Tampereen yliopisto

Juha Savimäki

AVOIMEN LÄHDEKOODIN VERKKO-KAUPAN SUOJAAMINEN

OpenCart-ohjelmiston tietoturva

Informaatioteknologian ja viestinnän tiedekunta
Kandidaatintyö
09 / 2019

TIIVISTELMÄ

Juha Savimäki: Avoimen lähdekoodin verkkokaupan suojaaminen
Kandidaatintyö
Tampereen yliopisto
Tietotekniikka
09 / 2019

Tässä kandidaatintyössä on päätavoitteena selvittää verkkokaupan tietoturvaan liittyviä epäkohtia valmiin ohjelmiston avulla. Verkkokauppojen määrän kasvaessa, yhä useammat kauppiaat hyödyntävät näitä valmiita ohjelmistoja tunnistamatta niiden tuomia riskejä. Valmiit ohjelmistot verkkokaupoille eivät yleensä ole sellaisenaan turvallisia ratkaisuja verkkokauppiaalle tai kaupassa vierailevalle asiakkaalle. Kandidaatintyössä käydään läpi avoimen lähdekoodin verkkokaupan suojaamiseen käytettävät keskeisimmät turvamekanismit perustamisesta ja päivittämisestä lähtien, aina valmiin kaupan päälle rakennettaviin ylimääräisiin suojauksiin ja rajoituksiin.

Kandidaatintyössä käytetään pohjana valmista ja suhteellisen kevyttä OpenCart-ohjelmistoa verkkokaupoille. Aineistona hyödynnetään alan julkaisuja dokumentaatiosta ohjeistuksiin ja tieteellisiin julkaisuihin, sekä alalla karttunutta työkokemusta. Aineiston avulla saadaan käyttöön tärkeimmät menetelmät tietoturvauhkien selvittämiseen ja haavoittuvuuksien löytämiseen. Kandidaatintyön alussa käydään myös läpi teoriaa yleisellä tasolla, sekä peilataan tätä myöhemmässä vaiheessa käsiteltäviin käytännön toimiin OpenCart-ohjelman osalta.

Tärkeimpinä menetelminä ja haavoittuvuuksien paikkauskeinoina käsitellään CHMOD-arvoja (engl. Change Mode), TLS-sertifikaattia (engl. Transport Layer Security), SEO URL-osoitteita (engl. Search Engine Optimization ja engl. Uniform Resource Locator), .htaccess-tiedostoa, MySQL-tietokantaa (engl. My Structured Query Language) ja tietokantaan liittyviä lomakkeita. Kandidaatintyön jokaisessa vaiheessa todetaan verkkokauppaohjelmiston tarvitsevan lisää suojausta tietoturvauhkia ja haavoittuvuuksia vastaan, sekä esitetään tarvittavat yksityiskohtaiset toimenpiteet.

Kandidaatintyö on laajuudeltaan melko suppea verkkokaupan tietoturvan laajamittaiseen läpikäyntiin, mutta antaa hyvän ymmärryksen olemassa oleviin tietoturvauhkiin ja niiden perusteisiin.

Avainsanat: OpenCart, verkkokauppa, tietoturva, suojaaminen, hakkerointi

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

CHMOD	engl. Change Mode, ohjelma tiedostojen ja hakemistojen käyttöoikeuksien hallintaan
CMS	engl. Content Management System, sisällönhallintajärjestelmä
GD Library	engl. Graphics Drawing Library, ohjelma
GDPR	engl. General Data Protection Regulation, EU:n tietosuojalaki
HTTP	engl. Hypertext Transfer Protocol, protokolla
HTTPS	engl. Hypertext Transfer Protocol Secure, suojattu protokolla
IP-osoite	engl. Internet Protocol address
LDAP	engl. Lightweight Directory Access Protocol, verkkoprotokolla
Mbstring	engl. Multibyte String, PHP-laajennus
MySQL	engl. My Structured Query Language, relaatiotietokantaohjelmisto. Nimessä ”My” ei tarkoita suomeksi ”minun”, vaan on tekijän tyttären nimi.
MySQLi	engl. My Structured Query Language improved, relaatiotietokantaohjelmisto
PHP	engl. PHP: Hypertext Preprocessor, ohjelmointikieli
SEO	engl. Search Engine Optimization, hakukoneoptimointi
SQL	engl. Structured Query Language, kyselykieli
SSL	engl. Secure Sockets Layer, tietoverkkosalausprotokolla
TLS	engl. Transport Layer Security, suojaussertifikaatti
URL	engl. Uniform Resource Locator, verkkosivun osoite
XML	engl. Extensible Markup Language, Standardi / tiedostomuoto
ZIP	engl. Zip, tarkoittaen ”Move at high speed”, tiedostomuoto
Zlib	engl. Zip Compression Library, ohjelmakirjasto

1. JOHDANTO

Verkkokaupat ovat entistä enemmän syrjäyttämässä perinteisiä kaupanteon muotoja ja yhä useammin verkkokauppa pystytetään omatoimisesti ilman teknologista osaamista. Yleensä käytössä on valmis verkosta ladattavissa oleva ohjelmisto, joka on saatu täysin ilmaiseksi, tai geneerinen kuukausimaksullinen kaupallinen versio. Näissä tilanteissa käytettävyys ja ulkoasu menevät yleensä aina tietoturvan edelle, mikä luo monenlaisia riskejä verkkokaupan toimintaan. Asiaan perehtymätön verkkokauppias saa helposti ohjelmistojen mainosteksteistä vääränlaisen näkemyksen siitä, että kaikki asiat ovat tietoturvaa myöten automaattisesti kunnossa, jolloin tarpeelliset toimenpiteet jäävät yleensä poikkeuksetta tekemättä. Tämä aiheuttaa riskejä verkkokauppiaan lisäksi myös verkkokaupassa ostoksia tekevälle asiakkaalle, jonka henkilö- ja maksutiedot voivat joutua vääriin käsiin.

Tämä kandidaatintyö perehtyy avoimen lähdekoodin verkkokauppaohjelmiston tietoturvaan. Ohjelmistoksi on valittu vapaasti ladattavissa oleva OpenCart versio 3.0.0.0 ja työssä tutustutaan sen luontaisiin ominaisuuksiin sellaisenaan. Näin pyritään selvittämään ohjelmiston keskeisimmät tietoturvauhat ja esittämään ratkaisuja niiden korjaamiseksi. Kandidaatintyössä on tarkoituksena tutkia aihetta teoreettisesti erilaisia lähteitä ja karttunutta osaamista hyödyntäen. Tässä kandidaatintyössä ei oteta tarkemmin kantaa käytettävissä oleviin testaustyökaluihin tai -menetelmiin.

