LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Drupal-ohjelmistokehyksen tietoturvallisuus

Pennanen, Sami
Sippola, Roni

2015 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Drupal-ohjelmistokehyksen tietoturvallisuus

Sami Pennanen
Roni Sippola
Tietojenkäsittely
Opinnäytetyö
Joulukuu, 2015

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Pennanen, Sami & Sippola, Roni

Drupal-ohjelmistokehyksen tietoturvallisuus

Vuosi 2015 Sivumäärä 38

Tämän opinnäytetyön tarkoituksena on ollut perehtyä Drupal-sisällönhallintajärjestelmän tietoturvallisuuteen. Drupal-järjestelmä on WWW-pohjainen ohjelmistokehys, jolla käyttäjä pystyy luomaan verkkosivuja. Tavoitteena on ollut löytää heikkouksia ja haavoittuvaisuuksia, joille Drupal-ohjelmistokehyksen käytössä voi altistua. Työssä on myös perehdytty uhkatilanteiden ennaltaehkäisyyn. Kehittämisen kohteena työssä on ollut Drupal ja sen tietoturvallisuus Seniori365.fi-verkkopalvelussa. Lisäksi tavoitteena on ollut pyrkiä ennaltaehkäisemään ja estämään tietoturvallisuutta uhkaavien tilanteiden syntymistä sisällönhallintajärjestelmässä.

Työ on toteutettu InnoEspoo-hankkeen osaajaverkostossa, johon kuuluvat Espoon kaupunki, espoolaisia yrittäjiä sekä Omnia-ammattiopiston, Laurea-ammattikorkeakoulun ja Aalto-yliopiston opiskelijoita, opettajia ja kehittäjiä. Seniori365.fi-palvelu on toteutettu InnoEspoo-hankkeen aikana. Seniori365.fi-palvelun kehitystyö kuuluu Laurean omiin kärkihankkeisiin. Sivusto on kehitetty Drupal-sisällönhallintajärjestelmällä ja se valittiin opinnäytetyökohteeksi konseptinsa monipuolisuuden vuoksi. Seniori365.fi-palvelu on saanut myös kansainvälistä tunnustusta ansaittuaan maaliskuussa 2015 Pariisissa Design for All Foundationin Best Practice – palveluinnovaatiopalkinnon, lokakuussa 2015 Lontoossa EU-WIIN naisinnovaattoreiden innovaatiokilpailun sosiaalinen innovaatio –kategorian palkinnon sekä lokakuussa 2015 Japanissa IAUD Award –designkilpailun Co-Design-kategorian palkinnon.

Työssä perehdytään sivuston rakenteeseen, moduuleihin ja lisäosiin, joiden hyviin käytänteisiin, luotettavuuteen ja turvallisuuteen keskitytään tarkemmin. Työssä käydään yleisesti läpi, minkälainen käsitys Seniori365.fi-palvelukehittäjillä on sisällönhallintajärjestelmän tietoturvauhista ja miten ne on otettu huomioon sivuston ylläpidossa.

Opinnäytetyössä rakennettiin Drupal-sisällönhallintajärjestelmän yleinen tietoturvaohjeistus, jossa tietoturvakäytänteet käydään läpi sivuston kehitys- ja ylläpitovaiheissa. Ohjeistusta voi hyödyntää myös olemassa olevien Drupal-sivustojen tietoturvallisuuden tarkistamisessa ja varmentamisessa.

Asiasanat: Drupal, Sisällönhallintajärjestelmä, Tietoturvallisuus

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Degree Programme in Business Information Technology

Pennanen, Sami & Sippola, Roni

Information Security of Drupal Content Management Framework

Year 2015 Pages 38

The topic of this thesis was to study the information security of Drupal content management framework. Drupal is a free web content management system, which allows users to develop websites. The main focus of the thesis was to find out whether there are any weaknesses and vulnerabilities that exists in the usage of Drupal as a web site development tool and how to prevent the situations where Drupal site could be compromised. This information was applied to Seniori365.fi web service.

Seniori365.fi was created through a project by InnoEspoo, which consists of organizations from Espoo, the city of Espoo and students, teachers and innovators from Omnia Vocational school, Aalto University and Laurea University of applied sciences. Seniori365.fi project is further developed with Laurea University of applied sciences. The web page is created with Drupal content management system. Seniori365.fi web site, was selected as the topic of the thesis due to the versatility of the concept. The web site has received three international awards; the Best practice award in March 2015 in Paris, the Best social innovation award in October 2015 in London and the Best co-design award in October 2015 in Japan.

In Seniori365.fi web service, the focus was on the structure, modules, add-ons and also on the best practices, reliability and information security of these factors. The thesis includes general information about Seniori365.fi developers' knowledge in the area of Drupal information security, and the precautions they have planned in the case of the site being compromised.

A general information security guide for Drupal content management system was created in the thesis. The guide includes best practices for Drupal sites in the development and administration process. The guide is utilized in Seniori365.fi service and it can also be utilized in inspecting and securing already built sites.

Keywords: Drupal, Content Management System, Information Security

Sisällys

1 Johdanto 6
1.1 Työn tausta ja lähtökohdat 6
1.2 Työn tavoite ja tarkoitus 6
1.3 Työn rakenne 7
2 Osaajaverkoston esittely 7
2.1 InnoEspoo 8
2.2 Seniori365.fi-palvelun esittely 8
3 Sisällönhallintajärjestelmät 9
3.1 Drupal-sisällönhallintajärjestelmä 10
3.2 Drupalin kolmannen osapuolen resurssit 12
4 Tietoturvallisuus 16
4.1 Tietoturvallisuus sisällönhallintajärjestelmissä 17
4.2 Drupalin riskit ja haavoittuvuus 17
4.3 Esimerkkejä Drupalin tietomurroista 18
5 Yleinen tietoturvaohjeistus Drupalin käytölle 20
6 Seniori365.fi–palvelun analysointi 22
6.1 Sivuston moduulit 23
6.2 Tietoturvahaastattelun analysointi 24
6.3 Sivuston analysointi 26
6.4 Seniori365.fi-palvelun yhteenveto 28
7 Pohdinta 29
7.1 Luotettavuus 30
7.2 Eettisyys 30
7.3 Kehittämisehdotukset 31
Lähteet 32
Kuvat 34
Taulukot 35
Liitteet 36

1 Johdanto

1.1 Työn tausta ja lähtökohdat

WWW-pohjaisilla sisällönhallintajärjestelmillä tarkoitetaan työkaluja, jotka mahdollistavat sisällöntuotantoa verkossa. Nämä järjestelmät alkavat olla yleisessä käytössä nettisivujen kehityksessä. Ohjelmistokehyksiä on vuosien saatossa ollut monia erilaisia, mutta vasta viime vuosina ne ovat alkaneet olemaan tarpeeksi kehittyneitä levitäkseen laajemmin yleiseen käyttöön. Sisällönhallintajärjestelmien tarkoitus on mahdollistaa käyttäjälle helppo, vaivaton, joustava ja nopea tapa luoda tasokkaita nettisivuja. Suurimpia etuja on sivustojen luominen ilman vaativaa tietoteknistä osaamista tai ammattiosaamista koodaamisessa.

Vaikka WWW-sisällönhallintajärjestelmiä on monia, vain muutamat ovat yleistyneet verkkosivujen kehitystyökaluina. Työhön valittiin Drupal-järjestelmä, sillä se on yksi suosituimmista ja yleistyneimmistä järjestelmistä. Seniori365.fi-verkkosivusto valittiin esimerkkitapaukseksi opinnäytetyötä varten, koska se on kehitetty Drupal-sisällönhallintajärjestelmällä. Työssä käydään läpi Drupalin toimintaperiaatteita, suosiota ja selvennetään, miksi sen käyttö on yleistynyt.

Avoimen lähdekoodin sisällönhallintajärjestelmillä helpotetaan esimerkiksi yksityishenkilön blogin tai yrityksen verkkosivustojen kehitystä. Järjestelmien ominaisuuksissa on kuitenkin eroja, joihin kuuluvat esimerkiksi visuaalinen käyttäjänhallinta, ohjelmointi ja sisällöntuotanto. Drupalilla saman lopputuloksen voi saavuttaa monilla eri tavoilla ja rajoituksia on hyvin vähän. Drupalin toiminnollisuutta on tarkoitus avata ja selventää yksityiskohtaisemmin.

1.2 Työn tavoite ja tarkoitus

Opinnäytetyön tavoitteena on ennaltaehkäistä tietoturvallisuutta uhkaavien tilanteiden syntymistä Drupal-sisällönhallintajärjestelmässä sekä kehittää Seniori365.fi-sivuston tietoturvallisuutta. Tietoturvallisuuden kehitykseen rakennettiin yleinen tietoturvaohjeistus, joka toimii niin Seniori365.fi-verkkosivustolla kuin jo rakennetuilla Drupal-verkkosivustoilla.

Työssä perehdytään tarkemmin, miten altis Drupal on ollut tietoturvauhille ja minkälaisia ongelmia tietoturvassa tähän mennessä on ilmennyt. Sisällönhallintajärjestelmien käytön yleistyessä on tärkeää ymmärtää järjestelmien tuomat tietoturvariskit ja -uhat. Tämän takia on ajankohtaista tutustua siihen, kuinka altis Drupal-sisällönhallintajärjestelmä on tietoturvauhille.

Laurea-ammattikorkeakoulun tuottama Seniori365.fi-projekti valittiin opinnäytetyön kohteeksi. Tämä sivusto on toteutettu Drupal–sisällönhallintajärjestelmällä. Sitä ylläpitää ja kehittää noin puolivuosittain vaihtuva ryhmä opiskelijoita Laurea-ammattikorkeakoulusta. Opinnäytetyössä perehdytään kyseiseen sivustoon ja etsitään siitä mahdollisia haavoittuvuuksia lähteiden perusteella. Tämän lisäksi sivuston kehitystiimin kanssa keskustellaan sisällönhallintajärjestelmien tietoturvaan liittyvistä asioista. Tavoitteena on parantaa kyseisen sivuston tietoturvallisuutta ja antaa kehitysehdotuksia mahdollisesti ilmenevistä ongelmista sekä ennaltaehkäistä tulevia tietoturvauhkia.

Opinnäytetyössä kehitettiin yleinen tietoturvaohjeistus Drupal-sisällönhallintajärjestelmän käytöstä ja haavoittuvuuksista sekä asioista, joita kehittäjän olisi hyvä huomioida luodessaan sivuston kyseisellä järjestelmällä. Ohjeistuksessa käydään läpi yleistä toiminnollisuutta sekä tietoturvallisuuteen liittyvien asioiden tarkistusta ja varmentamista kyseisessä käyttöympäristössä. Tätä ohjeistusta hyödynnettiin Seniori365.fi-sivuston analysoinnissa.

1.3 Työn rakenne

Opinnäytetyön toisessa luvussa esitellään osaajaverkosto ja sivusto. Kolmannessa luvussa käydään yleisemmin läpi sisällönhallintajärjestelmien tarkoitusta ja perehdytään Drupalin käyttöön sekä sen toiminnollisuuteen. Neljännessä luvussa avataan sisällönhallintajärjestelmien tietoturvallisuutta ja uhkia. Samassa kappaleessa käydään läpi, minkälaisille riskitekijöille ja haavoittuvuuksille Drupal-sisällönhallintajärjestelmä voi altistaa sekä minkälaisia tietomurtoja Drupalissa on ajan myötä ilmennyt. Viidennessä luvussa luodaan helppokäyttöinen ja käyttäjäystävällinen tietoturvaohjeistus Drupal-sisällönhallintajärjestelmän käytölle. Tällä pyritään saamaan kehittäjiä tietoisiksi siitä, minkälaisilla keinoilla tietoturvauhkia voidaan ennaltaehkäistä ja minkälaisia riskejä on olemassa. Kuudennessa luvussa perehdytään Seniori365.fi–palvelun sisältöön ja sen tietoturvallisuuteen, hyödyntäen opinnäytetyöhön luotua tietoturvallisuusohjeistusta. Pohdinnassa tullaan käymään läpi koko opinnäytetyöprosessia, työn lopputulosta, lähteiden luotettavuutta ja eettisyyttä sekä miten Seniori365.fi-palvelua voitaisiin jatkossa kehittää opinnäytetöillä.

