voi käyttää ainoastaan kerran

Äänestäminen tapahtuu siten, että tietokantaan tallennetaan ääni ja tieto äänen käytöstä. Uudelleen äänestäminen samalla opiskelijanumerolla eli samoilla atk-tunnuksilla ei ole mahdollista. Äänestämisestä useammilla atk-tunnuksilla katso kohta “Äänestäjän henkilöllisyyden varmentaminen”.

Järjestelmä voi teoriassa hajota (komponenttien hajoaminen) tai se voidaan sammuttaa kesken äänestyksen, jolloin yhden käyttäjän ääni saattaa jäädä rekisteröitymättä vaikka äänioikeus on merkitty käytetyksi. Oletettavasti näissä tilanteissa vaalit uusittaisiin. Tältä riskiltä täydellinen suojautuminen on kohtuuttoman kallista.

Annettujen äänten ja laskennan tarkistus äänestyssalaisuutta vaarantamatta

Jokaisesta äänestäneestä henkilöstä saadaan tietää ajankohta jolloin tämä on äänestänyt, eli äänen antaneet henkilöt on mahdollista selvittää jälkikäteen.
Äänien täydellinen tarkastuslaskenta ei sinänsä ole mahdollista. Äänestäessä ääni lisätään ehdokkaan äänisummaan eikä tietoa siitä, kenelle ääni kohdistui tallenneta minnekään muualle. Tarkistuslaskenta on mahdollista suorittaa siten, että lasketaan kaikkien äänestäneiden henkilöiden määrä ja verrataan sitä kaikkien ehdokkaiden saamien äänien summaan. Mikäli summat täsmäävät, äänestystulos on oikea.
Mikäli summat eivät täsmää, ei ole mahdollista laskea ääniä uudelleen ja vaalit täytyy tällöin uusia. Tilanne on sama myös paperiäänestyksessä. Tämä on kuitenkin erittäin epätodennäköistä, sillä tieto äänikoikeuden käytöstä ja annetusta äänestä tallennetaan siten, että käytännössä vain laitteistohäiriö tai katastrofaalinen ohjelmistohäiriö voisivat johtaa siihen, että tieto äänioikeuden käytöstä tallennetaan ilman että ääntä tallennetaan. Äänestäjän ääni ei voi mennä tietokantaan siten, että tieto äänioikeuden käytöstä ei tallennu.

Perustuu avoimeen lähdekoodiin

Käsite avoin lähdekoodi voidaan tulkita kahdella tavalla. Avoimen lähdekoodin voidaan katsoa tarkoittavan sitä, että kaikki järjestelmän lähdekoodi on saatavilla. Toisaalta tämän lisäksi voidaan myös vaatia, että lähdekoodi on lisensoitu jollain avoimella lisenssillä (Creative Commons, GNU General Public Licence, MIT Licence jne).

Ensimmäinen vaatimus on vaalijärjestelmälle tärkeä, koska äänestäjien on kohtuutonta olettaa luottavan vaalijärjestelmän toimittajaan. Luotettavan äänestysjärjestelmän tulee perustua avoimeen lähdekoodiin siten, että yleisöllä on mahdollisuus tutustua järjestelmän toimintaan. Tämä toteutuu täysin ja auditoijat ovat päässeet tarkastelemaan järjestelmän lähdekoodia. Tarvittaessa myös järjestelmän käyttämien kirjastojen lähdekoodia olisi ollut mahdollista tarkastella, mutta sitä ei katsottu tarpeelliseksi.

Lähes koko koodi on lisensoitu GNU Lesser General Public -lisenssillä, joka täyttää avoimuuden ehdot. Poikkeuksina ovat tiedostot LoginCheck.java (Copyright 2005 Kalle Kivimaa), GetSTVVote.jsp-tiedostossa sijaitseva JavaScript-skripti (Copyright 2004 Jarno Elonen).

Lisäksi STV-vaalitavassa käytettäväss BigFraction.java-tiedostossa mainitaan sen olevan Michael Gillelandin tekemä, mutta ei mainita levittämisen ehtoja. Etsimme alkuperäistä tiedostoa ja löysimme sen osoitteesta **http://www.merriampark.com/fractions.htm**, mutta senkään yhteydessä ei ole mainintaa levityksen lisenssiehdoista.

Järjestelmäkuvauksessa on myös määritelty mitä muutoksia näihin avoimen lähdekoodin ohjelmistoihin on tehty. Nämä muutokset ovat hyvin triviaaleja ja koskevat vain käyttöliittymän tekstejä sekä käyttäjän tunnistamista Aallon tarjoaman Shibboleth-autentikaation avulla.

Laskee äänestystulokset vaalijärjestyksen 37-40 §§ mukaisesti

Vaalijärjestys kuvailee niin kutsutun d'Hondtin vaalitavan. Vaalijärjestyksen mukaan edustajat voivat liittoutua vaaliliitoiksi ja vaaliliitot keskenään edelleen vaalirenkaiksi. Vertailuluku määräytyy ehdokkaan sijoittumisen mukaan liiton listalla ja liiton saamien kokonaisäänien mukaan kaavalla $\frac{aanet}{p}$, missä p on ehdokkaan paikka listalla (alkaen paikasta 1).
Mikäli vaaliliitto kuuluu renkaaseen, asetetaan renkaaseen kuuluvien liittojen ehdokkaat paremmuusjärjestykseen edellämainittujen vertailulukujen perusteella ja lasketaan näille lopulliset vertailuluvut renkaan yhteisäänistä samalla kaavalla.