Seuraavan luvun teoreettinen osuus käsittelee verkkokaupan tietoturvaa yleisellä tasolla ja esittelee erilaisia näkökulmia tietoturvaan liittyen. Varsinaisen OpenCart-verkkokauppaan kuuluvan vaiheen alussa selvitetään ohjelmiston asettamat vaatimukset palvelimen, versioiden ja muiden ominaisuuksien osalta, jonka jälkeen tutkitaan näiden tuomia uhkia. Tämän jälkeen tehdään katsaus asennusprosessiin ja sen jälkeisiin ohjeistettuihin toimenpiteisiin. Kun teoreettinen asennus kaikkine ohjeistettuine toimenpiteineen on valmis, tutkitaan ohjelmiston hallintapaneelia ja tehdään siellä tarvittavat tietoturvaan liittyvät valinnaiset määritykset. Sitten tarkastellaan asennettua ohjelmistoa eri näkökulmista ja löydetään tietoturvan kannalta kriittisiä uhkia, joihin ehdotetaan korjauksia. Lopuksi vedetään yhteen tässä kandidaatintyössä läpikäydyt oleellisimmat asiat.

2. YLEISESTI VERKKOKAUPAN TIETOTURVASTA

Kokonaisuudessaan verkkokauppa on moniulotteinen rakennelma, joka koostuu palvelimista, tietoliikenneverkoista, erilaisista ohjelmistoista ja päätelaitteista. Verkkokauppaan liittyy myös monia erilaisia rooleja, kuten verkkokauppias, palveluntarjoajat ja verkkokaupan asiakas. Näiden lisäksi verkkokauppa vetää puoleensa epärehellisiä toimijoita, kuten huijareita ja hakkereita. Näillä epärehellisillä toimijoilla on yleensä rahallinen tai maineen kasvattamiseen liittyvä intressi vaikuttaa verkkokaupan toimintaan, murtautua sinne tai pyrkiä saavuttamaan erilaisia aineellisia hyötyjä. Verkkokauppias, palveluntarjoajat tai kaupan asiakas luonnollisesti haluavat välttyä kaikilta näiltä epärehellisten tahojen toimilta.

Asiakkaan luottamus verkkokaupan kokonaisuuteen voi loppukädessä vaikuttaa ostopäätökseen, mikä vaikuttaa olennaisesti verkkokaupan menestymiseen. Pääsääntöisesti palvelinten ja verkkojen ylläpito on asiantuntevissa käsissä, jolloin riittävästä tietoturvan tasosta on huolehdittu ammattimaisella otteella. Riittävän tietoturvan tasosta huolehditaan yleensä seuraamalla turvallisen tuotekehityksen ohjeita, jossa käsitellään tietoturvaa vaatimuksista ja uhkien mallinnuksesta lähtien, aina käyttöönottoon ja ylläpitoon. Samassa Kyberturvallisuuskeskuksen julkaisemassa ohjeessa on viitattu The Open Web Application Security Project -yhteisön julkaisemaan listaan kymmenestä tärkeimmästä verkkosovelluksia koskevasta turvallisuusriskistä. Tämä lista suomennettu alla olevaan Kuvaan 1. [10]

Kuva 1. Kymmenen tärkeintä verkkosovelluksia koskevaa turvallisuusriskiä [10].

Asiakkaan käyttämät päätelaitteet sen sijaan voivat olla käytännössä minkälaisia vain, joten ne ovat jo sellaisenaan suuri tietoturvariski. Monesti suurimpana riskinä on kuitenkin asiakas tai verkkokauppias itse, joka aiheuttaa omalla tahattomalla toiminnallaan vahinkoa tai ei huomaa huijausyrityksiä ajoissa. Tämän kandidaatintyön osalta olennaisin osuus on kuitenkin verkkokauppaohjelmiston turvallisuus.

Verkkokauppaohjelmistoissa on paljon erilaisia tietoturvariskejä, jotka ovat tunnetuimpien valmisohjelmistojen osalta yleisesti tiedossa ja näin ollen vapaasti selvitettävissä Internetistä. Monesti ohjelmistoa ylläpitävät ja jakelevat tahot eivät kuitenkaan tarjoa valmiiksi suojattuja ratkaisuja, vaan tietoturvasta huolehtiminen jää verkkokauppiaan vastuulle. Verkkokauppojen ohjelmistoissa löytyy suunnittelu- ja koodausvirheitä, jotka avaavat hakkereille väyliä päästä luvatta sisään verkkokauppaan, kuten lomakkeiden ja muiden syötteitä sallivien toimintojen kautta. Toisaalta itsestäänselvyydet, kuten tiedosto- ja kansiorakenne suojauksineen tai käyttäjätunnuksien oletusarvot, saattavat

päästää vihamieliset toimijat olemattomalla vaivalla sisään verkkokauppaan.

Verkkokaupoissa liikkuu monesti arkaluonteista tietoa luottokorttien numeroista henkilötietoihin. Usein epärehellisen toimijan motiivina on saada haltuunsa näitä tietoja ja väärinkäyttää niitä. Tällöin nämä kaikki oleelliset tiedot ja niiden haltuun saamiseksi käytettävät metodit on tärkeää tunnistaa ennalta, jotta tiedot pystytään suojaamaan parhaalla mahdollisella tavalla.

Verkkokaupan arkaluonteisten tietojen kaappaamiseksi on tässä luvussa aiemmin mainittujen tapojen lisäksi yleisesti käytössä tietoliikenteen seurantaa ja varsinkin sosiaalista manipulointia. Tietoliikenteen seuranta on laaja kokonaisuus, joka sisältää aiemmin mainitut päätelaitteet, tietoverkot, palvelimet ja ohjelmistot. Sosiaalisessa manipuloinnissa puolestaan hyökätään suoraan käyttäjien, ylläpitäjien tai muiden läheisesti näihin liittyvien tahojen kimppuun. Heitä yritetään erilaisten kekseliäiden keinojen avulla saada luovuttamaan tunnuksensa tai antamaan tarpeettomia käyttöoikeuksia epärehelliselle taholle, jolloin hyökkääminen ja tietojen kaappaaminen helpottuu. [12] Sosiaalista manipulointia käytetäänkin usein ensisijaisena keinona epärehellisessä toiminnassa, varsinkin teknisten järjestelmien ollessa hyvin suojattuja.

Sosiaalista manipulointia vastaan suojautumiseksi on julkaistu useita erilaisia ohjeistuksia. Näissä ohjeistuksissa nostetaan keskeisinä teemoina esille kerroksiin perustuva turvallisuusstrategia ja käyttäjien tietoisuuden lisääminen, joita Tuomas Teirivaara käsittelee havainnollistavasti tutkielmassaan [7, s. 15-18]. Tietoliikenteen seurannan ja sosiaalisen manipuloinnin aiheiden laajuuden vuoksi, kumpaakaan ei käsitellä tässä kandidaatintyössä tämän tarkemmin.

Tietokantoihin tallennetaan yleensä kaikki oleellinen ja arkaluonteinen tieto, joten ne ovat monesti verkossa tapahtuvien hyökkäysten kohteena. Pääsy tietokantoihin voi tapahtua eri reittejä pitkin, joko aiemmin mainittuja keinoja hyödyntäen tai lomakkeiden ja lähdekoodin avulla. Näitä keinoja tarkastellaan OpenCart-ohjelmiston osalta myöhemmin luvussa 4.

