Opinnäytetyö (AMK)

Tietojenkäsittelyn koulutusohjelma

2019

Kenneth Nyman

WORDPRESS-VERKKOSIVUSTON TIETOTURVAA KOSKEVIEN UHKIEN ENNALTAEHKÄISEMINEN

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ AMK | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittelyn koulutusohjelma

2019 | 43 + 3

Kenneth Nyman

WORDPRESS-VERKKOSIVUSTON TIETOTURVAA KOSKEVIEN UHKIEN ENNALTAEHKÄISEMINEN

Jo yli kolmannes internetissä olevista verkkosivustoista on luotu käyttäen WordPressiä, maailman suosituinta sisällönhallintajärjestelmää, jonka suosio on yhä vain kasvussa. Suosion kasvaessa myös tietoturvaa koskevien uhkien määrä kasvaa, kun WordPress-verkkosivustoihin kohdistuvat tietoturvahyökkäykset vain yleistyvät.

Tutkimuksen tavoitteena oli selvittää, minkälaiset uhat vaarantavat WordPress-pohjaisten verkkosivustojen tietoturvaa ja miten näiltä uhilta voidaan suojautua. Toimeksiantajaa varten tuotettiin 12-askelinen tietoturvaopas konstruktiivisena tutkimuksena, joka pohjautuu pragmaattiseen eli käytännönläheiseen tietoon. Oppaassa on WordPress-verkkosivustoon tehtäviä tietoturvaparannuksia sekä askelia niiden käyttöönottoon. Tietoturvaopas näyttää, kuinka suuri merkitys eri asioilla on WordPress-verkkosivuston tietoturvaan, käyttäjätunnuksen päättämisestä lisäosien valitsemiseen. Jo muutamalla tietoturvaoppaan askeleella on mahdollista pienentää WordPress-verkkosivustoon kohdistuvien uhkien määrää.

Opinnäytetyössä käytettiin konstruktiivista tutkimusta, ja lähteistä saatuun tietoon oli helppo luottaa, sillä WordPressistä ja sen tietoturvasta on olemassa tietoa useissa eri lähteissä. Tietoturvaoppaan rakentamiseen saatujen tietojen paikkansapitävyys oli helppo tarkistaa, kun haettu tieto tuki teknistä toimivuutta.

Työn toimeksiantaja, hosting-palveluntarjoaja Domainkeskus käyttää tietoturvaopasta omilla kotisivuillaan valistaakseen asiakkaidensa tietämystä omien verkkosivustojensa tietoturvan tasosta. Domainkeskuksen kotisivuille tietoturvaopasta tullaan parantamaan kuvallisilla ohjeilla, jotta tietoturvaoppaan askeleet ovat helpompia hyödyntää.

ASIASANAT:

hyökkäykset, uhat, tietoturva, tietoturvaopas, WordPress

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology

2019 | 43 + 3

Kenneth Nyman

PREVENTION OF THE THREATS REGARDING THE SECURITY OF A WORDPRESS-BASED WEBSITE

More than a third of all the websites on the internet have been created using WordPress, the most popular content management system in the world. The popularity doesn't seem to come to an end, which directly reflects to the growing amount of information security threats concerning WordPress-based websites.

The purpose of the study was to find out what kind of threats are endangering the security of WordPress-based websites and how to protect them from these threats. A 12-step information security guide was created for the thesis' commissioner as a constructive research. The research is based on pragmatic and practical information. There is points in the guide how to harden the security of a WordPress-based website. The security guide will point out how important different things are to the security level of a WordPress-based website – all the way from choosing a username to the selection of different plugins. It is possible to reduce the threats a WordPress-based website is facing by following even a few of the security guides steps.

Constructive research was used in the thesis because there is a lot of information found in different sources regarding WordPress and its security. The information from the sources was easy to rely on, as the same information was found from several sources. The correctness of the information used to build the security guide was easy to confirm, as the information supported technical functionality.

The commissioner of this thesis, hosting service provider, Domainkeskus, uses the security guide on its own website to educate its customers about the level of security of their own websites. The security guide will be improved on the website of the commissioner, with a pictorial guide to help take advantage of the steps in the information security guide.

KEYWORDS:

attacks, information security, information security guide, threats, WordPress

SISÄLTÖ

LIITTEET

KUVAT

SANASTO

Botti	Ohjelma, joka suorittaa sille määrättyjä automatisoituja tehtäviä
Brute-force	Hyökkäys, jossa arvataan salasanaa monta kertaa peräkkäin
CAPTCHA	Testi joka erottaa botit ihmisistä, Completely Automated Public Turing test to tell Computers and Humans Apart
CMS	Sisällönhallintajärjestelmä, Content Management System
DoS	Palvelunestohyökkäys, Denial of Service
DDoS	Hajautettu palvelunestohyökkäys, Distributed Denial of Service
GPLv2	Vapaan lähdekoodin lisenssi, General Public License, version 2
PHP	Palvelinpuolen ohjelmointikieli
SQL	Ohjelmointikieli tietokantojen hallintaan
SQLi	SQL-Injektio
WordPress	Avoimen lähdekoodin sisällönhallintajärjestelmä
XSS	Koodinsyöttöhyökkäys, Cross-site scripting

1 JOHDANTO

Internetissä on yli 1,6 miljardia verkkosivustoa (Internet Live Stats 2019). Sivustoista yli puolet on tehty jollakin sisällönhallintajärjestelmällä. WordPress on yksi niistä, ja se on ollut jo vuosia maailman suosituin sisällönhallintajärjestelmä lukuisten ominaisuuksiensa ansiosta (W3Techs 2019a). Suosion vuoksi jokainen WordPress-pohjainen verkkosivusto on kiinnostava kohde hyökkääjille, eikä WordPressin tietoturvaan säännöllisin väliajoin kohdistuva kritiikki ainakaan karkota hyökkääjiä. Tekniikka ja hyökkääjien taidot kehittyvät jatkuvasti, joten mikä sen parempi kohde kuin sisällönhallintajärjestelmä eli CMS (content management system), jonka osuus kaikista internetsivuista on lähes kolmanneksen (W3Techs 2019b). Ei siis ihme, jos WordPress ja tietoturva samassa kontekstissa luovat negatiivisen mielikuvan asiantuntijoille.

Riippumatta siitä, mitä sivustoille yritetään tehdä, on se mahdollista käyttämällä WordPress-sivuille ladattavia lisäosia. WordPress-yhteisössä on olemassa suosittu sanonta: ”Siihen on olemassa lisäosa” (WPBeginner 2017). Sanonta on saanut merkityksensä siitä, että sivustoille ladattavia lisäosia on jo yli 50 000 (WordPress 2019a). WordPress-sisällönhallintajärjestelmä itsessään, eli WordPressin ydin ei ole se suurin tietoturvariski, vaan kolmannen osapuolen palvelut, niin kuin nämä asennettavat lisäosat sekä teemat, joita käyttäessä annat niille oikeuden kirjoittaa koodia sivustollesi.

Tämän opinnäytetyön tarkoitus on selvittää, minkälaisia uhkia WordPress-pohjaisiin sivustoihin kohdistuu, mitä haittaa niistä on, mistä nämä uhat syntyvät ja miten niiltä voi suojautua. Toimeksiantajana toimii kotimainen hosting-palveluntarjoaja Domainkeskus, jonka asiakkaina ovat niin yritykset kuin luonnolliset henkilöt. Toimeksiantaja tulee hyödyntämään tätä opinnäytetyötä varten tehtyä tietoturvaopasta valistaakseen asiakkaidensa tietämystä verkkosivustojensa tietoturvasta.

Tässä opinnäytetyössä käytetään konstruktiivisia tutkimusmetodeja. Osana tutkimusta laaditaan olemassa olevaan tietoon perustuva tietoturvaopas WordPress-sivuston tietoturvan parantamiseksi sekä osoitetaan tietoturvaoppaan oikeudellisuus. Oppaassa tulee olemaan ratkaisuja siitä, kuinka oman sivustonsa tietoturvauhkia voi pienentää tai jopa ehkäistä.

2 WORDPRESS

WordPress on avoimeen lähdekoodiin perustuva web-pohjainen sisällönhallintajärjestelmä. Se on alun perin vuonna 2003 julkaistu blogialustaksi, joka on vuosien mittaan mm. helppokäyttöisyyden, muokattavuuden sekä maksuttomuuden vuoksi noussut maailman suosituimmaksi sisällönhallintajärjestelmäksi. Sen käyttöosuus kaikista sivuista, jotka on tehty käyttäen jotakin sisällönhallintajärjestelmää, on 60 % (W3techs 2019a). Sisällönhallintajärjestelmällä hallitaan verkkosivuston sisältöä. Se yksinkertaistaa verkkosivuille tuotettavan sisällön luomista ja muokkaamista.

WordPress-julkaisujärjestelmällä on mahdollista toteuttaa ja hallita digitaalista informaatiosisältöä kuten esimerkiksi kotisivuja, blogeja, palvelusivustoja, verkkokauppoja ja jopa sovelluksia (WordPress 2019b). WordPressin käyttäjistä on muodostunut suuri yhteisö ja sen ympärille on kasvanut suuri verkosto. Mikäli sivuston kanssa kohtaa jonkin ongelman tai muuten vain kysyy vinkkejä tai apua, on vastaus yleensä nopeasti saatavilla yhteisön monien viestintäkanavien vuoksi (WordPress 2019c).

WordPress, kuten monet muutkin sisällönhallintajärjestelmät ovat PHP-ohjelmointikielellä rakennettuja. PHP on suosituin www-palvelinympäristössä käytettävä ohjelmointikieli web-sivujen luontiin. Sen käyttöosuus kaikista verkkosivuista, jotka käyttävät tunnettua palvelinpuolen ohjelmointikieltä on noin 79 % (W3Techs 2019c). Tietokantana WordPress käyttää MySQL-ohjelmistoa, kaiken tuotetun tiedon varastoimiseen (WordPress 2019d). MySQL-tietokantaa hallitaan SQL-ohjelmointikielellä. MySQL on suosittu PHP:n kanssa käytettävä tietokantajärjestelmä, jonka on vuonna 1995 kehittänyt ruotsalainen yritys nimeltä MySQL AB. MySQL on nimetty toisen perustan tyttären Myn mukaan. Ruotsalaisen MySQL AB:n osti vuonna 2010 maailmanlaajuinen yritys nimeltä Oracle, joka nykyään kehittää MySQL-tietokantajärjestelmää (Refsnes Data 2019; Rieuf 2016). MySQL-tietokantajärjestelmää käyttävät monet maailman tunnetuimmista sivustoista, kuten esimerkiksi Facebook, Twitter, YouTube, ja Netflix (Oracle 2019).

WordPress ei välttämättä olisi noussut niin huimaan suosioon ilman sen ajatusta julkaisemisen sekä avoimen lähdekoodin sisältämistä vapauksista. ”Avoin lähdekoodi on yksi sukupolvemme voimakkaimmista ideoista”, sanoo Matt Mullweg (2011), WordPressin toinen perustaja. Avoin lähdekoodi ei tarkoita vain sitä, että voit tarkastella lähdekoodia, vaan voit maksutta ja vapaasti muokata, kopioida ja jakaa sitä (Open Source Initiative 2019). Tätä ajatusta on tukemassa WordPressin suuri yhteisö ja tästä syystä se on myös

lisensoitu GPLv2:n mukaisesti, mikä tarkoittaa, että kuka tahansa voi käyttää tai muokata sen ohjelmistoa maksutta (Kinsta 2018). GPL eli General Public License, on avoimeen lähdekoodiin perustuva lisenssi. GPL-lisenssi antaa luvan ohjelmiston kaupalliselle käytölle, koodin muokkaamiselle ja sen jakelulle, kunhan muokatun ohjelmiston koodissa on liitettynä lisenssi, muutokset alkuperäiseen ohjelmistoon verrattuna sekä kopio alkuperäisestä ohjelmistosta (FOSSA 2014). WordPress määrittelee sivuillaan perusoikeuksiksi neljä GPLv2 lisenssiin perustuvaa oikeutta:

1. Vapaus käyttää ohjelma mihin tahansa tarkoitukseen
2. Vapaus tarkastella, miten ohjelma toimii, ja muuttaa sitä tekemään haluamasi.
3. Vapaus uudelleenjakoon.
4. Vapaus levittää kopioita muokatuista versioista muille.
   (WordPress, 2019f)

WordPressin toiminnallisuuden laajentamiseksi kuka tahansa voi rakentaa siinä käytettäviä ohjelmistosovelluksia, jotka toimivat WordPress-ohjelmiston päällä - lisäosia ja teemoja. Näiden kolmansien osapuolien palveluiden vuoksi WordPressin toiminnallisuus on lähes rajaton - jokaiseen ongelmaan löytyy lisäosa (WPBeginner 2017). Tästä syystä myös sivuston tekeminen WordPressillä on mahdollista ilman minkäänlaista tietämystä ohjelmointikielistä (yleensä tietämys PHP-, SQL- ja HTML-kielistä on yleinen vaatimus sivuston luomiseksi).

2.1 WordPressin laajennukset

WordPress-yhteisössä on paljon kehittäjiä, jotka tuottavat jatkuvasti uusia laajennuksia muille ladattavaksi, jotta saavutetaan toimintoja, joita WordPress ei oletuksena tarjoa (WordPress 2019g). Lisäosia käytetään ohjaamaan sivuston toimintojen ja ominaisuuksien käyttäytymistä ja teemaa ohjaamaan sisällön esitystapaa (WordPress 2019h).