2 Osaajaverkoston esittely

Tässä kappaleessa esitellään opinnäytetyön kohdetta, Seniori365.fi-palvelua sekä sen taustalla toimivia tahoja. Kappaleen tarkoituksena on selkeyttää lukijalle Seniori365-palvelun tarkoitusta ja miten se on rakennettu.

2.1 InnoEspoo

InnoEspoo oli InnoOmnian rakentama kansainvälinen yhteistyöhanke, johon kuuluivat Espoon kaupunki, espoolaisia yrittäjiä, Laurea-ammattikorkeakoulun ja Aalto-yliopiston sekä Omnia-ammattiopiston opiskelijoita, opettajia ja kehittäjiä. Kaksivuotinen yhteistyöhanke päättyi huhtikuussa 2015. Tämän hankkeen päätarkoitus oli avata espoolaisille yrittäjille uusia toimintaympäristöjä ja kannustamaan heitä verkostoitumaan. (Tietoa meistä 2015.)

InnoEspoo-hanke kokosi muun muassa yrittäjiä tapaamiseen 12.12.2014, jossa yhteisen hankkeen, InnoEspoon toimiville yrittäjille tarkoitettujen koulutustilaisuuksien päätti myynti- ja verkostoitumistilaisuus Urban Mill –kaupunkikehittämisympäristössä Espoon Otaniemessä. Urban Mill tunnetaan yhteistyöstä Espoon kaupungin, oppilaitosten ja InnoEspoo-hankkeen kanssa, joten se oli sopiva paikka järjestää kyseinen verkostoitumistilaisuus. (InnoEspoo kokosi yrittäjät pikatreffeille 2014.)

2.2 Seniori365.fi-palvelun esittely

InnoEspoo-hankeessa kehitetty Seniori365.fi-palvelu yhdistää senioreiden sekä heidän omaistensa tarpeet ja yritysten palveluiden ja tuotteiden tarjontaan. Toukokuusta 2015 lähtien palvelu on kuulunut Laurea-ammattikorkeakoulun projekteihin. Palvelu toimii Espoon alueella ja sen lähikunnissa. Tämä helpottaa senioreita ja heidän omaisia löytämään juuri heille sopivia ratkaisuja.

Seniori365.fi-palvelun yhtenä tarkoituksena on luoda paikka, jossa seniorit ja heidän omaisensa voivat etsiä ja löytää palveluita sekä tuotteita tarjoavia yrityksiä arjessa kotona selviytymisen tarpeisiin. Palvelu kokoaa senioreille hyödyllisiä yrityksiä, palveluita ja tuotteita Espoosta ja sen lähikunnista. Palvelu on saanut kansainvälistä tunnustusta kolmelta eri taholta ja se palkittiin maaliskuussa 2015 Best Practice –palveluinnovaatiopalkinnolla, lokakuussa 2015 Lontoossa EU-WIIN naisinnovaattoreiden innovaatiokilpailun sosiaalinen innovaatio -kategorian palkinnolla sekä lokakuussa 2015 Japanissa IAUD Award –designkilpailun Co-Design -kategorian palkinnolla.

Seniori365.fi-sivustolta vanhemmat henkilöt ja omaiset saavat paljon erilaista tietoa oman ja lähipaikkakuntien yritysten tarjoamista hyvinvointipalveluista ja tuotteista sekä arjen apuvälineistä. Palvelussa on myös tarpeellista tietoa kotona selviytymiseen ja linkkejä esimerkiksi Espoon kaupungin senioripalveluihin. Sivustolta löytyy myös viihteellistä tekemistä, kuten pelejä ja jumppavideoita sekä suoralinkkejä erilaisiin medioihin. Palvelu ilmoittaa myös ajankohtaisista ja tulevista tapahtumista sekä uutisista Espoon alueelta.

Seniori365.fi-palvelu on opiskelijoiden ideoima ja kehittämä sekä toimii jatkuvasti oppimisympäristönä eri alojen opiskelijoille. Opiskelijat, jotka ylläpitävät palvelua huolehtivat sivuston teknisestä ylläpidosta ja toimivuudesta sekä hankkivat uusia yrityksiä palvelujen tarjoajiksi. Kehittäjien tehtäviin kuuluu myös sisällöntuottaminen, sivuston markkinointi senioreille ja heidän omaisilleen sekä Espoon alueen asiantuntijoille, toimijoille ja organisaatioille. Seniori365.fi-palvelun tarkoituksena on helpottaa ja rikastuttaa senioreiden arkea ja työllistää Espoon alueen yrittäjiä. (Tietoa meistä 2015.)

Seniori365.fi-sivuston kehitystiimissä on työskennellyt opiskelijoita ja ohjaavia opettajia. Opiskelijat ovat työskennelleet projektipäällikkönä, sovelluskehittäjinä ja sisällöntuottajina projektissa. Opiskelijatiimin koko on ollut noin kahdeksan opiskelijaa. Opiskelijaprojektipäällikkö tuottaa sisältöä sisällöntuottajien kanssa sekä johtaa projektia. Websovelluskehittäjät hoitavat palvelun ylläpitämisen ja kehittämisen. Sisällöntuottajat etsivät palveluita, tuottavat sisältöä ja hoitavat asiakaskontakteja.

3 Sisällönhallintajärjestelmät

Shreves & Dunwoodie (2011, 4) määrittelevät sisällönhallintajärjestelmät (englanniksi Content Management Systems tai lyhyesti CMS) työkaluiksi, joilla sisältöä saadaan tuotettua erilaisilla ohjelmilla. Verkkosivustojen sisällönhallintajärjestelmillä pystytään ohjelman avulla luomaan, hallitsemaan tai esittämään sisältöä verkkosivuilla. Tässä opinnäytetyössä keskitytään verkkosivustojen sisällönhallintajärjestelmiin ja näistä sisällönhallintajärjestelmistä Drupaliin.

Sisällönhallintajärjestelmät määritellään pääasiallisesti kolmen eri osa-alueen yhdistymisestä. Ensimmäinen osa-alue on dokumenttien ja työnkulkujen hallinta, toisena osa-alueena ovat ohjelmistokehityksen versionhallintaohjelmistot ja kolmantena asiakkuudenhallintaohjelmat sekä erilaiset verkkokauppasovellukset. Nämä osa-alueet koostavat siis sisällönhallintajärjestelmien kokonaisuuden ja mahdollistavat kehittäjille helpotetun sivuston hallinnan ja kehityksen. (Goodwin, S. & Vidgen 2002, 66 – 70.)

Näissä järjestelmissä yksi oleellisimmista asioista on sivupohjat, jotka pienillä sisältöyksiköillään koostavat WWW-pohjaiset verkkosivut ja verkkopalvelukokonaisuudet. Nämä kokonaisuutena mahdollistavat sivuston helpomman yhtenäisen ja keskitetyn ylläpidon sekä sen hallinnan. Suuri osa sisällönhallintajärjestelmien eduista perustuu kolmannen osapuolen tuottamiin ohjelmistoihin ja palveluihin, joilla sivuston toiminnollisuutta, sisältöä sekä muita ominaisuuksia saadaan lisättyä helposti, ilman oman koodin kirjoittamista.

3.1 Drupal-sisällönhallintajärjestelmä

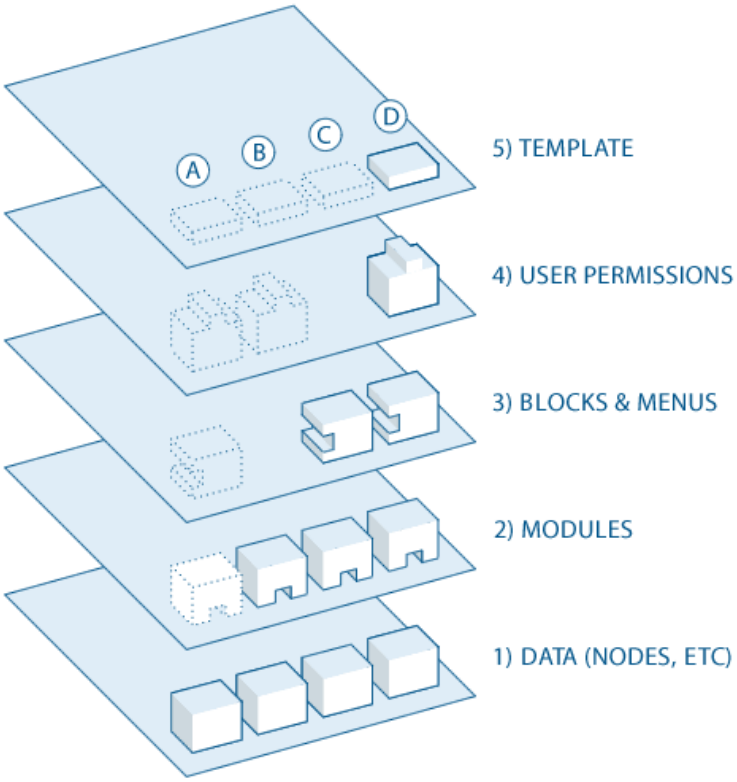
VanDyk (2008, 1) kertoo Drupalin käytöstä verkkosivujen rakentamisessa. Se on avoimen lähdekoodin WWW-sisällönhallintajärjestelmä, jonka toiminta painottuu sen yhteisön yhteistyöhön. Drupalin mukana tulevia ydintoimintoja voidaan täydentää kolmannen osapuolen tarjoamilla moduuleilla. Drupal on suunniteltu muokattavaksi ja sen muokattavuus saavutetaan moduuleilla tai yliajamalla Drupalin ydintoimintoja muuttamatta Drupalin ydinkoodia. Drupalilla voidaan myös onnistuneesti erottaa sisällönhallinta sisällön esittämisestä, joten se mitä nähdään verkkosivulla vieraillessa, poikkeaa sen muokkausnäkymästä.

Drupalin toiminta perustuu olennaisesti sen hallittavuuteen. Monissa sisällönhallintajärjestelmissä asiat toimivat erillään ja suorittavat asioita riippumatta muista toiminnoista. Tämä voi tuoda kehittäjälle ongelmia, kun halutaan toimintoja, jotka vaatisivat kommunikaatiota toimintojen välillä. Esimerkkinä sivustolle voitaisiin asentaa toiminto, joka listaa viimeisimmät artikkelit etusivulle, jos kuitenkin halutaan, että ainoastaan määritetyn kategorian viimeisimmät artikkelit listautuvat näkyville, tarvitaan kommunikaatiota toimintojen välillä. Tämä saattaisi luoda ongelman, joka aikaisemmin on jouduttu ratkaisemaan kehittämällä täysin uusi lisäosa, joka määrittelisi listauksen vain määritettyyn kategoriaan. Koska Drupal on helposti hallittavissa sekä moduulit kommunikoivat sivuston taustalla toimivan koodin kanssa, on helppo luoda ratkaisu edellä mainittuun ongelmaan. Erilaisilla muokatuilla moduuleilla voidaan räätälöidä helposti ratkaisuja kehittäjien vaihteleviin ongelmiin.

Drupalin toiminnasta puhuttaessa on ensiksi hyvä kertoa hieman sen toimintaperiaatteesta. Drupal käyttää hyväkseen nodeja eli solmuja. Solmu pitää sisällään tiedonpalasia, kuten esimerkiksi blogia kirjoittaessa se voisi sisältää artikkelin tekstin, otsikon, sisällön, luojan, luomisajan ja avainsanat. Osa solmun tiedoista on esillä, kun ulkopuolinen käyttäjä vierailee sivustolla, mutta osa solmun tiedoista on taustalla toimivaa meta-dataa, joka hallitsee esimerkiksi milloin ja millä sivulla solmu näytetään sekä millä hakusanoilla sen voi löytää. Tämän kaltaista taustalla toimivaa tietoa voi esimerkiksi olla edellä mainitut hakusanat, joilla artikkelin voi löytää, tai julkaisijan käyttäjätiedot.