Yksinkertaisimmillaan epärehellinen toimija voi päästä tekemään vahinkoa käyttämällä verkkokaupan omia toiminnallisuuksia, jos verkkokaupan hallintaan pääsee kirjautumaan sisään liian helposti. Tämä tapahtuu yleensä ylläpidon huolimattomuuden johdosta, kun käytössä on verkkokauppaohjelmiston oletusarvoiset tunnukset tai sisäänkirjautumista ei ole riittävän hyvin suojattu. Jälkimmäisessä vaihtoehdossa epärehellinen

toimija voi käyttää LDAP-injektiota (engl. Lightweight Directory Access Protocol), jossa erikoismerkkien avulla selvitetään kirjautumistiedot ja avataan tie verkkokaupan varsinaiseen hallintaan [11, s.235-236]. Toinen vastaava erikoismerkkejä hyödyntävä hyökkäystapa on SQL-injektiot [11, s. 241-245]. Tällaisilta keinoilta suojautumista käsitellään myöhemmin tässä kandidaatintyössä eri luvuissa hallintapaneelin ja lomakkeiden osalta.

Kaikkien edellä mainittujen tapojen lisäksi on olemassa monia muita erilaisia hyökkäystapoja, joita tässä kandidaatintyössä ei käsitellä. On kuitenkin hyvä huomata, että jokainen epärehellinen toimija voi käyttää täysin omanlaisiaan keinoja hyökkäykseensä, joten verkkokaupan ylläpidon aktiivisuudella on tärkeä rooli kaupan jatkuvassa suojaamisessa. Yhteistä hyökkäyksille on usein se, epärehelliset tahot kokoavat pienistä tiedonmuruista suuremman kokonaisuuden, jonka avulla voivat toteuttaa aikeensa. Seuraavissa luvuissa käsitellään muutamia yleisiä suojautumiskeinoja tarkemmalla tasolla.

3. VERKKOKAUPAN ASENNUS JA RAKENNE

Ennen verkkokaupan varsinaista asentamista tutustutaan tarkemmin OpenCart-ohjelmiston käyttöä varten asetettuihin vaatimuksiin. Näissä vaatimuksissa on määritelty ympäristö, jonka ohjelmisto vaatii toimiakseen tarkoituksenmukaisesti. Verkkokaupan toiminnan tarkoitus on siellä olevien tuotteiden myyminen, joten kauppiaan näkökulmasta kauppaan pitää pystyä lisäämään myytäviä tuotteita ja ottamaan näistä tilauksia vastaan myyntitapahtuman avulla. Näissä myyntitapahtumissa liikkuu asiakastietojen lisäksi myös maksusuorituksia. Asiakastietoja on Euroopan unionin alueella käsiteltävä GDPR-vaatimusten (engl. General Data Protection Regulation) mukaisesti, mutta tämä kandidaatintyö ottaa asiakastietoihin ja maksusuorituksiin kantaa vain ohjelmiston näkökulmasta eli siitä näkökulmasta, miten tietoa käsitellään ja minne se tallennetaan [13].

3.1 OpenCart-ohjelmiston vaatimukset

OpenCart-ohjelmiston minimivaatimukset sisältävät neljä erilaista kohtaa. Ensimmäisenä mainitaan, että ohjelmisto vaatii palvelimen, johon sen voi asentaa. Tähän suositellaan Apache-pohjaista palvelinta. Toiseksi kerrotaan, että tällä palvelimella täytyy olla valmiiksi asennettuna PHP (engl. PHP: Hypertext Preprocessor), josta käytössä on vähintään versio 5.4. Kolmantena kohtana on listattu, että palvelimelta täytyy löytyä tietokanta ohjelmiston käyttämän ja tuottaman datan tallentamiseksi. Tietokannaksi suositellaan MySQLi-tietokantaa (engl. My Structured Query Language improved), mutta tässä kandidaatintyössä käytetään yksinkertaisuuden vuoksi perinteistä MySQL-tietokantaa. Viimeisenä mainitaan, että palvelimella on oltava seuraavat Taulukon 1 PHP-kirjastot tai moduulit. [3]

Taulukko 1. PHP-kirjastot ja moduulit, muokattu lähteestä [3].

Curl
ZIP (engl. Zip, tarkoittaen ”move at high speed”)
Zlib (engl. Zip Compression Library)
GD Library (engl. Graphics Drawing Library)
Mcrypt
Mbstrings (engl. Multibyte String)
XML (engl. Extensible Markup Language)

Tietoturvan kannalta jokainen näistä vaatimuksista tuo omat riskinsä verkkokauppaan. Julkisessa verkossa palvelin altistuu erilaisille uhille riippuen palomuuristaan, palvelinohjelmistostaan, datastaan ja monesta muusta tekijästä. OpenCart-ohjelmiston vaatimuksissa on vanhentunut PHP-versio, joka altistaa verkkokauppoja tietoturvauhille. Tietokannan tietoturvan riskit liittyvät pääsääntöisesti datan selkokielisyyteen ja erilaisiin hyökkäyksiin, joissa hyödynnetään palvelimelle asennettuja ohjelmistoja. PHP-kirjastot ja moduulit tuovat myös jokainen omanlaisiaan riskejä tietoturvan kannalta, mutta tässä kandidaatintyössä tarkastellaan tilannetta verkkokauppaohjelmiston näkökulmasta, joten kaikki nämä palvelimen omat tietoturvariskit rajataan pois kandidaatintyön tarkastelusta.

3.2 OpenCart-ohjelmiston asennus

Verkkokauppaohjelmiston asennus suoritetaan tässä kandidaatintyössä teoreettisesti. Ohjelmiston asennusta varten haetaan pakattu tiedosto OpenCartin verkkosivuilta. Tiedoston pakkaus puretaan ja tarkastellaan sieltä löytyvää asennusohjetta. [1] Asennusohje sisältää yksinkertaiset ohjeet Linux-palvelimelle asentamista varten, joten kandidaatintyössä edetään ohjeiden mukaisesti.