Lisäosa (eng. plugin) on PHP:llä luoduista funktioista koostuva ohjelmisto, jolla perusohjelmistoon voi tuoda erilaisia toimintoja luomalla uutta tai manipuloimalla vanhaa koodia (Väisänen, 2018). Jos haluaa rakentaa esimerkiksi verkkokaupan, valokuvaussivun, portfolion, Wiki-verkkosivun, tai tehdä vaikka hakukoneoptimointia, ei niihin enää erikseen tarvitse laatia ratkaisua, sillä niihin on jo varmasti ladattavissa oleva lisäosa

(WPBeginner 2017). Pluginit ovat lähes välttämättömiä kunkin WordPress-sivuston toiminnallisuuden parantamiseksi, sillä WordPressissä ei oletuksena ole esimerkiksi lomakkeita. WordPressin tarjoamasta lisäosakirjastosta löytyykin jo yli 50 000 lisäosaa (WordPress 2019a).

WordPressin teema muuttaa sivuston ulkonäköä, mukaan lukien sen pohjaa, eli sivuston syöttökenttiä (mihin kohtaan voi lisätä tekstiä tai kuvia). WordPressin teema koostuu eri ohjelmointikielistä, kuten esim. HTML, CSS, JavaScript ja PHP-kielistä. Teemat sisältävät yleensä vähän yksinkertaista koodia, mistä syystä teemat eivät sisällä paljoa haavoittuvuuksia (Defiant 2018). Teeman muuttaminen muuttaa sivuston ulkonäköä, eli sitä miltä sivustosi näyttää sivuston vierailijalle. WordPressiin on mahdollista ladata kolmannen osapuolien tekemiä teemoja, joita on saatavilla tuhansittain. WordPressin omassa teemakirjastossakin on yli 7000 teemaa (WordPress 2019i).

2.2 Wordpressin tietoturva ja sitä koskevat heikkoudet

Vanhentuneet ohjelmistot, huonosti ylläpidetyt sovellukset ja huonosti konfiguroidut järjestelmät kuuluvat haavoittuvuuksiin, joita hyökkääjät käyttävät hyödyksi. Kun on kyse tietoturvasta ja käytetyimmästä julkaisujärjestelmästä, on riskit ja tietoturvan ylläpito otettava tosissaan.

Kyberturvallisuuskeskus määrittelee tietoturvan seuraavasti: ”Tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan tiedon luottamuksellisuus, eheys ja käytettävyys.” (Kyberturvallisuuskeskus 2019). Tarkoituksena on erilaisten tietojen, järjestelmien ja palveluiden suojaaminen ihmisiltä, joilla ei ole oikeutta niihin.

WordPressin tietoturvatiimi koostuu noin 50 asiantuntijasta, johon kuuluu muun muassa pääkehittäjiä ja tietoturvatutkijoita. Tiimi työskentelee usein myös toisten yritysten sekä julkaisujärjestelmien kanssa yhteistyössä haavoittuvuuksien ratkaisemiseksi. WordPress uskoo vastuulliseen tiedottamiseen ilmoittamalla tietoturvatiimille potentiaalisista haavoittuvuuksista välittömästi sellaisen löydettyä. Haavoittuvuuden varmistuttua ja kun sen vakavuus on määritetty, suunnittelee tiimi korjauksen ongelmaan, mikä voidaan lisätä WordPressin seuraavaan päivitykseen. Riippuen haavoittuvuuden vakavuudesta voi tiimi julkaista jopa välittömän turvapäivityksen. (WordPress 2019f)

Mikään järjestelmä ei ole täysin turvallinen, sillä jokaisessa järjestelmässä on omat haavoittuvuutensa. Olemalla suosituin julkaisujärjestelmä on tietoturvan kannalta sekä

huono että hyvä asia. Mitä suositumpi järjestelmä ja mitä enemmän huomiota järjestelmä herättää, sitä enemmän on hyökkääjiä tutkimassa ja löytämässä tietoturva-aukkoja. Suosion hyvä puoli on se, että WordPressin ympärillä olevaan yhteisöön sekä työntekijöihin kuuluu paljon tutkijoita ja kehittäjiä, jotka korjaavat näitä aukkoja ja oppivat niistä. Mitä enemmän tietoturva-aukkoja löydetään, sitä enemmän niitä myös korjataan ja sitä turvallisempi WordPress on. (Abela 2018)

WordPressin jokaisesta versiosta löydetään haavoittuvuuksia. On vain ajan kysymys, milloin tietyn WordPress-version tietoturva-aukot saadaan selville. Hyökkääjät kohdistavat hyökkäyksensä haavoittuvuuden omaavaan WordPress-verkkosivustoon, oli se sitten blogi, pienyrityksen kotisivut tai suuri uutissivusto. Nämä haavoittuvuudet eivät koske kaikkia WordPress-sivustoja, vaan niitä, joihin ei ole tehty tarvittavia tietoturvaparannuksia. WordPressin tietoturvatiimi korjaa haavoittuvuudet seuraavaan päivitykseen, mutta se ei välttämättä auta, sillä hyökkääjät voivat kohdistaa hyökkäykset sivustoihin, jotka käyttävät tiettyä WordPress-veriosta (Abela 2014). Pahimmillaan yhdestä versiosta, WordPressin 3.8.1 versiosta, on löydetty 70 erillistä haavoittuvuutta (Sucuri 2019). Valtaosa WordPress-asennuksista ovat niin sanotusti suoraan pakasta vedettyjä, joihin ei ole tehty mitään muokkauksia. Tämä aiheuttaa sen, että hyökkääjät osaavat kohdentaa hyökkäyksensä niihin paljon helpommin (Saeed 2017).

Suurin osa, eli lähes neljä viidesosaa kaikista verkkosivustoista on toteutettu käyttäen PHP-ohjelmointikieltä. Yksi suuri syy PHP:n suureen käyttöosuuteen on se, että oletuksena WordPress-verkkosivustot on rakennettu käyttäen sitä. PHP itsessään ei ole yksi WordPressin heikkous, vaan se, että suurin osa WordPress-verkkosivustoista käyttää edelleen vanhentunutta PHP-versiota (W3Techs 2019c). Vanhan PHP-version käyttö voi olla kriittinen heikkous WordPressin tietoturvaan, sillä se tuki on voitu lopettaa, niin kuin tällä hetkellä suurimmassa osassa WordPress-sivustoilla käytössä olevasta PHP 5-versiosta (PHP Group 2019a). Ajan tasalla olevissa, eli tuetuissa PHP-versioissa on edistetty tietoturvaa ja korjattu haavoittuvuuksia (PHP Group 2019b).

Laajennuksia on tuhansittain saatavilla, ja kuten WordPressin ydinkin, ovat laajennuksetkin alttiita haavoittuvuuksille. WordPress-laajennuksen asentaminen edellyttää kolmannen osapuolen koodin lisäämistä WordPress-sivustoon, ja niitä asentaessa tulee myös olla varovainen. Väärän lisäosan asentaminen voi nimittäin aiheuttaa virheitä sivustoilla, hidastaa sivua, luoda tahattoman haavoittuvuuden sivuston tietoturvaan tai jopa sisällyttää tahallisesti haitallista koodia (Kinsta 2018). Haitallinen koodi (eng. mali-

cious code) voi muun muassa muuttaa sivuston ulkonäköä esimerkiksi poliittisen tai uskonnollisen agendan edistämiseksi, kätkeä haitallisia mainoksia sivulle, käyttää sivuston vierailijoiden selaimia kryptovaluutan louhintaan tai vaikka uudelleenohjata vierailija kokonaan toiselle sivustolle (Hughes 2018). Ladattujen ja käytössä olevien lisäosien lukumäärä on verrattavissa sivuston turvallisuuteen. Mitä enemmän laajennuksia lisätään, sitä suurempi riski mahdollisille uhille (Moen 2017). Riski kasvaa entisestään, sillä WordPressissä ei oletuksena ole mahdollisuutta lisäosien automaattiseen päivitykseen.

Suurin osa laajennuksista on ilmaisia, eikä niihin näin ollen tarjota teknistä tukea, joten riskien minimoimiseksi on hyvä kysyä itseltään muutamia kysymyksiä ennen laajennuksen lataamista: Milloin laajennus on viimeksi saanut päivityksen? Onko se yhteensopiva nykyisen WordPress-version kanssa? Minkälaisia arvosteluja laajennus on saanut?

3 HAKKERIT

Kuka WordPress sivuni on oikein hakkeroinut? Miksi sivuilleni on hyökätty? Mitä joku hyötyy hakkeroimalla minun sivuni? Ovat yleisiä kysymyksiä ihmisiltä, joiden sivut on hakkeroitu. Yritän tässä luvussa antaa vastaukset näihin kysymyksiin, avata keitä mahdolliset hyökkääjät ovat ja mitkä heidän yleisimmät tarkoitusperänsä ovat.

Puhuttaessa tietokoneohjelmiston turvallisuuden hajottamisesta ja ohittamisesta käyttäen tietokonetta, puhutaan hakkeroinnista. Hakkerointi itsessään ei ole laitonta, ellei hakkeri vaaranna järjestelmää luvatta (Symantec 2019a). Perinteisesti hakkeri on taitava tietokonealan harrastaja, joka käyttää teknisiä taitojaan ongelmien korjaamiseen, on kiinnostunut ohjelmistoista ja haluaa oppia kuinka tietokoneet toimivat (Rouse 2017). Nykypäivän median mustamaalaus hakkereita kohtaan on kuitenkin johtanut hakkeri-sanan merkityksen muuttumiseen. Hakkerit sekoitetaan krakkereihin, eli henkilöihin, jotka käyttävät teknisiä taitojaan rikolliseen toimintaan henkilökohtaiseksi hyödykseen (Beaver 2018, 8).

Hakkerit jaetaan usein kolmeen erilliseen kategoriaan heidän tarkoitusperiensä vuoksi. Valkohattu-, harmaahattu- ja mustahattuhakkereihin. Nämä termit tulevat vanhoista lännenelokuvista, joissa sankarit usein käyttivät valkoisia hattuja ja roistot mustia (Rouse 2018a).

White-hat hackers (valkohattuhakkeri), joita kutsutaan myös eettisiksi hakkereiksi, toimivat lain oikealla puolella ja etsivät haavoittuvuuksia ohjelmistoista, järjestelmistä tai sivustoista lakien puitteissa turvallisuuden parantamiseksi. Yritykset ja valtiot palkkaavat valkohattuja etsimään haavoittuvuuksia yrityksen järjestelmistä sopimuksellisin rajoittein. Yritykset voivat myös olla asettamatta rajoitteita, jolloin haavoittuvuuksien etsiminen tapahtuu keinolla millä hyvänsä. Usein valkohattuhakkerit työskentelevät itsenäisesti tai yhdessä muiden valkohattujen kanssa. Valkohatut jakavat löytämänsä tiedot haavoittuvuuksista vain asiakkaidensa kanssa (Rouse 2018a). Monet tietoturvatutkijat ovat sitä mieltä, että valkohattuhakkerit parantavat internet-turvallisuutta, sillä heidän hakkerointinsa paljastavat heikkouksia, mikä innostaa muita parempiin turvallisuuskäytöntöihin (Call 2015). “Sometimes you have to demo a threat to spark a solution” on kuuluisa lausahdus kuuluistalta valkohattuhakkerilta, Barnaby Jackilta (Greenberg 2010).

Black-hat hackers eli mustahattuhakkereilla viitataan henkilöihin, jotka murtautuvat tietoverkkoihin, ohjelmistoihin ja sivustoihin omaksi hyödykseen. Monet mustahattuhakkerit tarjoavat tämänkaltaisia palveluita muille ostettaviksi, kuten esimerkiksi löytämiänsä haavoittuvuuksia. Ostajia näille palveluille voivat olla niin yksityishenkilöt, kuin rikollisjärjestötkin (Rouse 2017). Näitä hakkeroinnin palveluntarjoajia kutsutaan vuokrattaviksi hakkereiksi (eng. Hackers for hire). He ovat osa internetin organisoitua rikollisuutta (Beaver 2018, 29). Mustahattuhakkereiden taitotaso vaihtelee harrastelijasta kokeneisiin hakkereihin (Symantec, 2019a). Näitä ovat ne internetin lainsuojattomat, eli se osapuoli, jolta puolustaudutaan.

Grey-hat hackers (harmaahattuhakkeri) - mustahatun ja valkohatun sekoitus. Usein harmaahattuhakkeri yrittää etsiä haavoittuvuuksia järjestelmistä luvatta, ottaakseen yhteyttä näiden omistajiin, pyytäen pientä korvausta haavoittuvuuden korjaamiseksi. Jos järjestelmän omistaja ei vastaa tai noudata pyyntöä, voivat harmaahatut lähettää löytämänsä haavoittuvuuden muille nähtäväksi (Symantec 2019a). Harmaahakkerointi on kiistanalaista, sillä he eivät luontaisesti ole haitallisia aikomuksillaan. Harmaahatut asetetaan mustahattujen ja valkohattujen keskimaastoon, toisten auttamisen ja oman hyödyn välille.

Hyökkäys on paras puolustus. Hakkereiden menetelmät ovat pitkälti samanlaiset, vaikka tavoitteet eroavatkin toisistaan. Havaitakseen ohjelmistojen heikkoudet, on välillä ajateltava ja toimittava kuten hyökkäävä osapuoli. Hyökkäävän osapuolen tarvitsee löytää vain yksi haavoittuvuus, kun taas puolustavan tarvitsee löytää ja korjata ne kaikki.