Erilainen sisältö pystytään siis tallentamaan solmuihin, jotka sisältävät samat pohjatiedot. Tämän avulla Drupalin ydin ja moduulit pystyvät käsittelemään kaikkea sisältöä samalla tavalla. Solmun samat pohjatiedot mahdollistavat Drupalin käyttäjälle tarkan ja johdonmukaisen hallinnan siitä, miltä sisällön halutaan näyttävän sekä missä sen halutaan näkyvän. Suurin osa ajasta Drupalin käytössä kuluu määritellessä, mitä informaatiota näissä solmuissa halutaan säilyttää sekä miten rakenne kuten valikot, hakusanapuut ja paneelit esittävät nämä solmut.

Drupalin toiminta perustuu sen tapaan käsitellä sisältötyyppejä variaatioina samassa konseptissa eli solmussa. Tämä tarkoittaa sitä, että niin sanotut staattiset sivut, uutiset ja blogin artikkelit tallennetaan samalla tavalla. Käyttämällä valikkoja, views-moduulin listaamaa sisältöä ja block-sivusisältöä, voidaan sivuston navigointirakennetta suunnitella erikseen. (The Drupal overview 2015.)



Kuva 1: The Drupal Flow 2015 (Lähde: https://www.drupal.org/files/drupal_flow_0.gif)

Drupal-järjestelmän suurimpia etuja on sen ilmainen käyttö. Se tarkoittaa, että kuka tahansa voi asentaa ja käyttää Drupalia ilmaiseksi. Drupalin avoin lähdekoodi helpottaa ja nopeuttaa kehitystä, koska kaikki käyttäjät voivat halutessaan antaa oman panoksensa kehitystyössä. Moni voisi kuvitella, että avoin lähdekoodi tuo haasteita, jos käyttäjä pyrkii väärinkäyttämään palvelua. Drupal kuitenkin lupaa sivuillaan olevansa yhtä turvallinen, ellei jopa turvallisempi kuin suljetun lähdekoodin järjestelmät. Drupalin perusasetukset ovat määritelty siten, että sitä on mahdollisimman turvallista käyttää asennuksen jälkeen muokkaamatta asetuksia. Tietoturva-aukkoihin, kuten SQL-injection, Cross Site Scripting, Session Management, Cross Site Request Forgeries ja muihin tavanomaisiin hyökkäyksiin, on kehitetty standardin mukaiset ratkaisut, jotka takaavat turvallisemmat lähtökohdat Drupalin käyttöön. Drupalilla on myös oma tietoturvatiimi, joka jatkuvasti kehittää Drupalin tietoturvallisuutta. (Is Drupal secure 2015.)

Drupalin etuihin kuuluu myös sen muokattavuus ja modulaarisuus, joka mahdollistaa kehittäjän sivuston muokkaamisen, käyttämällä hyväksi muiden tekemiä moduuleja. Järjestelmä on valmiiksi optimoitu hakukoneille, joka parantaa sivuston näkyvyyttä ja Drupalin tarjoamat ominaisuudet kehittyvät jatkuvasti. Drupalin käytettävyys on viimevuosina parantunut merkittävästi. Asioita on kehitetty, paranneltu ja viimeistelty paljon. Huomioitavia parannuksia viimeisimmässä versiossa ovat: helpompi asennuspaketti, paranneltu sisällönlisäys, vedä ja pudota tiedostonsiirto, Word-tekstitiedostojen kopiointi, suoramuokkaus vaihtoehto, laajempi kielivalikoima, parempi mobiilituki, viimeistelty toiminta ja se vaatii vähemmän koodausta. Nämä muutokset ovat mahdollistaneet Drupalin nousun käytetyimpien sisällönhallintajärjestelmien joukkoon. (Overview of Drupal 7 vs. Drupal 8 2012.)

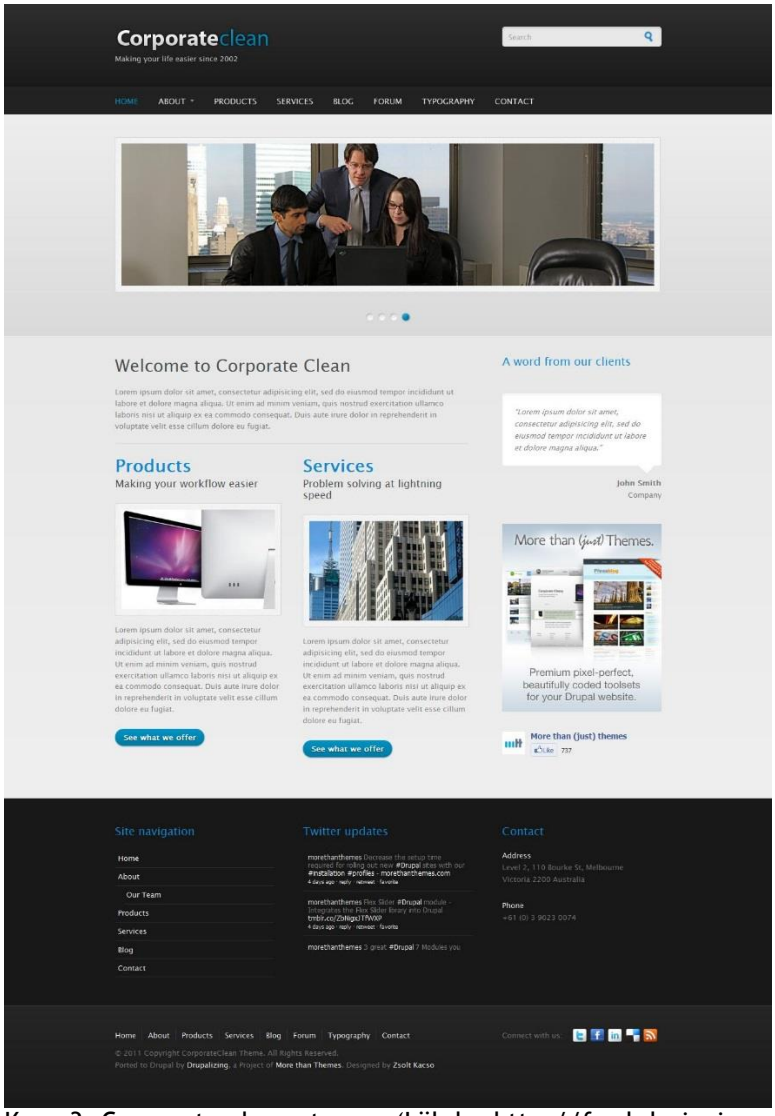
3.2 Drupalin kolmannen osapuolen resurssit

Drupal core eli pohja perusominaisuuksineen on toiminnassa onnistuneen asennuksen jälkeen. Se mahdollistaa järjestelmän laajentamisen ja muokkaamisen kolmannen osapuolen tarjoamilla pohjilla ja apuvälineillä. Yleisin tapa sivustojen rakentamisessa, on ladata ulkopuolisten kehittäjien tekemiä moduuleja, jotka sopivat omiin käyttötarkoituksiin. Näillä moduuleilla voidaan esimerkiksi helpottaa sivuston kehittämistä visuaalisesti ja tehdä muokattavissa olevia hakuja eri ehdoin tietokannasta. Näin voidaan esimerkiksi hakea tietokannasta halutun kategorian tuotteet ja listata ne omalla valitulla tavalla ilman SQL-kyselykielen tuntemusta.

Moduulien lisäksi käyttäjä voi ladata ja asentaa muiden tekemiä sivupohjia eli teemoja. Tämä tarkoittaa sitä, ettei kehittäjän tarvitse lähteä tyhjältä pohjalta, vaan hän voi suoraan valita toimivan sivupohjan ja lähteä muokkaamaan sitä haluamansa näköiseksi sekä omia tarpeitaan vastaavaksi. Teemoja löytyy ilmaiseksi, mutta osa kolmannen osapuolen tekemistä teemapohjista on maksullisia. Maksulliset sivupohjat ovat yleensä hyvin viimeisteltyjä ja tasokkaita sivupohjia. Alla on muutamia esimerkkejä erilaisista ilmaisista Drupalin teemoista.

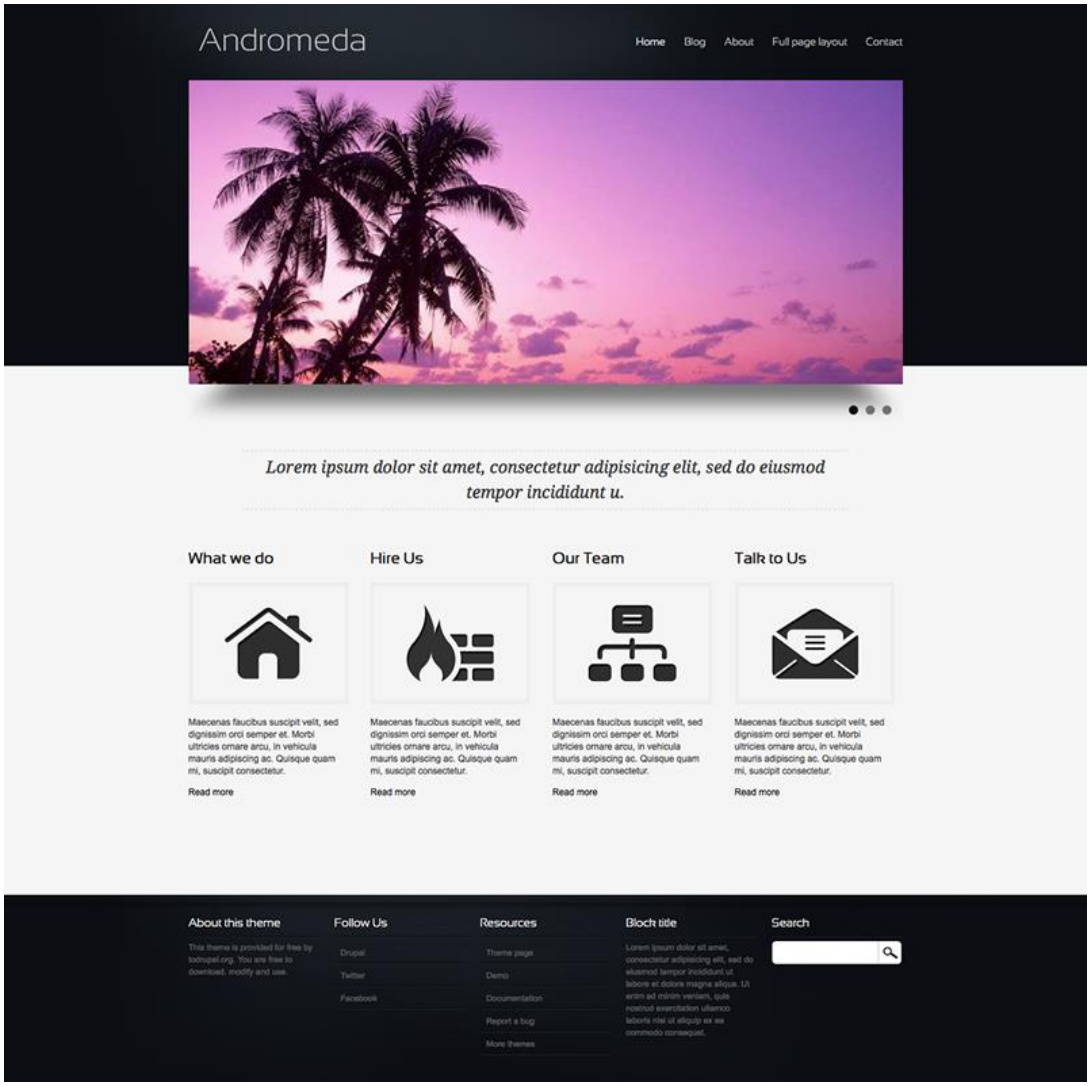
Kuva 2: Nexus-teema (Lähde: https://www.Drupal.org/files/project-images/nexus_theme.png)

Nexus-teema on elegantti ja responsiivinen Drupal-teema käyttäjältä Devsaran. Tätä teemaa voi helposti käyttää blogiin, pienyritykseen, portfolioon tai moneen muuhun verkkosivuun. Tämä teema on suunniteltu yksinkertaisilla elementeillä ja näin saadaan lopputulokseksi elegantti, moderni ja toimiva teema. Puhtaat elementit ovat käyttäjille helppoja ymmärtää ja ne tekevät sivustolla navigoimisesta mukavan kokemuksen. (Nexus Theme 2013)



Kuva 3: Corporate clean -teema (Lähde: http://fwebdesigning.com/sites/default/files/Best-Free-Drupal-Themes-Coporate-Clean.jpeg)

Corporate clean -teema on käännetty Drupal 7 -versioon. Sitä ylläpitää More than (just) Themes, mutta sen on suunnitellut ja julkaissut Zsolt Kasco. Teeman tarkoituksena on olla mahdollisimman puhdas, tyylikäs ja miellyttävä käyttökokemus. Se on suunniteltu etenkin yrityskäyttöön (Corporate Clean 2011.)