Asennusprosessi aloitetaan lataamalla kaikki tiedostot ja kansiot palvelimelle verkkokaupan juureen. Näiden lisäksi tehdään ohjeistetut tiedostonimien muutokset. Tiedostonimestä config-dist.php tulee config.php, ja tiedostonimestä admin/config-dist.php tulee admin/config.php. Seuraavaksi tarkastetaan ohjeistetuista tiedostoista ja kansiosta CHMOD-arvot, jotka määrittävät käyttöoikeudet kyseisiin tiedostoihin ja kansioihin. Tarkemmin ilmaistuna CHMOD-arvoilla määritetään, onko kyseistä tiedostoa tai kansiota mahdollista lukea, kirjoittaa tai suorittaa. Yleensä oikeuksia kuvataan numeroarvoilla, mutta myös erilaiset kirjainyhdistelmät ovat käytössä. [1]

Tässä kandidaatintyössä käsiteltävissä CHMOD-arvoissa on aina kolme numeroa, joista ensimmäinen kertoo omistajan oikeudet, toinen ryhmään kuuluvien käyttäjien oikeudet ja kolmas kaikkien muiden oikeudet. Jokaiselle näille käyttäjälle lasketaan käyttöoikeuden kuvaava kokonaissumma kyseisen käyttäjän numeron kohdalle, joka kertoo käyttäjän oikeudesta lukea, kirjoittaa tai suorittaa kyseistä tiedostoa tai kansiota. CHMOD-arvo voi olla mikä tahansa yhdistelmä näistä oikeuksista, tai se voi kieltää kaikki oikeudet. Nämä kokonaissummat lasketaan kertoimilla binääriluvuista ja niitä kutsutaan oktaaliluvuiksi. Alla oleva Taulukko 2 on Linux.fi-verkkosivun oppaasta, ja siinä on lueteltu oktaalilukujen käyttöoikeudet ja suluissa kerrotaan käytetyt kertoimet binäärilaskuissa [8].

Taulukko 2. Oktaalilukujen käyttöoikeudet, muokattu lähteestä [8].

0 = ei oikeuksia
1 = suoritus
2 = kirjoitus
3 = kirjoitus ja suoritus (2+1)
4 = luku
5 = luku ja suoritus (4+1)
6 = luku ja kirjoitus (4+2)
7 = luku, kirjoitus ja suoritus (4+2+1)

Tämän kandidaatintyön OpenCartin asennuksessa tarkastetaan, että halutut tiedostot ja kansiot ovat CHMOD-arvoilla 755. Tästä arvosta nähdään siis, että vain omistajalla on täydet oikeudet, sillä ensimmäinen lukuarvo on 7, eli sen pohjana oleva binääriluku 111 koostuu laskutoimituksesta 1 + 2 + 4 = 7 [8].

Viimeinen vaihe ennen verkkokauppaohjelmiston varsinaisen asennuksen suorittamista on MySQL-tietokannan asentaminen. Tämä asennus tehdään käytettävälle palvelimelle hyödyntäen esiasennettua palvelinohjelmistoa, kuten cPanel, mutta tämä kandidaatintyö ei ota tarkemmin kantaa palvelinohjelmistoihin. MySQL-tietokannan asennusvaiheessa määritellään kannalle käyttäjätunnukset, joita käytetään verkkokaupan asennuksessa [1].

Kun kaikki nämä edellä käsitellyt vaiheet on saatu onnistuneesti suoritettua, siirrytään verkkokauppaohjelmiston sisäänrakennettuun asennusohjelmaan, joka suorittaa verkkokaupan varsinaisen asennuksen. Aluksi asennusohjelmassa luetaan ja hyväksytään käyttöehdot, minkä jälkeen asennusohjelma avaa vaatimusten yhteenvetosivun. Tällä sivulla asennusohjelma vertaa vaatimuksia palvelimen asetuksiin ja versioihin. Kun kaikki nämä ovat minimivaatimusten mukaisia, asennus pääsee etenemään. Seuraa-

vaksi asennuksessa annetaan tietokannan tiedot sekä luodaan erilliset tunnukset verkkokaupan hallintaa varten. Näiden jälkeen verkkokaupan asennusohjelma suorittaa viimeiset vaiheet asennuksesta ja ilmoittaa asennuksen onnistumisesta. Tämä ei kuitenkaan tarkoita sitä, että asennusprosessi olisi suoritettu täysin loppuun, sillä palvelimelta täytyy käydä poistamassa install-asennuskansio, jotta asennettua verkkokauppaa vastaan ei pääsisi hyökkäämään sitä kautta asetustiedostoja hyödyntäen.

3.3 Asennuksen jälkeiset konfiguraatiot

Onnistuneen asennuksen jälkeen tarvitaan vielä erilaisten asetusten konfigurointia, jotta verkkokauppa saadaan toimimaan tarkoituksensa mukaisesti myyntialustana. OpenCart tarjoaa asetuksissa vaihtoehdon käyttää tietoliikennettä suojaavaa sertifikaattia, jolla voidaan salata käyttäjän Internet-selaimen ja palvelimen välinen tietoliikenne. Tällä heikennetään ulkopuolisten tahojen mahdollisuutta salakuunnella liikennettä tai tehdä siinä kulkeviin tietoihin ja viesteihin muokkauksia [9]. OpenCart-ohjelmistossa suojaus toteutetaan TLS-sertifikaatilla, josta OpenCart käyttää vanhentunutta nimeä SSL-sertifikaatti (engl. Secure Sockets Layer). Tämä kandidaatintyö ei ota tarkemmin kantaa TLS-sertifikaatin toimintaan, mutta hankitaan tarvittava sertifikaatti ulkopuoliselta toimittajalta ja asennetaan se palvelimelle käyttövalmiiksi. Tämän jälkeen TLS-sertifikaatti otetaan OpenCart-ohjelmistossa käyttöön laittamalla SSL-suojaus päälle asetuksista löytyvästä valintaruudusta [3].

Ohjelmiston ohjeet eivät kata täysin TLS-sertifikaatin asennusta, sillä ilman seuraavaa muutosta TLS-sertifikaattia ei saada käyttöön verkkokaupassa, eli verkkokaupan HTTPS-muotoiset (engl. Hypertext Transfer Protocol Secure) verkko-osoitteet eivät lähde toimimaan. Asennuksen juuressa sijaitsevat tiedostot config.php ja admin/config.php sisältävät tarvittavat määritykset HTTPS-osoitteen käyttämiselle. Alla oleva esimerkki kuvaa, kuinka näiden tiedostojen avulla voi verkkokaupassa eritellä HTTP- (engl. Hypertext Transfer Protocol) ja HTTPS-osoitteet tai käyttää toista niistä molemmassa tilanteessa, jos esimerkiksi koko verkkokauppa halutaan ulottaa HTTPS-osoitteiden piiriin.