Beaver (2018) jakaa hakkerit myös taitojensa puolesta kolmeen kategoriaan:

- Script kiddies
- Criminal hackers
- Security researchers

Sciprt Kiddie (hacker wannabe) eli internetin vandaali, hakkeriksi haluava tietokonealan noviisi, joka hyödyntää internetistä löytyviä valmiita työkaluja ohjelmistojen hakkerointiin. Heillä ei välttämättä ole edes mitään ymmärrystä siitä, mitä nämä työkalut tekevät, tai mitä seurauksia niillä on, vaikka osaisivat käyttää niitä (Beaver 2018, 27). Script Kiddie voidaan laskea aloittelevaksi mustahatuksi. WordPress-sivustot ovat oiva kohde heidän hyökkäyksiinsä, sillä he käyttävät valmiita työkaluja valmiiksi haavoittuneisiin kohteisiin.

Criminal hacker eli krakkeri on rikollinen hakkeri, joka aiheuttaa vahinkoa esimerkiksi tuhoamalla tietoja tai käyttämällä niitä omiin tarkoituksiinsa (Kielitoimisto 2018). Krakkerit murtautuvat järjestelmiin ilkein aikomuksin. Nämä henkilöt ovat ammattitasoisia hakkereita, jotka ovat luoneet osan hakkerointityökaluista, joita turvallisuusalankin ammattilaiset käyttävät (Beaver 2018, s.28). Krakkerit rinnastetaan mustahattuihin heidän tarkoitusperiensä vuoksi (Secpoint 2019).

Security researchers - tietoturvatutkijat ovat erittäin teknisiä tietoturva-asiantuntijoita, jotka eivät vain tutki tietokone-, tietoverkko- ja ohjelmistohaavoittuvuuksia vaan myös luovat työkaluja ja koodia niiden hyödyntämiseksi. (Beaver 2018). Usein tietoturvatutkijat ovat valkohattuhakkereita, jotka on palkattu tutkimaan yrityksen järjestelmän haavoittuvuuksia (Rouse 2018a).

3.1 Hakkerien motiivit

Kaikkiin verkkosivuihin kohdistuu hyökkäyksiä, ei pelkästään WordPress-sivuihin. Yli 500 WordPress-sivua luodaan päivittäin, mikä jo itsessään tekee WordPress-sivustoista suosituimman hakkeroimisen kohteen (Lawrence 2018; W3techs 2019d). Suosio ei kuitenkaan kerro mitään siitä mitä hakkerit oikeastaan hyötyvät sivujen hakkeroinneista? Jotta voidaan yrittää ymmärtää sivujen hakkeroinnin hyötyjä, tarvitsee ensin ymmärtää hyökkääjien motiiveja. Nämä hyökkääjät, hakkerit eivät kuitenkaan ole yksi yhtenäinen ryhmä, joten syitä ja motiiveja on monia. Nuixin vuosittaisessa kyberturvallisuusraportissa mainitaan yleisiä syitä, miksi hakkerit hakkeroivat:

- ego tai älyllinen haaste, oppiminen
- sosiaalisen ryhmän status
- rahallinen hyöty
- uteliaisuus tai viihde
- tietyn asian vuoksi tai ilkeyttään
- tietoturvatestaus.

  (Pogue 2017)

Oppiminen – monet oppivat tekemällä ja se pätee myös hakkerointiin. Monet aloittelevat hakkerit hyökkäävät vähemmän suojatuille sivuille oppimistarkoituksessa (WPBeginner 2018). Osa aloittelevista hakkereista ei välttämättä edes ymmärrä, tai halua ymmärtää tekojensa seurauksia. Oppimisen vuoksi hakkerointi ei lopu kokemuksen karttuessa.

Nuixin vuoden 2018 kyberturvallisuusraporttia varten haastateltiin 112 hakkeria, joista 86% sanoi edelleen hakkeroivansa oppiakseen sekä haasteen vuoksi. Oppiminen ja itsensä todistaminen ovat yleisiä syitä, minkä vuoksi WordPress-sivuille hyökätään. Kysymys kuuluukin, mihin joukkoon nämä aloittelevat hakkerit tulevat tulevaisuudessa kuulumaan. (Pogue 2018)

Sosiaalisen ryhmän status – maine on kaikki kaikessa, kun suojellaan omaa identiteettiä piiloutumalla keksityn hakkerinimen taakse. Tämä onkin yksi syistä, minkä vuoksi suuri osa hyökkäyksistä tapahtuu mainetta haaliessa. Mustahattuhakkereiden verkostossa on omat hierarkiansa. Muutamia vuosia sitten tämä verkosto käytti Darkode -nimistä foorumia, missä hakkereilla oli oma arvoasteikko. Tämä arvo muodostui hakkerille siitä, kuinka monet verkkosivut hän oli hakkeroinut sekä kuinka suuria tai tunnettuja hakkeroidut sivustot olivat. Asiakastyytyväisyys sekä vaikeuksien lukumäärä, joita hakkeri oli kohdannut hakkerointien aikana, olivat myös kriteereitä arvon muodostumiseen. Tämä arvo on suoraan verrannollinen hakkerin maineeseen. Arvoasteikkoa ylöspäin ovat kapuamassa niin kokeneet hakkerit kuin aloittelevat Script Kiddiesit. Arvoasteikolla nousemiseenkin on eri motiiveja. Osa hakee vain suosiota ja valtaa, kun toiset hakevat taloudellista hyötyä. Mitä suurempi arvo, sitä korkeammat hinnat voi palveluilleen asettaa. (Lawrence 2018)

Rahallinen hyöty – raha toimii motivaattorina työssä kuin työssä. Hakkeroimalla voi tienata rahaa monella tavalla. Mustahattuhakkerit voivat tienata rahaa esimerkiksi myymällä murretulta sivustolta varastettuja henkilötietoja, upottamalla murretulle sivustolle laittomia mainoksia, vaatimalla lunnaita hakkeroidun sivuston omistajalta tai vaikka varastamalla luottokorttitietoja (Abhiyan 2018). Vaikka rahan tulonlähde eri väristen hattuhakkereiden välillä eroaa täysin, tekevät he paljon samantyyppistä työtä, haavoittuvuuksien etsimistä. Yksi tienaa rahansa palkkana, toinen palkkiona suorittamastaan työstä ja kolmas kiristämällä tai myymällä löytöjään muille.

Tietyn asian vuoksi – politiikka ja uskonto liittyvät hyvin läheisesti tunteisiin, sillä ihmiset suhtautuvan hyvin tunteellisesti poliittisiin ja uskonnollisiin uskomuksiin ja ovat jopa valmiita tekemään rikoksia niiden nimissä (Shinder 2010). Tähän kategoriaan kuuluvat haktivistit ja kyberterroristit. Haktivismi koostuu kahden termin yhdistelmästä: ”hakkeri” ja ”aktivismi”. Haktivistit, toisin sanoen poliittisesti motivoituneet hakkerit, kuuluvat yleensä erillisiin järjestäytyneisiin hakkerointiryhmiin, jotka ajavat jotakin ideologiaa, hakkeroiden sivuja, jotka eivät tue heidän ajatuksiaan. Haktivistit haluavat lisätä ihmisten tietoisuutta asioista ja samaan aikaan pysyä nimettöminä (Beaver 2018, 29). Yksi tunnetuimmista

haktivistiryhmistä on sananvapautta puolustava Anonymous. Anonymous on kerännyt miljoonia seuraajia ympäri maailmaa useilla palvelin- ja verkkosivusto hyökkäyksillään, sekä kybersodan julistuksilla muun muassa Yhdysvaltain Kansallista turvallisuusvirastoa sekä terroristiorganisaatio ISIS:tä vastaan (Abela 2017; Baker 2015; Waqas 2013).

Kyberterrorismi eli internet terrorismi on vakavampi, vaarallisempi muoto haktivismista. Kyberterroristit käyttävät väärin internetin nimettömyyttä uhatakseen tiettyjä ryhmiä, uskontoja, uskomuksia tai poliittisia tahoja. Haktivismin tavoitteena on aiheuttaa sosiaalista tai poliittista muutosta, kun taas kyberterrosmin päämääränä on kylvää pelkoa ja tuhoa (Techopedia 2019a; Techopedia 2018b).

3.2 Kyberrikollisuuden asiantuntijan mietteitä hakkereista

Entisen poliisin, nykyisen IT-ammattilaisen, kyberrikollisuuden asiantuntijan Deb Shinderin (2010) mielestä harvat kyberrikokset tehdään pahoin aikein, vaan niinkin yksinkertaisesta syystä että he, hakkerit kykenevät siihen, eli omaavat taidot hyökkäyksen suorittamiseen. Motiiveina tämän kaltaisissa hyökkäyksissä on yleensä uteliaisuus, itsensä viihdyttäminen, tai kuten aikaisemmin mainittiin, itsensä haastaminen.

Shinderin mukaan tunteet toimivat myös yleisenä motiivina hyökkäyksille. Tunteilla hän tarkoittaa sitä, että kaikkein tuhoisimmat hakkerit toimivat tunteiden vallassa, olipa se tunne sitten viha, raivo, kosto, rakkaus tai epätoivo. Tähän kategoriaan voivat kuulua esimerkiksi kostonhimoiset entiset puolisot ja työntekijät, vihaiset oppilaat tai vaikka tyytymättömät asiakkaat. (Shinder 2010)

Puhuttaessa tietokone- eli kyberrikollisuudesta, on rikollisilla erittäin suuri etumatka lainvalvontaan verrattaessa. Kyberrikollisuuteen erikoistuneet lainvalvontaviranomaiset ovat kuitenkin ahkerasti kehittämässä tietämystään, taitojaan ja välineitään kyberrikollisten kiinniottamiseksi. Jälkien peittely on tärkeä osa kyberrikollista toimintaa kiinnijäämättömyyden varmistamiseksi, minkä suurin osa ammattilaishakkereista myös hallitsevat. Kyberrikollisia on laaja kirjo, mistä syystä rikollisten profilointia ei pidä vähätellä. Hyvin tehty profilointi rajaa etsittäviä rikollisia entisestään. **Shinderin lista** tyypillisistä ominaisuuksista, joita useimmat tietoverkkorikolliset omaavat:

- tekniset taidot (vaihtelee ”Script kiddies” -tason taidoista ammattilaishakkereihin).
- lain laiminlyönti tai niistä piittaamattomuus.

- korkea riskin sietokyky tai jännityksen tarve
- ”kontrollifriikki” -tyyppinen
- nauttii muiden päihittämisestä tai manipuloinnista
- motiivi rikoksen tekemiselle.
  (Shinder, 2010)

4 HYÖKKÄYKSET

Monilla yrittäjillä ja muilla sivuston omistajilla on tietoisuuden puute tietoturvariskeistä ja niiden seurauksista ja usko siitä, ettei heillä ole mitään mitä hakkerit haluavat tai mistä hakkerit hyötyvät. Niin sanottu ”Ei minun sivujani ennenkään ole hakkeroitu, ei hätää.” -mentaliteetti. Vaikka sivuilla ei olisikaan mitään, mistä hyökkääjät voisivat hyötyä vaikkapa rahallisesti, voivat hyökkääjät käyttää murrettuja sivustoja osana suurempia hyökkäyksiä (Rahman 2017).

Sisällönhallintajärjestelmillä luoduista sivustoista WordPress-pohjaiset verkkosivustot valikoituvat selvästi useimmin hyökkäysten kohteiksi (Cimpanu 2019). WordPress-sivustoja uhkaavat hyökkäykset voidaan jakaa kahteen ryhmään; kohdentamattomiin ja kohdennettuihin hyökkäyksiin (Abela 2014).

Kohdentamattomissa, eli automatisoiduissa hyökkäyksissä kohteet valitaan satunnaisesti. Järjestelmiin murtautuminen on yleensä ajatuksena näissä hyökkäyksissä, mutta kohteena ei ole mikään tietty yksilö tai ryhmä. Kohdentamaton hyökkäys saattaa olla verkkosivuston mainokseen piilotettu haittaohjelma, jota uhri pahaa aavistamattaan klikkaa, aloittaen haittaohjelman latauksen, saastuttaen työasemansa (Nichols 2016). Kohdistamattomasta hyökkäykset puhutaan myös silloin, kun hyökkääjät kohdistavat hyökkäyksensä esimerkiksi tiettyyn WordPress-versioon, hyödyntäen siinä olevaa haavoittuvuutta. Tästä hyökkäyksestä puhutaan kohdentamattomana, sillä siinä hyödynnetään internetistä satunnaisia sivustoja etsivää ohjelmaa. Uhreja ei valita yksitellen, vaan uhreihin valikoituu satunnaisesti joukko yksilöitä ja yrityksiä. Ohjelman tarkoituksena on suorittaa lukuisilla sivustoilla kysely, mikä määrittää onko sivustolla käytössä haavoittunut WordPress-versio (Abela 2014).

Kohdennetut hyökkäykset ovat huomattavasti harvinaisempia ja myös vaarallisempia kuin kohdentamattomat hyökkäykset. Kohdennetuissa hyökkäyksissä kohteena voi olla tarkkaan valittu uhri, jonka käyttäjätunnukselle, sivustolle tai järjestelmään halutaan murtautua. Automaattisten työkalujen sijaan hyökkäyksissä toimii ihminen, joka voi käyttää viikkoja, kuukausia tai jopa vuosia aikaa analysoidakseen kohteeksi valitsemaansa verkkosivustoa pienimmänkin haavoittuvuuden löytämiseksi (Abela 2014). Kohdennettuja hyökkäyksiä tekevät niin järjestäytyneet ryhmät kuin uusia tekniikoita opettelevat yksityiset hakkerit. Uutisotsikoissa kirjoitettavista kohdennetuista hyökkäyksistä puhutaan nimellä ”tietomurrot”. Tietomurron uhreiksi on valikoitunut suuria yrityksiä, joilta halutaan

varastaa tietoja (Trend Micro 2015). Uhreihin menneiden vuosien aikana on lukeutunut muun muassa LinkedIn, MySpace, Yahoo, Twitter ja Sony (McCandless 2019). Kohdennettuja hyökkäyksiä tehdään niin tietyn asian vuoksi kuin rahallista hyötyä ajatellen. Tietomurron kohteiksi joutuneilta yrityksiltä voidaan esimerkiksi kiristää rahaa tietomurron salaamiseksi, varastettu tieto voidaan kaupata mustassa pörssissä tai tiedot voidaan vuotaa julkiseksi haktivismin nimissä.