Kuva 4: Andromeda-teema (Lähde: https://www.Drupal.org/files/images/Andromeda_1.png)

Andromeda on käyttäjän arshadcn luoma teema vuodelta 2011. Se on tyylikäs ja puhdas Drupal 7 -teema (Andromeda 2011.)

Tärkeä tekijä Drupalissa on sen erittäin laaja ja avoin yhteisö. Tämä helpottaa kehittäjän sivustojen luontia, koska ongelmatilanteissa apua saa keskustelupalstoilta lähes varmasti. Drupal tarjoaa myös omia yleisiä ongelmaratkaisuja, kirjoja, kolmannen osapuolen ammattilaisia, koulutuksia, yhteisön pikaviestimahdollisuutta sekä omaa tukipalvelua ongelmatilanteissa. Drupalista löytyy myös lähetyksiä ja videoita, joissa on paljon materiaalia niin opetus kuin viihdetarkoitukseenkin (Third party resources 2013.)

4 Tietoturvallisuus

Perinteisessä tiedon arvoon liittyvässä määritelmässä tietoturvallisuus koostuu kolmesta käsitteestä. Tiedon käytettävyyteen eli sitä on mahdollista käyttää tarvittaessa, tiedon luottamuksellisuuteen eli vain henkilöt, joilla on oikeus voivat käsitellä tietoa ja tiedon eheyteen eli tiedon tahattomaan muuttumattomuuteen. Kaikkien näiden osa-alueiden huomioinnin jälkeen tietojen turvaaminen on hyvällä mallilla. (Hakala, Vainio & Vuorinen 2006, 4-6)

Alla oleva kuva määrittelee tietoturvan pääpiirteet. Luottamuksellisuus (englanniksi confidentiality), eheys (englanniksi integrity) ja käytettävyys (englanniksi availability) rakentavat siis kolmistaan käsitteen tietoturva. Kun kaikki kolme osaa toteutuvat yhtäaikaisesti, on tietoturva turvallisella tasolla.

Kuva 5: Tietoturvallisuuden määritelmä (Lähde: http://panmore.com/cms/wp-content/uploads/2015/07/The-CIA-triad-goals-of-confidentiality-integrity-and-availability-for-information-security-600x351.png)

Tässä työssä keskitymme lähinnä henkilöturvallisuuteen, tietoaineturvallisuuteen ja ohjelmistoturvallisuuteen. Henkilöturvallisuudella tarkoitetaan ohjelman käyttäjän ja kehittäjän roolia sisällönhallintajärjestelmässä. Tietoaineturvallisuudella tarkoitetaan tietojen säilyttämiseen, varmistamiseen, palauttamiseen ja tuhoamiseen liittyviä toimia. Ohjelmistoturvallisuudella tarkoitetaan ohjelmistoihin liittyviä käsitteitä, kuten ohjelmistojen testausta. Ohjelmistojen testauksella voidaan varmistaa sovellusten sopivuus käyttötarkoitukseen, ohjelmistojen keskinäinen yhteensopivuus sekä toiminnan luotettavuus ja virheettömyys. (Hakala ym. 2006, 11–12.)

Tietoturvallisuuden uhkia verkkosivuilla voivat yleisesti olla esimerkiksi haitallisten ohjelmistojen asennus, tietoliikenteen kuuntelu, tiedostojen väärinkäyttö, tietojenkalastelu (phishing) ja muut kohdistetut hyökkäykset sivustoille. Näillä keinoilla voidaan muun muassa yrittää saada käsiin salaista tietoa, käyttää tätä tietoa luvatta tai muokata sekä poistaa tietoa.

Tietoturvallisuudella pyritään siis varmistamaan kaikki salattava informaatio. Näin varmistetaan, että salattava informaatio pysyy tavoittelemattomissa sekä varmistetaan, ettei kukaan pääse väärinkäyttämään tai muokkaamaan tätä informaatiota. Tällä pyritään myös estämään tietojen vaurioituminen ja mahdollisesti muu haitallinen käyttö.

4.1 Tietoturvallisuus sisällönhallintajärjestelmissä

Tietoturvallisuus ja uhat sisällönhallintajärjestelmissä ovat lähes samat kuin tavallisessakin nettisivukehityksessä. Eroja sisällönhallintajärjestelmiä käyttäessä on siinä, että sisällönhallintajärjestelmät antavat rungon ja pohjan tietoturvallisuuskäytännöille, kun ilman tämän kaltaista järjestelmää pohjaa tietoturvallisuudelle ei ole. Mahdolliset haavoittuvuudet, joita sisällönhallintajärjestelmän rakenne ja ydin voivat sisältää, lisäävät omat riskinsä. Tapaukset, jossa peruuttamatonta vahinkoa saadaan aikaiseksi hyväksikäyttäen sisällönhallintajärjestelmässä sijaitsevaa virhettä, ovat kuitenkin harvinaisia. Tämä johtuu siitä, että kriittiset virheet ehditään yleensä aina löytämään ja korjaamaan päivityksillä ennen kuin niitä päästään hyväksikäyttämään.

Suurimmat riskit sisällönhallintajärjestelmissä ovat kolmannen osapuolen kehittämissä teemoissa ja moduuleissa, jotka voivat sisältää ohjelmointivirheitä ja muita haavoittuvuuksia. Näitä hyökkääjä pystyy yleisimmin käyttämään hyväkseen. Tämän takia asennettaessa kolmannen osapuolen tuottamia työkaluja tai muutakaan sisältöä, on tärkeä tarkistaa sen luotettavuus, suosio ja päivitysten tiheys. Moduulien omilla sivuilla on tuotu esille myös niissä huomatut virheet ja niiden korjausten tila. Drupalin ja moduulien päivitysten laiminlyöminen on suurin syy, miten hyökkääjä voi saada vahinkoa aikaan verkkosivustoilla.

4.2 Drupalin riskit ja haavoittuvuus

Drupalissa riskitekijät ovat pienet, niin kuin yleisestikin sisällönhallintajärjestelmissä. Riskejä voi kuitenkin syntyä muutamista eri tekijöistä. Ohjelmiston vanhentunut versio sekä ulkoiset lisäosat, jotka eivät ole ajan tasalla, luovat riskejä. Kolmannen osapuolen tuottama sisältö on suurin riskitekijä myös Drupalin käytössä. Tutkimusten mukaan tietoturva-aukoista yli 90 % on aiheutunut käyttäjän omasta tai kolmannen osapuolen tuottamasta teemasta tai moduulista, jonka koodi ei ole saanut samanlaista tietoturvatarkastusta kuin Drupalin itse tuottama koodi. (Is Drupal Secure 2015.)

Suuria riskejä WWW-pohjaisissa sisällönhallintajärjestelmissä aiheuttavat SQL-injektiot. Se on tekniikka, jonka avulla hyökkääjä pyrkii hyväksikäyttämään tietoturva-aukoja päästäkseen käsiksi järjestelmiin. SQL-injektiossa tietokantapalvelimelle annetaan SQL-komentoja, joita hyökkääjän ei pitäisi pystyä käyttämään. Koska komentoja on lukemattomia määriä ja niiden merkityksiä pystytään muuntamaan erikoismerkkejä käyttämällä, on mahdollista, että tietokannasta löytyy satunnaisia tietoturva-aukkoja. Drupalissa on sisäänrakennettuna suojausmetodeja, joilla tällaiset hyökkäykset pyritään estämään. Vahva tietokanta, API, tekee vaikeaksi luoda SQL-tietoturva-aukkoja ja tiedostojärjestelmä suodattaa vaarallisia tiedostopäätteitä, jotta palvelin ei pysty suorittamaan niitä. (Castrillo 2011.)

Cross site scripting (XSS) tietoturva-aukossa mahdollistuu koodin syöttäminen, jolla voidaan päästä tunkeutumaan verkkosivuille. XSS-aukolla voidaan pahimmassa tapauksessa pystyä kiertämään pääsynhallinta kokonaan. Haavoittuvuutta voidaan myös hyödyntää HTML-koodilla ja skripteillä. Jos sivusto ei ole tarpeeksi hyvin suojattu, se mahdollistaa hyökkääjän haitallisen komentosarjan syöttämisen esimerkiksi tekstikentän otsikkoon. Drupalissa on kuitenkin vahva suojausjärjestelmä, joka pystyy poistamaan vaarallisia elementtejä, suodattamalla epäluotettavien lähteiden luomaa sisältöä. (Castrillo 2011.)

Cross site request forgery (CSRF) on tapa, jolla pyritään hyödyntämään luvattomia käskyjä käyttäjältä, johon sivusto luottaa. Drupalissa on kuitenkin varmistettu, että käyttäjän toiminnot varmistetaan standarditekniikoiden avulla. (10 Most Critical Drupal Security Risks 2014.)

4.3 Esimerkkejä Drupalin tietomurroista

Drupalin niin kuin muidenkin sisällönhallintajärjestelmien parissa on ajan myötä törmätty erilaisiin tietoturvariskeihin ja -haavoittuvuuksiin. Lähiaikoina on tapahtunut suuria vaaratilanteita kyseisten ohjelmistojen parissa. Alla on muutamia esimerkkejä tietomurroista, joita WWW-pohjaisissa sisällönhallintajärjestelmissä on havaittu.

Viime vuoden lokakuussa Drupalin kehittäjät löysivät suuren tietoturvahaavoittuvaisuuden, jossa hyökkääjä pystyi SQL-injektio tekniikkaa hyödyntäen tunkeutumaan käyttäjien järjestelmiin. Onnistunut tunkeutuminen mahdollistaa tietojen varastamisen ja sivustojen sekä yritysten imagon heikkenemisen. Hyökkääjä pystyy onnistuneen hyökkäyksen jälkeen lisäämään omia tekstejä ja muuta sisältöä julkisille sivustoille tai muuten hyväksikäyttämään sivustoa esimerkiksi jakamalla haittaohjelmia. (Lemos 2014.)

Haavoittuvuuden julkiseksi tuomisen jälkeen aloitettiin järjestelmälliset hyökkäykset Drupal-sivustojen käyttäjiä kohtaan. Tilanne oli niin akuutti, että jos Drupal-sivustoa ei ehditty päivittämään seitsemän tunnin sisällä, se oli mahdollisesti jo altistunut hyökkäykselle. Tämän

kaltaiset SQL- tai tietokantahyökkäykset ovat vaarallisia, koska sivuston tietoihin päästään suoraan käsiksi käyttäjätunnuksista ja muista oikeuksista huolimatta. Tällaisessa tapauksessa voi olettaa, että arkaluontoiset tiedot ovat hyökkääjän käsissä. Hyökkääjä voi saastuttaa järjestelmän ja laittaa järjestelmän saastuttamaan muita vierailijoita ja käyttäjiä. Erilaisia ohjelmia käyttämällä voi kuitenkin nähdä, onko sivustolla hyökkäyksen jälkiä ja tarkastaa ovatko tiedostot mahdollisesti altistuneet hyökkäykselle. (Lemos 2014.)

Drupal ohjeistaa vaarantuneita sivustoja seuraavalla tavalla: laita sivusto hetkellisesti alas ja arvioi miten jatketaan. Käy kaikki koodi, tiedostot, käyttäjät, käyttöoikeudet ja roolit läpi rikosteknisiä tiedostojen tarkastusta hyväksikäyttäen. Noudata myös paikallisia standardeja käyttäjien ja mahdollisesti virkavallan tiedottamisessa. Halutessa sivuston voi myös rakentaa uudestaan alusta alkaen parhaan tietosuojan varmistamiseksi. Sivusto tulee palauttaa versioon missä se oli ennen hyökkäyksiä, puhdistaa palvelimen ohjelmat täydellisesti, asentaa ja päivittää Drupal sekä sen jälkeen palauttaa ohjelmisto. (Lemos 2014.)