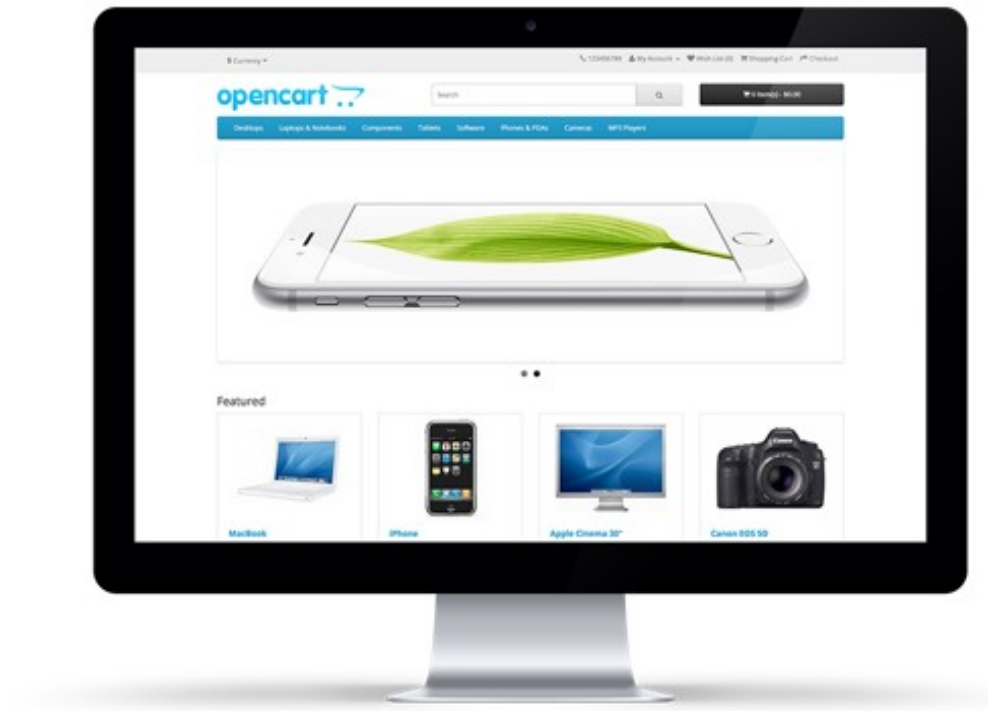
```
// HTTP
define('HTTP_SERVER', 'http://www.omadomain.fi/kauppa/');

// HTTPS
define('HTTPS_SERVER', 'https://www.omadomain.fi/kauppa/');
```

Käytetään edellä olleen esimerkin mukaista konfiguraatiota, jolloin kauppaan ohjelmoitu logiikka huolehtii siitä, mikä osuus sisällöstä käsitellään suojattuna ja mikä voi kulkea suojaamattomana verkossa.

Lisätään seuraavaksi myytävät tuotteet ja niihin liittyvät tiedot. Tämä kandidaatintyö ei ota tarkemmin kantaa lisättäviin tuotteisiin, mutta niiden osalta SEO URL-osoitteet, eli hakukoneoptimoidut sivujen osoitteet, ovat olennaisia tietoturvan kannalta. Kun yksittäisen tuotteen sivua tarkastellaan Internet-selaimessa, niin tuotteen URL paljastaa sivulla vierailevalle taholle osan verkkokaupan rakennetta. Tämä luo osaltaan tietoturvauhan, sillä pelkästään usealla sivulla vierailemalla voi saada selville lähes koko kaupan rakenteen, jota voi hyödyntää myöhemmin mahdollisessa hyökkäyksessä verkkokauppaa vastaan. Tätä uhkaa torjumaan, OpenCart-ohjelmisto tarjoaa hyvän ratkaisun SEO URL-osoitteiden muodossa. SEO URL-osoitteeksi voi määrittää yksittäiselle tuotteelle ja myös lähes kaikille yksittäisille sivuille kustomoidun URL-osoitteen, jolla alkuperäinen URL voidaan piilottaa. Tämä auttaa myös verkkokaupan hakukonenäkyvyydessä, sillä oikeinkäytettynä se voi selkeyttää kaupan markkinoinnillista puolta ja näkyvyyttä eri hakukoneissa.

SEO URL-osoitteet otetaan varsinaisesti käyttöön OpenCart-ohjelmiston hallintapaneelin kautta, mutta sen lisäksi tarvitaan muutoksia juurihakemistossa sijaitsevaan asennuksessa automaattisesti luotuun .htaccess.txt-tiedostoon. Hallintapaneelissa verkkokaupan asetuksista laitetaan SEO URL-osoitteet päälle valintaruudulla. Juurihakemistossa sijaitseva .htaccess.txt-tiedosto nimetään uudelleen .htaccess-tiedostoksi, jolloin se aktivoituu käyttöön OpenCart-ohjelmiston näkökulmasta. Tämän .htaccess-tiedoston sisältä muutetaan vielä SEO URL-asetuksista kyseinen toiminto päälle kirjoittamalla kohtaan SEO URL Settings seuraavanlainen määritys:

 # SEO URL Settings
RewriteEngine On



Kuva 2. Asennetun OpenCart-verkkokaupan etusivu [2].

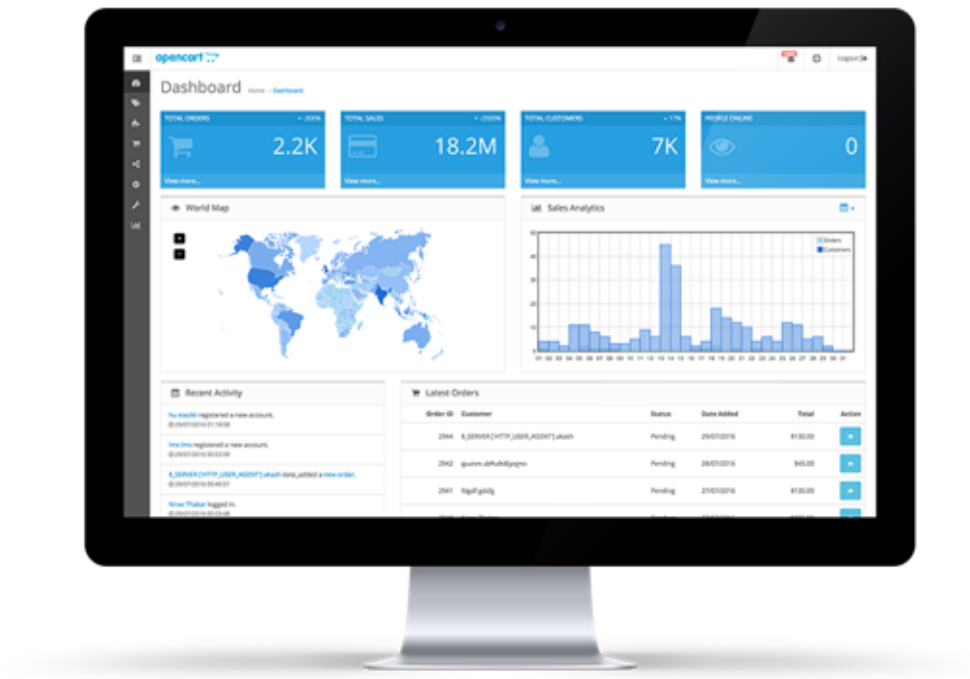
Tämän avulla SEO URL-osoitteet saadaan käyttöön ja niille nimetään jokaisen sivun mukaiset kuvaavat nimet, kuten https://www.omadomain.fi/kauppa/tuotteet. Kuvassa 2 on perusnäkymä valmiin verkkokaupan etusivusta [2].

4. HAAVOITTUVUUDET JA NIIDEN KORJAAMINEN

Tässä luvussa tutkitaan varsinaisen asennetun OpenCart-verkkokaupan haavoittuvuuksia ja selvitetään ratkaisuja niiden korjaamiseksi. Ensimmäiseksi tutkitaan rakenteesta selvästi nähtävillä olevia haavoittuvuuksia, jonka jälkeen etsitään lisää haavoittuvuuksia hakkereiden yksinkertaisimpia hyökkäystapoja käyttäen.