4.1 Hyökkäysmenetelmät

Tietoturva vaatii hyvän puolustuksen laatimisen lisäksi tietyn ajattelutavan. Ajattelutavan, joka pakottaa miettimään asiat hyökkääjän tai niin sanotusti skeptisestä näkökulmasta, kuten esimerkiksi nähdessään uutta teknologiaa tai jonkun uuden markkinoille tuodun keksinnön. Miten tätä voisi käyttää hyväksi? Miten tämän saa epäonnistumaan? Tämä ajattelutapa on tärkeä haavoittuvuuksien löytämiseen ja niiden ennaltaehkäisemiseen, mutta valitettavasti myös hakkerit usein omaavat tämän ajattelutavan (Schneier 2008). Useat menetelmät, joita hakkerit käyttävät osana hyökkäyksiään, ovat alun perin kehitetty tuottamaan jotain positiivista (Symantec 2019c). Näitä menetelmiä käyttäen luodaan automatisoituja työkaluja, joita käytetään osana laajamittaisia kohdentamattomia hyökkäyksiä (F-Secure 2019).

Botit ovat yksi esimerkki automatisoiduissa hyökkäyksissä käytettävänä aseena - hyvän teknologian käyttämisestä pahoihin tarkoituksiin. ”Botti” on peräisin sanasta ”robotti”. Botti on tietokoneohjelma tai komentosarja (eng. script) joka suorittaa sille määrättyjä automatisoituja tehtäviä. Tehtävät ovat usein erittäin yksinkertaisia, toistuvia ja aikaa vaativia, joihin ihminen käyttäisi huomattavasti enemmän aikaa. Botti on yhteydessä komentopalvelimeen, minkä kautta sitä ohjataan. Boteilla on useita käyttötarkoituksia, riippuen siitä, mitä ne on ohjelmoitu tekemään. Useimmiten niitä käytetään web-indeksoijana tai vuorovaikuttajana jossakin chat-palvelussa (Symantec 2019c; Cisco 2018). Päivittäin vastaantuleva botti on Googlebot, Googlen hakukoneen oma verkkoindeksointirobotti. Se etsii ja lukee verkkosivustoilta uutta ja päivitettyä sisältöä sekä ehdottaa, mitä pitäisi lisätä Googlen omaan hakemistoon (Google 2019). Indeksointibotti on käytännössä pieni robotti, joka vierailee verkkosivustoilla, etsien niissä tehtyjä muutoksia, jotta sivustoilla tehdyt muutokset voidaan ottaa hakukoneen tuloksissa huomioon.

Bottien useiden käyttötarkoitusten huono puoli on se, että niitä on helppo käyttää myös haitallisiin tarkoituksiin. Botteja käytetään usein itsestään levittyvänä haittaohjelmana,

mikä voi naamioitua laitteen normaalisti suorittamaksi prosessiksi ja näin ollen jää uhreilta helposti huomaamatta. Haittaohjelman tarkoitus on saastuttaa useita isäntälaitteita ja muodostaa yhteys takaisin komentokeskukseen, mistä saastuneita laitteita on helppo ohjata. Näitä laitteita voivat olla niin tietokoneet kuin älypuhelimet ja muutkin älylaitteet. Botit voivat muun muassa kerätä sähköposteja roskapostituslistaa varten, lähettää roskapostia tai tallentaa näppäinpainalluksia saastuneilta laitteilta keräten käyttäjätietoja, kuten tunnuksia ja salasanoja tai maksutietoja. Haittaohjelmia piilotetaan sivustojen mainoksiin ja roskapostiviesteihin (Symantec 2019b). Saastuneen laitteen käyttöoikeuksia myydään hakkerifoorumeilla, sillä niillä voi tehdä hyökkäyksiä muihin laitteisiin tai yhdistää saastuneen laitteen osaksi bottiverkkoa (O'Donell 2018).

Bottiverkko koostuu toisiinsa yhdistetyistä tietokoneista ja laitteista, joita ohjataan samasta paikasta, tekemään tiettyjä toimintoja. Näitä bottiverkossa olevia laitteita kutsutaan nimellä ”botti” tai ”zombie”. Bottiverkko koostuu tyypillisesti sadoista tai tuhansista saastuneista tietokoneista. Bottiverkkojen käyttö hakkereiden keskuudessa on suosittua, sillä bottiverkon käyttö mahdollistaa kaikkien bottiverkkoon yhdistettyjen tietokoneiden fyysisen ja verkollisen tehon kohdistamisen yhteen hyökkäykseen (O'Donell 2018). Suurimmat bottiverkot ovat koostuneet sadoista tuhansista saastuneista laitteista. Joulukuussa 2018 viranomaisille ilmoitettiin yli 20 000 saastuneen WordPress-asennuksen bottiverkosta. Tämä bottiverkko teki automatisoituja hyökkäyksiä muita WordPress-sivustoja vastaan (Cimpanu 2018). Bottiverkkoa käytetään aseena molemmissa, sekä kohdennetuissa että kohdentamattomissa hyökkäyksissä.

4.2 Yleisiä WordPress-sivuihin kohdistuneita hyökkäyksiä

WordPressistä on tähän päivään mennessä löydetty 3021 erillistä haavoittuvuutta, joita voidaan käyttää hyväksi osana hyökkäyksiä. Suurin osa haavoittuvuuksista esiintyy useassa WordPress-versiossa, mikä tekee hyökkäämisestä vieläkin helpompaa (Sucuri 2019). Tässä luvussa listaan suosiojärjestyksessä yleisiä WordPress-sivustoihin kohdistettavia hyökkäyksiä, joissa käytetään hyväksi WordPressin haavoittuvuuksia.

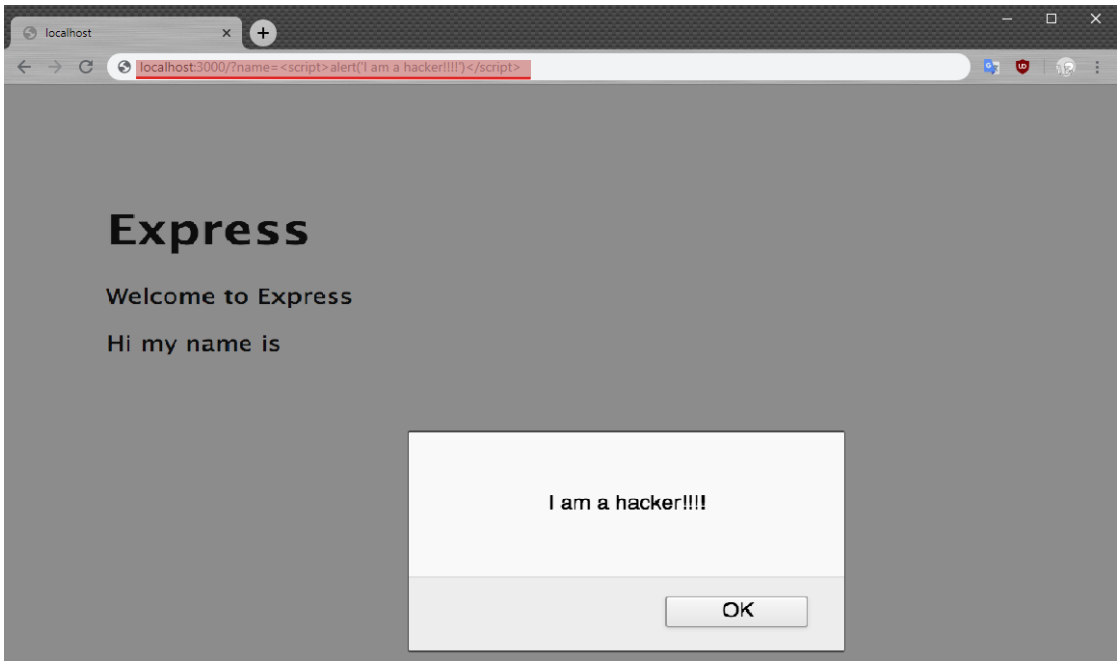
4.2.1 XSS – Cross-site scripting

Cross-site scripting (XSS) on koodinsyöttöhyökkäys, jossa käytetään hyväksi haavoittuvuutta, jonka avulla hyökkääjä voi ujuttaa ulkopuolista dataa, kuten esimerkiksi haitallista

koodia sivustolle. Tämä haavoittuvuus mahdollistaa lomakkeen täytön haittakoodilla, sen sijaan että ne täytettäisiin niille tarkoitetuilla tavoilla. XSS-hyökkäyksissä käytetään yleensä JavaScriptiä, koska se on yksi suosituimmista web-ympäristössä käytettävistä ohjelmointikielistä, ja sitä käyttämällä verkkosivustolle voidaan lisätä monia hyödyllisiä toiminnallisuuksia. JavaScriptin toiminnallisuuksia voidaan käyttää myös haittatarkoituksiin, kuten esimerkiksi verkkosivuston vierailijan evästetietojen varastamiseen tai vierailijan uudelleenohjaamiseen kokonaan toiselle sivustolle. (Rouse 2018b)

XSS-hyökkäykset jaetaan pysyviin ja ei-pysyviin hyökkäyksiin. Pysyvässä XSS-hyökkäyksessä hyökkääjä voi syöttää haittakoodia sivustoilla olevan web-sovelluksen, kuten esimerkiksi lomakkeen, haku- tai kommenttikentän kautta. Web-sovelluksen kautta syötetystä haittakoodista tulee pysyvä osa sivua, mikä tarkoittaa, että joka kerta kun sivusto ladataan, suorittaa haittakoodikin toimintonsa. (Rouse 2018b)

Ei-pysyvässä hyökkäyksessä, hyökkääjä lisää haitallista koodia suoraan verkkosivuston URL-osoitteeseen (Kuva 1). Jotta ei-pysyvä XSS-hyökkäys onnistuu, täytyy uhrin vierailla siinä nimenomaisessa URL-osoitteessa, mihin haitallinen koodi on kirjoitettu. Ei-pysyvän hyökkäyksen suorittaminen vaatii siis myös huijauksen, jossa uhrille toimitetaan koodia sisältävä URL-osoite. Peukaloidun URL-osoitteen voi toimittaa uhrille esimerkiksi osana roskapostia. Verkkosivustolla vieraillessa vierailijan selain suorittaa sivustolle piilotetun koodin, joka suorittaa sille määritetyt toiminnallisuudet, riippuen mitä koodi on ohjelmoitu tekemään (Chandel 2017).



Kuva 1. Esimerkki URL-osoitteeseen lisätystä haittakoodista.

Suurin osa XSS-hyökkäyksistä toteutetaan kohdentamattomina hyökkäyksinä, sillä hyökkäyksen kohteena ovat kaikki verkkosivustoilla vierailevat. XSS-hyökkäysten päätarkoitus on varastaa verkkosivustolla vierailevan käyttäjän tunnistautumisevästeet. Tunnistautumisevästeet sisältävät käyttäjän tunnistautumistiedot, joilla sivusto tunnistaa kuka sivuilla vierailee. Jos hyökkääjä saa käsiinsä verkkosivustolla vierailevan käyttäjän evästeet, voi hän esiintyä sivuilla tänä käyttäjänä ja suorittaa erityyppisiä toimia käyttäjän puolesta. Pahimmassa tapauksessa hyökkääjä pääsee käsiksi käyttäjän arkaluontoisiin tietoihin, kuten esimerkiksi kirjautumis- sekä luottokorttitietoihin. (Incapsula 2019a)

Vuonna 2018 hakkeriryhmä Magecart suoritti XSS-hyökkäyksen lentoyhtiö British Airwaysin verkkosivustolle. XSS-hyökkäyksessä hakkeriryhmä lisäsi JavaScriptin avulla sivustolle 22 koodiriviä, mikä tallensi kaikki sivuston täydennettäviin kenttiin syötetyt tiedot

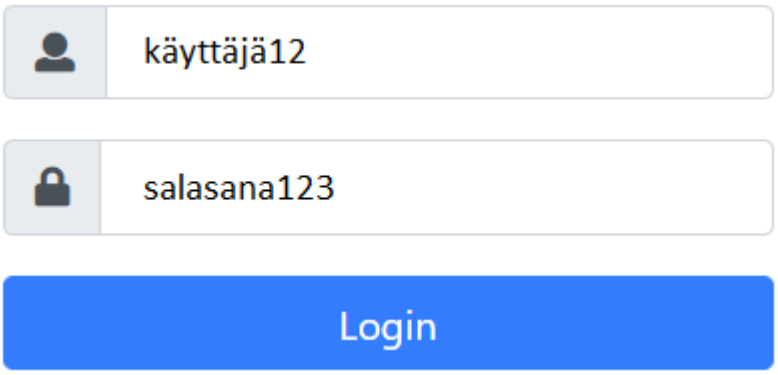
ja lähetti tallennetut tiedot hakkereiden palvelimelle. British Airwaysin maksunkäsittelysivusto ei ollut tarpeeksi hyvin suojattu, joten hakkerit saivat käsiinsä lähes 400 000 asiakkaan maksutiedot. (Matteson 2018)

4.2.2 SQL-Injektio, SQLi

Jokaisella WordPress-verkkosivustolla on tietokanta, jota hallitaan SQL-ohjelmointikielellä. SQL-komennoilla voidaan suorittaa kyselyitä tietokantaan, joka palauttaa kyselyn mukaisen sisällön. Joka kerta kun kävijä syöttää dataa tietokantapohjaisen verkkosivuston täydennettävään kenttään, kuten esimerkiksi sivustolla olevaan haku-, yhteydenotto- tai sisäänkirjautumiskenttään, suorittaa sivusto SQL-kyselyn tietokantaan. Verkkosivuille sisäänkirjautuminen on hyvä esimerkki tästä. Sisäänkirjautumisen yhteydessä käyttäjä syöttää käyttäjäkseen ”käyttäjä12” ja salasanakseen ”salasana123” (Kuva 2).

Verkkosivu tarkistaa SQL-kyselyllä, onko tuon nimistä käyttäjää olemassa ja onko käyttäjä syöttänyt oikean salasanan. Jos tiedot täsmäävät, käyttäjä onnistuu kirjautumaan sisälle (OWASP 2019). Sisäänkirjautumisen kysely SQL-komennolla:

```
SELECT * FROM users WHERE username='käyttäjä12' and password='salasana123'
```

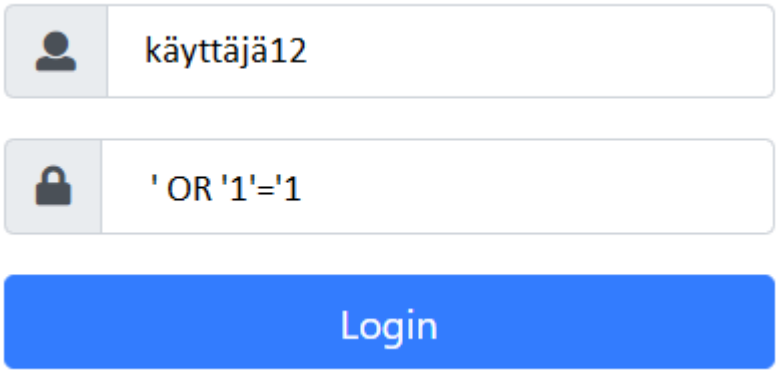


Kuva 2. Sisäänkirjautumiskenttä oikeilla tiedoilla.

SQL-injektiossa hyökkääjä suorittaa haitallisia SQL-komentoja käyttäen verkkosivuston täydennettäviä kenttiä, sen sijaan, että käyttäisi niitä, niiden tarkoitusten mukaisesti. Vain yksi haavoittuvuus täydennettävässä kentässä voi avata ulkopuoliselle pääsyn sivuston tietokantaan (Scacca 2018). Jos verkkosivuston tietoturvaan ei kiinnitetä huomiota, on verkkosivuston täydennettäviin kenttiin mahdollista kirjoittaa mitä tahansa, mukaan lukien erikoismerkkejä, jotka mahdollistavat SQL-komentojen kirjoittamisen. SQL-komento tulee syöttää aina siinä muodossa, että kysely palauttaa kelvollisen tuloksen. Jos suoritettavassa SQL-kyselyssä on virheitä, se ei palauta mitään tulosta. Satunnaisten SQL-komentojen syöttäminen ei siis johda mihinkään.

Syöttämällä SQL-komentoja, voi hyökkääjä kirjautua sisään sivustoille tietämättä käyttäjää tai salasanaa. Tässä esimerkki yksinkertaisesta SQL-injektiosta, missä käyttäjänimi on tiedossa, ja jäljellä on enää salasanan todennuksen ohitus (Kuva 3). SQL-injektiolla se on mahdollista ohittaa seuraavalla komennolla:

SELECT * FROM users WHERE username='käyttäjä12' and password= ' OR '1'='1



Kuva 3. Esimerkki SQL-injektiosta.

Komento mahdollistaa sisäänkirjautumisen, sillä käyttäjänimi on oikea ja lauseke ”1=1” on aina totta, palauttaen kelvollisen tuloksen (OWASP 2019).

SQL-injektiot ovat yksi kohdennetuissa hyökkäyksissä käytettävistä haavoittuvuuksista. Sen avulla tehdään tietomurtoja, tietovuotoja ja ilkivaltaa, joiden vaikutukset voivat olla erittäin laajalle ulottuvia. Onnistunut SQL-hyökkäys voi pahimmassa tapauksessa mahdollistaa kaiken tietokannassa olevan tiedon näkemisen, muuntelun tai jopa poiston. Sillä voi olla suuri vaikutus yrityksen maineeseen, aiheuttaen huomattavia taloudellisia tappioita. (Incapsula 2019b)

Vuonna 2011 Sonyn Playstation verkkoon tehtiin SQL-hyökkäys. Tietokannassa olevat tiedot eivät olleet salattuja, mistä syystä hyökkääjät saivat vuodettua yli 77 miljoonan käyttäjän käyttäjätiedot. Tiedoissa oli mukana myös kymmenien tuhansien käyttäjien maksutiedot. Hyökkääjät käyttivät haavoittuvuutta, joka mahdollisti yksinkertaisen SQL-injektion. Sony ei ollut välittänyt haavoittuvuudesta, mikä olisi ollut helposti paikattavissa, aiheuttaen kymmenien miljoonien taloudelliset tappiot hyvityksistä ja suuren loven yrityksen maineeseen. (Outpost24 2018)

4.2.3 Väsytyshyökkäys – Brute-force -hyökkäys

Väsytyshyökkäys, toiselta nimeltään raakahyökkäys, on yksinkertaisin tapa selvittää oikea salasana tai käyttäjätunnus puhtaasti arvaamalla vaihtoehtoja yrityksen ja erehdyksen kautta toivoen, että arvaus osuu lopulta oikeaan (O’Driscoll 2018). Tätä hyökkäystä voisi verrata perinteiseen kassakaapin salasanayhdistelmän arvaamiseen – kokeillaan

kaikki mahdolliset numeroyhdistelmät, kunnes kassakaappi aukeaa. Tosin kuin perinteisessä kassakaappiyhdistelmän arvauksessa, väsytyshyökkäyksessä käytetään hyväksi erilaisia automatisoituja työkaluja, yksittäisiä botteja sekä jopa tuhansista boteista koostuvia bottiverkkoja, jotka suorittavat tuhansia arvauksia sekunneissa (Kaspersky Lab 2019). Nämä työkalut ovat mahdollistaneet väsytyshyökkäysten eri variaatiot.

Yleisimmin käytetty variaatio on sanakirjahyökkäys, jota käytetään usein osana kohdennettua hyökkäystä. Sanakirjahyökkäyksessä apuna käytetään jonkinlaista sanalistaa salasanan arvaamiseen, kun käyttäjätunnus on jo tiedossa. Sanalista voi muun muassa sisältää yleisimmin käytettyjä salasanoja, tietomurrosta saatuja salasanoja tai vaikka yleisiä etu- ja sukunimiä. Sanalistat voivat sisältää jopa miljoonia sanoja, joita voidaan käyttää salasanoina. Sanakirjahyökkäykseen on mahdollista asettaa myös poikkeuksia, kuten esim. a-kirjain on korvattu numerolla 4 tai e-kirjain numerolla 3.

Vuonna 2015 Alibaban verkkokauppaan tehtiin sanakirjahyökkäys, jossa käytetty sanalista sisälsi toisen verkkokaupan, TaoBaon, 99 miljoonaa käyttäjätunnusta ja niiden salasanat. Hyökkäyksellä onnistuttiin vaarantamaan lähes 21 miljoonaa käyttäjätiliä eli noin viidennes arvauksista osui kohdalleen. Tämä vain korosti sitä, kuinka ihmiset käyttävät samoja sisäänkirjautumistietoja useassa paikassa, vaikka käyttäjätiedot olisivat olleet tietomurron kohteena jo aikaisemmin. (Buntinx 2017.)

Käänteisessä väsytyshyökkäyksessä hyökkääjä käyttää jo tiedossa olevaa salasanaa tai listaa yleisimmin käytetyistä salasanoista käyttäjätunnuksen arvaamiseen. Tätä hyökkäystä käytetään kohdentamattomana hyökkäyksenä, sillä kohteena ei ole yksittäinen käyttäjä, vaan hyökkäyksen tavoitteena on saada selville mahdollisimman monen käyttäjän kirjautumistiedot. (Cloudflare 2019a)

Väsytyshyökkäyksen suurin etu muihin hyökkäyksiin nähden on se, että mikäli sen onnistumiseen annetaan tarpeeksi aikaa, se toimii aina. Teoriassa kaikki salasanat on mahdollista murtaa käyttäen tätä hyökkäystapaa. Väsytyshyökkäyksessä käytetään hyväksi käyttäjätilin tai verkkosivuston heikointa lenkkiä; sen omistajaa. Mitä lyhyemmän ja helpomman salasanan omistaja on itselleen määrittänyt, sen helpompi salasana on murtaa.

Vaikka väsytyshyökkäys on helppo suorittaa, voi salasanan arvaukseen mennä päiviä, viikkoja tai jopa vuosia, riippuen salasanan monimutkaisuudesta, pituudesta sekä tietokoneen tehosta (O’Driscoll 2018).

Yleisin hyökkäys, joka kohdistuu WordPress-käyttäjään, on käyttäjän salasanan murtaminen väsytyshyökkäyksellä. WordPress ei oletuksena rajoita kirjautumisyrityksiä, vaikka salasanan arvaa monta kertaa peräkkäin väärin. Hyökkääjät voivat siis huoletta suorittaa väsytyshyökkäyksiään WordPress-sivustoja vastaan. Järjestelmänvalvojan käyttäjä on oletuksena nimeltään admin ja WordPressin kirjautumissivu on oletuksena muotoa http://www.esimerkki.fi/wp-login.php/. Nyt hakkeri tietää miltä sivulta hallintapaneeliin kirjaudutaan ja mikä on ylläpitokäyttäjä, jonka salasana tulee murtaa. WordPressin kiistelty ominaisuus tekee WordPressiä vastaan tehtävästä väsytyshyökkäyksestä vieläkin helpompaa, sillä epäonnistuneet kirjautumiset vahvistavat käyttäjätunnuksen, vaikka syöttäisi väärän salasanan. (Hacker Target 2013)

4.2.4 DoS – Denial-of-Service -attack, Palvelunestohyökkäys

DoS-hyökkäys eli palvelunestohyökkäys eroaa muista tässä opinnäytetyössä kirjoittamistani hyökkäystyypeistä, sillä sen tarkoituksena ei ole päästä käsiksi hyökkäyksen kohteena olevan tietoihin, vaan estää kohteeksi valitun verkkopalvelun toiminta. Hyökkäyksen tavoitteena on lamauttaa kohteena oleva palvelin, tietokone tai kokonainen verkko ylikuormittamalla sen resurssit niin suurella määrällä liikennettä, että se ei pysty käsittelemään sitä (Weisman 2019).

DoS-hyökkäyksellä yritetään riistää käyttömahdollisuus kohteeksi valitun palvelun käyttäjiltä. Jos esimerkiksi VR:n verkkokauppaan tehtäisiin onnistunut DoS-hyökkäys, olisi ihmisten mahdotonta ostaa junalippunsa verkosta. Hyökkäyksen kohteiksi valikoituvat usein isojen organisaatioiden ja yritysten verkkopalvelut. Muita tämänkaltaisia palveluita voivat olla erilaiset verkkosivustot, sähköposti- tai verkkopankkipalvelut sekä esimerkiksi eri sosiaaliset mediat.

Hajautetusta palvelunestohyökkäyksestä, eli DDoS-hyökkäyksestä puhutaan, kun hyökkäys tulee useammasta kuin yhdestä lähteestä samanaikaisesti. Osana hyökkäystä voidaan esimerkiksi käyttää luvussa 5.1 mainitsemaani bottiverkkoa, ikään kuin bottien armeijana (BullGuard 2019). Mitä enemmän botteja on osana DDoS-hyökkäyksessä käytettävää bottiverkkoa, sitä suuremmalla todennäköisyydellä hyökkääjä pääsee haluttuun lopputulokseen – palvelun totaaliseen lamauttamiseen.

Maailman suurin DDoS-hyökkäys suoritettiin vuonna 2018 GitHubiin, suosittuun kehitysalustaan. Hyökkäyksessä alustaa jumitettiin valtavalla määrällä liikennettä. Liikenne

nousi huipussaan 1,35 teratavuun sekunnissa. Onneksi GitHub käytti DDos-hyökkäyksiä vastaan suojauspalvelua, joka hälytettiin automaattisesti apuun hyökkäyksen käynnistyttyä. Suojauspalvelun vuoksi maailman suurin DDos-hyökkäys kesti vain 20 minuuttia (Cloudflare 2019b).

5 TIETOTURVAOPPAAN AVAUS

Osana opinnäytetyötä olen luonut tietoturvaoppaan, jonka askelia noudattamalla jokainen voi parantaa omien WordPress-verkkosivustojensa tietoturvan tasoa. Verkkosivuston tietoturvatasosta huolehtiminen on tärkeää yritykselle, sillä verkkosivut ovat yrityksen brändi, näyteikkuna, ensimmäinen osa yrityksestä, minkä asiakkaat näkevät. Jos verkkosivu ei ole turvallinen, saattaa asiakkuus loppua siihen. Tietoturvaoppaan askeleet olen koonnut suurimmaksi osaksi WordPressin omilta kotisivuilta, sekä muista opinnäytetyössä käyttämistäni lähteistä. Tietoturvaopas on opinnäytetyön liitteenä. Avaan tässä kappaleessa tekemääni tietoturvaopasta askel askeleelta.

5.1 Askel numero 1: Hyvän salasanan ja käyttäjätunnuksen valitseminen

Tärkein askel oman verkkosivuston tietoturvan parantamiseksi on hyvän salasanan sekä käyttäjätunnuksen valitseminen. Lyhyet ja helpot salasanat on helppo murtaa esimerkiksi aikaisemmin käsittelemälläni väsytyshyökkäyksellä. Mainitsinkin luvussa 4.2.3 ”Mitä lyhyemmän ja helpomman salasanan omistaja on itselleen määrittänyt, sen helpompi salasana on murtaa”. Mainitsin myös samassa luvussa, että pääkäyttäjä WordPressissä on oletuksena ”admin”. Vältä siis ”admin”- ja ”administrator”-käyttäjätunnuksia. Käyttäjätunnuksen tietäminen on jo puolet murtautumisesta. Poista myös kaikki ne toiminnallisuudet loppukäyttäjiltä, joita he eivät tarvitse, sillä mikäli hyökkääjä onnistuu murtautumaan jonkun toisen käyttäjätunnukselle, on tärkeää minimoida tuhon mahdollisuudet. Poista myös vanhat ja ylimääräiset käyttäjät, jotta murtautumisen riski pienenee.

5.2 Askel numero 2: Pidä WordPress päivitettynä

Jokaisessa WordPress-versiossa on haavoittuvuuksia. Mitä vanhempi WordPress-versio, sen tunnetumpia kyseisen version haavoittuvuudet ovat. Tietoturvapäivityksiä WordPressiin voidaan julkaista ilmoittamatta, yhtäkkisen vakavan haavoittuvuuden vuoksi kuten mainitsin luvussa 2, joten on ehdottoman tärkeää päivittää WordPress-versio aina uusimpaan mahdolliseen. WordPressissä on oletuksena ainoastaan pienten päivitysten, kuten esim. huolto- ja turvapäivitysten automaattinen päivitys käytössä.

WordPressiin on kuitenkin mahdollista asettaa automaattinen päivitys kaikkien versioiden päivittämiseen, joko lataamalla lisäosan, joka päivittää WordPress-version automaattisesti tai lisäämällä koodinpätkän wp-config.php tiedostoon. Yksi hyvä lisäosa tähän tarkoitukseen on erään pitkäaikaisen Plugin-kehittäjän luoma ”Advanced Automatic Updates”-lisäosa. Lisättävä koodinpätkä wp-config tiedostoon: define('WP_AUTO_UPDATE_CORE', true)

5.3 Askel numero 3: Pidä WordPress-laajennukset päivitettyinä

WordPress ei automaattisesti päivitä lataamiasi lisäosia. Lisäosat, ihan samalla tavalla kuin WordPressin ydin, voivat sisältää tietoturva-aukkoja. Sinun tulee välttää lisäosia, joiden kehitys on loppunut. Kehittäjien hylkäämät lisäosat huomataan helposti siitä, milloin lisäosaa on viimeksi päivitetty. Mikäli lisäosa ei ole saanut päivitystä 10-12 kuukauteen, on sen kehittäjä erittäin suurella todennäköisyydellä hylännyt sen tukemisen ja kehittämisen tehden siitä riskialttiin hakkerien löytämille tietoturva-aukoille. Jokainen käytössäsi oleva lisäosa on uusi tietoturvariski sivustollesi. Kuten WordPress-version päivittämisessä, laajennusten automaattinen päivitys on mahdollista joko lataamalla askel numero kahdessa mainitsemani ”Advanced Automatic Updates”-lisäosan, jonka avulla teemojen ja laajennusten automaattinen päivitys on mahdollista, tai lisäämällä seuraavat koodinpätkät wp-config tiedostoon:

```
add_filter( 'auto_update_plugin', '__return_true' );

add_filter( 'auto_update_theme', '__return_true' );
```

5.4 Askel numero 4: Suosi vain luotettuja teemoja ja lisäosia

Lisäosat ja teemat tulee ladata vain luotetuista lähteistä. Jotkut laajennukset, kuten esimerkiksi normaalisti maksulliset laajennukset, on mahdollista ladata kolmannen osapuolen sivustoilta, jolloin ladattavat laajennukset ovat kopioita alkuperäisistä laajennuksista, ja voivat sisältää kolmansien osapuolien lisäämää koodia. Kolmansien osapuolien sivuilta ladattavia lisäosia ei myöskään saa päivitettyä automaattisesti, mikä vain lisää tietoturvariskiä. Mikäli WordPressissäsi on asennettuna lisäosia, jotka eivät ole käytössä, kannattaa niiden asennus poistaa kokonaan. Lisäosien lukumäärä on suoraan verrannollinen WordPressin turvallisuuteen.

5.5 Askel numero 5: Vaihda tietokannan etuliitteet

Oletuksena WordPress-verkkosivuston tietokantojen etuliitteet ovat muotoa wp_. Hyökkääjän on erittäin helppo suorittaa yleisesti toimivia SQL-komentoja tehdäkseen SQL-injektioita WP-pohjaisille verkkosivustoille, kun he jo valmiiksi tietävät tietokannan rakenteen. Muuttaaksesi tietokantojen etuliitteitä, tulee sinun tehdä kolme muutosta. Ensimmäisenä wp-config.php-tiedostosta löydät rivin, jossa määritellään tuo etuliite: $table_prefix = ‘wp_’. Voit muuttaa tietokannan etuliitteen alkuperäisestä muodosta ”wp_” haluamaasi muotoon. Seuraavana tulee vaihtaa tietokannan taulujen nimet. Tämä onnistuu helpoiten suorittamalla SQL-komentoja MySQL-hallinnan kautta. Tietokannan taulu saadaan muutettua SQL-komennolla: RENAME table ’wp_xxxxxxx’ TO ’xx_ xxxxxxx’. Voit korvata kohdan ”xx_” nimeämällä sen miten tahansa, kunhan se sisältää vain numeroita ja aakkosia. Viimeisenä muutoksena on ”xx_options” ja ”xx_usermeta” taulujen sisällön muokkaus (alun perin ”wp_options” ja ”wp_usermeta”). Niiden sisällöistä tulee muuttaa sarakkeiden ”option_name” ja ”meta_key” kohdat muodosta ”wp_” muotoon ”xx_”. Suoritettavat SQL-komennot tietokantojen etuliitteiden vaihtoon löytyvät liitteestä 2.

5.6 Askel numero 6: Varmuuskopioi

Varmuuskopioi säännöllisin väliajoin tai varmista palveluntarjoajalta mahdollisuudet varmuuskopiointiin. Tämä on yksinkertainen tapa minimoida mahdollisten hyökkäysten aiheuttama tuho. Mikäli sivustoille on murtauduttu, kannattaa sivusto varmuuskopioida ja suorittaa huolellinen tarkistus, mikä on voinut aiheuttaa haavoittuvuuden, jota hyökkääjät ovat käyttäneet hyväksi. Jotkin päivitykset voivat myös rikkoa sivuston ulkonäön, jos päivitysten yhteydessä on esiintynyt yhteensopivuusongelma esimerkiksi WordPressin ja WordPress-laajennusten välillä. Kannattaa siis varmistaa varmuuskopioiden saatavuus.

5.7 Askel numero 7: Lisää tietoturvaa lisäosilla

WordPressin tarjoamassa lisäosakirjastossa on suuri määrä lisäosia WordPressin tietoturvan parantamiseksi. Näitä lisäosia ovat niin erilaiset skannauslisäosat, joilla verkkosivusto voidaan skannata haavoittuvuuksien sekä heikkouksen varalta, että erilaiset lisä-

osat, joilla tietoturvaa voidaan konkreettisesti lisätä. Lisäosat, joilla voidaan lisätä tietoturvaa, ovat esimerkiksi sellaiset, jotka muuttavat kirjautumistapaa. Alaluvuissa on kolme esimerkkiä.

5.7.1 Vaihda WordPressin kirjautumisosoite

Jokaisella WordPress-sivustolla oletuskirjautumisosoite sivuston hallintapaneeliin on /wp-login.php ja /wp-admin. Tämä tekee hyökkääjälle helpoksi aloittaa brute force-hyökkäys sivustoa kohtaan. Kirjautumisosoitteen muuttaminen on mahdollista esimerkiksi lisäosan ”WPS Hide Login” avulla. Lisäosan avulla kirjautumisosoite saadaan manuaalisesti vaihdettua oletuksesta johonkin toiseen. Mainitsemani lisäosat löytyvät liitteestä 2 suorine linkkeineen.

5.7.2 Ota käyttöön kaksivaiheinen tunnistautuminen

Kaksivaiheinen tunnistautuminen on yleistynyt ja on nykyään käytössä monilla alustoilla. Sen tehtävänä on varmistaa, että vain käyttäjätilin oikea omistaja voi käyttää tiliään. Hyökkääjän on lähes mahdoton murtautua käyttäjätillille, jolla on käytössä kaksivaiheinen tunnistautuminen, sillä hyökkääjän pitäisi käyttäjätilin lisäksi murtautua myös kohteeseen, jossa todennus tapahtuu. Todennus voi tapahtua esimerkiksi tekstiviestitse tai sähköpostitse vastaanotetun koodin avulla tai vaikkapa puhelimeen ladattavan sovelluksen avulla. Kaksivaiheisen tunnistautumisen saa käyttöön esimerkiksi ”Two-factor”-nimisellä lisäosalla.

5.7.3 Rajoita kirjautumisyritysten määrää

Kirjautumisyritysten rajoittaminen lisäosalla on hyvä suojausmenetelmä Brute-force hyökkäyksiä vastaan. Rajoituksen asettaminen poistaa bottien tekemät automatisoidut väsytyshyökkäykset sivustoa kohtaan. ”WP Limit Login Attempts” on yksi suosituimmista ilmaisista lisäosista, jonka avulla kirjautumisyrityksiä saadaan rajoitettua. Lisäosalla voidaan asettaa rajallinen määrä epäonnistuneita kirjautumisyrityksiä tai ottamalla käyttöön ajallinen viive epäonnistuneen kirjautumisyrityksen jälkeen.

5.8 Askel numero 8: Tilaa ja asenna sivustollesi käyttöön SSL-sertifikaatti

SSL-sertifikaatti suojaa yhteyden verkkosivustoilla kävijän sekä palvelimen välillä. Kun yhteys on salattu sertifikaatilla, eivät ulkopuoliset pääse vakoilemaan verkkosivuston liikennettä. Verkkosivuston liikenne sisältää kaiken verkkosivustolla kirjoitetun tiedon. Ilman sertifikaattia verkkosivuston liikenne, kuten esimerkiksi verkkosivuston kävijöiden täyttämät tiedot, näkyvät selkotekstinä. SSL-sertifikaatti salaa, eli muuttaa selkotekstin salakirjoitukseksi suojaten arkaluonteisetkin tiedot.

Google on myös kertonut suosivansa hakutuloksissaan SSL-sertifikaatilla suojattuja sivustoja. SSL-sertifikaatti tuo siis suojaa ja suosiota sivustolle ja turvallisuuden tunnetta sivuston kävijöille. SSL-sertifikaatin saa tilattua useilta hosting-palveluntarjoajilta Suomessa.

5.9 Askel numero 9: Pidä huoli PHP-version päivityksestä

PHP-version päivittäminen on lähes yhtä tärkeää kuin WordPressin itsensä ja sen laajennusten päivittäminen. PHP on se liima, joka pitää verkkosivustosi kasassa. Kuten mainitsin luvussa 2.2.1, vanhentunut PHP-versio voi olla kriittinen haavoittuvuus verkkosivustollesi. PHP-version päivitys ei ainoastaan ole turvallisempi, sillä se sisältää uusimmat turvaominaisuudet, vaan se myös nopeuttaa verkkosivustoa. PHP 7 on yli kaksi kertaa nopeampi kuin edeltäjänsä 5.6. Tarkista siis PHP-versiosi kysymällä sitä palveluntarjoajaltasi tai tarkista se itse palveluntarjoajasi hallintapaneelista.

Verkkosivustosi PHP-version voi palveluntarjoaja päivittää puolestasi. Huomioita ennen PHP-version päivittämistä:

- Ota varmuuskopio WordPressistäsi
- Päivitä WordPress ja sen laajennukset
- Tarkista PHP-yhteensopivuus teemojen ja laajennusten osalta. Se onnistuu ottamalla käyttöön esimerkiksi lisäosa ”PHP Compatibility Checker plugin”

5.10 Askel numero 10: Roskapostin estäminen

Lomakkeet verkkosivustoilla lisäävät roskapostibottien aiheuttamaa riesaa. Roskapostit on mahdollista karsia pois muutamalla keinolla. Lomakkeeseen on mahdollista asettaa CAPTCHA-kenttä, eli varmennusmenetelmä, joilla botit on mahdollista kitkeä pois. Varmennusmenetelmän on määrä erottaa botit ihmisistä. CAPTCHA-testi on monelle tuttu useilta verkkosivustoilta löytyvien kuvavarmenteiden kautta. Yksi suosituimmista CAPTCHA lisäosista on ”Google Captcha (reCAPTCHA)”.

Mikäli lomakkeen lähetystä ei halua vaikeuttaa, on mahdollista ottaa käyttöön yksi näkymätön kenttävaihtoehto lomakkeen lähetykseen. Tätä näkymätöntä kenttävaihtoehtoa kutsutaan ”honeypotiksi”, eli hunajapurkiksi. Ihmisvierailijat eivät tätä vaihtoehtoa näe, ja jättävät sen siitä syystä tyhjäksi. Roskapostibotit taas täyttävät kaikki lomakkeen kohdat umpimähkään automaattisesti, mukaan lukien ”honeypot”-kentän, mikä sitten paljastaa lomakkeelle, onko sen täyttäjä ihminen vai ei, ja estääkö se lomakkeen lähetyksen vai ei.

Useat lisäosat, joilla lomakkeita saadaan WordPressiin lisättyä, sisältävät mahdollisuuden ”honeypot”-kenttään, kuten esimerkiksi ”WPForms” sekä ”Ninja Forms”. Jos lomakelisäosassa ei ole ”honeypot”-mahdollisuutta, on siihen hyviä lisäosia, kuten esimerkiksi ”Contact Form 7 Honeypot”.

5.11 Askel numero 11: Wp-config

Ehkä jopa kaikkein tärkein WordPress-sivuston tiedosto on wp-config.php-tiedosto. Se sisältää muun muassa tietokannan nimen, sen pääkäyttäjän ja salasanan. Se kannattaa siis pitää turvassa. Mikäli käytössä on palvelin, jossa on käytössä .htaccess, on silloin mahdollisuus ottaa käyttöön toiminto, joka estää wp-config.php-tiedostoon pääsyn kaikilta ulkopuolisilta. Toiminnon saa otettua käyttöön lisäämällä wp-config.php-tiedostoon muutaman rivin koodia, jotka löytyvät liitteestä 2.

Wp-config.php tiedosto on myös mahdollista siirtää yhtä pykälää ylemmäs kansiohakemistossa, pois julkisesta ”root”- eli kotihakemistosta.

5.12 Askel numero 12: WordPressin sekä WordPress-laajennusten versioiden piilotus

Hyökkääjät etsivät tiettyjä WordPress-versioita hyökkäyksiään varten, sillä he voivat kohdentaa hyökkäyksensä verkkosivustoihin, jotka käyttävät tiettyä WordPress-versiota, niin kuin mainitsin luvussa 2.2.1. Tästä syystä kannattaa piilottaa WordPress ja WordPress-laajennusten versiot näkyvistä. WordPress-version saa piilotettua lisäämällä seuraavan koodinpätkän functions.php tiedostoon: remove_action(’wp_head’, ’wp_generator’); WordPress-laajennusten versiot saa piilotettua muilta poistamalla laajennuksen oman readme.html tiedoston.

6 LOPUKSI

Opinnäytetyön keskeisen tavoite oli luoda tietoturvaopas, jonka avulla WordPress-pohjaisen verkkosivuston tietoturvaa on mahdollista parantaa. Tietoturvaopas tullaan asettamaan esille toimeksiantajan kotisivuille kaikille jaettavaksi. Toivon, että useat päätyvät seuraamaan oppaan ohjeita ja toteuttavat WordPress-verkkosivustoihinsa tietoturvaparannuksia, jotka ennaltaehkäisevät internetmaailmassa yhä yleistyviä tietoturvauhkia.

WordPressin suosiolle ei näy loppua, mikä tulee jatkossakin heijastumaan WordPressistä löydettyjen haavoittuvuuksien runsauteen. Hyökkääjien taidot kehittyvät ja hyökkääjien rivistö vain kasvaa IT-maailman kukoistaessa. Pakasta vedetyt eli täysin muokkaamattomat WordPress-pohjaiset verkkosivustot tulevat edelleenkin olemaan ensimmäisenä tulilinjalla hyökkääjille, oli hyökkäyksen syy sitten itsensä todistaminen tai taloudellinen hyöty.

Opinnäytetyötäni tehdessä kuitenkin opin, että WordPressin tietoturvan saa jo pienellä panoksella hyvälle tasolle. Mielestäni liioitellaan, kun sanotaan, että WordPressiä ei kannata ottaa käyttöön, jos haluaa välttyä tietoturvaongelmilta. Sama pätee muihinkin verkkosivustoratkaisuihin, täytyy niidenkin tietoturvasta pitää hyvää huolta. Huomiota siihen ei välttämättä tarvitse kiinnittää yhtä paljon kuin WordPress-pohjaisten verkkosivustojen kohdalla, mutta sama periaate pätee. WordPress on maailman suosituin sisällönhallintajärjestelmä, ja juurikin se vetää hyökkääjät puoleensa. WordPressin suosiolle on syynsä, joten miksi pitäisi lopettaa maailman parhaimman sisällönhallintajärjestelmän käyttö vain siksi, että hyökkääjät kohdentavat hyökkäyksiään sillä tehtyihin verkkosivustoihin, kun pienillä tietoturvakohennuksilla saadaan estettyä suurin osa hyökkäyksistä.

Vaikka tietoturvaoppaan askeleet on suunniteltu nimenomaan WordPress-pohjaisille verkkosivustoille, voidaan niitä mukauttaa ja hyödyntää muissakin verkkoratkaisuissa. Hyvän salasanan ja käyttäjätunnuksen valitseminen oman tietoturvan suojaamiseksi nykypäivänä on kriittisen tärkeää, eikä ohjelmistojen päivittämistä voida korostaa liikaa.

Opinnäytetyö eteni hyvää vauhtia tehdessäni samanaikaisesti töitä toimeksiantajalle. Työtehtävissäni monet kohtaamani asiat auttoivat opinnäytetyöni laatimista. Mielenkiinto aihetta kohtaan vain kasvoi kirjoittaessani, mikä vain lisäsi intoani aiheen tutkimiseen ja

siitä lukemiseen. Tietoturvaoppaan kokoaminen onnistui mielestäni hyvin ja sainkin kerättyä kattavan oppaan, joilla WordPress-pohjaisia verkkosivustoja on mahdollista pelastaa tulevilta hyökkäyksiltä.

Opinnäytetyötäni aloittaessa mietin edelleen, mitä tutkimusmenetelmää haluan käyttää ja miksi. Aikomukseni oli tehdä kvalitatiivinen tutkimus haastattelun keinoin, mutta päädyin kuitenkin konstruktiiviseen tutkimusmenetelmään hieman asiaa tutkittuani. Aiheesta löytyi niin paljon lähteitä, ja lähteistä saatu tieto tuki teknistä toimivuutta eikä mielipiteitä, joten lähteisiin oli helppo luottaa. Lähteet olivat osin suurilta tietoturvayrityksiltä, joiden joukkoon mahtui muun muassa F-Secure, Cisco, Sucuri ja Cloudflare, sekä peräisin kokeneiden tietoturva-ammattilaisten artikkeleista. Artikkeleista saatu tieto oli helppo todeta oikeaksi, varsinkin jos sama tieto löytyi useasta eri lähteestä. Lähteistä saatuja tietoja oli helppo tarkistaa ja todeta niiden paikkaansa pitävyyden, kokeilemalla niitä omalla WordPress-pohjaisella verkkosivustolla. Eritysmaininta kuuluu myös WordPressin omille kotisivuille, josta löytyi paljon tietoa WordPressin haavoittuvuuksista ja niiden korjaamisesta.

Tietoturvaopas tullaan jakamaan toimeksiantajan yhteistyökumppaneille, joilta saadaan kokemuksia tuloksista ja mahdollista palautetta tietoturvaoppaan sisällöstä. Opasta tullaan myös parantamaan toimeksiantajan kotisivuille kuvallisilla ohjeilla, joilla tietoturvaoppaan askelia on helpompi hyödyntää. Kuvallisten ohjeiden avulla voi kuka tahansa ottaa käyttöön oppaassa mainittuja tietoturvaparannuksia.

LÄHTEET

Abela, R. 2014. What are Targeted and Non-Targeted WordPress Hack Attacks. Viitattu 5.2.2019 https://www.wpwhitesecurity.com/targeted-non-targeted-wordpress-hack-attacks/.

Abela, R. 2017. Why Would a Malicious Hacker Target Your WordPress? Viitattu 5.2.2019 https://www.wpwhitesecurity.com/why-malicious-hacker-target-wordpress/.

Abela, R. 2018. Crunching the Numbers – Too Many WordPress vulnerabilities Can Only Mean Good Things. Viitattu 1.2.2019 https://www.wpwhitesecurity.com/crunching-the-numbers-vulnerabilities-is-wordpress-a-really-insecure-web-application.

Abhiyan, 2018. Techniques that Hackers use to earn money from website (Top 3 methods in 2018). Viitattu 5.2.2019 https://thetechrim.com/technique-hackers-use-to-earn-money-from-website/.

Baker, K. 2015. Hacking group Anonymous declares war on ISIS in YouTube video saying it will use its knowledge to 'unite humanity'. Viitattu 18.2.2019 https://www.dailymail.co.uk/news/article-3320055/Hacking-group-Anonymous-declares-war-Isis-YouTube-video.html.

Beaver, K. 2018. Hacking for dummies, 6th edition. Hoboken: John Wiley & Sons, Inc.

BullGuard 2019. What are DoS and DDoS attacks? Viitattu 18.3.2019 https://www.bullguard.com/bullguard-security-center/internet-security/internet-threats/what-are-dos-and-ddos-attacks.aspx.

Buntinx, JP. 2017. Top 5 Brute Force Attacks. Viitattu 11.3.2019 https://themerkle.com/top-5-brute-force-attacks/.

Call, A. 2015. Hackers: The Internet's Immune System. Viitattu 5.2.2019 https://www.digicert.com/blog/hackers-are-internet-immune-system/.

Chandel, R. 2017. Beginners Guide to Cross Site Scripting (XSS). Viitattu 4.3.2019 https://www.hackingarticles.in/beginners-guide-cross-site-scripting-xss/.

Cimpanu, C. 2018. A botnet of over 20,000 WordPress sites is attacking other WordPress sites. Viitattu 22.2.2019 https://www.zdnet.com/article/a-botnet-of-over-20000-wordpress-sites-is-attacking-other-wordpress-sites/.

Cimpanu, C. 2019. WordPress accounted for 90 percent of all hacked CMS sites in 2018. Viitattu 3.6.2019 https://www.zdnet.com/article/wordpress-accounted-for-90-percent-of-all-hacked-cms-sites-in-2018/.

Cisco 2018. What Is the Difference: Viruses, Worms, Trojans, and Bots? Viitattu 12.2.2019 https://www.cisco.com/c/en/us/about/security-center/virus-differences.html.

Cloudflare 2019a. Brute Force Attack. Viitattu 11.3.2019 https://www.cloudflare.com/learning/security/threats/brute-force-attack/.

Cloudflare 2019b. Famous DDoS Attacks | The Largest DDoS Attacks Of All Time. Viitattu 1.4.2019 https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/.

Defiant 2018. Introduction to Writing Secure PHP Code. Viitattu 4.3.2019 https://www.wordfence.com/learn/how-to-write-secure-php-code/#where-and-why-vulnerabilities-appear-in-wordpress.

FOSSA 2014. GNU General Public License v2.0 (GPL-2.0). Viitattu 5.2.2019 https://tldrlegal.com/license/gnu-general-public-license-v2#summary.

F-Secure 2019. Kahdeksan myyttiä tietoturvasta. Viitattu 25.2.2019 https://www.f-secure.com/fi_FI/web/home_fi/online-security-myths.

Google 2019. Googlebot. Viitattu 22.2.2019: https://support.google.com/webmasters/answer/182072?hl=fi.

Greenberg, A. 2010. Researcher's Hack Can Make ATMs Spew Money. Viitattu 5.2.2019 https://www.forbes.com/sites/firewall/2010/07/28/researchers-hack-can-make-atms-spew-money/#2f5c9a0f3cd5.

Hacker Target 2013. Attacking WordPress. Viitattu 15.3.2019 https://hackertarget.com/attacking-wordpress/.

Hughes, J. 2018. How Malware Really Affects Your WordPress Website. https://www.elegantthemes.com/blog/tips-tricks/how-malware-really-affects-your-wordpress-website.

Incapsula 2019a. CROSS SITE SCRIPTING (XSS) ATTACKS. Viitattu 4.3.2019 https://www.incapsula.com/web-application-security/cross-site-scripting-xss-attacks.html.

Incapsula 2019b. SQL (STRUCTURED QUERY LANGUAGE) INJECTION. Viitattu 8.3.2019 https://www.incapsula.com/web-application-security/sql-injection.html.

Internet Live Stats 2019, Total number of Websites. Viitattu 24.1.2019 http://www.internetlivestats.com/total-number-of-websites/.

Kaspersky Lab 2019. What's a Brute Force Attack? Viitattu 11.3.2019 https://www.kaspersky.com/resource-center/definitions/brute-force-attack/.

Kielitoimisto 2018. Sanakirja. Krakkeri-sanan määritelmä. Viitattu 3.6.2019 https://www.kielitoimistonsanakirja.fi/.

Kinsta 2018. What is WordPress? Explained for beginners. Viitattu 5.2.2019 https://kinsta.com/knowledgebase/what-is-wordpress/.

Lawrence, S. 2018. Reasons Why Hackers Hack WordPress Sites. Viitattu 5.2.2019 https://www.malcare.com/blog/2018/06/26/reasons-why-hackers-hack-wordpress-sites/.

Mullenweg, M. 2011. Why Your Company Should Have a Creed. Viitattu 5.2.2019 https://ma.tt/2011/09/automattic-creed/.

Matteson, S. 2018. British Airways data theft demonstrates need for cross-site scripting restrictions. Viitattu 12.3.2019 https://www.techrepublic.com/article/british-airways-data-theft-demonstrates-need-for-cross-site-scripting-restrictions/.

McCandless, D. 2019. World's Biggest Data Breaches & Hacks. Viitattu 26.2.2019 https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

Moen, D. 2017. Ask Wordfence: How to Limit Security Risks From Plugins. Viitattu 31.1.2019 https://www.wordfence.com/blog/2017/11/plugin-security-risks/.