Tasatuloksen sattuessa sijoituksen ratkaisee arpa.

Äänestystuloksen laskentaa testattiin käyttämällä erilaisia skenaarioita, joista on laskettu oikea tulos taulukkolaskentaohjelmaa käyttäen.

Skenaariot

1. 3 vaaliliittoa, ei vaalirenkaita
2. Sama kuin aiempi, paitsi että 2 puoluetta on vaalirenkaassa.
3. Toinen äänestys siten, että 2 ehdokkaan äänet menevät tasan

Tulokset

1. Liitteen 2.1 mukaisien vaalien tulokset olivat oikeat ohjelmalla laskettuna.
2. Liitteen 2.2 mukaisien vaalien tulokset olivat oikeat ohjelmalla laskettuna.
3. Liitteen 2.3 mukaisien vaalien tulokset olivat oikeat ohjelmalla laskettuna.

Huom! Saman äänimäärän saaneiden (skenaario 3) keskinäinen järjestys vaihtelee laskentakertojen välillä. Toisin sanoen keskinäisen järjestyksen osalta tulokset voivat vaihdella kun hallintakäyttöliittymästä painetaan tuloksien laskenta -nappia.

Kun tuloksia lasketaan hallintakäyttöliittymästä, pitää laskettu tulos ottaa heti talteen varmuuden vuoksi, jotta mahdollisesti saman äänimäärän saaneiden arvottu keskinäinen järjestys tiedetään eikä sitä voida jälkeenpäin enää muuttaa käynnistämällä tulosten laskennan uudelleen.

Suositukset

Äänestysjärjestelmän toiminnan valvonta vaalin aikana

Äänestysjärjestelmän toimintaa vaalin aikana on vaikea valvoa. Jokainen valvontaominaisuus tuo mukanaan lisämahdollisuuksia järjestelmän väärälle toiminnalle tai uusille haavoittuvuuksille.

Ehdotamme että äänestysjärjestelmään ei tarpeettomasti kajota äänestyaikana. Järjestelmän ulkopuolelle valvonta suositellaan järjestettäväksi siten, että palvelimen päälläolo varmistetaan hakemalla äänestyksen liittyviä sivuja kerran minuutissa tai useammin. Lisäksi äänestäjille tulee tiedottaa, että mahdollisista ongelmista tulee ilmoittaa välittömästi järjestelmän ylläpitäjälle.

Äänestysjärjestelmän jatkokehitys

Järjestelmä olisi hyvä dokumentoida hieman paremmin. Käyttötapauskuvaukset ja paremmat ohjeet järjestelmän konfiguroinnista erilaisiin käyttötapoihin helpottaisivat sen käyttöönottoa muualla.

Järjestelmän tarjoamaa STV-äänten laskentatapaa ei ole auditoitu. Se on monimutkaisempi ja siten alttiimpi virheille. Mikäli STV-vaalitapaa halutaan käyttää tulevaisuudessa, on suositeltavaa tarkastaa sen toimivuus etukäteen.

Hallintakäyttöliittymä on kankea käyttää ja vaatii perehtymistä. Käyttöliittymän uudistaminen voisi olla hyvä jatkokehityskohde.

Mikäli XSS -haavoittuvuudet halutaan estää kokonaan, helppo ratkaisu asiaan on käyttää käyttöliittymän tulostuksissa J2EE:n standardin JSTL -tägikirjaston tulostukseen tarkoitettua `<c:out />` -tägiä, joka automaattisesti muuttaa tulostettavan muuttujan mahdollisesti sisältämät HTML-merkit turvallisiksi.

```
> <c:out value=”${muuttuja}” />
```

Tällä hetkellä tulostus hoidetaan yksinkertaisesti näin:

```
> <%= muuttuja %>
```

Järjestelmän mukana tulevaa kertakäyttöisten salasanojen generaattoria ei tule missään tapauksessa käyttää sellaisenan. Generaattori generoi salasanoja pseudosatunnaislukujen, ei aitojen satunnaislukujen avulla. Tämä olisi vielä hyväksyttävää, jos pseudosatunnaislukukeneraattorin siemenluku (seed) olisi satunnaisesti valittu. Tällä hetkellä generaattori käyttää oletusta eli järjestelmän kellonaikaa millisekunneissa, mikä

on ennustattavissa pienellä vaivalla. Tehtävä muutos ei ole suuri. Helpointa lienee välittää siemenluku komentoriviparametrina ja huolehtia sen satunnaisuudesta muilla tavoin. Luvun olisi suotavaa olla vähintään 9-numeroinen, mieluiten 10-numeroinen.

Liitteet

Liite 1: Vaatimusmäärittely

AYY:N SÄHKÖISEN ÄÄNESTYSJÄRJESTELMÄN TIETOTURVA-AUDITOINTI
Vaatimusmäärittely

Auditoijan tulee verifioida, että
1. vaalijärjestelmän käyttöliittymän tietoturvan taso on riittävä;
2. vaalijärjestelmän laskentaosan vaalipäivälle suunnitellun suojauksen taso on riittävä;
3. äänestäjän henkilöllisyys varmistetaan uskottavasti ennen äänestämistä;
4. äänestäjän henkilöllisyyttä ei pystytä jälkikäteen yhdistämään mihinkään tiettyyn annettuun ääneen;
5. äänestäjä voi käyttää äänioikeuttaan ainoastaan kerran;
6. vaalijärjestelmään tulee voida suorittaa annettujen äänten ja laskennan tarkistus (audit trail) kuitenkaan äänestyssalaisuutta vaarantamatta;
7. vaalijärjestelmä perustuu avoimeen lähdekoodiin;
8. järjestelmä laskee äänestystulokset annetuista äänistä vaalijärjestyksen 37-40 §§ mukaisesti;

Lisäksi auditoijan toivotaan esittävän suositukset
1. sopivaksi menetelmäksi valvoa sähköisen äänestysjärjestelmän toimintaa vaalin aikana;
2. äänestysjärjestelmän jatkokehittämiseksi.

Näiden havaintojen pohjalta auditoijan toivotaan esittävän 1.9. raportti keskusvaalilautakunnalle. Raportin tulee sisältää suositus siitä, voidaanko sähköistä äänestysjärjestelmää käyttää vaalien ääntenlaskentaan.

Liite 2.1 Vaaliskenaario 1.

Vaaliskenaario 1. Kolme vaaliliittoa, ei vaalirenkaita.

Puolue	Ehdokas	Äänet	Vertailuluku	Sijoitus

A	Aarne	100	200	9
A	Bertta	200	300	6
A	Celsius	300	600	3
B	Daavid	101	201	8
B	Eemeli	201	301.5	5
B	Faarao	301	603	2
C	Gideon	102	202	7
C	Heikki	202	303	4
C	Iivari	302	606	1

Liite 2.2 Vaaliskenaario 2

Vaaliskenaario 2. Kolme vaaliliittoa, A ja B vaalirenkaassa keskenään.

Puolue	Ehdokas	Äänet	Vertailuluku	Renkaiden vertailuluku	Sijoitus
A	Aarne	100	200	200.5	9
A	Bertta	200	300	300.75	6
A	Celsius	300	600	601.5	3

B	Daavid	101	201	240.6	7
B	Eemeli	201	301.5	401	4
B	Faarao	301	603	1203	1
C	Gideon	102	202	202	8
C	Heikki	202	303	303	5
C	Iivari	302	606	606	2

Liite 2.3 Vaaliskenaario 3

Vaaliskenaario 3. Ehdokkaat Faarao ja Iivari, Eemeli ja Heikki sekä Daavid ja Gideon saavat saman pareittain saman vertailuluvun. Tässä tapauksessa vaalijärjestelmä arpoo sijoitukset siten, että sattumanvaraisesti jompi kumpi pareista saa sijoituksen k ja toinen sijoituksen k+1.

Puolue	Ehdokas	Äänet	Vertailuluku	Sijoitus
A	Aarne	100	200	9
A	Bertta	200	300	6
A	Celsius	300	600	3
B	Daavid	101	201	7
B	Eemeli	201	301.5	4
B	Faarao	301	603	1
C	Gideon	101	201	7
C	Heikki	201	301.5	4

C	Iivari	301	603	1

Liite 3 Järjestelmän konfiguraatiokohdat

Virtuaalipalvelimen isäntäpalvelimella

- sudo loggaus etänä ja mailitse
- etäloggaaminen suoraan roottina estetty
- ei turhia palveluita
- palvelimen fyysinen pääsynhallinta ja -valvonta

Virtuaalipalvelimella

- kirjautumisten loggaus etänä ja mailitse
- etäkirjautumisen estäminen
- kaikki turhat palvelut pois päältä
- PostgreSQL hyväksyy yhteyksiä vain localhostista
- Apache esitetyn konfiguraation mukaisesti.
  - Lisäksi pitää estää pääsy hallinnointisivuille localhostin ulkopuolelta
  - ConfirmVote.jsp:n ja EndVote.jsp sallittu vain jos referer on vaalit.ayy.fi
- Uusin JBoss-versio
- Uusimmat tietoturvapäivitykset

PostgreSQL

- Haluttaessa varmistetaan, että candidate.votes -taulussa ei ole käyttäjän määrittämiä triggereitä

Webvoter

- Vaaleissa IsProduction on päällä
- Kaikkien oikeutettujen opiskelijanumerot ovat järjestelmässä
- JBossin virheilmoitukset, erityisesti stack tracet ovat piilossa

Mahdolliset pystypäätteet

- Poistetaan mahdollisuus asentaa lisäosia selaimeen tai käytetään selainta, joka ei lisäosia tue