4.1 Hallintapaneeli

OpenCart-ohjelmistossa hallintapaneeli on verkkokaupan asetusten määrittämiseen rakennettu erillinen sisäänkirjautumisen vaativa osio, johon vain ylläpitäjillä ja kaupan henkilökunnalla on tarkoituksenmukainen pääsyoikeus. Hallintapaneelin kautta hoidetaan myös tilaustenhallinta ja asiakaskommunikaatio. Kuvassa 3 on näkymä OpenCart-ohjelmiston hallintapaneelista [2]. OpenCartin rakennetta tutkittaessa huomataan, että verkkokauppaohjelmiston hallintapaneeli sijaitsee oletusarvoisesti aina samassa paikassa asennuksesta riippumatta. Se on siis käytännössä nimetty samalla kansionimellä ja sen sisäänkirjautumissivuun on vapaa pääsy. Huomataan myös, että sisäänkirjautumisyritysten lukumäärää ei ole rajoitettu.



Kuva 3. OpenCart-verkkokaupan hallintapaneeli [2].

Hallintapaneelin haavoittuvuuksien korjaamiseen voidaan käyttää monenlaisia eri ratkaisuja, mutta yksinkertaisimmin ne suojataan piilottamalla ne hakkereilta. Tämä ratkaisu ei tietysti koskaan täysin suojaa verkkokauppaa murtautumiselta, mutta se hidastaa hakkerin työskentelyä merkittävästi. OpenCart-ohjelmistossa koko hallintapaneeli on omassa kansiossaan, joten se voidaan hyvin yksinkertaisesti piilottaa nimeämällä kansio uudestaan [3]. Oletuksena kansion nimi on admin, joten jo pelkästään kääntämällä kansion nimi suomeksi, saataisiin käytännössä karsittua ulkomaiset hakkerit pois etsimästä oletusarvolla nimettyä hallintapaneelia. Tällä kertaa vaikeutetaan myös suomalaisten hakkereiden työtä, sillä heille pelkkä suomenkielinen käännös olisi kohtuullisen helppo arvattavaksi. Nimetään kansio sen sijaan melko satunnaisesti ”eioleasiaa123”, jolloin arvaaminen vaikeutuu. Jotta verkkokauppa toimisi tämän uudelleennimeämisen jälkeen oikein, muutetaan vielä config.php-tiedostossa olevat viisi hallintapaneelin polkua uuden nimen mukaisiksi.

Yritetään seuraavaksi välttää tilannetta, että hakkeri ymmärtäisi heti lähteä etsimään uudelleen nimettyä hallintapaneelin kansiota. Tähän tarkoitukseen sopii mainiosti alkuperäinen admin-kansio, josta voidaan tehdä niin sanottu hunajapurkki, joka houkuttelee hakkerin kimppuunsa. Luodaan siis uusi admin-kansio, sillä alkuperäinen on nimetty toisella tapaa. Tänne tyhjään admin-kansioon lisätään kaikki uudessa verkkokaupan asennuksessa olevat admin-kansion tiedostot, joilla ei ole mitään tekemistä varsinaisen verkkokaupan kanssa. Admin-kansion juuresta löytyy index.php-tiedosto, joka luo kävijälle hallintapaneelin sisäänkirjautumissivun. Lisätään tähän admin-kansiossa sijaitsevaan valekirjautumisen tiedostoon hakkerin IP-osoitteen (engl. Internet Protocol address) selvittävä yksinkertainen PHP-koodi:

$_SERVER['REMOTE_ADDR'];

ja luodaan siitä lokitiedosto. Aina tästä ei ole hyötyä, sillä hakkerit osaavat pääsääntöisesti suojata oman selustansa ja piilottaa varsinaisen IP-osoitteensa. Tämä kannattaa kuitenkin tehdä, sillä IP-osoitteen piilottaminen saattaa unohtua tai sitä ei koeta tärkeäksi, jolloin lokitiedoston avulla saadaan hakkerista olennaista tietoa talteen.

Suojataan vielä tämä uusi admin-kansio pitkällä salasanalla ja estetään pääsy siihen kaikista mahdollisista IP-osoitteista. Asetetaan ensin salasanalla kirjautuminen .htaccess-tiedostoon ja luodaan salasanaa varten erillinen .htpasswd-tiedosto [4]. Tämän jälkeen kirjoitetaan vielä .htaccess-tiedostoon:

deny from all

jolloin millään IP-osoitteella ei pääse kansioon käsiksi. Näin suojattuna hakkeri saattaa kuluttaa turhauttavan paljon aikaa kansion parissa, jolloin oikean hallintapaneelin toiminta olisi turvattuna. Tehdään salasanasuojaus ja IP-rajoitus myös varsinaiselle hallintapaneelille eioleasiaa123, mutta muutetaan IP-rajoitusta niin, että sisään pääsee vain omalla IP-osoitteella. Tehdään samanlainen suojaus myös verkkokaupan Catalog- ja System-kansioille [3].

4.2 CHMOD-arvot

Asennusvaiheessa käytössä oli paljon oikeuksia sallivat CHMOD-arvot tietyille tiedostoille ja kansioille. Nyt osa näistä olisi syytä suojata tiukemmilla oikeuksilla. Muutetaan tiedostojen CHMOD-arvoja seuraavasti Taulukon 3 mukaisesti.

Taulukko 3. Tiedostojen CHMOD-arvot

Tiedosto	CHMOD-arvo
config.php	444
index.php	444
admin/config.php	444
admin/index.php	444
system/startup.php	444

Tällä CHMOD-arvolla 444, tiedostoja pääsee vain lukemaan. Tämä tietysti aiheuttaa sen, että verkkokauppaa kehitettäessä saattaa tulla tilanteita, joissa CHMOD-arvoja pitää käydä muuttamassa, jos näitä kyseisiä tiedostoja pitää muokata. Siinä tilanteessa CHMOD-arvoja muutetaan tiedostojen muokkauksen ajaksi. Muokkaustöiden jälkeen CHMOD-arvot täytyy tietoturvasyistä vaihtaa takaisin arvoiksi 444.

4.3 Tietoturva-asetukset ja virhesivut

Aiemmin luotiin .htaccess-tiedostot tarvittaviin kansioihin suojaamaan kansioita salasanoilla ja rajoittamaan niihin pääsyä IP-osoitteen perusteella. OpenCartin asennuksen juuressa on valmis .htaccess-tiedosto määrittämässä verkkokaupalle ominaisia tietoturva-asetuksia. Tämä tiedosto nimettiin aiemmassa vaiheessa SEO URL-osoitteiden

yhteydessä .htaccess.txt-tiedostosta pelkäksi .htaccess-tiedostoksi, jotta asetukset saatiin käyttöön. Tiedostossa on myös muita valmiiksi kirjoitettuja ehtoja, jotka halutaan ottaa käyttöön. Aloitetaan lisäämällä tiedostoon asetus, joka estää tiedostolistauksen käytön:

Options -Indexes.