Toukokuun 29. päivä 2013 drupal.org:in tietoturvatiimi ilmoitti havainneensa luvattoman käytön käyttäjien tiedoissa drupal.org ja groups.drupal.org sivustoilla. Tämän luvattoman pääsyn tietokantoihin oli mahdollistanut kolmannen osapuolen ohjelmisto drupal.org palvelimilla. Drupal ei kuitenkaan halunnut tuoda esille tämän ohjelmiston kehittäjän tai yrityksen nimeä. Tämä haavoittuvuus ei liittynyt Drupalin omaan koodiin tai sisältöön, vaan kolmannen osapuolen tarjoamaan palveluun, jonka kautta haavoittuvuutta pystyttiin hyväksikäyttämään. (Drupal hit by massive data breach 2013.)

Tiedot, joita luvaton käyttäjä oli päässyt tarkastelemaan, sisälsivät muun muassa käyttäjänimiä, sähköpostiosoitteita, paikkakuntatietoja sekä hajakoodattuja salasanoja. Muita palvelimella olevia tietoja oli myös mahdollisesti päästy tarkastelemaan. Varotoimina kaikki drupal.org:in omat salasanat uusittiin ja seuraavalla kirjautumiskerralla kaikkien Drupalin käyttäjien salasanoja pyydettiin vaihtamaan. Drupal otti yhteyttä haavoittuvan ohjelmiston tarjoajaan ja saivat kyseisen ongelman korjattua. Drupal otti samalla seuraavat askeleet turvatakseen drupal.org:in infrastruktuurin jatkossa. Drupal.org:in infrastruktuuritiimi teki yhteistyötä heidän palvelinisäntänsä OSU Open Source Lab:in työntekijöiden kanssa, jotta uudelleen rakennettaessa tuotannossa sekä käyttöönotossa saatiin pääkehittäjien yhteistyöllä lisättyä turvallisemmat ytimet palvelimille. Virusten ja muuten haitallisten ohjelmien tarkistus ollaan muuttamassa rutiinityöksi muiden prosessien lisäksi. Drupal muutti myös vanhojen sivustojensa arkistot staattisiksi kopioiksi ylläpidon helpottamiseksi. (Drupal hit by massive data breach 2013.)

Sisällönhallintajärjestelmien yksi pysyvistä uhkista on brute force -hyökkäykset. Tällaisilla hyökkäystavoilla yritetään arvata oikeaa salasanaa tai avainsanaa kunnes sellainen löytyy.

Vuonna 2013 huhtikuussa tietoturva-asiantuntijat varoittivat lisääntyvistä hyökkäysten määristä, jotka kohdistuivat heikosti suojattuihin Wordpress, Joomla sekä Drupal -sivustoihin. Erilaiset tekoälyverkostot skannasivat sisällönhallintajärjestelmien asennuksia ja tämän jälkeen yrittivät kirjautua sisään käyttäjätunnuslistaa hyväksikäyttäen, joka sisälsi noin tuhat yleisintä käyttäjänimi ja salasana yhdistelmää. Hyökkäysten luoma ruuhka aiheuttaa tuhoa varsinkin webhotelleja tarjoavien yritysten keskuudessa. Se vahingoittaa palveluntarjoajia eniten, eikä ainoastaan sisään tulevan liikenteen takia, vaan myös sen palvelinhyökkäysten takia. Heti kun yksi palvelin saadaan kaapattua, sitä aloitetaan käyttämään apuna hyökkäyksissä ja yritetään murtamaan vielä isompia kohteita. Kyseisenä ajankohtana arvioitiin, että jopa yli 90 000 sivustoa pelkästään WordPress-alustoilla oli altistunut onnistuneelle hyökkäykselle. Kyseinen hyökkäys oli asiantuntijoiden mukaan erittäin hyvin organisoitu sekä erittäin hajautettu. Yhteensä yli 90 000 eri IP-osoitetta oli mukana hyökkäyksissä, kertoo Sean Valant sosiaalisen median manageri Hostgator.com yrityksestä. (Brute force attack on WordPress, Joomla & Drupal 2013.)

Erilaisia tapoja, joilla onnistuneen hyökkäyksen kohteeksi tulemista voidaan välttää. Yksi näistä tavoista on asentaa kolmannen osapuolen ohjelma, joka mahdollistaa kertakäyttöisten salasanojen käytön tekstiviestin tai puhelimeen ladattavan ohjelman kautta. Kehittäjä, joka pitää sivuston päivitykset ajan tasalla ja suojaa sivuston vahvoilla salasanoilla, ei todennäköisesti joudu tämän kaltaisten hyökkäysten onnistuneeksi kohteeksi. (Brute force attack on WordPress, Joomla & Drupal 2013.)

Drupalin 7.x ja uudemmat versiot sisältävät viestitulvan säätelyasetuksia (englanniksi flood control variables), jotka mahdollistavat kirjautumiskertojen, joko IP-osoitteiden perusteella tai käyttäjätunnusten perusteella. Oletuksena yhdestä IP-osoitteesta voidaan salasanaa yrittää 50-kertaa tunnissa ja yhden käyttäjän salasanaa viisi kertaa kuudessa tunnissa. Kehittäjä voi muokata asetuksista haluamansa määrän yrityskertoja, minimoidakseen onnistuneen brute force –hyökkäyksen todennäköisyyttä. (Brute force attack on WordPress, Joomla & Drupal 2013.)

5 Yleinen tietoturvaohjeistus Drupalin käytölle

Drupalin käytölle löytyy muutamia hyviä tietoturvaohjeistuksia, joita tullaan käymään läpi tässä kappaleessa. Yleisimmät tärkeät ohjeistukset, joita kehittäjän olisi hyvä tietää lähtiessään käyttämään Drupal-sisällönhallintajärjestelmää, tullaan läpikäymään tässä kappaleessa. Ohjeistuksen on tarkoitus olla mahdollisimman helposti ymmärrettävissä ja luettavissa. Drupalilla tehdyt sivustot ovat usein toteutettu eri tavoin, joten on mahdotonta antaa yhtä ohjeistusta, joka toimisi täydellisesti kaikissa sivustoissa. Tämä vaatisi sivuston tarkempaa

tutkimista ja perehtymistä sivustoon syvällisemmin. Shreves ym. (2011, 619) kertoivatkin hyvin, miten kaikilta mahdollisilta uhkilta suojautuminen on lähes mahdotonta sivuston kehittäjältä yksinään, mutta haavoittuvaisuuksia voidaan vähentää huomattavasti noudattamalla muutamia hyviä käytänteitä.

Ensimmäisenä ja ehkä tärkeimpänä ohjeena on, että Drupalin core eli ydin ja moduulit ovat ajan tasalla. Pyri päivittämään versiot aina uuden version ilmestyessä, koska vanhettuneet versiot sisältävät todennäköisemmin haavoittuvuuksia ja tapoja, joilla hyökkääjä pääsee hyväksikäyttämään sivustoa. (James 2014.)

Shreves ym. (2011, 620) mainitsevatkin, että kehittäjän ei tulisi koskaan ladata Drupalin ytimeen liittyviä tiedostoja mistään muualta kuin Drupalin virallisilta sivuilta. Jos kuitenkin näin tapahtuu, on aina varmistettava tiedostojen lähde, toimivuus ja eheys. He kertovat myös, miten jokainen lisättävä moduuli lisää tietoturvariskien määrää, joten olisi hyvä ladata ja asentaa vain sellaisia moduuleita, jotka ovat oikeasti tarpeellisia.

Moduulien latausvaiheessa on hyvä perehtyä sen luotettavuuteen katsomalla arvostelut, latauskerrat, etsimällä verkosta tietoa moduulista sekä varmistamalla sen viimeisin päivitys. Moduuli, jolle ei ole tullut päivityksiä kuukausiin tai vuoteen on tietoruvalliselta kannalta katsottuna vanhettunut, jolloin kannattaa tarkistaa löytyykö vastaavaa moduulia, jolle päivityksiä on ilmestynyt tiheämmin. (James 2014.)

Drupalilla on myös oma uutisosio tietoturvallisuuteen liittyen, jonka käyttäjä voi halutessaan tilata. Tämän avulla saadaan aina uusinta tietoa heti löytyneistä haavoittuvuuksista ja ongelmista. Shreves ym. (2011, 623) suosittelevat myös uutisosion tilaamista, koska se on ainoa tapa pysyä ajan tasalla tärkeistä tietoturvallisuuteen liittyvissä päivityksissä. Kriittisimmissä tapauksissa aikaa päivityksille on vain muutamia tunteja, jolloin nopea reagointi on välttämätöntä.

Kuten kaikessa tietoturvallisuuteen liittyvässä myös Drupalissa, on erittäin tärkeä käyttää vahvoja salasanoja. Siitä muistuttavat myös Shreves ym. (2011, 620), jossa he mainitsevat, että yleisin virhe on unohtaa oletustietoja tai käyttää yleisiä helposti arvattavia tunnuksia järjestelmänvalvojana. Moduulin avulla voidaan lisätä vaihtoehto, joka vaatii käyttäjältä määritellyn vahvuisia salasanoja. Salasanat voidaan myös määritellä vanhentuviksi, jolloin käyttäjän tulee vaihtaa salasanoja määritellyin aikavälein.

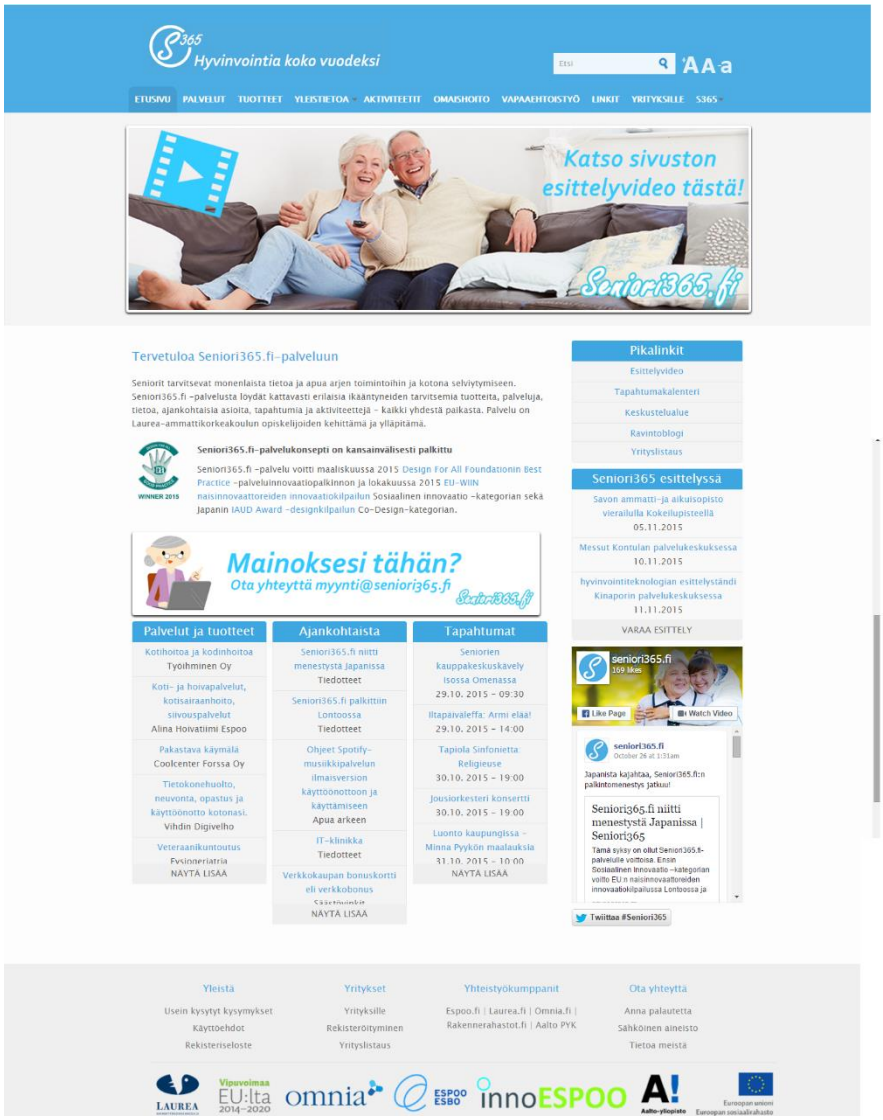
Rajoita tiedostomuotoja, joita voidaan siirtää palvelimelle ja määritä, ketkä voivat siirtää tiedostoja. Jos sivustolla on erillinen mahdollisuus lähettää omia tiedostoja, on tärkeä määrittää, että ainoastaan luotetut käyttäjät voivat näin tehdä. (James 2014.)