Nichols, A. 2016. Targeted Attack Vs. Untargeted Attack: Knowing The Difference. Viitattu 26.2.2019 https://www.anomali.com/blog/targeted-attack-vs-untargeted-attack-knowing-the-difference.

O'Donnell, A. 2018. What Is a Bot Net? Viitattu 22.2.2019 https://www.lifewire.com/what-is-a-botnet-2487267.

O'Driscoll, A. 2018. What a brute force attack is (with examples) and how you can protect against one. Viitattu 11.3.2019 https://www.comparitech.com/blog/information-security/brute-force-attack/.

Open Source Initiative 2019. The Open Source Definition https://opensource.org/docs/osd. Viitattu 31.5.2019

Oracle 2019. MySQL Customers. Viitattu 31.1.2019 https://www.mysql.com/customers/.

Outpost24 2018. TOP 10 of the world's largest cyberattacks. Viitattu 8.3.2019 https://outpost24.com/blog/top-10-of-the-world-biggest-cyberattacks.

OWASP 2019. Bricks Documentation. Viitattu 8.3.2019 https://sechow.com/bricks/docs/login-1.html.

PHP Group 2019a, Keeping Current. Viitattu 1.4.2019 https://www.php.net/manual/en/security.current.php.

PHP Group 2019b. Supported Versions. Viitattu 1.4.2019 https://www.php.net/supported-versions.php.

Pogue, C. 2017. The Black Report, Decoding the minds of hackers. Viitattu 5.2.2019 https://media.scmagazine.com/documents/287/nuix_the_black_report_2017_71550.pdf.

Pogue, C. 2018. The Black Report, Decoding the minds of hackers. Viitattu 5.2.2019 https://www.nuix.com/sites/default/files/report_nuix_black_report_2018_web_us.pdf.

Rahman, N. 2017. Why Do Hackers Bother with Small Sites? Viitattu 5.2.2019 https://medium.com/secjuice/why-do-hackers-bother-with-small-sites-20c297079ff6.

Rieuf, E. 2016. History of MySQL. Viitattu 3.6.2019 https://www.datasciencecentral.com/profiles/blogs/history-of-mysql.

Refsnes Data 2019. PHP MySQL Database. Viitattu 31.1.2019 https://www.w3schools.com/php/php_mysql_intro.asp.

Rouse, M. 2017. Hacker. Viitattu 5.2.2019 https://searchsecurity.techtarget.com/definition/hacker.

Rouse, M. 2018a. White hat. Viitattu 5.2.2019 https://searchsecurity.techtarget.com/definition/white-hat.

Rouse, M. 2018b. Cross-site scripting (XSS). Viitattu 4.3.2019 https://searchsecurity.techtarget.com/definition/cross-site-scripting.

Saeed, S. 2017. Find and Fix Vulnerabilities in Your WordPress Website. Viitattu 26.2.2019 https://www.collectiveray.com/wp/tips/find-fix-wordpress-vulnerabilities.

Scacca, S. 2018. SQL Injection Hack Explained for Better WordPress Security. Viitattu 8.3.2019 https://managewp.com/blog/sql-injection-hack-wordpress-security.

Schneier, B. 2008. Inside the Twisted Mind of the Security Professional. Viitattu 1.4.2019 https://www.wired.com/2008/03/securitymatters-0320/.

Secpoint 2019. What is a Black Hat? Viitattu 5.2.2019 https://www.secpoint.com/what-is-a-black-hat.html.

Shinder, D. 2010. Profiling and categorizing cybercriminals. Viitattu 12.2.2019 https://www.techrepublic.com/blog/it-security/profiling-and-categorizing-cybercriminals/.

Sucuri 2019. WordPress Vulnerability Statistics. Viitattu 5.2.2019 https://wpvulndb.com/statistics.

Symantec 2019a. What is the Difference Between Black, White and Grey Hat Hackers? Viitattu 5.2.2019 https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html.

Symantec 2019b. What are bots? Viitattu 26.2.2019 https://us.norton.com/internetsecurity-malware-what-are-bots.html.

Symantec 2019c. What is a botnet? Viitattu 26.2.2019 https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html.

Techopedia 2019a. What is Hacktivism? Viitattu 12.2.2019 https://www.techopedia.com/definition/2410/hacktivism.

Techopedia 2019b. What is Cyberterrorism? Viitattu 12.2.2019 https://www.techopedia.com/definition/6712/cyberterrorism.

Trend Micro 2015. Understanding Targeted Attacks: What is a targeted attack? Viitattu 26.2.2019 https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/understanding-targeted-attacks-what-is-a-targeted-attack.

W3Techs 2019a, Market share trends for content management systems. Viitattu 24.1.2019 https://w3techs.com/technologies/history_overview/content_management.

W3Techs 2019b, Usage of content management systems. Viitattu 24.1.2019 https://w3techs.com/technologies/overview/content_management/all.

W3Techs 2019c, Usage statistics and market share of PHP for websites. Viitattu 1.4.2019 https://w3techs.com/technologies/details/pl-php/all/all.

W3Techs 2019d, Word Wide Web Technology Surveys. Viitattu 3.6.2019 https://w3techs.com/.

Waqas, A. 2013. Anonymous Declares Global Cyber War on U.S. Government against Hammond's Sentence and NSA Spying. Viitattu 18.2.2019 https://www.hackread.com/anonymous-launches-global-cyber-war-on-u-s-government/.

Weisman, S. 2019. What are Denial of Service (DoS) attacks? DoS attacks explained. Viitattu 15.3.2019 https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html.

WordPress 2019a. Plugins. Viitattu 24.1.2019 https://wordpress.org/plugins/.

WordPress 2019b. Features. Viitattu 28.1.2019 https://wordpress.org/about/features/.

WordPress 2019c. Support forums in your language. Viitattu 31.1.2019 https://make.wordpress.org/support/handbook/contributing-to-the-wordpress-forums/support-forums-in-your-language/.

WordPress 2019d. Requirements. Viitattu 31.1.2019 https://wordpress.org/about/requirements/.

WordPress 2019f. Security. Viitattu 5.2.2019 https://wordpress.org/about/security/.

WordPress 2019g. Make WordPress. Viitattu 31.1.2019 https://make.wordpress.org/.

WordPress 2019h. Developer Resources. Viitattu 31.1.2019 https://developer.wordpress.org/.

WordPress 2019i. Theme Directory. Viitattu 31.1.2019 https://wordpress.org/themes/.

WPBeginner 2017. What are WordPress plugins? And how do they work? Viitattu 24.1.2019 https://www.wpbeginner.com/beginners-guide/what-are-wordpress-plugins-how-do-they-work/.

WPBeginner 2018. 11 Top Reasons Why WordPress Sites Get Hacked (and How to Prevent it). Viitattu 5.2.2019 https://www.wpbeginner.com/beginners-guide/reasons-why-wordpress-site-gets-hacked/.

Väisänen, T. 2018. WordPress lisäosat – minun suosikkejani. Viitattu 31.1.2019. https://teuvovaisanen.fi/2018/04/10/wordpress-lisaosat-minun-suosikkejani/.

LIITTEET

Liite 1. Tietoturvaopas WordPress-verkkosivustoa koskevan tietoturvan parantamiseksi
Liite 2: Tietoturvaoppaan avauksessa mainitut komennot ja lisäosat suorine linkkeineen

Tietoturvaopas WordPress-verkkosivustoa koskevan tietoturvan parantamiseksi

1. Salasana ja käyttäjätunnus
    - Käytä monimutkaista salasanaa
    - Käytä pitkää salasanaa (väh. 8 merkkiä)
    - Vältä yleisiä salasanoja, kuten esim. ”password”, ”salasana”, ”123456”
    - Jokaiselle sivustolle oma salasana
    - Vältä yleisiä käyttäjätunnuksia kuten Admin tai administrator
2. Pidä WordPress päivitettynä
    - Pidä huoli siitä, että WordPress-versio on päivitettynä aina uusimpaan mahdolliseen
    - Hanki lisäosa WordPress-version automaattista päivitystä varten tai muokkaa wp-config.php tiedostoa koodinpätkällä, joka mahdollistaa WordPress-version automaattisen päivityksen (koodinpätkän löydät liitteestä 2)
3. Pidä WordPress-laajennukset päivitettyinä
    - Kuten WordPress-version kanssa, pidä huoli, että laajennukset ovat päivitettynä aina uusimpaan mahdolliseen versioon
    - Tarkasta lisäosien päivitykset viikoittain manuaalisesti, lataa lisäosa laajennusten automaattista päivitystä varten, tai lisää wp-config.php tiedostoon koodinpätkät, jotka mahdollistavat laajennusten automaattisen päivityksen (koodinpätkät löydät liitteestä 2)
4. Suosi vain luotettuja teemoja ja lisäosia
    - Lataa teemat ja lisäosat vain luotetuista lähteistä
    - Varmista että lisäosaa päivitetään säännöllisesti
    - Poista tarpeettomat laajennukset WordPressistäsi (jokainen laajennus on uusi tietoturvariski)
5. Tietokannan etuliitteet

- Muuta tietokantojen etuliitteet muodosta ’wp_’ johonkin toiseen

6. Varmuuskopioi tai varmista varmuuskopioiden saatavuus palveluntarjoajalta
   - Lisäosien ja teeman päivitys saattaa vaikuttaa sivuston ulkonäköön
   - Varmuuskopiot tuovat turvaa, ”jos” tapauksia varten
   - Ongelmien sattuessa on mahdollista palauttaa varmuuskopiosta
7. Lisää tietoturvaa lisäosilla
   - Ota käyttöön kaksivaiheinen tunnistautuminen
   - Oletuskirjautumisosoite on /wp-login.php ja /wp-admin. Määritä kirjautumissivu uudelleen, jotta hyökkääjä ei löydä helppoa luukkua Brute-force -hyökkäyksille.
   - Rajoita kirjautumisyrityksiä
8. Tilaa ja asenna sivustollesi käyttöön SSL-sertifikaatti
   - Tilaa sertifikaatti sivustollesi (useilta palveluntarjoajilta saa tilattua SSL:n)
   - SSL-sertifikaatti salaa sivustolla tapahtuvan liikenteen
   - SSL-sertifikaatilla varustetun sivuston tunnistaa https:// -alkuisesta osoitteesta sekä lukon kuvasta osoiterivillä
   - Google suosii HTTPS-alkuisia verkkosivustoja
9. Pidä huoli PHP-version päivityksestä
   - Tarkista osoitteesta https://www.php.net/supported-versions.php/ onko PHP-versiosi enää tuettu.
   - Pyydä palveluntarjoajaasi vaihtamaan PHP-versio uusimpaan
   - Uusimmat PHP-versiot ovat turvallisempia ja suorituskykyisempiä
10. Roskapostin estäminen
    - Mikäli sivuilla on lomake, suosittelen ottamaan käyttöön CAPTCHA-varmenteen, joka karsii pois robotit
    - Ota käyttöön yksi näkymätön kenttävaihtoehto lisää lomakkeille, joka erottelee botit ihmisistä
11. Wp-config
    - Estä pääsy wp-config.php tiedostoon htaccessin kautta (komento löytyy liitteestä 2)
    - Siirrä wp-config.php yhtä pykälää ylemmäs kansiohakemistossa
12. WordPress-version piilotus
    - Poista readme.html tiedosto, jotta WordPress-asennuksen versio ei ole helposti saatavilla

Tietoturvaoppaan avauksessa mainitut komennot ja lisäosat suorine linkkeineen

Tietokantojen etuliitteiden vaihtoon suoritettavat komennot ovat seuraavat:

```
RENAME table `wp_commentmeta` TO `xx_commentmeta`;
RENAME table `wp_comments` TO `xx_comments`;
RENAME table `wp_links` TO `xx_links`;
RENAME table `wp_options` TO `xx_options`;
RENAME table `wp_postmeta` TO `xx_postmeta`;
RENAME table `wp_posts` TO `xx_posts`;
RENAME table `wp_termmeta` TO `xx_termmeta`;
RENAME table `wp_terms` TO `xx_terms`;
RENAME table `wp_term_relationships` TO `xx_term_relationships`;
RENAME table `wp_term_taxonomy` TO `xx_term_taxonomy`;
RENAME table `wp_usermeta` TO `xx_usermeta`;
RENAME table `wp_users` TO `xx_users`;
```

```
UPDATE `xx_options` SET `option_name`=REPLACE(`option_name`,'wp_','xx_')
WHERE `option_name` LIKE '%wp_%';
UPDATE `xx_usermeta` SET `meta_key`=REPLACE(`meta_key`,'wp_','xx_') WHERE
`meta_key` LIKE '%wp_%';
```

Tietoturvaoppaan avauksessa mainitut lisäosat suorine latauslinkkeineen:

Askel numero **2**: Advaned Automatic Updates https://fi.wordpress.org/plugins/automatic-updater/

Askel numero **7**: WPS Hide Login https://fi.wordpress.org/plugins/wps-hide-login/
Two-Factor https://fi.wordpress.org/plugins/two-factor/
WP Limit Login Attempts https://fi.wordpress.org/plugins/wp-limit-login-attempts/

Askel numero **9**: PHP Compatibility Checker https://fi.wordpress.org/plugins/php-compatibility-checker/

Askel numero **10**: Google Captcha (reCAPTCHA) https://fi.wordpress.org/plugins/google-captcha/
WPForms https://fi.wordpress.org/plugins/wpforms-lite/
Ninja Forms https://fi.wordpress.org/plugins/ninja-forms/
Contact Form 7 Honeypot https://fi.wordpress.org/plugins/contact-form-7-honeypot/

Htaccess tiedostoon lisättävät koodirivit, toimintoa varten, joka estää pääsyn wp-config.php tiedostoon:

```
<files wp-config.php>
order allow,deny deny
from all </files>
```