Näin ollen ulkopuoliset eivät pääse vapaasti selaamaan verkkokaupan tiedostorakennetta tai kansioiden ja tiedostojen nimiä. Tämä auttaa aiemmin nimetyn hallintapaneelin kansion suojaamista, sillä nyt hakkerit eivät näe kansion nimeä suoraan tiedostolistauksesta, vaan joutuvat arvailemaan sitä. Seuraavaksi estetään suora pääsy tiettyihin tiedostomuotohin määrittämällä tiedostoon rivit:

<FilesMatch "(?i)((\.tpl|\.ini|\.log|(?<!robots)\.txt))">
Require all denied
</FilesMatch>

Samassa .htaccess-tiedostossa on myös selkokielisten URL-osoitteiden käyttöönotto, jolla saadaan piilotettua verkkokaupan tiedostonimiä ja tarkempia polkuja. Näin saadaan lisää oleellista tietoa pois hakkereiden silmistä, mutta myös tehtyä verkkokaupan rakenteesta entistä käyttäjä- ja hakukoneystävällisempi. Selkokielisten URL-osoitteiden käyttöönotossa täytyy myös valita hallintapaneelista Selkokielisten URL-osoitteiden valintaruutu, sekä antaa tuotteille ja tuotekategorioille selkokieliset nimet URL-osoitteita varten.

Valmiiksi juuressa oleva .htaccess-tiedosto ei ota kantaa verkkokaupan virhesivuihin, joten muutetaan ne seuraavaksi. Hakkeri voi hyödyntää verkkokaupan näyttämän virhesivun virheen numeroa ja sen antamaan informaatiota toiminnassaan, joten estetään tämän tiedon antaminen hakkerille. Yleensä rehellisen käyttäjän ei tarvitse olla tietoinen minkälaisen virheen verkkokauppa antaa virhetilanteessa, joten luodaan yleinen virhesivu html-tiedostona, joka kertoo virheen tapahtuneen ja pahoittelee siitä aiheutunutta vaivaa. Tallennetaan tämä tiedosto kansioon error nimellä error.html.

Nyt voidaan lisätä juuressa sijaitsevaan .htaccess-tiedostoon rivi:

ErrorDocument 404 /error/error.html

Tämä rivi ohjaa virheen 404 sattuessa käyttäjän virhesivulle error.html. Seuraavaksi kopioidaan sama rivi jokaiselle mahdolliselle virhenumerolle muuttamalla vain virhenumeroa 404 halutuksi virhenumeroksi. Tämän jälkeen jokainen virhesivu ohjautuu samaan yleiseen virhesivuun, eikä sen perusteella voi enää päätellä mitään virhetilanteesta. Muussa tapauksessa verkkokauppaa vastaan hyökkäävä hakkeri olisi voinut virhenumeron perusteella nähdä, onko tiettyjä tiedostoja tai kansioita olemassa ja mihin kaikkiin niistä on rajattu pääsy.

4.4 MySQL-tietokanta

OpenCart-ohjelmisto käyttää MySQL-tietokantaa, johon luodaan tauluja ja tietueita kaikista yleisimmin muuttuvista tekijöistä, kuten tuotetiedoista ja tilauksista. Näistä jälkimmäinen sisältää kriittisiä tekijöitä tietoturvan kannalta, sillä siihen kuuluu tilaajan henkilökohtaisia tietoja, jotka voidaan yhdistää tilattuun tuotteeseen. Tilauksen maksutiedot kuuluvat myös tietokannan sisältöön, mutta OpenCart-ohjelmistossa käytetään yleensä PayPalin kaltaisia ulkoisia ratkaisuja maksuliikenteen hoitamiseen, joten arkaluonteisimpia tietoja ei aina tallenneta OpenCartin tietokantaan. Ulkoisten maksupalveluiden osalta maksutiedot käsitellään kyseisten palveluiden toimesta ja yleensä OpenCart vain vastaanottaa kuittauksen suoritetusta maksusta, joten maksupalvelut rajataan ulos tästä käsittelystä.

Olennaisin asia OpenCart-ohjelmiston MySQL-tietokannassa on kuitenkin se, että tietokanta on palvelimella selkokielisenä. Tämä tarkoittaa sitä, että pelkkä pääsy tietokantaan tuo lukemattoman määrän dataa mahdollisen tunkeutujan saataville. Suuren datamäärän joukosta voi tietysti olla hidasta ja vaikeaa löytää olennaisia asioita, mutta asiantuntevalle taholle se tarjoaa hyvän tietolähteen, josta löytyy tunnuksien ja salasanojen yhdistelmiä, sekä henkilötietoja.

Tietokannan suojaamista on hyvä suunnitella saatavilla olevan tiedon arkaluonteisuuden pohjalta, sillä MySQL-tietokannan suojaaminen kryptauksella aiheuttaa työläitä ja hidastavia muutoksia OpenCart-ohjelmistossa. Usein myös tietokantaan päässeellä tunkeutuvalla taholla on pääsy samalla palvelimella sijaitsevaan PHP-koodiin, jonka avulla saa selville käytettävän suojausmekanismin ja suojausavaimen. Tietokannan kryptaaminen on kuitenkin hyvä keino suojautua hyökkäyksiä vastaan, jos hyökkääjällä ei ole riittävästi keinoja tai tietoa käytettävänään.

Tässä kandidaatintyössä tarkastellaan perinteistä verkkokauppaa, jossa ei käytetä arkaluontoisia tietoja, joten kannan suojaamiseen ei oteta tarkemmin kantaa. Tästä syystä käydään vain hakemassa OpenCart-ohjelmistoon valmis lisäosa, joka kryptaa tietokannan tiedot ja päivittää samalla OpenCart-ohjelmiston tukemaan tietokannan kryptausta.

4.5 Lomakkeet

OpenCart-ohjelmistossa on useampi lomake erilaisiin käyttötarpeisiin. Lomakkeita on käytössä hallintapaneelissa ja varsinaisen kaupan puolella. Suurin osa lomakkeista on yhteydessä luvussa 4.4 käsiteltyyn MySQL-tietokantaan, sillä lomakkeen kentistä tallennetaan tietoa kyseiseen tietokantaan. Yhteys tietokantaan lisää epärehellisten tahojen mielenkiintoa lomakkeita kohtaan. Hyvin suojatun hallintapaneelin puolella hyökkäysten todennäköisyys pienenee ja kohdistuu suurimmalta osin luvussa 2 kuvattuun sosiaaliseen manipulointiin, mutta varsinaisen verkkokaupan puolella riskit hyökkäykselle ovat oletusarvoisesti suurempia.