Halutessaan voi myös varmistaa sivuston asetukset ja turvallisuuden käyttämällä moduulia, joka tarkastaa sivuston yleisimpien virheiden ja haavoittuvuuksien varalta. Moduulit tarkistavat tietoturvallisuuden perustason ja tarjoavat ratkaisukeinoja löytämiinsä ongelmiin. Tämän kaltaisia moduuleja ovat esimerkiksi Security Review ja Site Audit. Kannattaa myös käyttää sivustoja, jotka testaavat Drupal-sivuston aktiivisilta haittaohjelmilta. Näitä sivustoja ovat esimerkiksi Sucuri (2015) ja Unmaskparasites (2015). (James 2014.)

Käytä aina Drupalin tarjoamia tietoturvaratkaisuja ennen muita vaihtoehtoja. Turhat ja ylimääräiset moduulit on aina hyvä poistaa käytöstä ja sen jälkeen poistaa kokonaan palvelimelta. Vältä oman koodin lisäämistä ja SQL-kyselyiden käyttämistä Drupal API:n sijasta, jos et ole varma, mitä olet tekemässä. (James 2014.)

6 Seniori365.fi–palvelun analysointi

Seniori365.fi-palvelun analysointi aloitettiin luomalla tietoturvallisuuteen liittyvä haastattelu kehitystiimille. Haastattelu kirjoitettiin (Seniori365-haastattelu, 2015) luomamme tietoturvaohjeistuksen perusteella, jossa oli käytetty sähköisten lähteiden alan ammattilaisten yleisiä ohjeistuksia sekä kirjallisten lähteiden esille tuomia ohjeistuksia. Haastattelukysymykset lähetettiin ennakkoon kehitystiimille, jonka jälkeen pidimme kokouksen Otaniemen Laurean toimipisteellä Seniori365.fi-sivuston kehitystiimin kanssa. Haastattelu, joka pidettiin kehitystiimin kanssa, oli puolistrukturoitu ja sen vastauksia käytettiin sivuston analysoinnissa. Samalla sivuston rakennetta tutkittiin sekä kehitystiimin yleistä osaamista tietoturvan osalta.



Kuva 6: Seniori365.fi-sivuston ulkoasu (29.10.2015)

Yllä olevasta kuvasta näkee Seniori365.fi-verkkosivuston tämänhetkisen visuaalisen ulkoasun. Sivuston ulkoasu on tyyliltään elegantti, pelkistetty ja toimiva ratkaisu. Sivuston navigointi on tehty helpoksi, jotta se toimisi kaikenikäisillä käyttäjillä. Heikkonäköisemmät käyttäjät on otettu ulkoasussa huomioon oikeassa yläkulmassa sijaitsevassa osiossa, jossa tekstin kokoa voi muokata suuremmaksi ja pienemmäksi painikkeen avulla.

6.1 Sivuston moduulit

Seniori365.fi-sivustossa on yli sata eri moduulia, joista osa kuuluu Drupalin mukana tulevaan ydinpakettiin, mutta kuitenkin suurin osa on kehittäjien asentamia. Moduulien määrän ja tietoturvallisuussyiden takia, kaikkia kohdesivuston moduuleja ei listata ja käydä läpi. Tarkastellaan kuitenkin tärkeimpiä ja sivuston kannalta oleellisimpia moduuleja.

Verkkosivustolla käytettävää Views-moduulia Tomlinson (2010, 92) kuvailee kirjassaan Beginning Drupal 7, ensimmäiseksi tai toiseksi moduuliksi, joka tulee mieleen, kun kokeneelta Drupal-kehittäjältä kysytään heidän lempimoduuliaan. Views-moduuli on monitoimityökalu, joka mahdollistaa sisällön valitsemisen ja renderoimisen. Se helpottaa Drupalin käyttöä ja koodaamisen tarvetta monissa tilanteissa.

Suurin osa moduuleista on asennettu helpottamaan pääkäyttäjän sivuston muokkausta. sivuston käyttöä ja niillä pystytään määrittelemään sivuston käännöstöitä. Etusivun vaihtuva pääkuva on luotu Flexslider-moduulilla. Responsiivisien eli resoluution mukana skaalautuvia valikoita on luotu Responsive Menus -moduulilla. Sivustolle on lisätty moduuleilla sosiaalisen median integraatioita, Twitter block –moduulilla on helpotettu Twitterin integroimista Seniori365.fi-sivustolle. AddToAny-moduulilla artikkelit ja muut sivuston uutiset on mahdollista jakaa sosiaalisessa mediassa, kuten Facebookissa ja Twitterissä.

Foorumi eli keskustelupalsta ja siellä käytetty CAPTCHA-tunnistus on toteutettu moduulien Advanced Forum ja CAPTCHA avulla. CAPTCHA-tunnistus varmistaa kirjoittajan olevan ihminen, eikä automatisoitu kone tai ohjelma, joka pyrkii levittämään mainoksia tai muuta aiheetonta tietoa. Yritysten rekisteröintilomake on toteutettu Drupalin ulkopuolisella Webform-moduulilla. Palautelomake on luotu myös käyttämällä samaa moduulia. Hakukentän vieressä sijaitsevat tekstin fonttikoon muutokset mahdollistavat napit on luotu Text Resize -moduulilla.

Backup and Migrate -moduuli automatisoi varmuuskopioinnin sivustolla Drupal-tietokantaan, joka on säädetty tietyn aikavälein, mutta moduulilla on myös mahdollista ottaa varmuuskopio manuaalisesti (Tomlinson 2010, 94). Seniori365.fi–sivustolla tämä moduuli on säädetty ottamaan varmuuskopio kerran vuorokaudessa. Sivustolta löytyy varmuuskopioita helmikuuhun 2015 asti, joten moduuli käytännössä toimii myös versiohistoriana.

6.2 Tietoturvahaastattelun analysointi

Kehitystiimi ei ole saanut Drupalin käyttöön liittyvää tietoturvakoulutusta, mikä on alalla hyvin yleistä. Sivuston alkuperäinen kehittäjä oli kuitenkin antanut yleisiä tietoturvaohjeistuksia sivuston käyttöön liittyen. Kehitystiimillä on kuitenkin omakohtaista- ja koulussa hankittua kokemusta hyvistä käytänteistä sekä he mainitsivat opiskelevansa jatkuvasti lisää tietoturvallisuudesta sivuston ylläpitämisen yhteydessä. (Seniori365-haastattelu 2015.)

Tietoturvallisuuteen liittyvien yleisten Drupal-ohjeiden tarve on ajankohtainen. Näin sivustoon kohdistuvia uhkia pystyttäisiin vähentämään huomattavasti. Tämä johtuu siitä, että käyttäessä WWW-pohjaisia sisällönhallintajärjestelmiä suuri riskitekijä on käyttäjä ja niin kuin

VAHTI:ssa todetaan (VAHTI 2008, 23) ”Henkilöstä aiheutuvan riskin hallinnassa haasteena on ihminen”.

Seniori365.fi–palvelun kehitystiimi mainitsi ehkäisevänsä tietoturvauhkia jakamalla uusille käyttäjille mahdollisimman pienet oikeudet, niin että työnteko onnistuu, mutta vahinkoja tapahtuisi mahdollisimman vähän. Sivustolle ei voi myöskään rekisteröidä uutta käyttäjää, ellei ylläpitäjä luo uuden käyttäjän perustietoja. Tämä tarkoittaa sitä, että vain palvelussa työskentelevillä henkilöillä on käyttäjätunnukset sivustolle. Sivustolla käytössä olevia käyttäjiä ovat administrator sekä content manager–tason käyttäjät. Sivuston kehitystiimin jäsenille käyttöoikeudet on jaettu seuraavasti: websovelluskehittäjillä on täydet ylläpitäjän oikeudet (administrator) ja sisällöntuottajilla on rajatut sisällöntuottajan oikeudet (content manager). (Seniori365-haastattelu 2015.)

Käyttäjien roolit ja oikeudet vaikuttivat olevan hyvien käytänteiden mukaisesti Tomlinsonin (2010, 25-37) ohjeistuksen mukaan. Tietoturvallisuussyistä on erittäin tärkeä poistaa turhat ja vanhentuneet käyttäjät, joka oli kehitystiimillä hallussa.

Kehitystiimi mainitsee, että uusien moduulien asennuksessa etsitään aina sopivin vaihtoehto, mutta varmistetaan kuitenkin moduulin päivitysten tiheys, mahdolliset avoimet ongelmat sekä sen suosion. Kaiken edelleen ollessa kunnossa testataan moduuli vielä paikallisesti ennen virallisille sivuille tehtävää muutosta. Kehittäjät ovat ottaneet myös CAPTCHA – moduulin foorumeille ja blogien kommentointiin automaattisten roskapostiviestien estämiseksi. Sivuston versio ja moduulit pidetään myös ajan tasalla. (Seniori365-haastattelu 2015.)

Kehitystiimi oli selvästi yleisellä tasolla hyvin perillä Drupal-sivuston ylläpitämisestä. Moduulien päivitys tapahtuu hyvien käytänteiden mukaisesti. Shreves ym. (2011, 622) kirjoittavatkin, miten ensin on tärkeä varmistaa moduulin laatu, julkaisijan luotettavuus ja kokeilla toimivuus paikallisesti sekä tehdä varmuuskopio sivustosta ennen uuden moduulin asennusta julkiselle sivustolle. Huomioitavaa oli kuitenkin siinä, että kehitystiimillä on tapana poistaa käytöstä moduulit, mutta ei poistaa moduulia kokonaan järjestelmästä. Käyttämättömät moduulit jättävät jälkeensä erilaisia arvoja ja tietokantataulukoita, jotka suurina määrinä voivat alkaa kuormittamaan ja hidastamaan sivuston käyttöä.

Jos moduuli on ollut joskus käytössä, se on jättänyt tietokantaan taulukoita ja arvoja, jotka on hyvä saada pois sivustolta. Niin sanotut jalanjäljet, jotka ovat jääneet muistiin, ladataan PHP:n kautta ja voivat vaikuttaa Drupalin koukkuihin (englanniksi hook). Nämä arvot ja jalanjäljet poistuvat kun moduulin asennus poistetaan onnistuneesti kokonaan järjestelmästä. (Drupal performance tip – removing unused modules 2014.)

Ennakkotapauksia Drupalin tietoturvaan liittyen kehitystiimillä ei varsinaisesti ollut. Kuitenkin tapaus, jossa automatisoitu ohjelma oli kirjoittanut yli 700 anonyymiä mainosta venäjän kielellä sivuston foorumeille, muistui mieleen. Asia on kuitenkin korjattu käyttämällä aikaisemmin mainittua CAPTCHA-moduulia, joka sallii ainoastaan ihmisen kommentoimisen foorumeille käyttämällä kuvan ja tekstin tunnistamismetodia. (Seniori365-haastattelu 2015.)

Kehitystiimi ei seuraa Drupalin tietoturvapäivityksiä virallisella uutisosiolla, eivätkä olleet tilanneet tiedotepostia, koska eivät olleet kuulleet asiasta (Seniori365-haastattelu 2015). Nämä sähköposti-ilmoituksen varoittavat löydetyistä ja mahdollisista tietoturvaheikkouksista Drupaliin liittyen sekä niiden korjaustoimenpiteistä. Mainittuamme asiasta, kehittäjät tiedostivat riskit tähän asiaan liittyen ja aikoivat tehdä parannuksen asiaan.

Tämä on erittäin hyvä tapa pysyä ajan tasalla Drupaliin liittyvissä riskitilanteissa. Pahimmassa tapauksessa, kun kriittinen vika löydetään Drupalin koodista, voi Drupalin-version päivittämiseen olla aikaa vain alle muutama tunti, muuten sivusto voi mahdollisesti olla jo altistunut uhalle. Tämä aiheuttaisi paljon jatkotoimintapiteitä, jotka veisivät hyvin paljon resursseja.

Kehittäjät mainitsivat, että sivustolla vieraileva käyttäjä ei pysty lähettämään mitään tiedostoja ilman käyttäjätunnusta (Seniori365-haastattelu). Aikaisemmin mainitsimme, että sivuston käyttäjät luodaan ylläpitäjien kautta, joten turhia käyttäjiä ei sivustolle pääse kertymään. Tästä johtuen haitallisten tiedostomuotojen lähetys pitäisi olla mahdotonta, ellei uhka tule kehitystiimin sisältä.

6.3 Sivuston analysointi

Seniori365.fi-sivuston analysointi toteutettiin tietoturvaohjeistuksen sekä tietoturvahaastattelun perusteella. Paikan päällä pidetty haastattelu antoi reaaliaikaisesti tietoa kehitystiimin asenteesta ja tuntemuksesta tietoturvaa kohtaan sekä sivuston nykytilasta. Tietoturvahaastattelua käytiin läpi ja sen vastauksia verrattiin tietoturvaohjeistuksessa ilmenneisiin yleisimpiin parannuskehotuksiin.

Seniori365.fi-sivusto tarkistettiin, että Drupal-tiedostot sekä moduulien päivitykset olivat ajan tasalla. Kaikki oletussalasanat sekä käyttäjätunnukset olivat poistettu tai vaihdettu. Security Review –moduulilla skannattiin sivusto yleisimpien virheiden ja uhkien varalta. Tämä moduuli oli saanut useita suosituksia Drupal–yhteisöltä, tietoturvauhkien tarkastamiseen ja minimoimiseen.

	Untrusted roles do not have administrative or trusted Drupal permissions.	Details	Skip
✗	Base URL is not set in settings.php.	Details	Skip
✗	Errors are written to the screen.	Details	Skip
	PHP files in the Drupal files directory cannot be executed.	Details	Skip
✗	Dangerous tags were found in submitted content (fields).	Details	Skip
	Drupal installation files and directories (except required) are not writable by the server	Details	Skip
	Untrusted users are not allowed to input dangerous HTML tags.	Details	Skip
	Private files directory is outside the web server root.	Details	Skip
	No sensitive temporary files were found.	Details	Skip
	Only safe extensions are allowed for uploaded files and images.	Details	Skip
✗	There are Views that do not provide any access checks.	Details	Skip

Taulukko 1: Security Review -tulokset

Tulokset näyttivät hyviltä eikä kriittisiä uhkia näyttänyt löytyvän. Pieniä huomautuksia moduuli antoi kuitenkin siitä, että pääosoite ei ole määritetty settings.php tiedoston kautta. Security Review mainitsi, että esimerkiksi $base_url -funktiota hyväksikäyttämällä voi olla mahdollista kalastella (englanniksi phishing) yksityisiä tietoja. On siis suositeltavaa, että pääosoite asetetaan settings.php -tiedoston kautta. Näin turhat tietoturvauhat saadaan minimoitua.

Toinen huomio tuli virheilmoitusten näyttämisestä sivuston käyttäjille. Sivuston kaikki käyttäjät ovat kuitenkin kehitystiimin jäseniä, joten tämän huomion voi käytännössä sivuuttaa. Se kannattaa kuitenkin huomioida, jos sivustoa kehitetään tulevaisuudessa niin, että käyttäjäksi pystyvät rekisteröitymään muutkin jäsenet, kuin vain kehitystiimiin kuuluvat henkilöt.

Kolmantena uhkana moduuli ilmoitti vaarallisten avainsanojen käytöstä artikkelissa. Yksi sivuista sisälsi Javascript-koodikieltä, jolla haettiin sivupalkki näkyville. Koodi on kuitenkin vaaraksi vain, jos epäluotettavat käyttäjät pääsevät siihen käsiksi.

Viimeinen huomio tuli Views-moduulin käyttöoikeuksista. Moduuli pystyy tarkistamaan onko käyttäjällä oikeutta tehdä muutoksia. Osa sivustolla käytettävästä Views-moduulin sisällöstä ei tarkasta muokkaajan käyttöoikeuksia. Tällä ei kuitenkaan ole merkitystä niin kauan kuin muokkaajat ovat kehittäjiä. On kuitenkin suositeltavaa, että moduulia käytettäessä määriteltäisiin oikeuksia vähintään sen verran, että oikeuksista valitaan käyttöoikeuksien tarkistusvaihtoehto. Näin vähennetään mahdollisia tietoturvauhkia.

Kaikki Security Review moduulin huomiot olivat pienehköjä, mutta kuitenkin huomioon otettavia asioita tietoturvallisuuden kannalta. Ne koskivat suurimmalta osalta kuitenkin käyttäjärajapinnanhallintaa, jonka kehitystiimi on rajannut tehokkaasti. Kehitystiimin voi kuitenkin olla hyvä miettiä jatkon kannalta, tehdäänkö oikeuksien jakamiseen liittyviä toimia etukäteen siltä varalta, että tulevaisuudessa sivustolle pystyy rekisteröitymään myös ulkopuoliset henkilöt vai pysytäänkö nykyisissä ratkaisuissa.

Varmistimme Sucuri Inc. -yrityksen kehittämällä Sucuri (2015) -työkalulla ja saman yrityksen kehittämällä Unmaskparasites (2015) -työkalulla, ettei aktiivisia haittaohjelmia löydy Seniori365.fi-sivustolta. Kaikki näytti verkkotyökalujen mukaan olevan kunnossa, eikä aktiivisia haittaohjelmia löytynyt. Kehitystiimi priorisoi Drupalin omia tietoturvaratkaisuja, joka on kaikkein turvallisin vaihtoehto.

6.4 Seniori365.fi-palvelun yhteenveto

Yhteistyö Seniori365.fi-palvelun kehittäjien kanssa sujui ilman ongelmia. Ennakkoon hankituista taustatiedoista oli ehdottomasti hyötyä ja niiden avulla tietoturvahaastattelun vastausten analysointi oli huomattavasti helpommin toteutettavissa. Hankittu lähdemateriaali avusti sivuston ymmärtämistä, toimintaperiaatteita sekä sen analysointia.

Sivustolla oli paljon aktiivisia moduuleja ja niitä kaikkia päivitetään tiheästi, joka on hyvin tärkeää tietoturvariskien vähentämiseksi. Kehitystiimi miettii ennen moduulin asentamista, miten kulloisenkin tarpeen toteuttaisi parhaiten ja mikä olisi turvallisin vaihtoehto. He tutkivat moduulin kehittäjää, virheitä sekä siitä löytyviä avoimia ongelmia. Jos tämän jälkeen moduuli edelleen näyttää hyvältä, he ottavat sen paikalliseen kokeiluun. Tämänkin jälkeen moduulin näyttäessä hyvältä vaihtoehdolta, ottaa kehitystiimi sen käyttöön itse verkkosivulle. Tämä on tietoturvan osalta esimerkillistä toimintaa, jotta kolmannen osapuolen riskit pystytään minimoimaan.

Tietoturvallisuuden kannalta olisi oleellista, että uusille käyttäjille pidettäisiin aina tietoturvakoulutus, jotta työntekijä ei omalla toiminnallaan aiheuta uhkaa palvelun toiminnalle. Kehitystiimissä hoidetaan käyttäjänhallintaa hyvällä tasolla. Todennäköisyys käyttäjien tuomiin tietoturvauhkiin on paljon pienempi antamalla heille vain tarvittavat käyttöoikeudet. On suositeltavaa, että kehitystiimi tilaisi Drupalin tietoturvauutisten, jotta he pysyvät ajan tasalla tulevista tietoturvaongelmista Drupalin käyttöön liittyen.

Itse sivuston sisällön analysoinnista tuli vain muutamia huomautuksia, mutta niistä suurin osa oli käyttäjärajapinnan hallintaan liittyviä. Tämä asia hoidetaan sivustolla hyvällä tasolla, jo-

ten huomautuksien kohteista ei aiheutunut kovin suurta uhkaa. On suositeltavaa, että kehitystiimi arvioi itse sivuston analysoinnin kohdat ja kehittää sivustoa sen mukaan, jotta tietoturvariskit pysyvät minimaalisella tasolla.

Sivuston tietoturvallisuus on näiden osa-alueiden perusteella hyvällä mallilla. Olisi kuitenkin hyvä huomioida tässä työssä huomioituja riskejä ja uhkia sekä käyttää esille tuotuja ratkaisuja. Osa asioista saattaa tuntua itsestäänselvyyksiltä, mutta tietoturvan takaamiseksi on tärkeää, että niin suuret kuin pienetkin asiat huomioidaan. Näillä keinoilla tietoturvataso pystytään varmistamaan, jolloin sekä sivuston toiminta että tiedostot pystytään turvaamaan.

7 Pohdinta

Työn tavoitteena oli perehtyä Drupal-sisällönhallintajärjestelmän tietoturvallisuuteen. Työssä perehdyttiin myös siihen, miten mahdollisia uhkatilanteita ja haavoittuvuuksia voidaan parhaiten ennaltaehkäistä. Työn pääpainona oli kuitenkin kehittää Seniori365.fi-palvelun tietoturvallisuutta. Työssä edettiin esittelemällä työn lähtökohdat, tavoitteet ja rakenne sekä osaajaverkosto, jolle työ suunnattiin. Tämän jälkeen avattiin sisällönhallintajärjestelmiä yleisesti, jonka jälkeen perehdyttiin Drupalin-ohjelmakehykseen syvällisemmin. Ohjelmistokehyksen tietoturvallisuudesta kerättiin tietoperustaa kirjallisuuslähteistä ja artikkeleista. Kirjallisia ja sähköisiä lähteitä apuna käyttäen rakennettiin yleinen tietoturvaohjeistus, jonka pohjalta Seniori365.fi-palvelun tietoturvallisuutta analysoitiin.

Työn tavoitteet saavutettiin. Drupal-sisällönhallintajärjestelmää ja sen tietoturvallisuutta sekä Seniori365.fi-palvelua käsiteltiin tarvittavassa laajuudessa ja tutkimusongelman kannalta riittävän yksityiskohtaisesti. Seniori365.fi-palvelun tietoturvalisuuden analysoinnista jäi pois fyysisten uhkien ja ulkoisten palveluntarjoajien tuomat riskit, koska tarkoitus oli keskittyä Drupal-ohjelmistokehyksen tietoturvallisuuteen.

Tietoturvallisuus aiheena ja Drupal sisällönhallintajärjestelmänä olivat entuudestaan tuttuja. Drupal-sisällönhallintajärjestelmän tietoturvallisuuden tutkiminen toi esille paljon uutta tietoa, jota syvensi tietoperusta kirjallisuus- ja verkkolähteistä sekä Seniori365.fi-palvelun kehittäjien haastattelu. Yleinen tietoturvaohjeistus auttoi myös ymmärtämään ja hahmottamaan sekä selkeyttämään Drupalin tietoturvallisuutta sekä siinä huomioitavia asioita.

Drupalin tietoturvallisuus on jatkuvassa kehityksessä. On kuitenkin tärkeää, että käyttäjällä on jonkinlainen käsitys Drupalin tietoturvallisuudesta, haavoittuvuuksista ja riskeistä. Tämän takia olisi käyttäjän edunmukaista saada tietoturvaohjeistusta Drupalista ja sen käytöstä. Parempi tietoisuus ja vastuullisuus tietoturvallisuudesta ennaltaehkäisevät uhkatilanteita. Mitä

enemmän käyttäjä tietää ohjelmistokehyksen tuomista riskeistä ja niiden torjunnasta, sitä vähemmän niistä aiheutuu uhkatilanteita.

7.1 Luotettavuus

Opinnäytetyön lähteet valittiin kolmella pääperiaatteella: ensimmäisenä periaatteena oli lähteiden luotettavuus, toisena periaatteena oli lähteiden aiheellisuus ja kolmantena periaatteena oli lähteen ajantasaisuus.

Lähteiden luotettavuuden varmentaminen oli näistä kolmesta periaatteesta haasteellisin, sillä aiheesta löytyi hankalasti kirjallisia lähteitä ja julkisia tutkimuksia. Lähteitä jouduttiin tarkistamaan ja tutkimaan moneen otteeseen, ennen kuin niitä pystyi käyttämään opinnäytetyössä. Tärkeimpiä kriteereitä lähteiden luotettavuuden kriteereissä olivat lähteiden järkevät kommentit, sen luotettava lähde ja tutkimukset, jotka tukivat väitteitä. Nämä kriteerit vakuuttivat lähteen luotettavuutta ja käyttökelpoisuutta opinnäytetyötä ajatellen.

Drupalin tietoturvallisuudesta ei ole paljon aiheeseen kuuluvaa kirjallisuutta, joka hankaloitti lähteiden etsimistä entisestään. Ongelmallista oli myös se, että suurin osa kirjoista mainitsi Drupalin tietoturvallisuudesta ainoastaan muutaman rivin tekstiä, muuten sivuttaen aiheen. Tämän takia kirjallisten lähteiden käyttäminen työssä oli hieman hankalampaa. Tämä oli osaksi syy, miksi lähteissä käytettiin suurimmaksi osaksi verkkolähteitä muutamien kirjojen lisäksi.

Lähteiden ajantasaisuus on etenkin tietoturvallisuuden osalta hyvin tärkeää, koska tietoturvallisuusmetodit eivät ole samoja, mitä ne olivat kymmenen vuotta sitten. Tämän takia tietoturvallisuuteen liittyvät lähteet eivät voineet olla liian vanhoja. Vanhempia lähteitä kelpuutettiin opinnäytetyöhön vain, jos ne sisälsivät niin sanottua yleispätevää perustietoa, joka ei ole vanhentunut vuosien saatossa.

7.2 Eettisyys

Opinnäytetyön eettisyyden säilyttämisen vuoksi haastatteluun vastanneiden kehittäjien henkilötiedot pidetään anonyymeinä. Tutkielmaan osallistuminen oli vapaaehtoista, joten kehittäjien varaamaa aikaa kyselyyn vastaamiseen, haastatteluun sekä kehitysehdotusten lukemiseen ja kuuntelemiseen arvostettiin erittäin paljon. Pyrimme tekemään opinnäytetyöstä eettisesti kestävän ja varmentaa senioreille suunnatun hyvinvointisivuston tietoturvallisuutta. Sivuston tietoturvallisuuden varmentamisella pystytään takaamaan tietoturvallinen toimintatapa ja sivuston jatkuva palveluntarjonta.

7.3 Kehittämisehdotukset

Tämä opinnäytetyö keskittyi pääpainoltaan Drupalin tietoturvallisuuteen. Seniori365.fi-palvelua pystyttäisiin kuitenkin kehittämään jatkossa tulevilla opinnäytetöillä. Tietoturvallisuutta pystyttäisiin kehittämään palvelulle sopivilla aiheilla, kuten esimerkiksi: Tietoturvallisuus ulkoisten palveluntarjoajien osalta, Henkilöstöturvallisuus ja Laitteistoon kohdistuva tietoturvallisuus. Näistä kaikista aiheista voisi sen jälkeen tehdä yhdistetyn tietoturvallisuus yhteisohjeistuksen, jonka avulla Seniori365.fi-palvelun tietoturvallisuus varmistettaisiin ja kerätty tieto laitettaisiin käytäntöön. Tämä takaisi palvelun turvallisen ja tasaisen toiminnan sekä palvelun jatkuvuuden.

Lähteet

Artikkelit:
Goodwin, S. & Vidgen, R. 2002. Content, content, everywhere...time to stop and think? The process of web content management. Computing & control engineering journal, volume 13, issue 2. Huhtikuu. 66-70.

Julkaisemattomat lähteet:
Kehitystiimi, M. 2015. Seniori365-haastattelu. 21.10.2015. Seniori365.fi. Espoo

Kirjalliset:
Hakala, M., Vainio, M., & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland Oy.

Shreves, R. & Dunwoodie, B. 2011. Drupal 7 bible. Indianapolis: Wiley Publishing, Inc.

Tomlinson, T. 2010. Beginning Drupal 7. New York: Springer-Verlag New York, Inc.

Vandyk, J. 2008. Pro Drupal development. New York: Springer-Verlag New York, Inc.

Sähköiset:
Andromeda. 2011. Drupal. Viitattu 29.10.2015.
https://www.drupal.org/project/andromeda

Brute force attack on WordPress, Joomla & Drupal. 2013. Sandeepsankaye. Viitattu 5.8.2015.
https://sandeepsankaye.wordpress.com/2013/04/15/brute-force-attack-on-wordpress-joomla-Drupal/

Castrillo, P. 2011. The 10 most critical Drupal security risks. Viitattu 5.8.2015.
http://www.cameronandwilding.com/blog/pablo/10-most-critical-Drupal-security-risks

Corporate clean. 2011. Drupal. Viitattu 29.10.2015.
https://www.drupal.org/project/corporateclean

Drupal hit by massive data breach. 2013. InfoSecurity. Viitattu 27.7.2015.
http://www.infosecurity-magazine.com/news/drupal-hit-by-massive-data-breach/

Drupal performance tip – removing unused modules. 2014. Enginx. Viitattu 27.10.2015.
http://enginx.com/blog/drupal-performance-tip-removing-unused-modules/

Is Drupal secure. 2015. Drupal. Viitattu 27.7.2015. https://www.drupal.org/documentation/is-Drupal-secure

James, H. 2014. 5 mistakes to avoid on your Drupal website - Number 2: Security. Viitattu 12.8.2015. https://www.acquia.com/blog/5-mistakes-avoid-your-drupal-website-number-2-security

Kapiainen-Heiskanen, P. 2014. InnoEspoo kokosi yrittäjät pikatreffeille. Viitattu 13.10.2015. http://pienyrityskeskus.aalto.fi/fi/current/news/innoespoo_kokosi_yrittajat_pikatreffeille/

Lemos, R. 2014. Drupal sites had “hours” to patch before attacks started. Viitattu 15.7.2015. http://arstechnica.com/security/2014/10/drupal-sites-had-hours-to-patch-before-attacks-started/

Nexus Theme. 2013. Drupal. Viitattu 29.10.2015. https://www.drupal.org/project/nexus

Overview of Drupal 7 vs. Drupal 8. 2012. Drupal. Viitattu 10.7.2015 https://www.drupal.org/node/1674208

The Drupal overview. 2015. Drupal. Viitattu 23.7.2015. https://www.drupal.org/getting-started/before/overview

Third party resources. 2013. Drupal. Viitattu 15.7.2015. https://www.drupal.org/node/289913

Tietoa meistä. 2015. Seniori365. Viitattu 13.10.2015 http://www.seniori365.fi/tietoa-meist%C3%A4

10 most critical Drupal security risks. 2014. Fortune Innovations. Viitattu 12.8.2015. http://birmingham.fortuneinnovations.com/news/10-most-critical-drupal-security-risks

Verkkotyökalut:
Sucuri. 2015. Sucuri Inc.. Käytetty 22.10.2015. https://sitecheck.sucuri.net/

Unmaskparasites. 2015. Sucuri Inc.. Käytetty 22.10.2015 http://www.unmaskparasites.com/

Kuvat

Kuva 1: The Drupal Flow 2015 11
Kuva 2: Nexus teema 13
Kuva 3: Corporate clean teema 14
Kuva 4: Andromeda teema 15
Kuva 5: Tietoturvallisuuden määritelmä..... 16
Kuva 6: Seniori365.fi-sivuston ulkoasu (29.10.2015) 23

Taulukot

Taulukko 1: Security Review -tulokset 27

Liitteet

Seniori365-haastattelu 37

Seniori365-haastattelu

1. Miten teitä on ohjeistettu tietoturvan osalta?

   Tietoturvasta ei ole annettu erikseen koulutuksia, mutta sivuston alkuperäinen kehittäjä on antanut yleisiä tietoturvaohjeistuksia sivuston käyttöön liittyen. Sivuston tietoturvallisuuden opiskelu ja varmistaminen kuuluvat myös osaksi työnkuvaamme.

2. Oletteko miten tutustuneet Drupalin tietoturvaan?

   Olemme tutustuneet Drupalin tietoturvan perusteisiin koulussa ja parantaneet osaamistamme samalla kun olemme kehittäneet sivustoa.

3. Millä keinoin ehkäisette tietoturvariskejä?

   Jaamme uusille käyttäjille mahdollisimman vähän oikeuksia. Annamme vain sen verran oikeuksia, että työn teko onnistuu. Moduuleja asentaessa etsimme ensin sellaisen, joka vastaa toiminnoiltaan haluamaamme. Sen jälkeen varmistamme moduulin päivitysten tiheyden ja sen mahdolliset avoimet ongelmat sekä suosion. Jos kaikki näyttää edelleen hyvältä, testataan moduuli vielä ensin paikallisesti ennen kuin se siirretään live versioon.

   Olemme ottaneet käyttöön myös CAPTCHA – moduulin foorumille sekä blogien kommentointiin automaattisten roskapostiviestien estämiseksi

4. Onko teillä mitään ennakkotapauksia, tietoturvan osalta, joihin olette joutuneet reagoimaan? Jos on, niin miten?

   Varsinaisia vaaratilanteita ei ole ollut, mutta ennen CAPTCHA – moduulin asentamista oli yhden viikonloppuna aikana tullut yli 700 anonyymia foorumi viestiä, jotka sisälsivät lähinnä mainoksia venäjäksi.

5. Seuraavatko Drupalin tietoturvapäivityksiä uutisosiolla? (äkillisten tapausten varalta) Ovatko ne mahdollisesti tilattu sähköpostiin kriittisten tapausten takia?

   Emme olleet kuulleet kyseisestä osiosta, mutta näyttää hyödylliseltä.

6. Onko lähetettävien tiedostojen tiedostomuotoja rajattu mitenkään?

   Kyllä. Sallittuja lähetettäviä tiedostomuotoja ovat ainoastaan gif, png, jpg ja jpeg – tiedostomuodot. Tämä estää haitallisten tiedostomuotojen lähettämistä sivustolle.

7. Otetaanko turhat moduulit pois käytöstä ja poistetaan järjestelmästä?

   Turhat moduulit poistetaan käytöstä, mutta kaikkia ei ole poistettu järjestelmästä.

8. Onko sivustolle lisätty omia koodeja tai muuta Drupalin oman API:n lisäksi?

   Kyllä

9. Onko uudella käyttäjällä salasanavaatimuksia rekisteröityessä? tai vanhentuuko ne?

   Käyttäjätunnukset luodaan aina admin-paneelin kautta, joten rekisteröityminen ei ole tällä hetkellä mahdollista. Salasanat eivät tällä hetkellä vanhene, eikä sen kummempia salasanavaatimuksia ole.

10. Jos teillä tulee tarvetta uudelle moduulille, miten valitsette sen?

    Etsimme moduulin jonka avulla voi toteuttaa halutun toiminnon, varmistamme että sitä päivitetään aktiivisesti, tarkastamme onko siinä avoimia ongelmia, kokeilemme sitä lokaalisti, jossa testaamme sen (mahdolliset bugit sivulla) ja jos olemme tyytyväisiä, otamme sen käyttöön myös tuotantoon. (katso kysymys 3)

Omia muistiinpanoja:

1. Tarkistetaan viimeisimmät Drupal core päivitykset.
   - Päivitykset ovat ajantasalla.
2. Katsotaan Drupalin moduulien
   - Päivitykset on ajantasalla.
3. Kysytään onko default passwordit ja nimet sekä turhat käyttäjät vaihdettu / poistettu.
   - Kyllä
4. Katsotaan Security Review ja Site Audit moduuleilla tilanteita
   - Skannattu
5. Käydään läpi http://sitecheck.sucuri.net/ ja http://www.unmaskparasites.com/ aktiivisten haittaohjelmien varalta.
   - Puhtaat tulokset
6. Priorisoidaan Drupalin tarjoamat tietoturvaratkaisut ennen muiden tarjoamia ratkaisuja.
   - Kyllä