Tampereen ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Jyrki Haapamäki

Opinnäytetyö

Joomla!:n tietoturva

Työn ohjaaja Lehtori Petri Heliniemi

Tampere 4/2010

Tekijä	Jyrki Haapamäki
Työn nimi	Joomla!:n tietoturva
Sivumäärä	43
Valmistumisaika	huhtikuu 2010
Työn ohjaaja	Petri Heliniemi

Tiivistelmä

Tässä opinnäytetyössä käsitellään Joomla!-sivuston tietoturvaa. Työn tavoitteena on arvioida Joomla!-sivustojen tietoturvaa yleisesti sekä löytää sivustojen mahdollisia tietoturvaan liittyviä heikkouksia. Työn tarkoituksena on myös antaa joitain ohjeita, joiden avulla sivuston ylläpitäjä voi parantaa oman sivustonsa tietoturvan tasoa.

Työssä käydään läpi internetsivustoihin liittyvää tietoturvan teoriaa ja esitellään joitain tietoturvaorganisaatioita, joiden kautta voi löytää tietoa tietoturvaan liittyvistä aiheista. Lisäksi käsitellään yleisimpiä internetsivustojen tietoturvaan liittyviä uhkia, niiden vaikutuksia sivustojen toimintaan sekä esitellään keinoja niiltä suojautumiseksi.

Joomla!:n osalta käydään läpi järjestelmän yleiset piirteet ja vaatimukset. Joomlan!:n tietoturvaa arvioidaan tilastotietojen sekä tietoturvan yleisten periaatteiden pohjalta. Lopuksi esitellään joitain keinoja, joiden avulla sivuston ylläpitäjä voi parantaa sivustonsa tietoturvaa.

Tuloksena kävi ilmi, että Joomla!-sivuston yleinen tietoturva on kohtuullisella tasolla. Tuloksena kävi myös ilmi, että sivuston ylläpitäjä voi toimillaan suuresti vaikuttaa sivustonsa tietoturvaan sekä hyvässä että pahassa. Sivuston tietoturvan kannalta olisi tärkeää noudattaa käyttäjäoikeuksien ja salasanojen hallinnassa annettuja ohjeita sekä huolehtia kaikkien ohjelmistojen päivitysten ajantasaisuudesta. Toisaalta varsinkin epämääräisten lisäosien asentaminen voi heikentää sivuston tietoturvaa.

Avainsanat tietoturva, tietoturvallisuus, Joomla!-sivuston tietoturva, internetsivuston tietoturva

Author	Jyrki Haapamäki
Thesis	Joomla! site security
Pages	43
Time of graduation	April 2010
Thesis supervisor	Petri Heliniemi

Abstract

This thesis handles the security of an Internet site that is made with the Joomla! content management system. The goal of the thesis is to evaluate the security of a Joomla! site in general and to find possible vulnerabilities those sites may have. Another goal is to make a short guide about the Joomla! site security for the people who administrate a Joomla! site on their own.

The thesis includes theory about information security and introduces some Internet organizations which handle information security issues. The thesis also introduce some of the most common threats of Internet web sites, explains how those threats affect the functionality of web sites, and introduces some ways to protect the sites from those threats.

The thesis discusses some of the basic principles and requirements of Joomla! system. The security of Joomla! site is estimated through some statistical information and through some common information security principles. Finally, some ways to improve the security of a Joomla! site are introduced.

The final conclusion was that a Joomla! site's security is at a decent level when using the settings that come with the basic installation. It was also found out that an administrator can greatly affect the security of the site. It is important for the administrator to follow good user- and password policies and to take care of the security updates of all the installed programs. On the other hand, installation of some insecure add-ons can weaken the security of the website.

Keywords data security, information security, Joomla! site security, website security

Sisällysluettelo

1 Johdanto ja tavoitteet

Tietoturva on nykyisin todella tärkeässä roolissa lähes kaikkien ihmisten jokapäiväisessä elämässä. Tietoturva koskettaakin nykyisin jollain tapaa kaikkia ihmisiä, esimerkiksi pankkikortin käyttö vaatii jonkinlaisia tietoturvaan liittyviä toimia. Moni ei näitä välttämättä edes ajattele tietoturvaan liittyvinä, vaan kokee ne pikemminkin maalaisjärjen mukaisena toimintana. Internetin kautta hoidetaan nykyään monia jokapäiväiseen elämään kuuluvia asioita. Monien tällaisten asioiden hoidossa joudutaan käsittelemään arkaluontoista tietoa, kuten esimerkiksi henkilö- tai pankkitietoja. Tällaisten tietojen joutuminen ulkopuolisten käsiin on vähintäänkin epämiellyttävää. Joissain tapauksissa tästä voi koitua myös suurta taloudellista vahinkoa.

Internetin tietoturvaa käsittelevä tieto muuttuu koko ajan nopealla tahdilla ja muutaman kuukauden vanha tieto voi jo olla vanhentunutta. Uusia viruksia ja matoja tehtaillaan koko ajan ja käytettävistä ohjelmistoista löytyy jatkuvasti uusia haavoittuvuuksia. Kukaan ei voi sanoa olevansa perillä tietoturvasta, jos on perehtynyt alan tietoon viimeksi vaikkapa vuosi sitten. Tietoturvasta huolehtivien ihmisten olisikin tärkeätä pysyä koko ajan perillä alan viimeisimmistä käänteistä. Parhaiten tällaista tietoa löytyy alan organisaatioiden sivustojen kautta, painettu tieto on monesti vanhentunutta jo ilmestyessään.

Joskus tietoa julkaisevalla taholla voi olla kytköksiä arvioitavaan tuotteeseen ja julkaistun tiedon puolueettomuus voidaan täten kyseenalaistaa. Käyttämistäni lähteistä Joomla!:n kehittäjien sekä muiden laite- ja ohjelmistovalmistajien julkaisema tieto voi olla puolueellista. Valmistajista riippumattomien lähteiden julkaisema tieto sen sijaan on todennäköisesti luotettavaa.

Työn tavoitteena on esitellä joitain internetsivustojen yleisimpiä uhkatekijöitä, arvioida Joomla!-sivustojen tietoturvan tasoa ja esitellä joitain keinoja, joilla ylläpitäjä voi huolehtia sivustonsa tietoturvasta. Työn aihe tuli lähinnä omasta kiinnostuksestani sekä mielenkiinnosta siihen, kuinka turvallinen Joomla!:lla tehty sivusto on. Joomla!:n avulla monet sellaisetkin käyttäjät, jotka eivät hallitse mitään dynaamisten sivustojen tekniikoita, voivat helposti luoda monimutkaisia dynaamisia sivustoja. Tällaisessa tilanteessa uhkana on se, että ylläpitäjä ei ymmärrä kovin paljoa piiloon jäävistä tekniikoista, eikä niiden vaikutuksesta sivuston tietoturvaan. Tällöin järjestelmän tulisikin perusasetuksillaan olla turvallinen, jotta tavallisen peruskäyttäjänkin tapauksessa tietoturva olisi hyvin hoidettu.

2 Tietoturva

Tietokoneiden ja tietojärjestelmien tietoturva voidaan karkeasti jakaa tietotekniseen tietoturvaan ja sosiaaliseen tietoturvaan. Tällöin tietoteknisellä tietoturvalla tarkoitetaan laitteistojen-, ohjelmistojen- ja tietoliikenteen tietoturvaa. Sosiaalisella tietoturvalla taas tarkoitetaan järjestelmän käyttäjien ja ylläpitäjien tietoturvaan vaikuttavia toimia. Joskus käytetään myös termejä ulkoinen ja sisäinen tietoturva, jolloin ulkoisella tietoturvalla tarkoitetaan tietoteknistä tietoturvaa ja sisäisellä tietoturvalla sosiaalista tietoturvaa. (Wikipedia 2009.)

Tietotekninen tietoturva pitää sisällään kaikki itse laitteistoihin ja ohjelmistoihin liittyvät tietoturvan osa-alueet. Näihin kuuluvat muun muassa ohjelmistojen päivitysten- ja versionhallinta, käyttöoikeuksien ja salasanojen hallinta, verkon tiedonvälityksen suojaaminen ja laitteistojen fyysinen suojaaminen. Erikseen voidaan puhua vielä verkkosovellusten tietoturvasta, jolloin rajoitutaan käsittelemään vain verkkosovellusten tietoturvaa.

Sosiaalisen tietoturvan osa-aluetta pidetään monesti järjestelmien kannalta suurimpana riskinä (Tietokone 2009). Tärkeimpänä osana sosiaalista tietoturvaa on salasanojen käyttö, koska muun muassa erilaiset salasanojen kalastelut sähköpostitse ovat nykyään melko yleisiä. Sosiaaliseen tietoturvaan vaikuttavat salasanojen lisäksi myös monet muut käyttäjien toimet, kuten annetun tietoturvaohjeistuksen noudattaminen ja yleinen verkkokäyttäytyminen. Myös tietojärjestelmien ulkopuolinen käyttäytyminen voi vaikuttaa tietoturvaan. Esimerkiksi hukattu kannettava tietokone voi pitää sisällään kaiken henkilökohtaisen materiaalin ja salasanat. Mikäli kyseistä tietokonetta ei ole suojattu, tai suojaus on heikko, ovat kaikki nämä tiedot epärehellisen löytäjän käytettävissä.

2.1 Käsitteitä

Tietoturva merkitsee eri ihmisille eri asioita. Käytännön puhekielessä tietoturvalla käsitetään yleensä järjestelmien ja tiedon suojaamista ulkopuolisilta. Useimmiten tietoturva miellettäneen tietokoneiden ja tietojärjestelmien tietoturvana. Yksityishenkilöille tietoturva yleensä käytännössä merkitsee esimerkiksi oman tietokoneen tai puhelimen suojaamista ulkopuolisilta.

2.1.1 Tietosuoja

Valtionhallinnon tietoturvakäsitteistön mukaan tietosuoja (en. privacy protection, data protection) pitää sisällään ihmisten yksityiselämän suojan ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä (Valtionhallinnon tietoturvakäsitteistö 2003a). Tietosuojaa koskevia lakeja ovat muun muassa Henkilötietolaki, Laki yksityisyyden suojasta työelämässä sekä Sähköisen viestinnän tietosuojalaki. Näillä pyritään parantamaan yksityisyyden suojaa. Lakien lisäksi tietosuojaa säätelevät myös monet luottamuksen, hyvän moraalin ja etiikan sanelemat käyttäytymissäännöt.

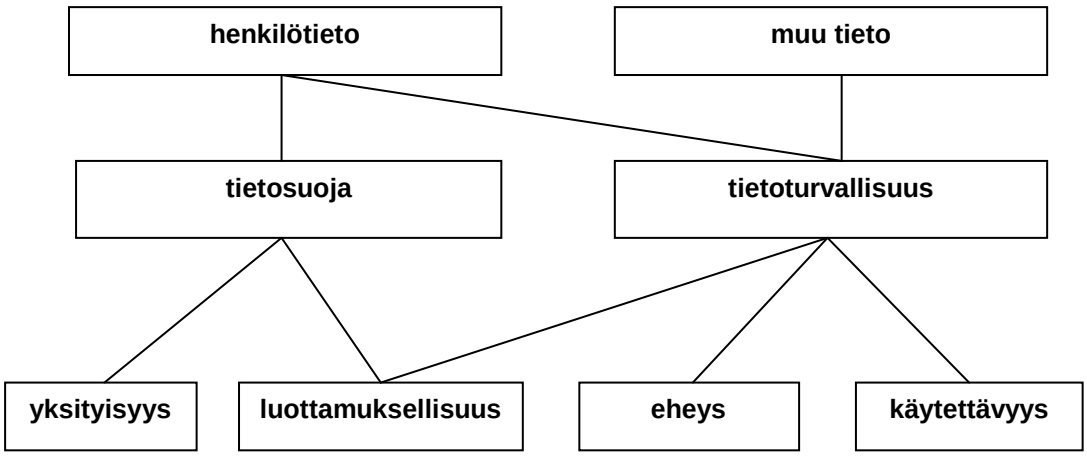
2.1.2 Tietoturvallisuus eli tietoturva

Samaisen valtionhallinnon tietoturvakäsitteistön mukaan tietoturva käsitteenä on synonyymi sanalle tietoturvallisuus. Tietoturvallisuus (en. information security) on määritelmänsä mukaan tavoitetila, jossa tiedot, tietojärjestelmät ja palvelut saavat asianmukaista suojaa niin, että niiden luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat uhkat eivät aiheuta merkittävää vahinkoa yhteiskunnalle ja sen jäsenille. (Valtionhallinnon tietoturvakäsitteistö 2003a.)

Valtionhallinnon tietoturvakäsitteistön mukaiset määritelmät edellä mainituille termeille ovat seuraavat:

- Luottamuksellisuus; tiedot ovat vain niiden saatavilla, joille ne on tarkoitettu.
- Eheys; tiedot ovat paikkansapitäviä, eivätkä niitä voi muuttaa muut kuin ne, joille on annettu muutosoikeudet.
- Käytettävyys; tietoihin pääsee käsiksi riittävän nopeasti ja helposti.

Termi tietoturvallisuus pitää myös sisällään lainsäädännön ja muut toimenpiteet, joilla pyritään varmistamaan edellä mainittu tietoturvallisuus. Valtionhallinnon tietoturvakäsitteistö jaottelee tietoturvallisuuden kahdeksaan toimenpidealueeseen: hallinnollinen, henkilöstö-, fyysinen, tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuus. Edellä viitattu Valtionhallinnon tietoturvakäsitteistö on osana MOT Tietotekniikan liiton ATK-sanakirjan versiota 5.0. Kuvassa 1 on esitetty edellä mainittujen käsitteiden välisiä suhteita. (Valtionhallinnon tietoturvakäsitteistö 2003a.)



Kuva 1: Käsitteiden kohteita ja painopisteitä (Valtionhallinnon tietoturvakäsitteistö 2003a)

Nykyisin tätä tietoturvan klassista määritelmää on laajennettu. Yleisimpään laajennettuun määritelmään on lisätty luottamuksellisuuden, eheyden ja käytettävyyden lisäksi myös kiistämättömyys ja pääsynvalvonta. (Hakala 2006).
Hakalan (2006) mukaan näiden käsitteiden määritelmät kuuluvat seuraavasti:

- Kiistämättömyys käsittää järjestelmän kyvyn tunnistaa ja tallentaa luotettavasti sitä käyttävän käyttäjän tiedot.
- Pääsynvalvonta, menetelmät, joilla estetään käyttäjiä käyttämästä laitteita tai tietoliikenneyhteyksiä muihin kuin niille tarkoitettuihin tehtäviin.

Yrityksillä on yleensä luotuna tietoturvapolitiikka ja sen pohjalta määritelty tietoturvasuunnitelma. Tietoturvasuunnitelma sisältää ne käytännön keinot, joilla tavoiteltuun tietoturvan tasoon pyritään. Tietoturvasuunnitelman pohjalta on monesti luotu erilaisia tietoturvaohjeita, jotka koskevat jotain tiettyä tietojärjestelmää tai prosessia. Loppukäyttäjille jaettavat ohjeistukset ovat yleensä tietoturvaohjeita. (Hakala 2006.)

2.2 Avoin lähdekoodi ja tietoturva

Avoimen lähdekoodin ohjelmistolla tarkoitetaan ohjelmistoa, jonka lähdekoodi on vapaasti saatavilla. Yleensä ohjelmaa saa myös vapaasti kopioida, muokata ja levittää. Ohjelmiston käyttöä ja levitystä koskevat ehdot vaihtelevat jonkin verran riippuen siitä, mitä avoimen lähdekoodin lisenssiä käyttäen kyseinen ohjelma on lisensoitu. Tunnetuin avoimen lähdekoodin ohjelmisto lienee nykyään Linux-käyttöjärjestelmä. Avoimen lähdekoodin ohjelmistoja kehittävät yleensä voittoatavoittelemattomat järjestöt, mutta myös kaupallisia kehittäjiä löytyy. (Open Source Definition 2009.)

Avoimen lähdekoodin vastakohtana ovat suljetun lähdekoodin ohjelmistot. Yleensä suljetun lähdekoodin ohjelmistot ovat kaupallisia ohjelmistoja, joita myy jokin yritys taloudellista voittoa saavuttaakseen. Suljetun lähdekoodin ohjelmiston ostaja saa yleensä käyttöönsä vain ohjelmiston käytettävän version ja siihen liittyvän dokumentit, ei itse lähdekoodia.

Tietoturvan kannalta avoin lähdekoodi on usein kaksiteräinen miekka. Koska avoimen lähdekoodin sovellusten lähdekoodi on hyökkäyksiä suunnittelevien tahojen saatavilla, voivat nämä koodia tutkimalla ehkä löytää koodista virheitä ja haavoittuvuuksia, joita hyväksikäyttäen he pystyvät tunkeutumaan ohjelmistoa käyttävään järjestelmään. Suljetun lähdekoodin sovelluksissa lähdekoodi on yleensä salaista ja näin myös sen tutkiminen vaikeampaa. Toisaalta edellä mainittu voidaan nähdä myös avoimen lähdekoodin etuna. Lähdekoodin ollessa kaikkien vapaasti nähtävissä, voi kuka tahansa löytää koodista virheen tai haavoittuvuuden ja joko korjata sen itse tai lähettää ohjelmiston kehittäjille tiedon virheestä. Löytyneiden haavoittuvuuksien korjausaika onkin aktiivisissa avoimen lähdekoodin ohjelmistoissa yleensä lyhyt, joskus korjaus voi tulla jopa muutaman tunnin sisällä vian havaitsemisesta.

Avoimen lähdekoodin ohjelmistot ovat yleensä jonkin tietyn ohjelmiston kehittämiseen keskittyvän yhteisön kehittämiä ja lisäksi kehitystyöhön voivat aktiivisesti osallistua myös jotkut ohjelmistojen käyttäjät ja muut vapaaehtoiset. Mikäli kyseisen yhteisön mielenkiinto ohjelmiston kehittämiseen loppuu, jäävät tietoturvapäivitykset ja muut korjaukset jonkun muun tehtäväksi tai ne loppuvat kokonaan. Toisaalta sama koskee myös kaupallisia ohjelmistoja. Uuden version tullessa markkinoille tai ohjelmistoa kehittävän yrityksen lopettaessa kokonaan toimintansa, loppuu monesti myös kyseisen ohjelmiston kehittäminen. Tällöin uusia tietoturvapäivityksiäkään ei yleensä enää julkaista ja käyttäjillä on vaihtoehtona vain uuden ohjelmiston ostaminen.

Avoimen lähdekoodin etuna voidaan pitää sitä, että avoimen lähdekoodin yhteisöjä eivät yleensä paina niin kovat aikataulurajoitukset kuin kaupallisia ohjelmistofirmoja. Joskus kaupallinen ohjelmisto on voitu pakosta julkaista keskeneräisenä, koska taloudellinen paine valmiin tuotteen julkaisemiseksi on kova. Avoimen lähdekoodin ohjelmistossa ei yleensä ole tällaisia pakotteita niin voimakkaina olemassa, eikä ohjelmistoilla ole pakottavaa deadlinea, mihin mennessä sen on valmistuttava. Kehittäjillä onkin usein pelissä vain oma ja ryhmänsä kunnia, jolloin keskeneräisiä ohjelmistoja ei ehkä julkaista kovin helposti.

Pelkästään sen perusteella, onko ohjelmisto avoimen lähdekoodin ohjelmisto, ei voida kuitenkaan sanoa yksiselitteisesti, että ohjelmisto olisi turvallisempi tai turvattomampi kuin vastaava suljetun lähdekoodin sovellus. Kaikkia ohjelmistoja on tutkittava tapauskohtaisesti ja tulokset ovat täysin riippuvaisia vertailtavista ohjelmistoista. (Tietoviikko 2009a.)

2.3 Tietoturvaorganisaatioita

Verkossa toimii monia tietoturvaan keskittyviä organisaatioita, joiden tavoitteena on parantaa verkon tietoturvaa antamalla ajantasalla olevaa tietoa käyttäjille. Osa näistä organisaatioista toimii yhteistyössä ja niiden avulla on mahdollista hankkia tietoa ja koulutusta alan teknologioista ja menetelmistä. Jotkut organisaatiot tarjoavat myös työkaluja ja tilastoja tietoturvaan liittyen.

2.3.1 CERT

CERT Coordination Center (CERT/CC) on tietoturva-alan tutkimus- ja kehityskeskus, jota hallinnoi Carnegie Mellon University. Yhdysvaltain hallituksen alainen DARPA (Defense Advanced Research Projects Agency) vaati tällaisen keskuksen perustamista vuonna 1988 Morris-madon pysäytettyä 10% internetin toiminnasta. Nykyisin CERT/CC on osa suurempaa CERT-ohjelmaa, US-CERT (The United States Computer Emergency Readiness Team), jonka tavoitteena on kehittää teknologioita ja järjestelmänhallintakäytäntöjä verkkohyökkäysten ehkäisemiseksi. (CERT 2009.)

Monissa maissa toimii myös omia kansallisia CERT-organisaatioita, jotka toimivat yhteistyössä keskenään. Suomessa toimiva CERT-FI on Viestintäviraston alaisuudessa toimiva kansallinen tietoturvaviranomainen, joka julkaisee muun muassa tietoturvaa koskevia varoituksia ja ohjeita. (CERT-FI 2009a.)

2.3.2 SANS

SANS (SysAdmin, Audit, Network, Security) Instituutti on vuonna 1989 perustettu tietoturvaan erikoistunut organisaatio, joka tarjoaa koulutusta, sertifikaatteja ja tietoa tietoturvan alueelta. SANS tarjoaa ilmaiseksi lukuisia tietoturvaan liittyviä tutkimusdokumentteja sekä alan uusimpia uutisia. SANS:n henkilöstöön kuuluu tietoturva-alan am-

mattilaisia eri puolilta maailmaa. SANS rahoittaa toimintaansa maksullisista koulutuksista sekä painotuotteista saamillaan varoilla. (SANS 2009.)

Internet Storm Center

SANS ylläpitää Internet Storm Center -keskusta, johon kerätään ajantasaista tilastotietoa verkkohyökkäyksistä. Tietoa kerätään palomuurien ja tunkeutumisenestojärjestelmien logeista tuhansilta vapaaehtoisilta ympäri maailman. ICS pyrkii havaitsemaan verkkohyökkäykset aikaisessa vaiheessa ja reagoimaan niihin nopeasti ja näin rajoittamaan niiden aiheuttamaa vahinkoa. Vuonna 2001 perustetun ICS:n edeltäjä oli Incidents.org, joka oli suunnattu auttamaan Y2K-ongelmasta kärsiviä julkisia ja yksityisiä tahoja. ICS:n ensimmäinen onnistunut tehtävä oli Li0N-madon havaitseminen, ja sen vaikutusten onnistunut rajoittaminen vuonna 2001. ICS:n sivustolla raportteja hyökkäyksistä voi tarkastella muun muassa lähteiden IP-osoitteiden, palveluntarjoajien ja maiden perusteella. Lisäksi on nähtävillä muun muassa, mihin porttiin hyökkäyksiä eniten kohdistuu. Sivuilta selviää lisäksi muun muassa internetin senhetkinen uhkataso, eli kuinka paljon haitallista liikennettä internetissä on kyseisellä hetkellä. (Internet Strom Center 2009.)

Mielenkiintoista tietoa on esimerkiksi lista lähteistä, joista on tullut eniten hyökkäyksiä. Kirjoitushetkellä (24.10.2009) tämän listan kärjessä on erään Korealaisen palveluntarjoajan IP-osoite, jolta on tullut yli 95000 hyökkäystä. Ensimmäinen hyökkäys on raportoitu jo yli kuukausi sitten, joten tätä IP:tä ei ole ainakaan suljettu toiminnasta kovin nopeasti. Sivustolla kerrotaan, että osa IP-osoitteista on ns. ’valheellisia esiintymisiä’ (eng. false positive), joissa kyseinen IP-osoite ei ole itse asiassa hyökkääjä, vaan on joutunut listalle jostain muusta syystä. Tällaisia valheellisia tuloksia syntyy tyypillisesti muun muassa P2P-verkkoihin osallistuvista koneista, sähköposti- ja DNS-palvelimista. (Internet Strom Center 2009.)

2.3.3 Muita tietoturvaorganisaatioita

Center for Internet Security (CIS)

Center for Internet Security eli CIS tarjoaa menetelmiä ja välineitä organisaatioiden ja niiden kumppanien internetin käyttöön liittyvien järjestelmien ja laitteiden tietoturvasta huolehtimiseen. CIS ei ole sidoksissa mihinkään valmistajaan tai laitteeseen, vaan se on voittoatavoittelematon yhdistys. CIS:n sivustolta löytyy muun muassa suuri määrä erilaisia tietoturvaa käsitteleviä dokumentteja sekä työkaluja. (CIS 2009.)

SCORE

SCORE on SANS:n ja CIS:n yhteistyöhanke, jonka tavoitteena on laatia erilaisia tietoturvaa koskevia käytäntöjä ja tarkastuslistoja. Listat laaditaan konsensusperiaatteella avoimen postituslistoilla käytävän keskustelun pohjalta. (SCORE 2009.)

National Vulnerability Database

National Vulnerability Database eli NVB on tietokanta, joka sisältää muun muassa tietoa erilaisista tietoturvaa heikentävistä ohjelmistovirheistä ja asetuksista. NVB on Yhdysvaltain hallituksen alaisen National Institute of Standards and Technology:n tietoturvaan erikoistuneen osaston alaisuudessa.

Tietokannan tavoitteena on muun muassa mahdollistaa automaattinen haavoittuvuuksien hallinta ja tietoturvan arviointi. Tietokantaan voi tehdä muun muassa hakuja tietyn tuotteen haavoittuvuuksista. Hakuihin on mahdollista asettaa erilaisia rajoittimia muun muassa päivämäärän ja vakavuusasteen mukaan. (NVB 2009.)

Security Focus

Security Focus on maailman laajin tietoturva-ammattilaisten yhteisö, joka tarjoaa valmistajariippumatonta tietoturvaan liittyvää tietoa erilaisille kohderyhmille. Sivuston kautta voi muun muassa liittyä erilaisille tietoturvaa käsitteleville postituslistoille ja selata eri alustoja koskevia tietoturva-artikkeleita. (Security Focus 2009.)

OWASP

Open Web Application Security Project eli OWASP on avoimen lähdekoodin sovellusten tietoturvan parantamiseen tähtäävä avoin yhteisö. Yhteisön tavoitteena on auttaa kehittämään, hankkimaan, käyttämään ja ylläpitämään luotettavia sovelluksia. OWASP:lla on monia tietoturvaan liittyviä projekteja, joilla pyritään parantamaan yleistä tietoturvatasoa. OWASP Top 10 on lista, jolle on kerätty kymmenen kriittisintä verkkosovellusten haavoittuvuutta. (OWASP 2009.)

Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures eli CVE ei ole varsinaisesti verkon tietoturvaorganisaatio, vaan tietoturvahaavoittuvuuksien sanasto. Kaikille CVE:n listalle otetuille haavoittuvuuksille annetaan yksilöllinen tunniste, jonka perusteella eri haavoittuvuudet tunnistetaan. Sanaston avulla voidaan varmistaa, että käyttäessään tiettyä termiä kaikki osapuolet tarkoittavat samaa asiaa. (CVE 2009.)

2.4 Tietoturvauhkat

Tietoturvauhkia on monen tyyppisiä ja niiden hyväksikäytöllä on erilaisia vaikutuksia kohdejärjestelmien toimintaan. Jotkin uhkat ovat lähinnä teoreettisia, kun taas joitain toisia voidaan käyttää hyväksi todella laajalla rintamalla. Kohteena olevan järjestelmän kannalta olisi tärkeää tietää, mitkä uhkat ovat todennäköisimpiä, ja miten vakavia vaikutuksia niiden hyväksikäytöllä on järjestelmän toimintaan.

Tietoturvauhkia voidaan jaotella erilaisin tavoin. CERT-FI esittää kolme erilaista jaottelumallia. (CERT-FI 2009b.)

Kohteen mukainen jaottelu

- Palvelimet ja palvelinsovellukset. Palvelinten ja niiden käyttöjärjestelmien haavoittuvuudet, esimerkiksi WWW- ja sähköpostipalvelinohjelmistot.
- Työasemat ja loppukäyttäjäsovellukset. Käyttäjien työasemien ja niiden käyttöjärjestelmien sekä ohjelmistojen haavoittuvuudet.
- Verkon aktiivilaitteet. Esimerkiksi reitittimet, modeemit ja palomuurit.
- Matkaviestinjärjestelmät. Kannettavat päätelaitteet, kuten esimerkiksi puhelimet.
- Sulautetut järjestelmät. Laite ja ohjelmisto muodostavat yhdessä sulautetun järjestelmän, kuten esimerkiksi digitaalisia tv-lähetyksiä vastaanottava digitaalinen vastaanotin.

Hyökkäystavan mukainen jaottelu

- Paikallinen. Hyökkääjä pääsee paikallisesti käsiksi kohteeseen ja käyttää sitä paikallisesti tai pääteyhteyden avulla.
- Ilman kirjautumista. Hyökkäys tapahtuu ilman, että hyökkääjä kirjautuu järjestelmään.
- Etäkäyttö. Hyökkäys tapahtuu verkkoyhteyden kautta ilman, että hyökkääjä pääsee fyysisesti kohdejärjestelmän luokse.
- Ilman käyttäjän toimia. Hyökkäys kohdistuu suoraan haavoittuvuuteen ilman, että käyttäjältä vaaditaan mitään toimia.

Hyväksikäyttötavan mukainen jaottelu

- Komentojen mielivaltainen suorittaminen. Tällainen haavoittuvuus on erittäin vakava, koska hyökkääjä voi käyttää järjestelmää samoin kuin järjestelmän käyttöön oikeutettu tavallinen käyttäjä.

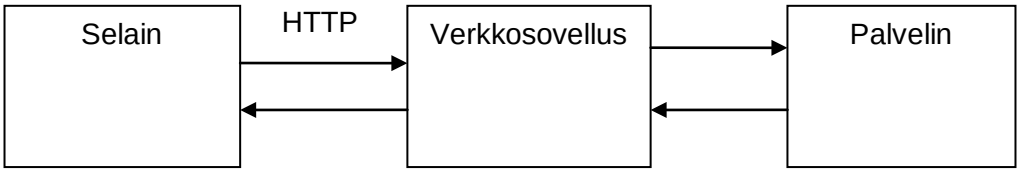
- Käyttövaltuuksien laajentaminen. Tällöin tavallinen käyttäjä saa jollain keinolla valtuutensa laajennettua esimerkiksi ylläpitäjän valtuuksiksi ja voi tehdä järjestelmälle käytännössä lähes mitä haluaa.
- Tietojen muokkaaminen. Hyökkääjä pääsee esimerkiksi muokkaamaan verkkosivuston sivujen sisältöä. Ei vaadi välttämättä kirjautumista.
- Luottamuksellisen tiedon hankkiminen. Hyökkääjä pääsee esimerkiksi lukemaan kiitolevylle talletettuja tiedostoja ja saa näin käsiinsä hänelle tarkoittamattomia tietoja. Näitä tietoja voidaan mahdollisesti käyttää vakavampien hyökkäysten tekemiseen.
- Palvelunestohyökkäys eli DoS (Denial of Service). Saadaan esimerkiksi WWW-sivusto tai sähköpostipalvelin pois toiminnasta kuormittamalla sitä runsailla palvelupyynnöillä. Erikoistapauksena palvelunestohyökkäyksestä on hajautettu palvelunestohyökkäys eli Ddos (Distributed Denial of Service), tällöin hyökkäys tapahtuu useista lähteistä. Ddos:n tapauksessa lähteet ovat yleensä jonkin haittaohjelman saastuttamia koneita, jotka ovat näin hyökkääjän hallinnassa.
- Suojauksen ohittaminen. Hyökkääjä pääsee ohittamaan suojauksen, kuten esimerkiksi palomuurin tai autentikointipalvelun.

2.4.1 Internetsivustojen tietoturva

Internetsivustot voidaan jakaa staattisiin ja dynaamisiin sivustoihin. Staattisissa sivustoissa sisältö pysyy samana, jollei sitä erikseen muokata. Dynaamisissa sivustoissa taas sisältö voi muuttua esimerkiksi selausajankohdan tai käyttäjän toimien perusteella. Dynaaminen sisältö voidaan luoda joko asiakkaan selaimen tai palvelimen tuottamana. Mikäli sisältö luodaan asiakkaan puolella, tapahtuu tämä selaimessa esimerkiksi JavaScript-koodin muodossa. Palvelimen puolella sisällön luonti tapahtuu yleensä siten, että asiakkaan selain lähettää pyynnön palvelimelle, palvelimella toimiva sovellus tekee pyyntöön liittyvät toimenpiteet, ja lähettää tulokset takaisin asiakkaan selaimeen. Palvelimella toimiva ohjelmisto voi olla toteutettu esimerkiksi PHP-, Perl- tai ASP-kielillä.

Verkkosovellus on palvelimella toimiva sovellus, joka vastaa verkkoselaimen HTTP-protokollan välityksellä lähettämiin pyyntöihin. Verkkosovelluksen toteutukseen voidaan käyttää esimerkiksi PHP-, ASP- tai Perl-ohjelmointikieliä. Palvelimella täytyy olla asennettuna jokin palvelinohjelmisto, jonka päällä verkkosovellus toimii.

Kuvassa 2 on esitetty dynaamisen sivuston toimintaperiaate yksinkertaistetussa muodossa.



Kuva 2: Dynaamisen sivuston toimintaperiaate

Verkkopalvelun tietoturva koostuu kokonaisuudessaan monesta eri osa-alueesta. Verkkopalvelun tietoturvaan vaikuttavia tekijöitä ovat muun muassa palvelimen, sillä toimivien ohjelmistojen ja tiedonsiirron tietoturva. Tällöin kokonaisuus on käytännössä yhtä hyvä kuin sen heikoin lenkki. Mikäli jokin osa-alueen tietoturva on hoidettu huonosti, voidaan sen kautta murtaa koko sivuston suojaus.

Sivustojen tietoturva on tärkeää itse sivustojen ja niillä olevan tiedon suojelemiseksi ulkopuolisilta. Erityisen tärkeää tietoturvasta huolehtiminen on sellaisilla sivustoilla, joilla käsitellään arkaluontoisia tietoja, kuten esimerkiksi henkilötietoja tai hoidetaan rahaliikennettä. Vaikka itse sivustolla ei käsiteltäisikään mitään arkaluontoista tietoa, voidaan murrettuja sivustoja kuitenkin käyttää esimerkiksi haittaohjelmien edelleen välittämiseen, jolloin sivustot ovat vaaraksi kaikille niitä käyttäville.

2.4.2 Haavoittuvuudet

Haavoittuvuuden erään määritelmän mukaan termi merkitsee järjestelmän alttiutta tietoturvallisuutta uhkaaville tekijöille (Valtionhallinnon tietoturvakäsitteistö 2003b). IBM:n vuotuisessa tietoturvaraportissa taas käytetään haavoittuvuudelle määritelmää, jonka mukaan haavoittuvuus on mikä tahansa haavoittuvuus, ilmitullut seikka tai järjestelmäasetus, joka voi johtaa järjestelmän luotettavuuden, yhtenäisyyden tai saatavuuden heikkenemiseen. (IBM X-Force 2008 Trend and risk report 2008.)

Edellä mainitun IBM:n raportin mukaan haavoittuvuuksia löydettiin vuonna 2008 13,5 % enemmän kuin vuonna 2007. Yhteensä haavoittuvuuksia löydettiin vuonna 2008 7406 kappaletta. Tämä on 19 % kaikista raportin kymmenvuotisen historian aikana löytyneistä haavoittuvuuksista. Eniten ovat lisääntyneet juuri verkkosovellusten haavoittuvuudet, joita oli vuonna 2008 jo 54 % kaikista haavoittuvuuksista. Tästä voidaan helposti huomata, miten haavoittuvuuksien määrä on viime vuosina kasvanut verkkosivustojen ja niiden käyttäjien lisääntyessä sekä verkkosovellusten muuttuessa monimutkaisemmiksi. Vuoden 2008 lopussa oli 53 % sinä vuonna löydetyistä haavoittu-

vuuksista vielä ilman toimittajan tekemää paikkausta. Verkkosovelluksien haavoittuvuuksissa vastaava luku oli 74%. Vaikuttaisi siis siltä, että todella iso osa löydetyistä verkkosovellusten haavoittuvuuksista on paikkaamatta. (IBM X-Force 2008 Trend and risk report 2008.)

2.4.3 Murtautumisten motiivit

Joskus aikaisemmin murtautumisten motiivina useimmiten oli vain murtautujien halu testata omaa osaamistaan verrattuna sivustojen tietoturvaan. Tällöin murtautujilla ei monestikaan ollut suurta tarvetta aiheuttaa sivustolle mitään oleellista vahinkoa. He saattoivat esimerkiksi vain tuoda julki päässeensä sivustolle sisään. Näin saavutettiin alalle vihkiytyneissä piireissä mainetta ja kunniaa. Tällaisessa maineentavoittelussa suurimman kunnian sai se, joka murtautui parhaiten suojatulle sivustolle. Viime vuosina murtautujien motiivit ovat kuitenkin muuttuneet. Nykyään monet verkkosivustoille hyökkäyksiä suunnittelevat tahot ovatkin osa ammattimaista rikollisuutta. Tällöin heidän ainoa motiivinsa on saada rahallista hyötyä murtautumisesta. Sivustoilta saatuja käyttäjä- tai muita arkaluontoisia tietoja voidaan myydä eteenpäin ja niillä saatetaan vaikkapa kiristää alkuperäisiltä omistajilta rahaa. Mitä helpompi löydettyä haavoittuvuutta on käyttää hyväksi, ja mitä enemmän rahaa murtautumisesta saavutetuilla tiedoilla saa, sitä houkuttelevampaa sivuston haavoittuvuuden hyväksikäyttö murtautujalle on. Joskus motiivina voi olla myös henkilökohtainen syy, kuten esimerkiksi kosto. Tällöin esimerkiksi entinen työntekijä voi kostaa irtisanomisena murtautumalla entisen työnantajansa järjestelmään ja sabotoimalla sitä. (Gillman 2009.)

2.4.4 Vaikutukset

Yleensä hyökkääjät tekevät sivustolle murtautuessaan joitain muutoksia sivuston toimintaan. Vähiten haittaa murrosta on, mikäli hyökkääjät vain lisäävät sivustolle jonkin viestin siitä, että murtautuminen on tapahtunut. Tällöin ylläpitäjän on yleensä helppo huomata, että murtautuminen on tapahtunut ja palauttaa sivusto takaisin toimintaan.

Mikäli murtautujat haluavat aiheuttaa sivustolle todellista vahinkoa ja he pääsevät käsiksi sivuston koko rakenteeseen, on vahinko yleensä suurempi. Sisältöä voidaan kopioida, tuhota ja muunnella tai itse sivuston toiminta voidaan estää.

Pahin vaihtoehto lienee se, että hyökkääjät pääsevät käsiksi sivuston sisältöön ja rakenteeseen, mutta eivät tee mitään sellaista, josta kävisi välittömästi ilmi, että sivustolle on murtauduttu. Tällöin sivustolle voidaan asentaa esimerkiksi jokin haittaohjelma, joka leviää sivustolta eteenpäin. Tällöin kaikkien sivustolla vierailevien tietoturva voi olla uhattuna. Mikäli asennettu haittaohjelma esimerkiksi saa selville heidän käyttäjä- ja salasanatietojansa, on hyökkääjän mahdollista käyttää näitä tietoja hyväkseen myöhemmin. Monesti käyttäjillä on samat tunnukset useille eri sivustoille ja näin hyökkääjä voi saamillaan tiedoilla murtautua myös joillekin muille sivustoille. Siksi ylläpitäjän olisikin murtautumisen havaittuaan aina tärkeää sulkea sivusto välittömästi pois käytöstä ja ilmoittaa murrosta palveluntarjoajalle.

2.4.5 Suojautumiskeinot

Mikäli sivustolla on käytössä vanhoja ohjelmistoversioita, huonoa koodia tai järjestelmän salasanat ovat heikkoja, on sivusto suuremmassa vaarassa joutua hyökkäyksen kohteeksi kuin sivustot, joilla edellä mainituista seikoista on pidetty hyvää huolta.

Päivitykset

Ehkä tärkein toimenpide, jolla sivuston turvallisuuteen voidaan vaikuttaa, on pitää sen päivitykset tietoturvan osalta ajantasalla. Tällä varmistetaan se, että vanhentuneiden ohjelmistojen mukana tulevat haavoittuvuudet eivät vaikuta järjestelmän tietoturvaan. Taulukossa 1 on listattu haavoittuvuuksien yleisimmät hyväksikäytön ajankohdat vuositasolla. Taulukosta voidaan helposti nähdä, että vilkkaimmat haavoittuvuuksien hyväksikäyttöajankohdat ajoittuvat lomien ajalle tai juuri niitä ennen. Mikäli tarkasteluun otetaan viikkoa pidempi ajanjakso, suosituimmaksi haavoittuvuuksien paljastumisajankohdaksi paljastuvat kesäkuukaudet. Yhteistä näille ajankohdille on se, että silloin suuri osa ihmisiä on lomalla. Ihmisten ollessa lomilla voi olla, että mahdollista hyökkäystä ei edes havaita useisiin päiviin. Myös järjestelmän korjaus voi kestää henkilöstön lomien takia tavallista kauemmin. Näin hyökkääjille jää paljon aikaa tehdä haluamansa toimenpiteet ennen järjestelmän sulkemista ja paikkausta. Olisikin tärkeää, että järjestelmän ylläpitoa ei unohdettaisi täysin lomien ajaksi.

Taulukko 1: Haavoittuvuuksien suosituimmat hyväksikäyttöajankohdat (IBM X-Force 2008 Trend and risk report 2008)

Vuosi	*Viikko jona eniten haavoittuvuuksia paljastui*
2000-2005	Viikko ennen joulua
2006	Viikko ennen pyhäinpäivää
2007	Kesä
2008	Viikko ennen joulua

Nollapäivähaavoittuvuudet

Nollapäivähaavoittuvuuksilla tarkoitetaan tietoturva-aukkoja, jotka on jo saatettu julkiseen tietoon tai käytetty hyväksi, mutta joihin ei vielä ole korjausta. Joskus nollapäivähaavoittuvuuden hyväksikäyttö on kuitenkin mahdollista estää tai ainakin rajoittaa sen aiheuttamia vahinkoja käyttämällä jotain muuta keinoa. Järjestelmästä tai ohjelmistosta voidaan ottaa esimerkiksi asetuksia muokkaamalla pois jokin toiminto, joka altistaa kyseiselle haavoittuvuudelle. Tällöin järjestelmää voidaan ehkä turvallisesti käyttää siihen saakka, että korjaus on saatavilla.

Käyttäjäoikeudet

Käyttäjäoikeuksien hallinnointi ja ajantasalla pitäminen ovat järjestelmän tietoturvan kannalta oleellisessa asemassa. Kunnollinen käyttäjäoikeuksien hallinnointi tarkoittaa, että käyttäjille annetaan vain sen verran oikeuksia kuin he tarvitsevat, ei yhtään enempää. Mikäli esimerkiksi joku ylläpitäjän asemassa oleva käyttäjä luopuu tehtävästään, on hänen oikeutensa välittömästi alennettava tai poistettava. Erään raportin mukaan esimerkiksi Microsoftin järjestelmien kriittisistä haavoittuvuuksista jopa 92 prosenttia olisi vaarattomia, jolleivät käyttäjät kirjautuisi järjestelmään ylläpitäjän oikeuksin (Beyond Trust 2009). Ylläpitäjän tunnuksilla kirjautuneena ei myöskään tulisi tehdä mitään muuta kuin sivuston ylläpitoon liittyviä tehtäviä. Ei tulisi esimerkiksi vierailla muilla sivustoilla, koska tällöin on vaarana, että ylläpitotunnukset joutuvat ulkopuolisten käsiin. Sivustolle ei tulisi myöskään olla turhaan kirjautuneena ylläpitäjän tunnuksilla, vaan kirjautua ulos heti kun ylläpitoon liittyvät tehtävät on suoritettu.

Salasanat

Salasanojen ja varsinkin ylläpidon salasanojen on oltava vahvoja ja niistä on pidettävä hyvää huolta. Salasanojen tulisi olla pitkiä, mutta silti helposti muistettavia. Mitään merkityksellisiä sanoja ei tulisi käyttää, koska ne ovat helpommin arvattavissa. Salasanoja

ei tulisi koskaan kirjoittaa ylös mihinkään selväkielisinä. Mikäli ne on tarve kirjoittaa muistiin, on käytettävä jotain salausta. Salanoissa tulisi olla sekä kirjaimia, numeroita että erikoismerkkejä. Salasanoille tulisi myös asettaa maksimiaika, jonka jälkeen ne on vaihdettava. Salasanahistoria tulisi tallentaa ja historian tulisi olla ainakin 10 salasanan mittainen, jolloin samaa salasanaa ei saisi tuona aikana käyttää. Samoin olisi asetettava minimiaika, jottei salasanaa vaihdettaisi liian usein ja historia pyörisi läpi liian nopeasti. (System administrator security best practices 2001.)

2.4.6 Verkkosovellusten kriittisimmät haavoittuvuudet

OWASP on kerännyt Top 10-listaa verkkosovellusten kannalta kriittisimmistä haavoittuvuuksista. Lista on julkaistu vuosina 2004 ja 2007, seuraava lista julkaistaan alkuvuodesta 2010. Listalle on tietoturva-asiantuntijoiden toimesta kerätty kymmenen haavoittuvuutta, joiden julkaisemisen avulla pyritään viemään ohjelmistokehityskulttuuria turvallisen koodintuottamisen suuntaan. Turvallinen koodi olisikin tietoturvan kannalta erittäin oleellista. Näin mahdollisia tietoturva-aukkoja ei olisi ohjelmistoissa läheskään niin paljon kuin niitä nykyään on. Allaolevat haavoittuvuudet ovat vuoden 2007 listalta. (OWASP Top 10 2007.)

1. Cross site scripting, josta käytetään myös lyhennettä XSS. XSS-haavoittuvuuden hyväksikäyttö on mahdollista kaikissa verkkosovelluksissa, mikäli käytettävissä ohjelmistoissa on sen sallivia virheitä. XSS:ssä sovellus lähettää käyttäjältä saamaansa tietoa selaimelle tarkistamatta tiedon sisältöä. XSS:n avulla hyökkääjä voi suorittaa uhrin selaimessa skriptin, joka esimerkiksi kaappaa istunnon, saastuttaa sivuston tai tekee jotain muuta vahinkoa. Yksinkertaisimmillaan XSS paljastaa käyttäjälle toisen käyttäjän aikaisemmin antaman syötteen alla esitetyllä tavalla.

```
echo $_REQUEST['userinput'];
```

XSS-haavoittuvuuksilta voidaan suojautua tekemällä ohjelmistoissa tarkastuksia, joilla syötettyä ja tulostettavaa tietoa tarkastetaan. Erityisen tärkeää on tarkistaa, ettei syötteessä ole erikoismerkkejä, kuten esimerkiksi ’<’ tai ’>’, joiden avulla on mahdollista upottaa jokin skripti syötteeseen.

2. Injektiot, etenkin SQL-injektio, ovat yleisiä verkkosovelluksissa. Injektiossa käyttäjän lisäämää tietoa lähetetään suoritettavaksi osana kyselyä. Injektion avulla hyökkääjä voi luoda, lukea, päivittää tai poistaa mitä tahansa tietoa palvelimella. Pahimmillaan hyök-

kääjä saa koko järjestelmän haltuunsa ja voi tehdä sille käytännössä mitä tahtoo. Mikäli esimerkiksi allaolevassa tapauksessa hyökkääjän on mahdollista päästä käsiksi muuttujaan 'name', voi hän antaa sille arvon, jolla alkuperäinen kysely muuttuu aivan toiseksi kuin on alunperin tarkoitettu.

```
$name = $_POST[“name”];
mysql_query(“SELECT * FROM users WHERE name='$name'”);
```

Jos muuttujalle annetaan esimerkiksi arvo `“'; DROP TABLE; #”`, muodostuu kyselyyn kolme erillistä kyselyä, joista keskimmäinen poistaa koko users taulun.

```
SELECT * FROM users WHERE name='';
DROP TABLE users;
#'
```

SQL-injektioilta suojaudutaan periaatteessa samoilla keinoilla kuin XSS:ltä, eli tarkistetaan syöte ennen sen käsittelyä. Erityisen tärkeää on tarkistaa, että syötteeseen ei jää mitään vaarallisia erikoismerkkejä.

3. Remote file inclusion menetelmää käytetään hyökättäessä sivustolle vieraalta koneelta. Tällöin hyökkääjä lisää omaa haitallista koodiaan sivustolle, jonkin funktion tai syötetiedoston avulla.

```
<?php
global $mosConfig_absolute_path;
include($mosConfig_absolute_path . "/my_file.php");
?>
```

Mikäli hyökkääjä pääsee esimerkiksi vaihtamaan yllä olevaan php-koodiin tiedoston nimen paikalle jonkin muun, esimerkiksi omalla sivustollaan olevan tiedoston osoitteen, on hänellä mahdollisuus murtautua sivustolle. Tämän tyyppinen hyökkäys voidaan estää asettamalla PHP asetukset register_globals ja allow_url_fopen pois päältä.

4. Insecure direct object reference tapahtuu, kun verkkosovellus paljastaa URL:n tai lomakkeen parametrina jonkin järjestelmän sisäisen rakenteen, kuten tiedoston nimen tai tietokannan avaimen. Tällöin hyökkääjä voi päästä käsiksi sivuston sisäiseen rakenteeseen tämän parametrin avulla.

Tämä voidaan ehkäistä siten, että ei paljasteta suoria viittauksia käyttäjille. Suorien viittausten peittämiseksi voidaan viittauksissa käyttää esimerkiksi indeksejä.

5. Cross site request forgery, lyhennettynä CSRF, pakottaa kirjautuneen uhrin selaimen lähettämään valmiiksi hyväksytyn pyynnön haavoittuvalle verkkosovellukselle. Tämän jälkeen sovellus pakottaa uhrin selaimen tekemään jonkin hyökkääjän haluaman toimen. CSRF:n vakavuus on sitä vakavampi, mitä voimakkaamman verkkosovelluksen se kaappaa.

```
GET http://bank.com/transfer.do?acct=tili_nro&amount=summa
```

Haavoittuva verkkosovellus voi esimerkiksi lähettää ylläolevaan tapaan parametreinä tietoa, tässä tapauksessa arvot tili_nro ja summa. Tällöin vihamielinen hyökkääjä voi lähettää verkkosovelluksen käyttäjälle esimerkiksi sähköpostitse viestin, johon on lisätty valmis pyyntö hyökkääjän haluamilla parametreillä. Tällöin esimerkiksi kuvaan voidaan piilottaa linkki alla olevalla tavalla.

```
<img src="http://bank.com/transfer.do?acct=1001&amount=100000"
width="1" height="1" border="0">
```

Kuvaa klikattaessa selain lähettää pyynnön bank.com sivustolle käyttäjän sitä edes huomaamatta.

Sovelluksissa voidaan pienentää tämänkaltaisten hyökkäysten riskiä esimerkiksi vaatimalla aina autentikointia GET- ja POST-parametrien ja evästeiden yhteydessä ja kirjaamalla ei-aktiiviset käyttäjät tietyn ajan kuluttua automaattisesti ulos sovelluksesta. Käyttäjä voi osaltaan estää tämäntapaisten hyökkäysten tapahtumisen omalta selaimeltaan kirjautumalla aina ulos sivustoilta ennen vierailua toisella sivustolla ja tyhjentämällä evästeet aina session jälkeen.

6. Tietovuoto ja huono virheenkäsittely. Sovellukset voivat vuotaa tietoa asetuksistaan tai sisäisestä toiminnastaan. Sovellukset voivat myös paljastaa tietoa sisäisestä rakenteestaan sillä, miten kauan ne suorittavat tiettyjä tehtäviä tai antamiensa virheilmoitusten kautta. Hyökkääjät käyttävät tätä tietoa varastaakseen arkaluontoista tietoa tai suunnitellakseen tulevia hyökkäyksiä.

Vaikutuksia voidaan ehkäistä huolehtimalla, että virheilmoituksissa ei kerrota mitään yksityiskohtia virhetilanteen laadusta. Voidaan esimerkiksi käyttää yhtä standardimuotoista virheilmoitusta kaikissa virhetilanteissa.

7. Autentikoinnin tai istunnon hallinnan rikkominen. Tätä kautta saadut tiedot mahdollistavat käyttäjä- tai ylläpitotunnuksien kaappauksen. Järjestelmissä tulisi käyttää vain järjestelmän valmiita tunnistusmekanismeja, ei itse tehtyjä tai muunneltuja menetelmiä. Salasanan unohtamisen yhteydessä käytettävien toimintojen, kuten esimerkiksi ”salainen kysymys”-tyyppisten ratkaisujen kanssa, olisi noudatettava erityistä tarkkuutta.

8. Huonot salausmenetelmät. Arkaluontoista tietoa salataan joko huonoilla salausmenetelmillä tai tehdään virheitä hyvien salausmenetelmien soveltamisessa. Tulisi käyttää hyviä salausalgoritmeja ja huolehtia avainten turvallisesta säilytyksestä.

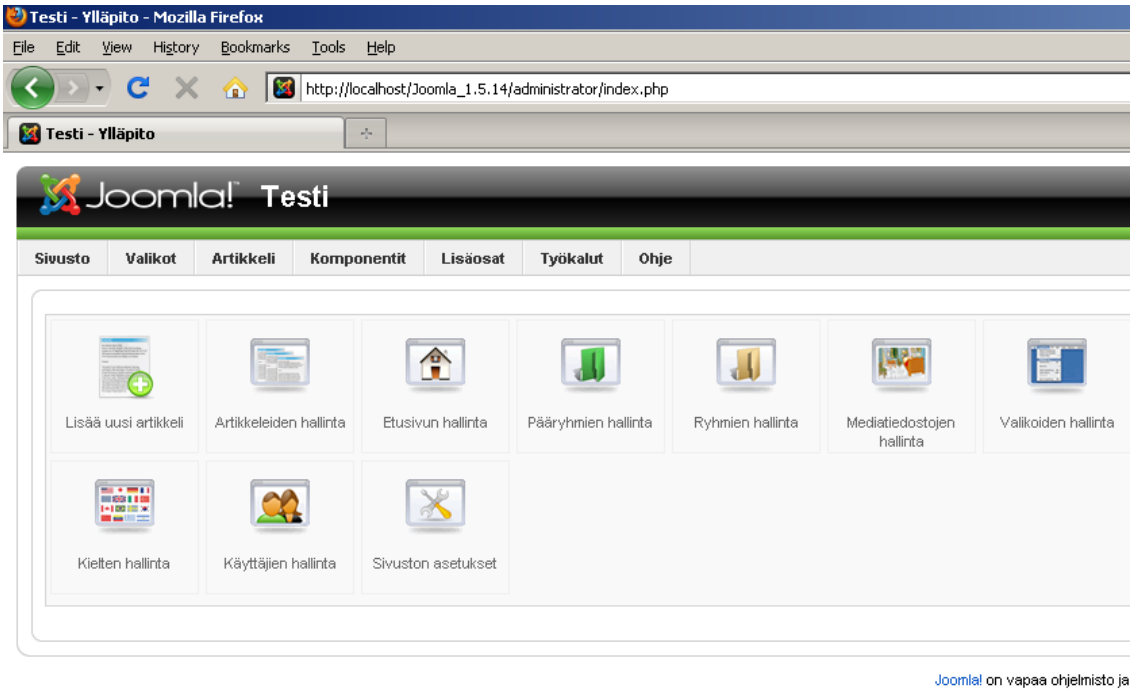
9. Huono tietoliikenteen suojaus. Ohjelmistot eivät käytä salausta tärkeiden tietojen välityksessä. Salausta tulisi käyttää kaikissa autentikoiduissa yhteyksissä, muuten autentikointitiedot ovat vaarassa paljastua sivullisille. Myös kaikki välitettävä arkaluontoinen tieto, kuten luottokortti tai terveystieto tulisi olla salattua.

10. URL viittausten huono valvonta. Usein ainoa suoja URL:lle on, että jos käyttäjällä ei ole niihin oikeutta, linkkejä niihin ei näytetä sivustolla. Mikäli URL:n viitataan suoraan, voidaan kuitenkin päästä tällaiselle sivulle ja päästä käsiksi sivuihin tai funktioihin, joihin käyttäjän ei ole tarkoitus päästä. Pääsyä arkaluontoisiin funktioihin tulisi valvoa, eikä vain luottaa siihen, että kukaan ei löydä kyseistä funktiota.

3 Joomla!

Joomla! (tästä eteenpäin Joomla) on avoimen lähdekoodin WWW-sisällönhallintajärjestelmä. WWW-sisällönhallintajärjestelmät ovat sovelluksia, joilla voidaan helposti luoda ja ylläpitää WWW-sivustoja. Sisällönhallintajärjestelmän avulla käyttäjän ei välttämättä tarvitse käsin muokata itse koodia, vaan järjestelmä sisältää valmiit työkalut sisällön luontiin ja muokkaukseen. Sisällönhallintajärjestelmä auttaa myös sivuston sisällön organisoinnissa, sisältö voi olla tekstiä, kuvia, videoita tai lähes mitä tahansa sivustolla olevaa materiaalia. Järjestelmä antaa valmiin kehitysympäristön, jota jokainen voi muokata halunsa mukaan. Joomlan avulla voidaan tehdä sekä julkisia WWW-sivustoja että erilaisia intranetsivustoja.

Joomla on tehty PHP-ohjelmointikielellä ja se käyttää MySQL-tietokantaa tietojen tallennukseen. Asennus tapahtuu WWW-palvelimelle, sivuston hallinnointi hoidetaan WWW-selaimen kautta. Hallinnointia varten kirjaudutaan ylläpitäjän tunnuksilla ylläpitoliittymään, jonka kautta sivustoa voidaan muokata halutulla tavalla. Kuvassa 3 on esitetty Joomlan ylläpitoliittymä.



Kuva 3: Kuvakappaus Joomlan ylläpitoliittymästä

Joomla on lisensoitu GPL-lisenssillä, joten sen käyttö on vapaata. GNU GPL on lyhennys sanoista GNU General Public License. GPL-lisenssin on luonut Richard Stallman vuonna 1989. Monet avoimen lähdekoodin sovellukset käyttävät GPL-lisenssiä ja se

onkin nykyään käytetyin avoimen lähdekoodin lisenssi. GPL-lisenssin perusperiaatteena on, että käyttäjällä on oikeus muuttaa, jakaa ja välittää GPL-lisenssin alaisia ohjelmia ja niiden lähdekoodia. Muokkaajan täytyy sitoutua siihen, että syntynyttä tuotetta ja sen lähdekoodia jaellaan edelleen GPL-lisenssin ehtojen mukaan. (GNU GPL 2009.)

3.1 Versiohistoria

Joomlan kehitystyö alkoi vuonna 2005, jolloin se eriytyi Mambo-projektista erinäisten vapaan lähdekoodin määritelmää ja käyttöä koskevien erimielisyyksien vuoksi. Joomlan kehitysryhmään siirtyneiden mielestä Mamboa oltiin viemässä liikaa kaupalliseen suuntaan ja ehkä jopa siirtymässä kokonaan pois GPL-lisenssin alaisuudesta. (Joomla! 2009.)

Joomla versio 1.0.0 julkaistiin 16. syyskuuta 2005. Tämä versio oli käytännössä sama kuin Mambo 4.5.2.3 muutamilla käytettävyys-, tietoturva- ja virhekorjauksilla parannettuna. Joomla versio 1.5 julkaistiin 22. tammikuuta 2008. Suurimmat muutokset aikaisempiin 1.0.x versioihin verrattuna olivat ylläpitopuolella, ylläpitoliittymä on helppokäyttöisempi, selkeämpi ja helpommin muokattavissa. Toiminnallisia parannuksia ovat muun muassa hakukoneystävälliset URL-osoitteet. Tämän jälkeen uusia kehitysversioita on tullut tasaisin väliajoin. Tällä hetkellä uusin versio on 1.5.15, joka julkaistiin 4. marraskuuta 2009. Versio 1.6 on tällä hetkellä kehitysvaiheessa. (Joomla! 1.5 Version history 2009.)

3.2 Vaatimukset

Joomla vaati toimiakseen palvelinohjelmiston, SQL-tietokannan sekä PHP-kielen tuen. Käytännössä nämä usein tulevat käyttöön palveluntarjoajan puolesta. Mikäli sivustoa halutaan muokata ja testata omalla koneella, on nämä ohjelmistot asennettava omalle koneelle. Nämä kaikki löytyvät avoimen lähdekoodin ohjelmistoina ja on myös saatavissa valmiita asennuspaketteja, joissa Apache-palvelinohjelmisto, MySQL ja PHP on yhdistetty yhdeksi asennuspaketiksi. Näitä paketteja löytyy kaikille yleisimmille käyttöjärjestelmille. Taulukossa 2 on esitetty Joomla 1.5.x-version vaatimukset ohjelmistoversioiden osalta.

Taulukko 2: Joomla! 1.5.x vaatimukset ohjelmistoversioiden osalta (Joomla! 1.5.x requirements 2009)

Ohjelmisto	*Suositeltu versio*	*Vähimmäisvaatimus*	*Osoite*
PHP	5.2. +	4.3.10	http://www.php.net
MySQL	4.1.x +	3.23	http://www.mysql.com
Apache	2.x +	1.3	http://www.apache.org
Microsoft IIS	7	6	http://www.iis.net

Joomla ei tue vielä MySQL 6.x- ja PHP 5.3-versioita. Koska PHP:n uusimmassa versiossa 5.3.1 on korjattu joitain version 5.2.x vikoja, olisi tärkeää käyttää uusinta versiota. Tämä ongelma muodostaa tietoturvariskin Joomla-järjestelmille.

Joomla on suunniteltu Apache-palvelinohjelmistoa varten, mutta toimii myös Microsoft IIS:n kanssa, vaikka tämä ei olekaan virallisesti tuettu. (Joomla! 1.5.x requirements 2009.)

3.3 Lisäosat

Joomlaan on mahdollista asentaa monia kolmansien osapuolien tekemiä lisäosia. Näillä lisäosilla voidaan järjestelmään lisätä ominaisuuksia, joita siinä ei pelkän asennuspaketin puolesta ole. Osa lisäosista on kaupallisia ja osa ilmaisia. Lisäosa on yleisnimitys komponenteille, moduuleille ja liitännäisille. Lisäksi on saatavissa kielipaketteja, joiden avulla sivuston ja käyttöliittymän kieli on mahdollista vaihtaa. Näitä kaikkia lisäosia on saatavilla muun muassa Joomla Extensions -sivustolta.

Komponentit ovat lisäosista suurimpia ja monimutkaisimpia. Komponentteja voi ajatella sovelluksina, jotka muokkaavat sivun rakennetta. Asennuspaketissa on valmiina joitain komponenteiksi luettavia osia, kuten muun muassa kyselyt, linkit, mainospalkit ja kontaktit. Moduulit ovat komponentteja kevyempiä ja muunneltavampia lisäosia. Moduulit tuovat ohjelmaan lisää toiminallisuutta. Liitännäinen taas on tietyn tehtävän suorittamiseen suunniteltu toiminto, se voi esimerkiksi käsitellä jostain lähteestä tulevaa tietoa, muokata sitä ja näyttää lopuksi käsitellyn version. Joomlaan on saatavilla myös suomenkieliset kielipaketit.

3.4 Joomlan tietoturva

Joomlaa on joskus sanottu verkon reikäisimmäksi ohjelmaksi (Tietoviikko 2009b). Se, että reikiä löytyy, on toki huono asia, mutta vielä oleellisempaa on se, paikataanko löytyneet haavoittuvuudet nopeasti niiden löytymisen jälkeen. Päivitysten tiheys kertoo yleensä siitä, että löytyneitä haavoittuvuuksia on paikattu ja virheitä karsittu. Joomlaan on tullut sen version 1.5 versiohistoriassa 23 kuukauden aikana 16 päivitystä, eli uusia päivityksiä on julkaistu lähes kerran kuukaudessa. Haavoittuvuuksien nopean paikkauksen myötä mahdollisuus nollapäivähaavoittuvuuksien hyväksikäyttöön pienenee ja ainakin periaatteessa ohjelmiston tietoturvan taso paranee.

Ripeä päivitystahti kertoo myös siitä, kuinka aktiivista kehitysryhmän työskentely on. Avoimen lähdekoodin ohjelmistoissa kehitysyhteisön aktiivisuus on oleellista ohjelmiston kehityksen ja tietoturvan kannalta. Toisaalta ripeä päivitystahti voidaan nähdä myös merkkinä siitä, että ohjelmistossa on paljon virheitä, joita päivityksillä sitten joudutaan paikkaamaan.

3.4.1 Tilastoja

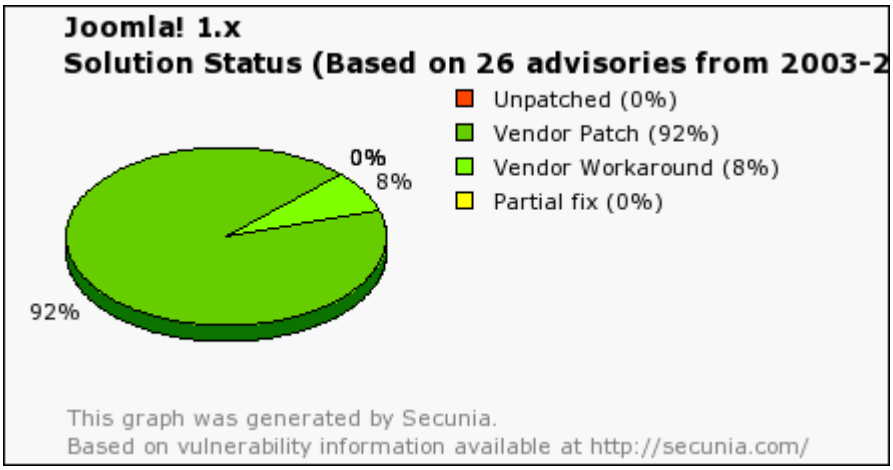
Ohjelmiston tietoturvaa voi jollain tasolla arvioida sitä koskevien tilastotietojen perusteella. Tilastot voivat toisaalta antaa tilanteesta myös väärän kuvan riippuen siitä, kuka tietoja on kerännyt, miten tietoja on kerätty, ja mitä tietoja on kerätty. Ohjelmistojen valmistajien omat tilastot voivat olla epäluotettavia toimittajien pyrkiessä antamaan tuotteestaan parhaan mahdollisen kuvan. Samoin arvioidun ohjelmiston valmistajan kilpailijoiden antamiin tietoihin tulee suhtautua varauksella, koska kilpailijat luonnollisesti haluavat antaa tuotteesta huonon kuvan parantaakseen oman tuotteensa asemaa. Joskus jopa puolueettomilla arvioijilla voi olla kytköksiä arvioitavaan tuotteeseen, tai sen kilpailijaan, joten puolueetonkaan arvio ei aina anna täysin puolueetonta kuvaa arvioitavasta tuotteesta.

Secunia

Tanskalainen ohjelmistojen haavoittuvuuksia seuraava tietoturvayhtiö Secunia pitää listaa ohjelmistoista havaituista haavoittuvuuksista. Yhtiön sivuilla on nähtävissä eri ohjelmistoista havaittujen haavoittuvuuksien määrä, ja montako paikkaamatonta haavoittuvuutta ohjelmistosta kyseisellä hetkellä löytyy. Joomlan osalta ei ole eritelty versioita 1.0.x ja 1.5.x, vaan viitataan kaikkiin Joomlan versioihin 1.x. Secunia painottaa, että tilastojen tuloksia ei voi käyttää suoraan eri ohjelmistojen vertailuun, koska moni

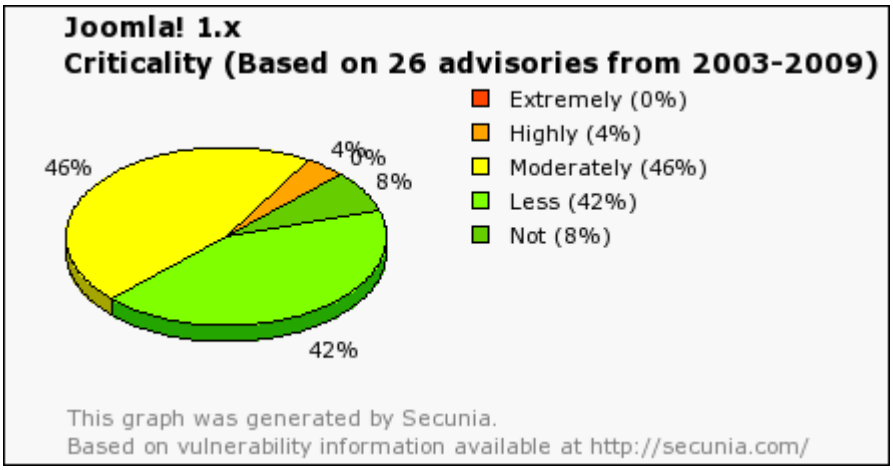
ohjelmisto voi sisältää kolmansien osapuolien komponentteja. Tällöin eri komponenteissa ilmenneet haavoittuvuudet luetaan mukaan itse ohjelmiston haavoittuvuuksiin. (Secunia 2009.)

Joomlan osalta Secunian tilastot näyttävät, että siitä on kaikkiaan 26 tiedotusta ja tällä hetkellä korjaamattomia haavoittuvuuksia ei ole. Joomlan tilanne on siis tältä osin varsin hyvä, vaikka haavoittuvuuksia onkin löydetty aika paljon. Vertailukohtina esimerkiksi Microsoft Internet Explorer versiosta 8.x on 5 tiedotusta, joista 2 on edelleen korjaamatta. Mozilla Firefox versiosta 3.5.x on 5 tiedotusta, eikä yhtään paikkaamatonta. Kuvassa 4 on esitetty Joomlan paikkaamattomien haavoittuvuuksien osuus. (Secunia 2009.)



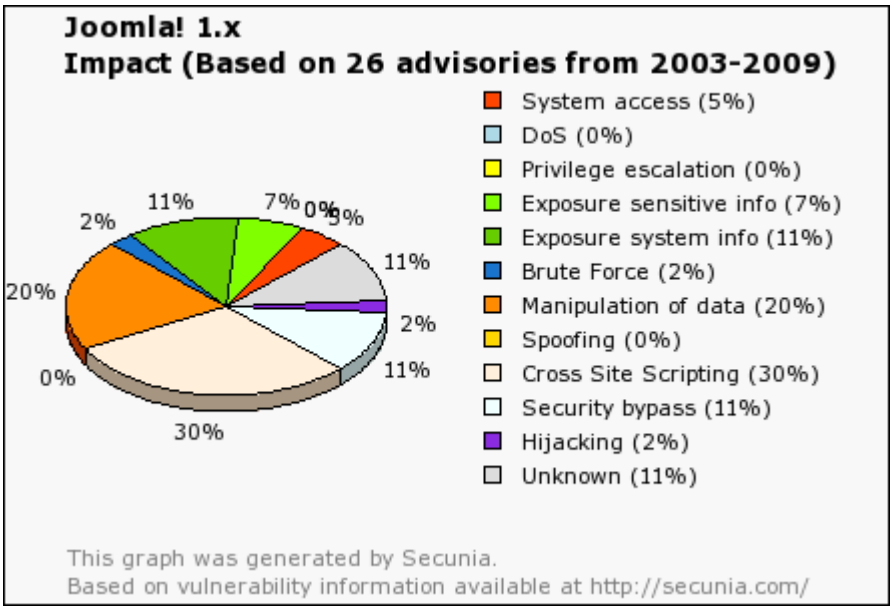
Kuva 4: Joomla! 1.x-paikkausten tila (Secunia 2009)

Kuvassa 5 on esitetty Joomlasta löydettyjen haavoittuvuuksien osuudet haavoittuvuuksien vakavuusasteen mukaan. Tämän mukaan erityisen vakavia haavoittuvuuksia ei olisi löytynyt, vaan suurin osa haavoittuvuuksista olisi vakavuudeltaan keskitasoa. (Secunia 2009.)



Kuva 5: Joomla! 1.x-haavoittuvuudet vakavuusasteen mukaan (Secunia 2009)

Yleisin haavoittuvuuden hyväksikäyttömenetelmä on Cross Site Scripting, 30% haavoittuvuuksista on XSS:n liittyviä. Toiseksi yleisin hyväksikäyttömenetelmä on tiedon manipulointi, jonka osuus on 20%. Nämä kaksi muodostavat siis puolet Joomla-järjestelmien hyväksikäytetyistä haavoittuvuuksista. Pelkästään nämä haavoittuvuustyypit poistamalla olisi siis mahdollista oleellisesti parantaa Joomlan tietoturvaa. Kuvassa 6 on esitetty Joomlasta löydettyjen haavoittuvuuksien osuudet haavoittuvuuksien hyväksikäyttömenetelmien mukaan. (Secunia 2009.)



Kuva 6: Joomla! 1.x-haavoittuvuudet tyypeittäin (Secunia 2009)

IBM X-Force 2008 Trend and risk report

IBM:n vuoden 2008 turvallisuusraportissa on mainittu uusina tulokkaina vuoden 2008 listalle kolme uutta tulokasta. Tulokkaat ovat Joomla, Drupal ja TYPO3. Nämä kaikki kolme ovat avoimen lähdekoodin WWW-sisällönhallintajärjestelmiä. Yhteistä näille kolmelle on myös se, että nämä kaikki kolme on toteutettu PHP-ohjelmointikielellä ja kaikki käyttävät tietokantoja. (IBM X-Force 2008 Trend and risk report 2008.)

Taulukossa 3 on esitetty eri valmistajien tuotteiden osuudet löydetyistä haavoittuvuuksista. Joomlan sijoitus listalla on todella korkea, sen edellä ovat vain kolme suurta valmistajaa Microsoft, Apple ja Sun. Esimerkiksi suurten valmistajien IBM:n ja Mozillan tuotteista on löydetty vähemmän haavoittuvuuksia kuin Joomlasta.

Taulukko 3: Eri valmistajien tuotteiden osuus haavoittuvuuksista (IBM X-Force 2008 Trend and risk report 2008)

Sija	*Valmistaja*	*Osuus haavoittuvuuksista*
1.	Microsoft	3,16%
2.	Apple	3,04%
3.	Sun	2,19%
4.	Joomla!	2,07%
5.	IBM	2,00%
6.	Oracle	1,65%
7.	Mozilla	1,43%
8.	Drupal	1,42%
9.	Cisco	1,23%
10.	TYPO3	1,23%

3.4.2 Asennus ja ylläpito

Joomla on suunniteltu siten, että järjestelmä voidaan asentaa selaimen kautta ja lisäksi järjestelmää voidaan ylläpitää ja muokata mistä tahansa pelkän selaimen ja ylläpitotunnuksien avulla. Tämä on tärkeä ominaisuus monille sivustoille, joilla ylläpitäjiä on monta ja heidän fyysinen sijaintinsa voi olla jopa eri puolilla maapalloa. Tästä aiheutuu kuitenkin joitain tietoturvaan liittyviä ongelmia.

Jotta asetuksia, salasanoja ja kaikkea muuta mahdollista sivustoihin liittyvää voitaisiin muokata internetselaimen välityksellä, on kaikkien järjestelmän tiedostojen sijaittava palvelimen public_html-kansiossa. Kyseinen kansio on kuitenkin se kansio, johon ilman varotoimia on periaatteessa vapaa pääsy kaikkialta internetistä. Näin ollen vierailijoilla on periaatteessa mahdollisuus päästä käsiksi esimerkiksi configuration.php-tiedostoon, joka sisältää muun muassa tietokannan tietoja, kuten käyttäjätunnuksen ja salasanan.

Joomlassa on seitsemän eri käyttäjätyyppiä jaoteltuina kahteen eri ryhmään. Kaksi pääryhmää ovat ylläpitäjät, joilla on oikeus ylläpitoliittymään sekä käyttäjät, joilla on oikeus vain sivuston julkiselle puolelle. Ylläpitoryhmään kuuluu kolme eri käyttöoikeustasoa järjestäjä, ylläpitäjä ja pääylläpitäjä. Käyttäjäryhmään taas kuuluvat tasot vieraat, rekisteröityneet, kirjoittajat ja julkaisijat.

Joomlan asennusohjelma pakottaa asennuksen lopuksi poistamaan asennustiedostot sisältävän hakemiston. Tällöin asennuspaketin tiedostot eivät jää palvelimelle vaarantamaan sen tietoturvaa.

Joomlan kaikkien php-tiedostojen alussa on suoran URL-viittauksen estävä rivi, `defined( '_JEXEC' ) or die( 'Restricted access' );`. Näin estetään suora viittaus järjestelmän php-tiedostoihin muualta kuin index.php-tiedostosta.

3.4.3 Lisäosat

Kehittäjien mukaan Joomlan huonon tietoturvamaineen suurin syy ovat Joomla-sivustoille asennetut huonot lisäosat. Itse Joomlan ytimestä ei heidän mukaansa löydy paljoa haavoittuvuuksia. Lisäosia on saatavilla niin suuri määrä, että niiden vioista ei ole mahdollista pitää täydellistä listausta. Joomlan virallisella lisäosa-sivustolla, http://extensions.joomla.org/, on tällä hetkellä listattuna yli 3600 lisäosaa. Lisäksi on olemassa vanhoja lisäosia, joita ei enää löydy listalta. Monien vanhojen lisäosien kehitystyö on jo loppunut tai niistä ei edes ole tehty 1.5.x-versioon tarkoitettua versiota. Silti tällaisia lisäosia on paljon käytössä, joten ongelma on todella laaja. (Being ”The Vendor” for security issues 2009.)

Joomlan kehitysryhmä pitää listausta vaarallisista lisäosista. Listalla on lueteltu tunnetut vaaralliset lisäosat (Joomla! vulnerable extension list 2009). Listalla lisäosista annetaan nimi, versio numerot, joita ongelma koskee, sekä ratkaisu, jolla ongelma poistuu. Monilla vanhoilla lisäosilla, joiden kehitystyö on jo loppunut, ratkaisuna on vain ky-

seisen lisäosan poistaminen. Joomlassa on mahdollista poistaa lisäosa käytöstä ilman, että sen asennusta poistetaan. Tästä voi muodostua yksi ongelma lisää. Mikäli ylläpitäjä vain ottaa lisäosan pois käytöstä, varsinainen haavoittuvuus voi jäädä järjestelmään, koska lisäosan tiedostoja ei siivota pois palvelimen hakemistoista.

Yleensä ohjelmistojen tietoturvaa arvioitaessa lisäosien haavoittuvuuksia ei kuitenkaan eritellä itse tuotteen haavoittuvuuksista. Käyttäjän kannalta tämä onkin oikein, sillä hänen kannaltaan vain kokonaisuudella on merkitystä. Käyttäjälle ei ole suurtakaan eroa sillä, onko haavoittuvuus itse ohjelmistossa, vai asennetuissa lisäosissa. Ohjelmistojen kehittäjien pitäisikin ehkä tiivistää yhteistyötään lisäosien toimittajien kanssa, jotta tuotteen tietoturva kokonaisuudessaan paranisi. Itse tuotteen kannalta tämä olisi tärkeää, koska eri valmistajien haavoittuvat lisäosat heikentävät suuresti itse tuotteen tietoturvan tasoa.

3.4.4 Kehitysyhteisö

Avoimen lähdekoodin sovelluksissa kehitysyhteisön organisaation toimivuudella ja aktiivisuudella on suuri merkitys sovelluksen tietoturvan tasolle. Joomlan kehitysyhteisön periaatteena on välttää turhaa hierarkiaa ja pitää toiminta niin vapaana kuin mahdollista. Organisaatiossa on kuitenkin erikseen nimetty kehitysryhmä, virheiden jäljittämiseen ja korjaukseen erikoistunut ryhmä sekä tietoturvaan keskittyvä ryhmä.

Kehitysryhmä
Kehitysryhmän tehtävänä on johtaa ja ohjata kehitystyötä ennalta päätettyjen periaatteiden mukaan. Lisäksi ryhmä muun muassa ohjaa eri ryhmien välistä kommunikaatiota. Kehitysryhmää johtaa kehitysryhmän koordinaattori.

Bug squad
Virheiden korjausryhmän tehtävänä on seurata ilmoitettuja ohjelmistovirheitä, pitää niistä kirjaa ja tehdä vaadittavat korjaukset. Uusien versioiden julkaisun yhteydessä ryhmä hoitaa myös niiden testauksen ja laadunvarmistuksen.

Tietoturvaryhmä
Joomlan tietoturvasta huolehtiva ryhmä on nimeltään Joomla Security Strike Team, lyhyemmin JSST. Ryhmä seuraa tietoturvan tilaa sekä 1.0.x- että 1.5.x-versioiden osalta. Ryhmän sivuston kautta on mahdollista tilata Joomlan tietoturvauutisista raportoiva RSS-syöte (Joomla! Security Feed 2009).

Kun uusi haavoittuvuus löydetään, tulisi siitä ilmoittaa JSST:lle ryhmän sivuilla olevan lomakkeen kautta. Samoin tulisi ilmoittaa muualla havaituista haavoittuvuuksista, joista ryhmä ei ole antanut tiedonantoa.

Ryhmän tavoitteet ovat:

- Ilmoitetut Joomlan ytimen haavoittuvuudet tutkitaan ja niihin reagoidaan.
- Joomlan uusien julkaisujen koodi tutkitaan ennen julkaisua, jotta mahdolliset uudet haavoittuvuudet paljastuisivat.
- Vastataan julkisuudessa esitettyihin Joomlaa koskeviin tietoturvakysymyksiin.
- Autetaan kehitysyhteisöä ymmärtämään Joomlan tietoturvaa.

Ryhmän tiedonantopolitiikkaan kuuluu, että havaituista haavoittuvuuksista ilmoitetaan julkisesti vasta, kun kyseiseen haavoittuvuuteen on julkaistu korjaus. Tällä pyritään estämään korjaamattomien haavoittuvuuksien hyväksikäyttö. Toisaalta tämä myös estää muita kehittäjiä korjaamasta aukkoa, ja täten voidaan itseasiassa viivyttää korjauksen ilmestymistä. Ryhmän tiedonannot pyrkivät antamaan haavoittuvuudesta niin paljon tietoa kuin mahdollista, mutta eivät sisällä yksityiskohtaisia tietoja havaituista haavoittuvuuksista.

Ryhmän hoitaa myös Joomlan julkisuussuhteita, pyrkien reagoimaan Joomlasta kirjoitettujen artikkeleiden tietoturvaa koskeviin virheisiin. Ryhmä etsii ja arvioi Joomlasta kirjoitettuja tietoturva-artikkeleita. Mikäli artikkeli sisältää paikkansa pitävää tietoa löydetystä haavoittuvuudesta, jota ei vielä ole korjattu, ryhmä pyytää artikkelin julkaisijaa viivyttämään julkaisua kunnes haavoittuvuus saadaan korjattua. Mikäli kyseinen artikkeli taas sisältää tietoa, joka ei pidä paikkansa, kertoo ryhmä artikkelin kirjoittajille, että tieto ei ole paikkansapitävää ja pyytää näitä korjaamaan tai poistamaan artikkelin. Ryhmä vastaa myös eri tahojen esittämiin tietoturvakysymyksiin ja tarvittaessa tarkistaa artikkeleita ennen niiden julkaisua.

Ryhmä on jaotellut tietoturvauhkat tasoihin niiden vaikutuksen ja vakavuuden mukaan. Tasot ovat kriittinen, keskitaso, kohtalainen ja matala. Vaikutuksen mukaan kriittisiin haavoittuvuuksiin kuuluvat muun muassa nollapäiväuhkat, joissa koko sivuston hallinta on uhattuna. Korkeaan tasoon taas kuuluvat haavoittuvuudet, joita hyväksikäyttäen sivuston tiedot ovat vaarassa. Kohtalaisen tason haavoittuvuuksissa tunkeutujalla on mahdollisuus kirjoittaa tai muokata sivuston sisältöä, matalaan tasoon taas kuuluvat haavoittuvuudet, joissa on vain mahdollista lukea sivuston sisältöä. Vastaavaa jaottelua käytetään uhkien vakavuuden mukaiseen arviointiin. Vakavampia ovat uhkat, joissa

hyväksikäyttö on mahdollista ilman mitään lisätietoa sivustosta, kuten salasanoja tai muita sellaisia. Tällaiset hyökkäykset ovat helpoimpia toteuttaa ja niiltä on vaikein puolustautua. Korkean vakavuustason uhissa hyökkäys on suhteellisen helppo toteuttaa ja sen toteuttaminen voi vaatia ulkopuolisen tiedon hyväksikäyttöä. Kohtalaisen vakavuusriskin synnyttävissä uhissa hyökkäyksen toteutus ei ole helppoa, ja se voi vaatia arkaluontoista tietoa sivustosta. Matalan vakavuustason uhkat taas ovat vaikeita toteuttaa ja vaativat arkaluontoista tietoa tai joitain erityisolosuhteita, jotta hyväksikäyttö onnistuisi.

Ryhmän julkaisupolitikkaan kuuluu, että kaikki vakavat haavoittuvuudet johtavat uuden paikatun version julkaisuun välittömästi. Mikäli haavoittuvuus on vakavuudeltaan keskitasoa, voi se johtaa uuden version julkaisuun, riippuen haavoittuvuuden luonteesta. Vain pienen riskin aiheuttavat haavoittuvuudet korjataan seuraavassa aikataulun mukaisesti julkaistavassa versiossa. Kaikkiin tietoturvapäivityksiin liitetään tieturvailmoitukset, joissa kerrotaan päivityksen tiedot. (Joomla! Security Strike Team 2009.)

4 Ratkaisuja Joomlan tietoturvan parantamiseksi

Ylläpitäjän valinnoilla on suuri merkitys Joomla-sivuston tietoturvalle. Ylläpitäjä voi parantaa sivustonsa tietoturvaa tekemällä joitain hyviä ratkaisuja tietoturvan suhteen. Toisaalta ylläpitäjä voi helposti myös heikentää sivuston tietoturvaa esimerkiksi turvattomia lisäosia asentamalla.

4.1 Palveluntarjoaja

Turvallisen sivuston luomisen lähtökohtana on luotettavan palveluntarjoajan valinta. Mikäli tarkoituksena on itse ylläpitää palvelinta omalla koneella, on tärkeää tutustua palvelimen ylläpitoon ja turvallisten asetusten määrittelemiseen esimerkiksi asiaa käsittelevien oppaiden avulla. Joomlaa varten palvelimella täytyy olla PHP- ja MySQL-tuki. Yleensä halvimmilla internetliittymän mukana tulevilla kotisivutiloilla tätä ominaisuutta ei ole. Yleensä ei kannata ottaa halvinta mahdollista palveluntarjoajaa, vaikka korkea hintakaan ei kuitenkaan aina takaa palvelun tasoa. Jotain palveluntarjoajan resursseista kertoo se, miten heidän tukipalvelunsa toimii. Mikäli palvelu toimii 24 tuntia vuorokaudessa, kertoo tämä, että firma on panostanut käyttäjätukeen, ja että sillä luultavasti on resursseja hoidella ongelmatilanteet nopeasti.

Palveluntarjoajan maineella on yleensä syynsä. Mikäli jokin palveluntarjoaja on hyvässä maineessa, on oletettavaa, että se myös hoitaa tehtävänsä hyvin. Tämä ei aina pidä paikkaansa ja tilanne voi muuttua siten, että ennen luotettava palveluntarjoaja ei ole sitä enää nykyään tai päinvastoin. Lukemalla esimerkiksi käyttäjäkommentteja eri läheteistä selviää kuitenkin, miten asiakkaat suhtautuvat palveluntarjoajaansa. Hyvä merkki palveluntarjoajan suhtautumisesta tietoturvaan on, jos tämä vaatii kaikkia FTP-yhteyksiä käytettävän joko SSH:n tai SFTP:n kautta.

Palveluntarjoajan ohjelmistoversiot kertovat myös jotain palvelimen tietoturvasta. Mikäli Apachesta, PHP:stä tai MySQL:stä käytetään vanhoja versioita, on niissä mahdollisesti piilevät tietoturvaongelmat riskinä myös palvelimella olevalle ohjelmistolle. Huonon merkin palveluntarjoajasta antaa se, mikäli palvelimen PHP-asetuksissa on register_globals määriteltynä oletusarvoisesti päälle. PHP register_globals on tarpeellinen vain vanhoja PHP4-versioita käyttävillä sovelluksille. Uudemmilla PHP5-versiota käyttävillä asetuksen päälläolo aiheuttaa vain tarpeettoman tietoturvariskin.

On myös järkevää asentaa omalle kotikoneelle testiympäristö, jolla sivustoa voi käyttää. Tällöin voi testata kaikki sivuston asetukset ja muutokset testikoneella ennen niiden viemistä palvelimelle. Mahdollisten virhetilanteiden korjaaminen on huomattavasti helpompaa suljetussa ympäristössä, kuin sivuston ollessa jo julkisessa käytössä.

4.2 Ohjelmistopäivityksistä huolehtiminen

On tärkeää huolehtia, että sivustolla on käytössä viimeisimmät versiot Joomlasta ja sen lisäosista. Helppo tapa pysyä selvillä Joomlan ytimen päivitystilanteesta on tilata versiopäivityksistä kertova RSS-syöte. Päivitykset kannattaa myös asentaa välittömästi, koska viimeistään silloin niiden paikkaamat haavoittuvuudet tulevat julkiseen tietoon. Mikäli käytössä on Joomlan versio 1.0.x, olisi järkevää siirtyä käyttämään uudempaa 1.5.x-versiota. Vanhassa versiossa ja varsinkin sen lisäosissa voi olla haavoittuvuuksia.

Joomlaan löytyy myös jotain valmiiksi räätälöityjä asennuspaketteja, joissa voi olla esimerkiksi joitain lisäosia valmiiksi asennettuina. Joomlan päivitykset tulisi kuitenkin aina asentaa Joomlan virallisilta sivuilta ladatuilta asennuspaketeilta. Mikäli asentaa joitain muunneltuja asennuspaketteja, on aina vaarana, että niiden mukana tulee jotain tieturvaan liittyviä ongelmia. Asennuspaketin tarkistamiseen on lisäosa nimeltä Joomla Diagnostics, jonka avulla asennuspaketin eheyden voi tarkistaa.

On aina muistettava huolehtia Joomlan itsensä lisäksi myös käytettävien lisäosien versionhallinasta. Joomla-sivuston suurimmat tietoturvariskit liittyvät juuri epäturvallisiin lisäosiin. Varsinkin versiolle 1.0.x tarkoitetut lisäosat voivat olla jo aktiivisen kehitystyön ulkopuolella, jolloin niihin ei enää tule uusia päivityksiä. Monet voivat käyttää ytimen versiota 1.0.x, koska heillä on jokin siinä toimiva lisäosa, jota he haluavat välttämättä käyttää. Tällöin olisi viisaampaa etsiä uudempaan versioon vastaava lisäosa ja siirtyä käyttämään sitä. Joomlan lisäosasivustolta löytyy RSS-syöte, jossa ilmoitetaan uusista päivityksistä sivustolla jaettaville lisäosille (Joomla! Extension Update 2009). Tämän syötteen tilaamalla pysyy helposti selvillä käyttämiensä lisäosiensa päivitystilanteesta. On myös tärkeää tarkistaa, että käytetty lisäosa ei ole vaarallisten lisäosien listalla. Mikäli lisäosa löytyy listalta, löytyy sieltä myös ohjeistus tilanteen korjaamiseksi. Yleensä tämä hoituu joko päivittämällä lisäosa tai poistamalla se kokonaan. Lisäosista on hyvä asentaa aina vain Stable-versioita, usein saatavilla on myös eri testausvaiheissa olevia versioita, joissa on vielä monia viimeistelemättömiä ominaisuuksia.

Tärkeää olisi myös poistaa kaikki komponentit, joita ei käytä. Mikäli sivustolle jää esimerkiksi jokin vanha lisäosa, voi se aiheuttaa riskin vaikka ei olisikaan käytössä. On myöskin hyvä tarkistaa asennuksen poiston jälkeen järjestelmän kansioista, onko poistetun osan tiedostot ja kansiot todella kaikki poistuneet. Jotkin asennukset poistavat vain sovelluksen itse Joomlasta, jättäen tiedostot ja hakemistot edelleen levylle. Tällöin tiedostot kannattaa poistaa levyltä itse.

4.3 Lisäosat avuksi

On olemassa myös suuri joukko sivuston tietoturvan hallinnassa hyödyllisiä lisäosia. Nämä lisäosat voivat auttaa ylläpitäjää ylläpidollisissa tehtävissä tai tuoda lisäominaisuuksia ylläpidon avuksi. Joomla-lisäosasivuston Access & Security -kategoriasta löytyy yli sata sivuston tietoturvasta huolehtimisessa auttavaa lisäosaa. Näiden avulla voi muun muassa asettaa palomuureja ja virustorjuntaa, suodattaa roskapostia, valvoa sivuston liikennettä ja tehdä monia muita tehtäviä kuten huolehtia varmuuskopioinnista. On mahdollista asentaa esimerkiksi lisäosa, joka ylläpitäjän kirjautumisen jälkeen lukitsee ylläpitoliittymän ja lähettää annettuun sähköposti-osoitteeseen vahvistuskoodin. Vasta syötettyään koodin pääsee kirjautumaan ylläpitoliittymään.

Myös itse sivuston toteutustapaa voi yrittää piilottaa hyökkääjiltä. Joomla-sivustolle on esimerkiksi mahdollista asentaa lisäosa, jonka avulla on mahdollista vaikeuttaa hyökkääjiä tunnistamaan sivustoa Joomlalla tehdyksi. Näin voidaan yrittää ehkäistä hyökkäyksiä, jotka on suunniteltu nimenomaan Joomla-sivustoja kohtaan.

Näissä lisäosissa voi tietenkin piillä myös vaara, mikäli niitä käytetään väärin tai niiden päivityksistä ei huolehdita. Varsinkin erilaiset autentikointia muokkaavat lisäosat voivat väärin käytettyinä tehdä sivuston alttiiksi hyökkäyksille.

4.4 Käyttäjätunnukset ja salasanat

Joomlan asennusohjelma luo pääylläpitäjä tunnuksen nimeltä *admin*. Tällä tunnuksella ja asennusvaiheessa annetulla salasanalla pääsee kirjautumaan ylläpitoliittymään ensimmäistä kertaa. Ensimmäisen kirjautumisen yhteydessä kannattaa ehdottomasti luoda uusi pääylläpitäjän tunnus ja poistaa oletuksena annettu ylläpitotunnus *admin*. Tämä tunnus on kaikkien tiedossa, ja sitä yritetään mitä todennäköisimmin ensimmäi-

senä käyttää, mikäli sivustolle yritetään murtautua. Salasanojen hallinnassa kannattaa muutenkin noudattaa alan suosituksia.

4.5 Varmuuskopiointi

Sivustosta on hyvä ottaa varmuuskopio tietyin väliajoin. Näin varmistetaan, että ongelmien ilmaantuessa on aina mahdollista saada sivusto uudelleen toimintaan. Koska Joomla tallentaa tietoa sekä tietokantaan että hakemistorakenteeseen, on varmuuskopiot otettava sekä tietokannasta että hakemistorakenteesta. Hakemistorakenteeseen tulee muutoksia vain Joomlan asennuksessa ja asennettaessa lisäosia. Tietokantaan on tallennettuna sivustolle lisätty sisältö.

Olisi hyvä, että aina muutoksen jälkeen on mahdollista siirtyä takaisin edelliseen tilaan. Näin ollen aina ennen uusien lisäosien asennusta tai muuta suurta muutosta sivuston toiminnassa olisi hyvä ottaa varmuuskopio sivuston hakemistorakenteesta ja tietokannasta. Varmuuskopioinnin voi tehdä joko manuaalisesti tai käyttää siihen suunniteltuja lisäosia. Varmuuskopiointiin tarkoitetut lisäosat muodostavat tietenkin jälleen yhden mahdollisen riskin sivuston tietoturvalle.

4.6 Tiedostojen ja kansioiden suojaus

Mikäli käytössä on Apache-palvelinohjelmisto, kuten Joomlan tapauksessa yleensä on, on mahdollista ottaa käyttöön .htaccess-tiedosto. Joskus mahdollisuus .htaccess-tiedoston käyttöön on voitu estää palveluntarjoajan asetuksilla. Käyttämällä .htacess-tiedostoa voi esimerkiksi suojata salasanalla haluamiaan hakemistoja, esimerkiksi administrator-kansion. Suojausta kannattaa yleensä käyttää vasta, kun sivustoon on asennettu kaikki tarvittavat lisäosat, koska lisäosien asennuksessa tulee luultavasti ongelmia, mikäli hakemistojen oikeuksia on rajoitettu.

Joomlan perusasennuksessa juurihakemistoon tallennetaan htaccess.txt-niminen tiedosto. Tässä tiedostossa on joitain valmiiksi tehtyjä asetuksia, jotka voi ottaa käyttöön vaihtamalla tiedoston nimeksi .htaccess. Tätä ennen on hyvä varmuuskopioida htaccess.txt-tiedosto ja tallentaa se johonkin varmaan paikkaan. Mikäli sivusto ei toimi .htaccess-tiedoston kanssa, voi aina palata takaisin poistamalla tai nimeämällä uudestaan .htaccess-tiedoston.

Tiedostoa .htaccess muokkaamalla voi tehdä monenlaisia sivustoa suojaavia ratkaisuja. Esimerkiksi lisäämällä alla olevan teksti .htaccess-tiedostoon, voidaan estää ulkopuolisten pääsy sekä .htaccess- että configuration.php-tiedostoihin.

```
<Files .htaccess>
order allow,deny
deny from all
</Files>

<FilesMatch "configuration.php">
Order allow,deny
Deny from all
</FilesMatch>
```

.htaccess-tiedoston avulla on mahdollista tehdä monia muitakin rajoittavia toimenpiteitä, kuten suojata kansioita salasanoilla, estää tyypillisten hyökkäysskriptien suoritus tai estää halutuista IP-osoitteista saapuva liikenne. Mikäli ylläpito tapahtuu aina samasta IP-osoitteesta, on myös mahdollista esimerkiksi estää ylläpitoliittymään pääsy kaikista muista osoitteista.

4.7 Jos murto tapahtuu

Mikäli sivustolle on murtauduttu, tulisi toimia rauhallisesti ja harkita jokainen liike etukäteen. Hätiköiden tilanteen voi tehdä vielä pahemmaksi. Seuraavan listan ohjeita noudattamalla on mahdollista minimoida murron aiheuttamat vahingot (Joomla! site compromised 2009).

1. Muuta kaikki tärkeät salasanat. On oletettavissa, että salasanat ovat tunkeutujien hallussa, joten ne on tärkeää muuttaa. Erityisesti ylläpidon-, FTP-yhteyden ja tietokannan salasanat tulee muuttaa.
2. Tarkista järjestelmän logeista, milloin murto tapahtui ja mitä tiedostoja on muuteltu. Ota huomioon, että myös logeja on voitu muokata.
3. Listaa tiedostot, joita on viimeaikoina muokattu.
4. Tarkista murtautumisen jälkeen luodut uudet tiedostot.
5. Tarkista murtautumisen jälkeen muutetut tiedostot.
6. Tarkista ajastetut tehtävät, niitä voi olla lisätty hyökkääjien toimesta.
7. Ilmoita palveluntarjoajalle tarpeelliset murtoon liittyvät tiedot.

8. Poista koko public_html-kansio.

9. Poista tietokannasta tarvittavat tietueet.

10. Asenna uudelleen sekä tietokanta että tiedostot varmuuskopioista.

11. Vaihda kriittiset salasanat jälleen uusiksi.

12. Mikäli et ole tehnyt säännöllistä varmuuskopiointia aikaisemmin, aloita se nyt.

13. Seuraa sivustoasi, hyökkääjillä on tapana palata samoille sivustoille uudelleen.

5 Pohdinta

Työtä aloittaessani olin aika skeptinen Joomla-sivustojen tietoturvan suhteen. Aikaisemmin lukemieni uutisten perusteella sivustot olivat yleisesti hyökkääjien kohteina ja niiden tietoturva aika heikoissa kantimissa. Asiaan lisää perehdyttyäni tulin kuitenkin siihen johtopäätökseen, että suurimmat puutteet eivät ole itse Joomlassa, vaan pikemminkin asennetuissa lisäosissa ja ylläpitäjien piittaamattomuudessa tietoturvan suhteen. Itseasiassa Joomlan tietoturvan taso ei suurestikaan poikkea muiden yleisesti käytettävien ohjelmistojen tasosta.

Työn toisena tavoitteena oli tehdä sivustojen ylläpitäjille ohjeistus, jonka perusteella he voivat parantaa sivustonsa tietoturvaa. Tämä osoittautui vaikeammaksi kuin olin alunperin suunnitellut. Tämä johtuu pääasiassa siitä, että tietoturvan osalta tilanne elää koko ajan löydettyjen uusien haavoittuvuuksien ja julkaistujen tietoturvapäivitysten myötä. Mitään absoluuttista listaa ei varmaankaan ole edes mahdollista saada aikaan, vaan oleellista on, että ylläpitäjä noudattaa annettuja ohjeita ja suosituksia sekä pitää itsensä ajan tasalla päivitysten ja löydettyjen haavoittuvuuksien suhteen.

Ohjeistuksen osalta tavoitteiden toteutumisessa parannettavaa olisi vielä ollut, mutta aikaa ohjeistuksen laatimiseen olisi kulunut huomattavasti enemmän kuin sitä on käytettävissä. Itse opin työn kautta paljon uutta tietoturvan osalta, joten tältä osin asetetut tavoitteet toteutuivat.

Lähteet

Being ”The Vendor” for security issues 2009.
[online] [viitattu 14.10.2009].
http://community.joomla.org/blogs/community/1029-on-being-qthe-vendorq.html

Beyond Trust 2009.
[online] [viitattu 18.10.2009].
http://pm.beyondtrust.com/company/pressreleases/03Feb2009.aspx

CERT 2009.
[online][viitattu 21.11.2009].
http://www.cert.org/cert/

CERT-FI 2009a.
[online] [viitattu 24.10.2009].
http://www.cert.fi/index.html

CERT-FI 2009b.
[online][viitattu 21.11.2009].
http://www.cert.fi/haavoittuvuudet/2009.html

CIS 2009.
[online][viitattu 21.11.2009].
http://www.cisecurity.org/

CVE 2009.
[online][viitattu 21.11.2009].
http://cve.mitre.org/

Gillman 2009, Hacking goes pro 2009, Engineering and Technology vol. 4 2009
s. 26-29.

GNU GPL 2009.
[online] [viitattu13.10.2009].
http://www.gnu.org/licenses/gpl-3.0.html

Hakala 2006. Tietoturvallisuuden käsikirja s.4. Jyväskylä: Docendo

IBM X-Force 2008 Trend and risk report 2008.
[online] [viitattu 18.10.2009].
http://www-935.ibm.com/services/us/iss/xforce/trendreports/xforce-2008-annual-report.pdf

Internet Strom Center 2009.
[online][viitattu 21.11.2009].
http://isc.sans.org/

Joomla! 1.5 Version history 2009.
[online][viitattu 13.10.2009].
http://docs.joomla.org/Joomla_1.5_version_history

Joomla! 1.5.x requirements 2009.
[online] [viitattu 13.10.2009].
http://www.joomla.org/about-joomla/technical-requirements.html

Joomla! 2009.
[online] [viitattu 13.10.2009].
http://en.wikipedia.org/wiki/Joomla!

Joomla! Extension Update 2009.
[online] [viitattu 15.10.2009].
http://feeds.joomla.org/JoomlaExtensionsUpdated

Joomla Security Feed 2009.
[online] [viitattu 15.10.2009].
http://feeds.joomla.org/JoomlaSecurityNews

Joomla! Security Strike Team 2009.
[online] [viitattu 15.10.2009].
http://developer.joomla.org/security.html

Joomla! site compromised 2009.
[online] [viitattu 15.10. 2009].
http://docs.joomla.org/Help!_Your_site%27s_been_compromised._Now_what%3F

Joomla! vulnerable extension list 2009.
[online] [viitattu 14.10.2009].
http://docs.joomla.org/Vulnerable_Extensions_List

NVB 2009.
[online][viitatu 21.11.2009].
http://nvd.nist.gov/home.cfm

Open Source Definition 2009.
[online] [viitattu 29.11.2009].
http://opensource.org/docs/osd

OWASP 2009.
[online][viitattu 21.11.2009].
http://www.owasp.org/index.php/Main_Page

OWASP Top 10 2007.
[online][viitattu 21.11.2009].
http://www.owasp.org/index.php/Top_10_2007

SANS 2009.
[online][viitattu 21.11.2009].
http://www.sans.org/

SCORE 2009.
[online][viitattu 21.11.2009].
http://www.sans.org/score/

Secunia 2009.
[online] [viitattu 16.10.2009].
http://secunia.com/advisories/product/5788/?task=statistics

Security Focus 2009.
[online][viitattu 21.11.2009].
http://www.securityfocus.com/

System administrator security best practices 2001.
[online] [viitattu 14.10.2009].
http://www.sans.org/reading_room/whitepapers/bestprac/system_administrator_security_best_practices_657

Tietokone 2009.
[online][viitattu 14.10.2009].
http://www.tietokone.fi/uutiset/2009/pahimman_tietoturvariskin_naet_peilista

Tietoviikko 2009a.
[online] [viitattu 21.11.2009].
http://www.tietoviikko.fi/taustat/article238188.ece

Tietoviikko 2009b.
[online] [viitattu 14.10.2009].
http://www.tietoviikko.fi/kehittaja/article324999.ece

Valtionhallinnon tietoturvakäsitteistö 2003a. s. 50-51
[online] [viitattu 14.10.2009].
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/50903/50902_fi.pdf

Valtionhallinnon tietoturvakäsitteistö 2003b. s. 10
[online][viitattu 18.10.2009].
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/50903/50902_fi.pdf

Wikipedia 2009.
[online] [viitattu 29.11.2009].
http://fi.wikipedia.org/wiki/Tietoturva