Näihin verkkokaupan puolella sijaitseviin lomakkeisiin on OpenCart-ohjelmistossa vapaa pääsy julkisessa verkossa ja tämä on lomakkeiden tarkoituskin, sillä niillä kerätään oleellista tietoa käyttäjiltä. Kerättävään tietoon kuuluu käyttäjän henkilötietoja, tilaustietoja, maksutietoja ja viestintää. Tähän tietoon on vihamielisten toimijoiden helpointa päästä käsiksi PHP-hyökkäyksen avulla, jossa hyödynnetään vihamielisen toimijan omia syötteitä lomakkeessa. Tämän vuoksi onkin tärkeintä, että käyttäjän syötteisiin ei luoteta, kuten Sampo Tolvanen tutkielmassaan toteaa. [5]

Näiltä syötteiltä suojaudutaan parhaiten rajoittamalla ja validoimalla käyttäjän antamia syötteitä. Tässä kandidaatintyössä tehdään rajoitukset ja validoinnit määräämällä jokaiselle lomakkeen kentälle omat sallitut merkkinsä. Käytännössä rajoitetaan kentät käyttämään syötteinä kirjaimia ja numeroita, sekä sallimaan tietyt erikoismerkit vain sähköpostiosoitteen tai viestin ollessa syötteinä. Sähköpostiosoitteelle validoidaan myös sen oikea muoto. [6] Tehdään edellä mainitut validoinnit suoraan OpenCart-ohjelmiston lomakkeiden koodiin. Näin suoraviivaisella toimenpiteellä saadaan tässä kandidaatintyössä käytettävän verkkokaupan lomakkeiden suojaus riittävälle tasolle.

5. YHTEENVETO

Tämän kandidaatintyön perimmäisenä tarkoituksena on ollut analysoida valmista avoimen lähdekoodin verkkokauppaohjelmistoa tietoturvan näkökulmasta ja nostaa esimerkin kautta esille verkkokauppoihin yleisesti liittyviä välttämättömiä tietoturvatöitä. Esimerkkinä käytettyä OpenCart-verkkokauppaohjelmistoa tutkittaessa huomattiin useita tietoturvaan olennaisesti liittyä uhkia, joita ei ohjelmiston valmiin version osalta oltu ratkaistu tai oltu kytketty oletuksena päälle. Jokainen näistä uhkista oli hyvin helposti tunnistettavissa ja niiden ehkäiseminen oli yksinkertaista, tosin joissain tapauksissa myös työlästä.

Tässä työssä tehtiin aluksi katsaus verkkokaupan asentamiseen ja siihen liittyviin konfiguraatioihin. Asennus oli itsessään suoraviivainen prosessi OpenCart-ohjelmiston valmiin asennuspaketin ansiosta. Asennuksen aikana ja sen jälkeen vaadittiin erilaisia konfiguraatioita, joista tärkeimmät olivat oikeiden CHMOD-arvojen asettaminen, TLS-sertifikaatin asentaminen ja SEO URL-osoitteiden käyttöönotto. Näillä suojattiin keskeisimmät tiedostot, tiedon liikkuminen ja hakemistorakenne.

Seuraavaksi tarkasteltiin erilaisia haavoittuvuuksia ja esiteltiin ratkaisuja niiden korjaamiseksi. OpenCart-ohjelmiston hallintapaneeliin rakennettiin lisäsuojausta pienillä määrityksillä ja tehtiin hakkereita varten hunajapurkki. CHMOD-arvot tarkastettiin ja päivitettiin suojaamaan oleellisimpia tiedostoja. Tehtiin muutoksia .htaccess-tiedostoon ja päivitettiin virhesivujen toimintaa. Tärkeimpänä vaiheena käsiteltiin MySQL-tietokantaa ja siihen liittyviä lomakkeita. MySQL-tietokanta todettiin selkokieliseksi, joten se suojattiin käyttämällä kryptausta. Tietokantaan tallentavat lomakkeet suojattiin rajoittamalla käyttäjän syötteessä antamien merkkien käyttöä.

Tämän kandidaatintyön tavoitteet löytää tietoturvauhkia ja niihin soveltuvia korjauksia täyttyivät, sillä OpenCart-ohjelmistosta oli sellaisenaan löydettävissä useita erilaisia uhkia ja näihin yksiselitteisiä tai muuten tiedossa olevia ratkaisuja. Kandidaatintyön pohjalta heräsi erilaisia jatkotutkimusajatuksia, sillä tässä tutkittujen asioiden lisäksi löytyi monia eri kohteita, joita ei kandidaatintyön laajuuden vuoksi saanut lisättyä mukaan. Näihin jatkotutkimusajatuksiin kuuluvat tietoliikenteen erilaiset ratkaisut, laitteistoilla olevien ohjelmistojen vaikutukset ja myös erilaisten maksuliikenteeseen liittyvien ratkaisujen tuomat

näkökulmat. Nämä voisivat soveltua diplomityön tai tohtoritutkinnon laajuuteen paremmin. Tässä kandidaatintyössä tutkittuja asioita olisi mahdollista myös tutkia vielä syvällisemmin laajemmassa kokonaisuudessa.

LÄHTEET

[1] OpenCart 3.0.0.0 asennusohje, OpenCart Ltd. Saatavissa (viitattu 5.7.2019): https://www.opencart.com/index.php?route=cms/download/download&download_id=49

[2] OpenCart demo, OpenCart Ltd. Saatavissa (viitattu 17.9.2019): https://www.opencart.com/index.php?route=cms/demo

[3] OpenCart documentation, OpenCart Ltd. Saatavissa (viitattu 30.5.2019): http://docs.opencart.com/en-gb/introduction/

[4] Password Protection, Htaccess Tools. Saatavissa (viitattu 11.7.2019): http://www.htaccesstools.com/articles/password-protection/

[5] PHP-hyökkäykset, Sampo Tolvanen, TTY, 2012. Saatavissa (viitattu 4.9.2019): https://wiki.tut.fi/Tietoturva/Tutkielmat/PhpHyokkaykset

[6] PHP Tutorial > PHP Forms Advanced Validation. Saatavissa (viitattu 4.9.2019): https://developer.hyvor.com/tutorials/php/forms-validation-advanced

[7] Tuomas Teirivaara, Tietoturva ihmiselementti: sosiaalinen manipulointi, 2010. Saatavissa (viitattu 19.9.2019): http://urn.fi/URN:NBN:fi:jyu-201711134239

[8] Tiedoston Oikeudet, Linux.fi. Saatavissa (viitattu 21.8.2019): https://www.linux.fi/wiki/Tiedoston_oikeudet

[9] The Transport Layer Security (TLS) Protocol Version 1.3, IETF, RFC 8446. Saatavissa (viitattu 21.8.2019): https://tools.ietf.org/html/rfc8446

[10] Turvallinen tuotekehitys, Kyberturvallisuuskeskus, 2018. Saatavissa (viitattu 30.5.2019): https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Turvallinen_tuotekehitys_Suomi_J003_2018.pdf

[11] Matt Walker, All In One CEH Certified Ethical Hacker exam guide 3rd edition, McGraw-Hill Education, USA, 2017, 502 p.

[12] What is Social Engineering, European Union Agency for Cybersecurity. Saatavissa (viitattu 19.9.2019): https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering

[13] Yleinen Tietosuoja-asetus, Sinun Eurooppasi. Saatavissa (viitattu 17.9.2019): https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm