Karelia-ammattikorkeakoulu
Tradenomi (AMK), Tietojenkäsittely

Tietoturva dynaamisella verkkosivustolla

Karina Kröger

Opinnäytetyö, joulukuu 2021

www.karelia.fi

Karelia AMMATTIKORKEAKOULU	**OPINNÄYTETYÖ** **Joulukuu 2021** **Tietojenkäsittelyn koulutus** Tikkarinne 9 80200 JOENSUU +358 13 260 600 (vaihde)

Tekijä
Karina Kröger

Nimeke
Tietoturva dynaamisella verkkosivustolla

Toimeksiantaja
Pohjois-Karjalan ja Japanin Naganon metsäbiotalousyhteistyön kehittämisen hanke

Tiivistelmä

Tämä opinnäytetyö käsittelee tietoturvaa dynaamisella verkkosivustolla. Opinnäytetyön tarkoituksena on antaa yleisluontoinen kokonaiskuva verkkosivuston kehitysprosessista ja sen tietoturvasta. Opinnäytetyön tavoitteena on antaa ratkaisuja erilaisten tietoturvariskien ja tietoturvahaavoittuvuuksien ennaltaehkäisemiseksi. Opinnäytetyössä tutkittiin Pohjois-Karjalan ja Japanin Naganon metsäbiotalousyhteistyön hankkeen virtuaalisen Showroom-ympäristön tietoturvatoteutusta.

Opinnäytetyön menetelmänä käytettiin laadittua kyselyä, jonka avulla Showroom-verkkosivuston tietoturvaa testattiin. Verkkosivuston kehittäjille lähetettiin kysely Showroom-verkkosivuston tietoturvasta. Kyselystä saadun tiedon sekä tehdyn tutkimustyön pohjalta pystyttiin laatimaan parannusehdotuksia virtuaalisen Showroom-verkkosivuston tietoturvan parantamiseksi.

Tietoturvaa voitaisiin vielä parantaa sijoittamalla tietokanta omalle palvelimelle. Jatkossa tietoturvan parantamiseen verkkosivustolla voitaisiin käyttää tässä opinnäytetyössä tehtyä tarkistuslistaa. Tarkistuslistan tarkoituksena on parantaa verkkosivuston tietoturvaa ja toimia tietoturvan suunnittelussa muistilistana. Tietoturva pitäisi suunnitella aina hyvin etukäteen, sillä näin voidaan ennaltaehkäistä suuria tietoturvariskejä sekä minimoida mahdollisia tietoturvahaavoittuvuuksia.

Kieli suomi	Sivuja 34 Liitteet 1 Liitesivumäärä 1

Asiasanat
verkkosivusto, tietoturva, tietokanta

Karelia
UNIVERSITY OF APPLIED SCIENCES

THESIS
December 2021
Degree Programme in Business Information Technology

Tikkarinne 9
80200 JOENSUU
FINLAND
+ 358 13 260 600 (switchboard)

Author
Karina Kroger

Title
Security on a Dynamic Website

Commissioned by
North Karelia and Japan Nagano Forest Bioeconomy Project

Abstract

This thesis is about security on a dynamic website. The purpose of this thesis is to provide a general overview of the website development process and website security. The aim of this thesis was to provide solutions to prevent various security risks and security vulnerabilities. Thesis examined the security implementation of the Virtual Showroom environment, developed in the cooperation between North Karelia and Japan Nagano Forest Bioeconomy Project.

Thesis method was a survey that tested the security of the Showroom website. Website developers were sent a query about the security of the Showroom website. Based on the information obtained from the survey and the research work carried out, suggestions for improvement were made to improve the security of the virtual Showroom website.

Website security could be further improved by placing the database on its own server. In the future, a checklist made in this thesis could be used to improve security on the website. The purpose of the checklist is to improve website security and to serve as a checklist in website security planning. Website security should always be planned well in advance, as this will prevent high security risks and minimize potential security vulnerabilities.

Language
Finnish

Pages 34
Appendices 1
Pages of Appendices 1

Keywords
website, web-security, database

Sisältö

Liitteet

1 Johdanto

Tässä opinnäytetyössä tarkastellaan tietokantoja käyttävän dynaamisen verkkosivuston mahdollisia tietoturva-aukkoja. Opinnäytetyössä tarkastellaan mitä olisi hyvä ottaa huomioon tietoturvallisessa verkkosivuston toteutuksessa, kun asiaa tarkastellaan erityisesti tietokannan tietoturvan näkökulmasta.

Tämän opinnäytetyön tavoitteena on esitellä verkkosivuston sekä tietokantojen kehittyneimpiä tietoturva-aukkoja ja haavoittuvuuksia. Opinnäytetyön tarkoituksena on tarkastella mahdollisia tietoturva-aukkoja ennaltaehkäiseviä menetelmiä erityisesti verkkosivuston tietokannan suojaamisen näkökulmasta. Tämän opinnäytetyön päätavoitteena on antaa ratkaisuja tietoturvallisen dynaamisen verkkosivuston toteuttamiseen.

Tässä opinnäytetyössä tarkastellaan verkkosivusto kehityksen kokonaiskuvaa lyhyesti ja yleisluonteisesti, sen tarkempiin tekniikoihin syventymättä. Opinnäytetyössä tarkastellaan verkkosivustokehityksen jakautumista eri osa-alueisiin sekä kahteen pääkategoriaan. Opinnäytetyön tarkoituksena on muodostaa yleisluontoinen kokonaiskuva verkkosivuston kehittämisestä ja sen tietoturvasta.

Opinnäytetyö pohjautuu Pohjois-Karjalan ja Japanin Naganon metsäbiotalousyhteistyön kehittämisen hankkeeseen, jossa toteutettiin virtuaalinen Showroom-ympäristö. Virtuaalisen Showroom-ympäristön tavoitteena oli esitellä Pohjois-Karjalaisia metsäalan yrityksiä sekä toimijoita. Verkkosivuston tehosteena toimi 360-asteinen panoraamakuva. 360-asteisessa panoraamakuvassa oli Suomen Koli-kansallismaisema. Kolin 360-panoraamakuvassa vaihtui Suomen neljä vuodenaikaa. Showroom-ympäristön vuodenajat vaihtuivat verkkosivustolla panoraamakuvaa liikuttaessa.

2 Verkkosivuston perusrakenne ja toteutustavat

Verkkosivusto on käsitteenä laaja sekä sisältää useita pienempiä osa-alueita. Verkkosivustokehityksessä kaikilla näillä osa-alueilla on omat keskeisimmät toiminnallisuudet sekä yleisesti käytetyimmät kehitystyökalut. Kun nämä pienemmät osa-alueet nidotaan yhteen, muodostuu niistä isompi kokonaisuus, verkkosivusto itsessään.

Verkkosivuston käyttäjä ei välttämättä kiinnitä niin suurta huomiota, minkä tyyppisellä verkkosivustolla tarvittava toiminta suoritetaan. Verkkosivuston sujuvan toiminnan sekä ylläpidon kannalta verkkosivuston tyypillä on kuitenkin hyvinkin iso merkitys. Seuraavissa kappaleissa tarkastella verkkosivustojen jakautumista toiminnallisuuden näkökulmasta erilaisiin verkkosivustotyyppeihin sekä verkkokehityksen kannalta kahteen tärkeään pääkategoriaan.

2.1 Staattinen verkkosivusto

Verkkosivustot voidaan karkeasti jakaa kahteen verkkosivustotyyppiin. Verkkosivuston kaksi tyyppiä ovat dynaamiset verkkosivustot sekä staattiset verkkosivustot. Staattisten verkkosivujen toimintaperiaate on paljon yksinkertaisempi kuin esimerkiksi dynaamisten verkkosivustojen toimintaperiaate. Staattisissa verkkosivustoissa ajatuksena usein on, että verkkosivustot luotaisiin kertajulkaisuna. (Tapala 2016.)

Kun verkkosivustot ovat toteutettu kertajulkaisuna, niitä tarjoillaan palvelimelle jatkossa aina muuttumattomina, seuraavaan julkaisukierrokseen asti. Toisin sanoen, staattiset verkkosivustot ovat aina samanlaiset. Staattiset verkkosivustot muuttuvat vain ja ainoastaan, jos verkkosivuston tietoja muokataan tai päivitetään suoraan palvelimelta. (Tapala 2016.)

2.2 Dynaaminen verkkosivusto

Dynaamiset verkkosivustot muodostetaan aina tietokannassa olevan tiedon pohjalta. Toisin sanoen, dynaamiset verkkosivut muodostuvat vasta kun selain pyytää sitä komennoilla. Dynaamiset verkkosivut ovat staattisia verkkosivuja huomattavasti joustavampia, mutta asettavat palvelimelle enemmän vaatimuksia. (Tapala 2016.)

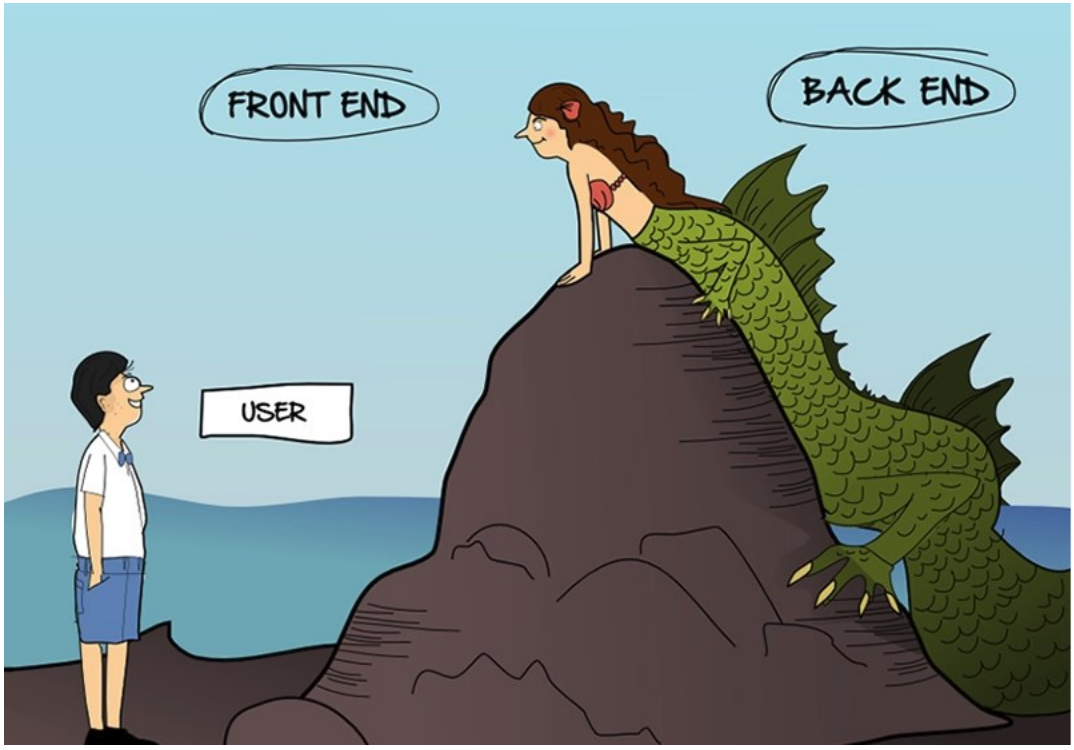
Dynaaminen verkkosivusto palauttaa käyttäjälle pyydetyn asianmukaisen tiedon. Nykyään on olemassa useita dynaamisia verkkosivustoja, joita hallitaan tietokannan kautta. Hotellihuoneiden saatavuuden tarkistaminen olisi esimerkki tällaisesta tietokantaa käyttävästä, dynaamisesta verkkosivusta. Verkkosivuston tietokannan päätarkoituksena on mahdollistaa kykyä käyttää, tallentaa ja hallita suurta tietomäärää helposti ja turvallisesti. Tietokanta on tietokokoelma, jota voidaan halutulla tavalla käyttää ja hallita. Tietokantatiedot voidaan järjestää taulukoiksi, riveiksi ja sarakkeiksi. (Javapoint 2021.)

Dynaamisen verkkosivuston rakentamiseen yksi yleisesti käytetty ohjelmointikieli on dynaaminen komentosarjakieli (JavaScript). JavaScript huolehtii nimenomaan dynaamisesta toiminnallisuudesta verkkosivustoilla. JavaScriptiä käytetään selaimen rajoitusten hallintaan, verkkoselaiminen asynkroniseen kommunikaatioon sekä käyttäjälle näytettävään sisällön hallintaan. (Wikipedia 2021.)

2.3 Verkkokehitys yleisesti

Verkkokehityksellä tarkoitetaan kaikkea kehittämistä, joka toimii Internetin kautta. Verkkokehityksellä yleensä tarkoitetaan verkkosivuston rakentamista, luomista sekä ylläpitoa. Verkkokehitys sisältää useita osa-alueita. Yleisimpiä verkkosivuston osa-alueita ovat esimerkiksi verkkosivujen suunnittelu, ohjelmointi, tietokantahallinta sekä verkkosivun julkaiseminen. (Geeksforgeeks 2021a.)

Verkkokehitys voidaan jakaa kahteen pääkategoriaan. Verkkokehityksen kaksi pääkategoriaa (kuva 1) ovat käyttäjäpuoli (frontend) sekä taustapuoli (Backend). Frontend keskittyy käyttäjäpuolen kehittämiseen, kun taas Backend keskittyy verkkosivuston taustan kehittämiseen. (Geeksforgeeks 2021a.)



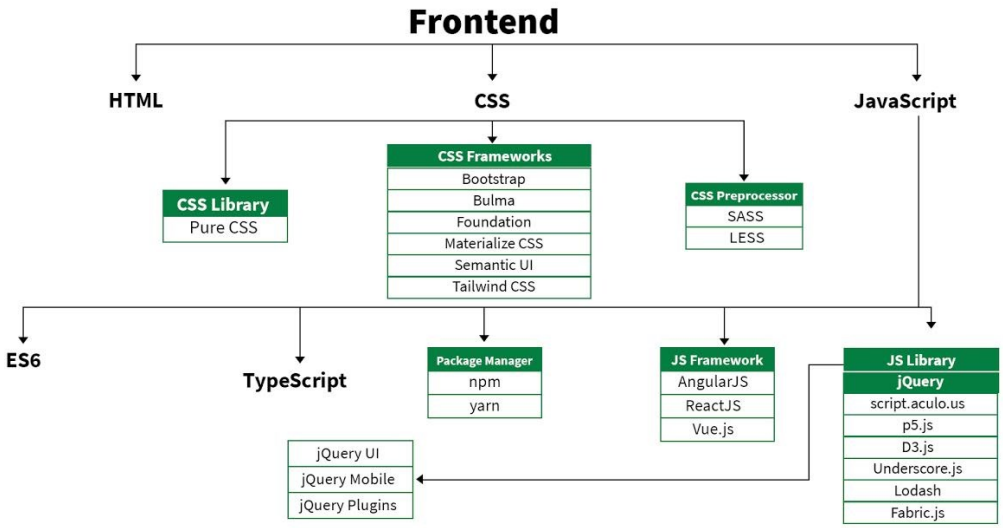
Kuva 1. What is the difference between Front-End and Back-End Web Development? (Geeksforgeeks 2019).

2.4 Frontend verkkokehitys

Verkkokehityksen frontend (kuva 2) keskittyy karkeasti verkkosivuston luurangon muodostamiseen. Frontend verkkokehitys keskittyy yleisesti ottaen kaikkeen mikä on käyttäjälle näkyvissä. Frontend keskittyy verkkosivuston käyttäjäystävällisyyteen, visualisuuteen sekä verkkosivuston responsiivisuuteen. (Geeksforgeeks 2021a.)

Frontend verkkokehityksessä perusrungon muodostamiseen käytetyimpiä ohjelmointikieliä ovat hypertekstin merkintäkieli (HTML, HyperText Markup Language) sekä tyylisivut (CSS, Cascading Style Sheets). HTML-kieli huolehtii

verkkosivuston perusrakenteesta, kun taas CSS-tyylisivut helpottavat verkkosivuston esittämistä käyttäjälle sekä huolehtivat verkkosivuston tyylittelystä. (Geeksforgeeks 2021a.)



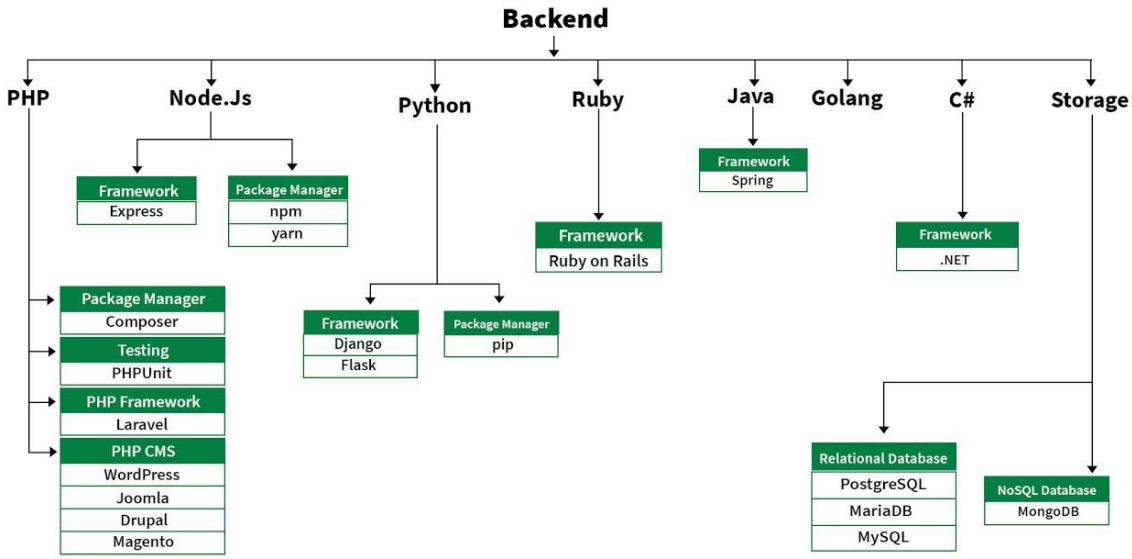
Kuva 2. Frontend Design Roadmap (Geeksforgeeks 2021a).

2.5 Backend verkkokehitys

Verkkokehityksen Backend (kuva 3) keskittyy vahvasti verkkosivuston taustan kehittämiseen. Verkkosivuston taustan kehittäminen tarkoittaa yleensä kaikkea sitä toiminallisuutta, jota käyttäjä ei pysty silmin havaitsemaan. Verkkosivuston Backend huolehtii tietojen järjestämisestä, tallentamisesta sekä hallinnasta. Verkkosivuston Backend myös huolehtii kommunikoinnista Frontend käyttöliittymän kanssa sekä varmistaa verkkosivuston sujuvan toiminnan. Verkkosivuston Backend tarkoittaa yleensä verkkosivuston palvelinpuolta ja tietokantaa sekä nimenomaan tietokannan hallintaa. (Geeksforgeeks 2019a.)

Backend verkkokehitykseen on käytössä joukko omia ohjelmointikieliä, mutta yleisimpiä teknologioita Backend-kehittämisessä on esimerkiksi Hypertext Preprocessor (PHP), joka on palvelinpuolen skriptikieli. Muita yleisesti hyväksyttyjä sekä käytettyjä Backend-ohjelmointikieliä ovat esimerkiksi hyvin

skaalautuva Java, tehokas ja integroituva Python, sekä avoimeen lähdekoodiin perustuva Node.js. (Geeksforgeeks 2021a.)



Kuva 3. Backend Design Roadmap (Geeksforgeeks 2021a).

Verkkosivustoilla käytetään suuria määriä tietoa, mutta kaikkea tietoa ei voida säilöä verkkosivustolla. Tietokanta on tämän vuoksi hyvin tärkeä osa verkkokehitystä ja kuuluu olennaisesti Backend-puoleen. Tietokantaan säilötään halutut tiedot verkkosivulta ja siksi myös tietokannan hallintajärjestelmä on tärkeä. Tietokannan hallintajärjestelmä mahdollistaa tiettyjen toimintojen suorittamisen helposti ja nopeasti sekä säilöö ja tallentaa suuren määrän tietoa, yhteen sovellukseen. Markkinoilla on saatavilla monia tietokantavaihtoehtoja, mutta yksi käytetyin avoimeen lähdekoodiin perustuva markkinoilla oleva tietokanta on MySQL-tietokanta. (Geeksforgeeks 2021b.)

Tietokannan hallintajärjestelmä käyttää tietokannan hallintaan suunniteltua strukturoitua kyselykieltä (SQL, Structured Query Language). SQL-kieli on yksi yleisimpiä kieliä, jota käytetään nimenomaan relaatiotietokantojen hallinnoimiseen. SQL-kyselyt ovat käskynä kirjoitettuja komentoja ja niiden päätarkoituksena on hakemistorakenteiden muokkaaminen, tietorivien lisääminen, päivittäminen sekä poistaminen. (Sirkin 2021.)

3 Tietoturva yleisellä tasolla

Verkkosivuston kehittäjän täytyy ymmärtää mitä tietoja verkkosivustolla näytetään ja tallennetaan sekä millä tavoin näitä arkaluontoisia tietoja pystytään parhaalla mahdollisella tavalla suojaamaan verkkoliikenteen vaaroilta. Tietoturva aiheena on monelle meille tuttu jollain tasolla ihan jokapäiväisestä elämästä. Monet meistä ovat kuulleet uutisista tietomurroista tai ovat lukeneet lehdestä pysäyttävistä kyberhyökkäyksistä.

Monien suomalaisen tuoreessa muistissa on esimerkiksi merkittävä Vastaamo Psykoterapia keskukseen kohdistunut tietomurto, joka tapahtui marraskuussa 2018. Vastaamon tietomurrossa paljastui kymmenien tuhansien suomalaisten arkaluontoisia terveystietoja, kun hyökkääjälle aukesi pääsy tietokantaan päivitettyjen serverimuutosten vuoksi. Vastaamon serverien päivitysmuutokset jättivät taakseen huomattavan tietoturva-aukon, joka mahdollisti merkittävän tietomurron. (Kärkkäinen 2020.)

3.1 Tietoturvan määritelmä

Tietoturva käsitteenä pitää sisällään lukuisia ennaltaehkäiseviä toimenpiteitä, joita esimerkiksi palveluntarjoajat ovat ottaneet käyttöön suojatakseen tietokantaa ja tiedonhallintaohjelmistoja tietoverkkohyökkäyksiltä. Tietoturvan yleisin tarkoitus on suojata tietokannan tietoja ennakoivasti haittaohjelmilta, erilaisilta uhilta, palvelunestohyökkäyksiltä sekä tietojenkalasteluhyökkäyksiltä. (Lanigan 2020.)

Tietoturva voidaan saavuttaa yleisesti ottaen monilla erilaisilla toimenpiteillä. Tietoturva voidaan parantaa esimerkiksi automaatiolla, virtaviivaisilla prosesseilla, hyvin koulutetuilla asiantuntijoilla sekä vuorokauden ympäri toimivilla suojaustyökaluilla. (Lanigan 2020.)

3.2 Kyberturvallisuus käsitteenä

Kyberturvallisuus käsitteenä tarkoittaa yleensä sellaisia toimenpiteitä, joilla voidaan ennakoivasti hallita ja tarvittaessa myös sietää kyberuhkia sekä niiden vaikutusta. Yleensä kybertoimintaympäristön toiminnan häiriintyminen aiheutuu toteutuneesta tietoturvauhasta. Kyberturvallisuuteen pyrittäessä tietoturvalla on keskeinen rooli. Tietoturvan lisäksi kyberturvallisuuteen pyritään toimenpiteillä, joiden tarkoituksena on turvata kybertoimintaympäristöstä riippuvaisia fyysisen maailman toiminnot. (TKS 2018.)

Tietoturvasta puhuttaessa yleensä tarkoitetaan tiedon saatavuutta, eheyttä ja luottamuksellisuutta. Kyberturvallisuudella taas yleensä viitattaan digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuuteen sekä sen vaikutukseen toimintoihin. (TKS 2018.)

3.3 Kyberhyökkäykset

Kyberhyökkäyksillä eli tietoverkkohyökkäyksillä tarkoitetaan sitä, kun ei laillinen käyttäjä pyrkii samaan luvattoman pääsyn tietokoneeseen, tietojärjestelmään tai tietokoneverkkoon. Tietoverkkohyökkäyksen voi käytännössä aloittaa kuka tahansa, mistä tahansa. Tietoverkkohyökkäyksen aiheuttajana voi olla yksittäinen henkilö tai isompi ryhmä. (Pratt 2021.)

Tietoverkkohyökkäyksien motiiveja on olemassa useita ja näitä voivat olla esimerkiksi tarve muuttaa, estää, poistaa, manipuloida tai varastaa joitakin järjestelmissä olevia tietoja. Tietoverkkohyökkäyksen tarkoitusperää voi myös olla tarve poistaa jotakin käytöstä tai aiheuttaa huomattavaa häirintää yrityksen liiketoiminnalle tai yksittäiselle henkilölle. Tietoverkkohyökkäyksiä voidaan aloittaa käyttämällä yhtä tai useampaa erilaista hyökkäystapaa. (Pratt 2021.)

Kyberhyökkäyksiä suorittavia ihmisiä pidetään tietoverkkorikollisina. Yleisimpiä nimiä tietoverkkorikollisille on hakkeri, huono toimija tai uhkailija. Suurin ja yleisin syy tietoverkkohyökkäyksille on tarkoitus aiheuttaa vahinkoa. Erityisesti

tietoverkkorikollisten tarkoituksena on monesti saada taloudellinen hyöty kyberhyökkäyksillä. Tietoverkkorikoksilla pyritään varastamaan usein arkaluontoisia tietoa, kuten luottokorttitietoja tai henkilön henkilökohtaisia tietoja. Verkkorikolliset pyrkivät näillä tiedoilla saamaan hyökkäyksen kohteeksi joutuneelta uhrilta rahaa tai fyysistä tavaraa varastetun henkilöllisyyden perusteella. (Pratt 2021.)

3.4 Kyberhyökkäysten historia

Historian yksi merkittävimmistä ja tarkoitusperältään tahaton kyberhyökkäys tapahtui kolmekymmentä vuotta sitten, kun Robert Morris halusi saada selville, kuinka monta laitetta Internetiin on yhdistetty. Morris kirjoitti ohjelman, jolla pääsi matkustamaan tietokoneelta toiselle. Morrisin ohjelma pyysi jokaista saavutettua laitetta lähettämään signaaliin hänen omalle ohjauspalvelimellensa. Morrisin ohjelmasta tuli historiassa ensimmäinen oman luokan kyberhyökkäys, jota nykyään kutsutaan hajautetuksi palvelunestoksi eli DDoS-hyökkäykseksi. (Theconversation 2018.)

Hajautettu palvelunestohyökkäys syntyy, kun joukko internetiin yhdistettyjä laitteita lähettää verkkoliikennettä yhteen osoitteeseen. Tämä toiminto kuormittaa verkkoliikennettä niin paljon, että koko järjestelmä sammuu tai verkkoyhteydet estetään kokonaan. DDoS-hyökkäykset ovat yhä yleisempiä hyökkäyksen muotoja. Robert Morrisin kehittämä ohjelma loi loputtoman pohjan mahdollisille haavoittuvuuksille ja tuhoille. Robert Morrisin kirjoittama ohjelma tunnetaan historiassa myös nimellä ”Morris-mato”. (Theconversation 2018.)

4 Kehittyneet kyberuhat

Tunnettu Morrisin Mato on jäänyt elämään kehittyneiden tietoturvauhkien joukkoon DDoS-kyberhyökkäyksen muodossa. Internetin vaarallisessa maailmassa on olemassa kuitenkin myös joukko muita kehittyneinä kyberuhkina

pidettyjä tietoturvahaavoittuvuuksia. Kehittyneellä tietoturvauhalla tarkoitetaan yleisesti ottaen kaikkea sellaista uhkaa, joka hyvästä tietoturvasta huolimatta pystyy läpäisemään suojaukset.

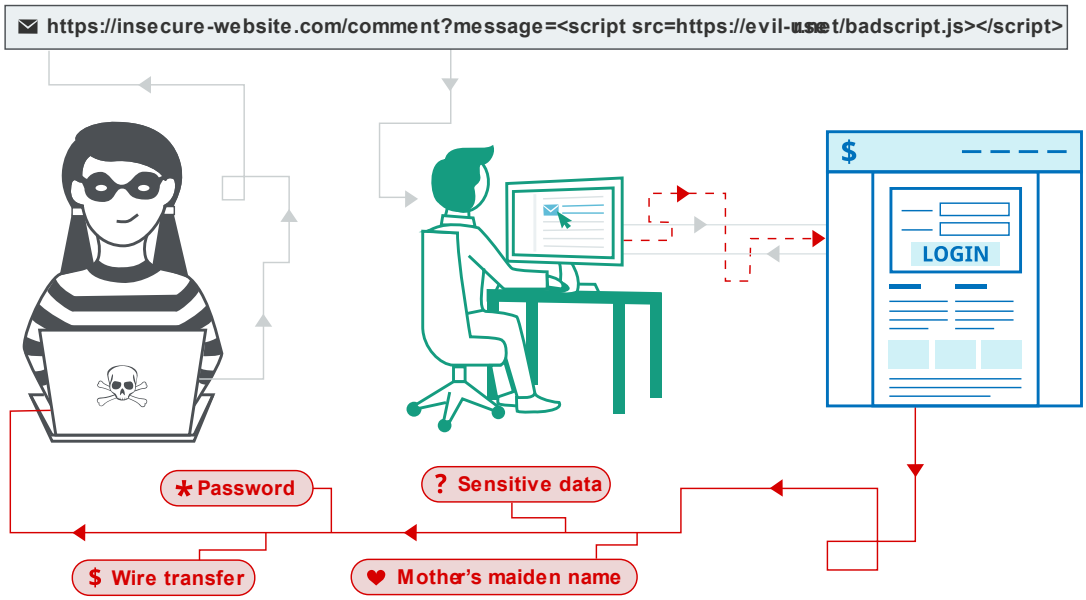
Kehittyneet tietoturvahaavoittuvuudet ovat suuri uhka verkkosivustoille sekä tietokannoille. Kehittyneet tietoturvauhat olisi hyvä ottaa huomioon niin verkkosivuston kehittämisen näkökulmasta, kuin myös verkkosivuston jatkuvan ylläpidon kannalta. Seuraavaksi tarkastellaan muutamia merkittävimpiä ja kehittyneimpiä tietoturvauhkia verkkosivustojen sekä tietokannan näkökulmasta.

4.1 Sivustojen välinen komentosarja

Sivustojen välinen komentosarja (XSS, Cross Site Scripting) on termi, jota käytetään kuvaamaan verkkosuojahaavoittuvuutta. XSS-hyökkäyksessä (kuva 4) hyökkääjä laittaa JavaScript skriptejä muiden käyttäjien selaimiin. XSS-hyökkäyksessä hyökkääjä saa käyttöönsä sivuston valtuutusevästeet. Kun hyökkääjällä on onnistunut saamaan valtuutusevästeet käytössään, hän voi kirjautua käyttäjänä verkkosivustolle. XSS-hyökkäyksessä hyökkääjällä on pääsy kaikkiin samoihin tietoihin kuin laillisella käyttäjällä olisi, hyökkääjä pääsee kiinni käyttäjän yhteystietoihin, luottokorttitietoihin sekä salasanojen vaihtoon. (Xiong, Xuan, Zhao & Huang 2012.)

XSS-hyökkäyksessä on kaksi päätyyppiä. Ensimmäinen päätyyppi on heijastettu XSS-hyökkäys, jossa haittaohjelma tulee yleensä nykyisestä HTTP-pyynnöstä. Toinen päätyyppi on tallennettu XSS-hyökkäys, jossa haittaohjelma tulee yleensä sivuston tietokannasta. Vähemmän tunnettu DOM-pohjainen XSS-hyökkäys on haavoittuvuus, joka yleensä esiintyy asiakaspuolen koodissa palvelinpuolen koodin sijasta. XSS-haavoittuvuudessa hyökkääjä, joka käyttää sivustojen välistä komentosarjojen haavoittuvuutta, pystyy naamioitumaan lailliseksi käyttäjäksi. Tämä toiminto mahdollistaa hyökkääjän pääsyn käyttäjän kirjautumistietoihin. Päästyään käyttäjän kirjautumistietoihin, hyökkääjä pystyy suorittaa samoja toimintoja kuin laillinen käyttäjä sekä kykenee esimerkiksi

lisäämään muita ikäviä haittoja verkkosivustolle. (Xiong, Xuan, Zhao & Huang 2012.)



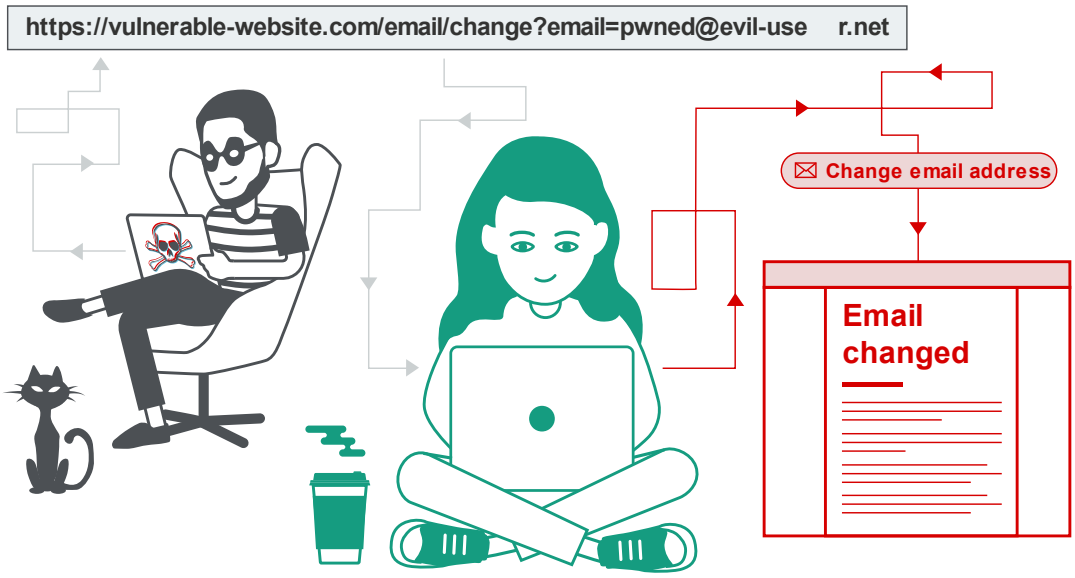
Kuva 4. Cross-site scripting (Portswigger 2021a).

4.2 Sivustojen välinen pyyntöväärennös

Sivustojen välinen pyyntöväärennös (CSRF, Cross Site Request Forgery) on termi, jota yleensä käytetään, kun hyökkääjä saa uhrin eli laillisen käyttäjän suorittamaan haluamansa toiminnon tahattomasti (kuva 5). Laillisen käyttäjän tahaton toiminto voi olla esimerkiksi salasanan vaihtaminen, sähköpostin vaihtaminen tai laillisen käyttäjän varojen siirtäminen. CSRF-hyökkäyksessä riippuen toiminnon luonteesta hyökkääjä saattaa saada täyden hallinnan laillisen käyttäjän tilistä. Jos hyökkääjän uhrilla eli laillisella käyttäjällä on CSRF-hyökkäyksen syntyessä etuoikeutettu rooli vaarantuessa sovelluksessa, saattaa hyökkääjä pystyä hallitsemaan kaikkia toimintoja ja laillisen käyttäjän tietoja. (Portswigger 2021.)

CSRF-hyökkäysten ideana yleensä on se, että hyökkäys kohdistuu verkkosivustoon, joka ei osaa erottaa toisistaan kelvollista pyyntöä ja hyökkääjän hallitsemaa väärennettyä pyyntöä. Hyvä esimerkki tästä

hyökkäyksestä olisi pankin käyttämä verkkosivusto, joka voisi olla altis CSRF-hyökkäykselle. Hyökkääjä luo uuden URL-osoitteen ja yrittää saada käyttäjän napsauttamaan hänen luomaan väärennettyä osoitetta. Kun käyttäjä suorittaa tahattomasti hyökkääjän haluamansa toiminnon ja on myös samanaikaisesti aktiivisessa istunnossa pankin verkkosivustolla, pyrkii hyökkääjä siirtämään laillisen käyttäjän varat hänen tililtään. Hyökkääjät voivat yrittää hyödyntää CSRF-haavoittuvuutta monella tavalla. (Synopsys 2021.)



Kuva 5. Cross-site request forgery (Portswigger 2021b).

4.3 Palvelunestohyökkäys

Palvelunestohyökkäys (DoS, Denial of Service Attack) on termi, jota yleensä käytetään kuvaamaan tietoturvauhkaa, joka ilmenee kun, hyökkääjä estää käyttäjiä käyttämästä laillisia resursseja. DoS-hyökkäyksessä hyökkääjä voi evätä käyttäjiltä pääsyn verkkoon, tietokonejärjestelmiin tai muihin palveluihin. DoS-hyökkäyksissä hyökkääjä tyypillisesti täyttää verkkoliikenteen siten, että käyttäjän pääsy niihin on hankaloitunut tai estetty kokonaan. (Ferguson & Loshin 2021.)

Nykypäivän DoS-hyökkäysten motiivina on yleensä halu vahingoittaa kohteeksi joutuneen yrityksen tai organisaation mainetta tai liiketoimintaa. DoS-hyökkäystä epäiltäessä olisi hyvä ottaa yhteyttä internet-palveluntarjoajaan. Palvelun hidas suorituskyky voi esimerkiksi johtua DoS-hyökkäyksestä. Palveluntarjoajalta olisi hyvä varmistaa mistä palvelun hidas suorituskyky johtuu. Internet-palveluntarjoajat pystyvät ohjaamaan liikenteen tarvittaessa uudelleen ja näin estämään mahdolliset DoS-hyökkäykset. Verkkoliikenteen uudelleenohjaus voi tasapainottamaan kuormitusta ja näin myös lieventää merkittävästi mahdollista DoS-hyökkäystä. (Ferguson & Loshin 2021.)

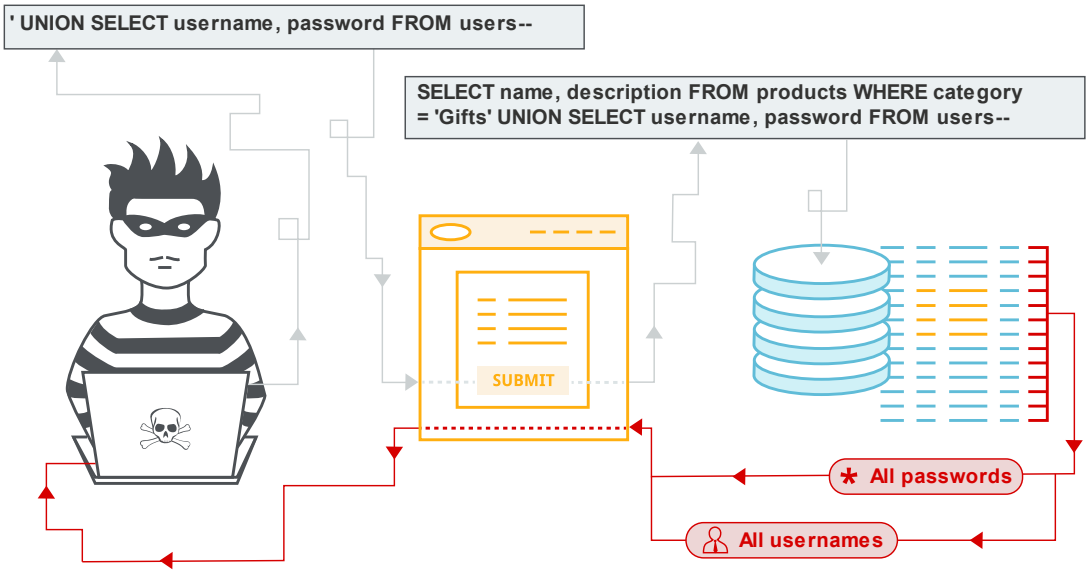
4.4 SQL-ruiskutus

Nykypäivän suurten organisaatioiden hallinnassa on valtava määrä arkaluontoista tietoa. Kaikki tämä tieto kerätään, tallennetaan ja hallinnoidaan yleensä tietokantoihin. Tämä tekee tietokannoista erittäin arvokkaan ja esisijaisen kohteen kyberhyökkäyksille. Tietokantoihin kohdistuva, yksi yleisin ja kehittynein kyberhyökkäys on SQL-ruiskutushyökkäys (SQL injection). (Xiong, Xuan, Zhao & Huang 2012.)

SQL-ruiskutushyökkäys on termi, jota käytetään kuvaamaan toimintaa jossa, hyökkäys koostuu SQL-kyselyn lisäämisestä, eli toisin sanoen ruiskutuksesta asiakkaan sovellukseen syöttämien tietojen kautta (kuva 6). SQL-ruiskutukset ovat hyvin yleisiä PHP- ja ASP-sovelluksissa. SQL-ruiskutushyökkäyksen onnistuessa hyökkääjä voi lukea arkaluontoista tietoa tietokannasta sekä muokata tietokannan tietoja poistamalla, lisäämällä tai muokkaamalla niitä. (Security Project 2021.)

SQL-ruiskutushyökkäyksessä hyökkääjä pystyy suorittamaan tietokannan hallintatoimia, joilla voi olla vakavat seuraukset. SQL-ruiskutushyökkäyksessä hyökkääjällä on yleensä pääsy kaikkeen arkaluontoiseen tietoon. Hyökkääjällä on esimerkiksi pääsy hallitsemaan tietokantatietojen täydellistä paljastumista. Hyökkääjällä on myös yleensä pääsy tietokantatietojen tuhoamiseen sekä

henkilöllisyyden väärentämiseen. Yleisesti ottaen SQL-ruiskutushyökkäys luokitellaan erittäin vakavaksi tietoturvauhkaksi. (Security Project 2021.)



Kuva 6. SQL injection (Portswigger 2021c).

5 Verkkosivuston perustietoturvatasot

Tietoturva ei yleisesti ottaen ole yksiselitteinen asia vaan tarvitsee jatkuvaa valppautta ja varautumista sivuston ylläpidolta. Kaikilla käyttäjillä on vapaa pääsy verkkosivustoille ja näin ollen olisi todella tärkeää huolehtia verkkosivustojen riittävistä tietoturvatasoista. Verkkosivustojen tietoturva on käsitteenä hyvin laaja eikä se sisällä yhtä ja ainoaa oikeaa tapaa, jolla varmistetaan täydellinen verkkosivustojen tietoturva.

Verkkosivustojen kehittämiseen sekä ylläpitoon on kuitenkin olemassa yleisiä suosituksia, joilla voidaan varmistaa perustietoturvatasot kaikilla verkkosivustoilla. Seuraavaksi tarkastellaan niitä tapoja, joiden avulla perustason tietoturva voitaisiin tarkistaa ja varmistaa kaikilla verkkosivustoilla.

5.1 Verkkopalvelin

Yksi verkkoinfrastruktuurin tärkeimmistä ja kriittisimmistä osista on sen verkkopalvelin. Verkkopalvelin vastaa verkkosivuston palvelun ylläpidosta, tiedostojen ylläpidosta sekä siihen liittyvän koodin ylläpidosta. Verkkopalvelimen turvallisuuden näkökulmasta verkkosivustojen kehitystyössä olisi esimerkiksi tärkeää pitää eri tarkoituksiin käytettäviä ympäristöjä omilla verkkopalvelimilla. Kehitystyössä käytettyjä ympäristöjä voisivat esimerkiksi olla kehitys- ja testiympäristöt sekä erillinen tuotantoympäristö. (Cyblance 2021.)

Eri ympäristöjen käyttäjäoikeuksia sekä pääsyä näihin eri ympäristöihin ja järjestelmiin olisi syytä pitää aina roolien tasolla sekä pyrkiä välttämään tarpeettoman isojen oikeuksien antamista käyttäjille, ellei tähän ole erikseen perustetta. Tietoturvan varmistamiseksi verkkosivustolla olisi hyvä pitää verkkopalvelin aina päivitettynä uusimmilla ja ajankohtaisimmilla tekniikoilla sekä määritellä esimerkiksi sallitut palvelimet ja muut lokit. (Cyblance 2021.)

5.2 Tietokanta- ja verkkosovellus palomuurit

Hyvä tapa suojautua tietokannan tietoturvauhkilta on ottaa käyttöön tehokkaat palomuurit. Palomuurit ovat ohjelmistoja, jotka pystyvät suodattamaan haitallisen verkkoliikenteen. Palomuurit suodattavat tietyistä sovelluksista tai verkkopalvelimelta tulevan verkkoliikenteen ja niiden tarkoituksena on myös suojata tietokannasta lähtevien yhteyksien muodostumista, ellei sille ole perustetta. (eSecurity Planet 2021.)

Tietokannan palomuurin lisäksi on myös tärkeää käyttää verkkosovellusten palomuureja. Hyvin yleinen väärinkäsitys on siinä, että verkkopalvelimen suojaamisella ei ole mitään tekemistä tietokannan kanssa. Tämä ajattelutapa ei ole ollenkaan paikkansapitävä. Hyvä sovelluspalomuuri suojaa verkkosivustoa useilta yleisiltä kyberhyökkäyksiltä sekä uhilta kuten, verkkosivustojen väliseltä komentosarjalta (CSRF) sekä SQL-ruiskutushyökkäyksiltä. Palomuuri voi auttaa pitämään tietokantaan tallennetut arkaluontoiset tiedot poissa uteliailta katseilta

sekä estämään hyökkääjän SQL-kyselyjen syöttämisen. (AppliCure Technologies 2021.)

5.3 Tietokantapalvelin

Tietokanta on osa, jonka tietoturvaan pitäisi erityisesti panostaa. Tietokannan olisi hyvä aina sijaita omalla erillisellä tietokantapalvelimella, joka sijaitsisi vielä erikseen oman erillisen palomuurin takana. Tietokantaa ei koskaan pitäisi sijoittaa verkkopalvelimen kanssa samalle demilitarisoidulle alueelle (DMZ), joka selkokielellä tarkoittaa aliverkkoa. Verkkopalvelimeen hyökätään yleensä todennäköisemmin, koska se sijaitsee DMZ-alueella eli on siten julkisesti saatavilla. Jos verkkopalvelin vaarantuu ja tietokantapalvelin toimii samalla koneella, hyökkääjällä on pääsy tietokantaan ja tietoihin pääkäyttäjänä. Oman tietokantapalvelimen asennus on monimutkaisempaa, mutta tietoturvaedut ovat kaiken vaivan arvoisia. (AppliCure Technologies 2021.)

Tietokantapalvelimen tietoturvallisuuden takaamiseksi olisi hyvä aina pitää päivitykset ajan tasalla suosittujen kirjatietojen kanssa ja huolehtia vaadittavista käyttöjärjestelmän korjauksista. Verkkoliikennettä sekä palvelulokeja olisi hyvä seurata ja varmistaa asianmukainen mekanismi palvelinliikenteen sekä lokien seuraamiseksi. Käyttäjien kouluttaminen on monesti avainasemassa tietoturvan kannalta. Kaikki palvelimille tehtävät muutokset olisi hyvä kirjata, tarkistaa ja hyväksyä erikseen. Tietokannan kirjautumistietoja olisi tärkeää suojata sekä salata ottamalla käyttöön erilliset käyttäjätunnukset erillisille verkkosovelluksille. (Cyblance 2021.)

5.4 Tietokannan pääsynvalvonta

Tietokannan suojaus koostuu yleisesti ottaen kahdesta osasta, tietovierailusta sekä tietojen palauttamisesta. Tietovierailulla tarkoitetaan sitä, että käyttäjällä on laillinen pääsy oikeaan tietoon. Tietojen pääsyrajauksella rajataan yleensä käyttäjän pääsy kaikkeen ylimääräiseen tietoon, johon pääsy ei ole tarpeen.

Tietojen palautuksella yleensä tarkoitetaan sitä, että tietokanta pystyy palauttamaan pyydetyt tiedot täydellisesti ja turvallisesti. (Xiong, Xuan, Zhao & Huang 2012.)

Tietokannan suojauksessa olisikin hyvin tärkeää ottaa huomioon, että mahdollisimman vähän ihmisiä pääsisi tietokantaan. Järjestelmänvalvojilla olisi hyvä olla vain vähimmäisoikeudet tietokantaan ja vain sellaiset oikeudet, joita he tarvitsevat työssään. Pienemmille organisaatioille suppeat oikeudet eivät ehkä ole käytännöllistä, mutta käyttöoikeuksia olisi hyvä siinä tapauksessa hallita vähintään ryhmien tai roolien avulla. (eSecurity Planet 2021.)

Jos kyseessä on suurempi organisaatio, on suositeltavaa harkita käytön hallinnan automatisointia kulunhallintaohjelmiston avulla. Tämä toiminto antaa valtuutetuille käyttäjille väliaikaisen salasanan ja oikeudet, joita he tarvitsevat päästäkseen tietokantaan. Toiminto myös kirjaa suoritetut toimet ja estää järjestelmänvalvojia jakamasta salasanoja. Vaikka järjestelmänvalvojat voivat pitää salasanojen jakamista kätevänä, tämä tekee tietokannan asianmukaisen turvallisuuden ja vastuuvelvollisuuden lähes mahdottomaksi. (eSecurity Planet 2021.)

Tietokannan suojaamiseksi olisi myös hyvä varmistaa, että tilin tavanomaisia suojausmenettelyjä noudatetaan, kuten otetaan käyttöön vahvat salasanat. Käyttäjätilit olisi aina hyvä lukita kolmen tai neljän pieleen menneen kirjautumisyrityksen jälkeen. Olisi hyvä ottaa käyttöön menettely, jossa käyttäjätilit poistettaisiin käytöstä, kun henkilöstö on lähtenyt tai siirtynyt eri tehtäviin. Tietokannan toimintaa olisi myös hyvä seurata jatkuvasti. Tämä tarkoittaisi käyttöjärjestelmän ja tietokannan kirjautumisten sekä kirjautumisyritysten jatkuvaa seurantaa. (eSecurity Planet 2021.)

Tietokantaa olisi tärkeää seurata ja tarkistaa lokeja säännöllisesti epänormaalin toiminnan havaitsemiseksi. Organisaatiossa voitaisiin myös luoda automaattisia hälytyksiä ilmoittaakseen asianomaisille kuten tiimin jäsenille, kun mahdollisesti haitallista toimintaa on havaittu. Tehokkaan valvonnan avulla voidaan havaita, milloin tili on vaarantunut tai onko työntekijä suorittanut mahdollisesti

epäilyttävää toimintaa. Seuranta auttaa määrittämään jakavatko käyttäjät tilejä sekä varoittaa, jos tilit on luotu ilman lupaa tai jos asialla on ollut mahdollisesti hakkeri. (eSecurity Planet 2021.)

5.5 Kehittyneiden kyberuhkien torjunta

Kehittyneillä tietoturvauhkilla tarkoitetaan yleensä sellaisia uhkia, jotka pystyvät vahingoittamaan verkkosivustoa tai tietokantaa suojauksesta huolimatta. Kehittyneimpiä tietoturvauhkia verkkosivuston näkökulmasta ovat sivustojen välinen komentosarjahyökkäys (XSS), sivuston välinen pyyntöväärennös (CSRF), palvelunestohyökkäykset (DoS ja DDoS) sekä SQL-ruiskutushyökkäys (SQL injection), joka kohdistuu verkkosivuston tietokantaan.

Verkkosivustojen komentosarjahyökkäyksen ennaltaehkäisemiseksi (XXS) on hyvin tärkeää varmistaa, että verkkosovellukset, jotka hyväksyvät käyttäjien syöttämät syötteet, on ”desinfioitu”. Verkkosivujen kehittäjän näkökulmasta tulee varmistaa, että verkkosivuston syötteet suodattavat pois kooditulot, kuten esimerkiksi HTML ja JavaScript-koodit. Verkkosivuston käyttäjän on hyvä poistaa komentosarjat käytöstä selaimillaan ja välttää epäilyttävien osapuolten tai lähettäjien linkkien napsauttamista. (Trendmicro 2021.)

Paras tapa suojautua sivuston välistä pyyntöväärennöstä vastaan (CSRF) on sisällyttää CSRF-istuntotunniste asiaan kuuluviin pyyntöihin. Tunnisteen pitäisi olla ennustettavissa suurella entropialla, kuten istuntomerkkien yleensä. CSRF-tunnisteen täytyy olla sidottu käyttäjän istuntoon sekä tiukasti tarkistettu kaikissa tapauksissa ennen asianomaisen toimenpiteen suorittamista. (Portswigger 2021.)

Palvelunestohyökkäystä sekä hajautettua palvelunestohyökkäystä (DoS ja DDoS) vastaan puolustautumiseen useat asiantuntijat suosittelevat tuotteita, jotka pystyvät havaitsemaan DoS ja DDoS-hyökkäyksiä. Näiden palveluiden tarkoituksena on toimia samoilla periaatteilla kuin jotkut tunkeutumisen

havaitsemisjärjestelmät, tunkeutumisen estojärjestelmät sekä palomuurit tekevät. (Ferguson & Loshin 2021.)

Yleensä DoS-hyökkäyksen kohdistuessa palvelimeen hyökkäyksestä saatetaan toipua nopeasti järjestelmän uudelleenkäynnistämisellä. Jos taas DoS-hyökkäys kohdistuu verkkoliikenteeseen, on toipuminen hankalampaa. Hyökkäys voi myös olla eri lähteistä saapuva hajautettu DDoS-hyökkäys, josta toipuminen on yleensä hankalaa. (Ferguson & Loshin 2021.)

Paras tapa suojautua tietokantaan kohdistuvaa SQL-ruiskutushyökkäystä vastaan on kartoittaa mahdolliset riskit ja pyrkiä ennaltaehkäisemään ne etukäteen. SQL-ruiskutushyökkäyksen ennaltaehkäisemiseksi on tärkeää varmistaa syötteen validointi. Syötteen validointi varmistaa sen, että syöte on hyväksytyn tyylinen. Syötteen tulee olla oikean pituinen sekä muotoinen. (Positive Technologies 2019.)

Syötteen validointiprosessin ideana on, että vain läpäissyt arvo voidaan tässä tapauksessa käsitellä. Syötteen validointiprosessi auttaa torjumaan syöttömerkkijonoon lisättyjä komentoja. Syötteen validointiprosessin päätarkoituksena on siis varmistaa, että syöte on turvallista hyväksyä. Syötteen validointiprosessi on tavallaan sama kuin katsoisi, kuka koputtaa oveen ennen varsinaista oven avaamista. (Positive Technologies 2019.)

SQL-ruiskutushyökkäyksen ennaltaehkäisemiseksi on myös tärkeää varmistaa parametriset kyselyt. Parametriset kyselyt ovat keino SQL-käskyn esikääntämiseen. SQL-käsky käännetään, että voidaan antaa parametrit käskyn suorittamista varten. Tämän menetelmän avulla tietokanta voi tunnistaa koodin sekä erottaa sen syötetiedoista. Parametristen kyselyjen käyttäminen on yksi tapa vähentää SQL-ruiskutushyökkäysten riskiä. (Positive Technologies 2019.)

6 Pohjois-Karjalan ja Japanin Naganon metsäbiotalousyhteistyön hanke

6.1 Opinnäytetyön toteutuksen kuvaus

Tämän opinnäytetyön toimeksianto sekä toteutus kytkeytyy Karelia-ammattikorkeakoulun Japanin Naganon metsäbiotalousyhteistyön hankkeeseen. Karelia-ammattikorkeakoulu toteutti yhdessä Pohjois-Karjalan maakuntaliiton, Luonnonvarakeskus LUKE:n, Itä-Suomen yliopiston, Pohjois-Karjalan koulutuskuntayhtymä Riverian ja Business Joensuu Oy:n kanssa 2-vuotisen Pohjois-Karjalan ja Japanin Naganon metsäbiotalousyhteistyön kehittämisen hankkeen. (Pohjois-Karjalan Maakuntaliitto 2019.)

Metsäbiotalousyhteistyön hanke konkretisoi lokakuussa 2019 Joensuussa solmittujen kahden metsäbiotalouden laaja-alaisen kehittämisyhteistyö aiesopimuksen toteutusta, ja rakensi monitahoista yhteistyötä kumppani alueiden Pohjois-Karjalan, Japanin Naganon maakunnan ja Naganon Inan kaupungin välille. (Pohjois-Karjalan Maakuntaliitto 2019.)

Hankkeen tavoitteena oli pohjoiskarjalaisten metsäbiotalousalan yritysten ja tutkimus-, kehitys, ja koulutusorganisaatioiden monipuolisen osaamisen, asiantuntemuksen, tuotteiden ja palveluiden vienti Japaniin metsätalouden kehittämiseksi maassa. Vastavuoroisesti hankkeessa oli tarkoitus avustaa japanilaista osaamista, asiantuntemusta ja yrityksiä yhteistyön rakentamisessa ja verkostoitumisessa pohjoiskarjalaisten toimijatahojen kanssa. (Pohjois-Karjalan Maakuntaliitto 2019.)

6.2 Virtuaalinen Showroom-ympäristön toteutus

Pohjois-Karjalan ja Japanin Naganon metsäbiotalousyhteistyön hanke toteutettiin Karelia-ammattikorkeakoulun tietojenkäsittelyn koulutusohjelman eri

koulutusalojen opiskelijoiden projektitöinä. Metsäbiotalousyhteistyön hanke niputettiin kevään 2021 Web-ohjelmoinnin opintojen ICT-toimeksiantoprojektiin.

ICT-toimeksiantoprojektin tavoitteena oli virtuaalisen Showroom-ympäristön suunnittelu sekä toteuttaminen Pohjois-Karjalan metsäbiotalousalan ja sen toimijoiden esittäytymistä ja yhteydenpitoa varten. ICT-toimeksiantoprojektin ryhmätöiden tavoitteena oli toteuttaa 360-panoraamakuvalla tehostetut virtuaaliset Showroom-ympäristöt.

Virtuaalisen Showroom-ympäristön taustatehosteeksi luotiin Suomen eri vuodenajoilla vaihtuva 360-panoraamakuvan Kolin kansallismaisemasta. Kolin 360-asteen panoraamakuvassa vaihtuivat Suomen neljä eri vuodenaikaa. Panoraamakuvan vuodenajat vaihtuvat 360-kuvaa pyörittäessä verkkosivustolla. Käyttäjä pystyi pyörittämään kuvaa haluamaansa suuntaan.

Showroom verkkosivustolle lisättiin 360-asteisen kuvatehosteen lisäksi erilaisia toimintoja yritysesittelyä varten. Verkkosivustolle lisättiin valikoita, yrityskuvauksia sekä tietoja eri toimialayrityksistä. ICT-toimeksiantoprojektin lopussa valittiin yksi verkkosivusto, jonka työstämistä jatkoi kaksi Karelia-ammattikorkeakoulun kehittäjää ICT-toimeksiantoprojektin päädyttyä.

7 Verkkosivuston tietoturvan testaus

Valmis verkkosivusto olisi hyvä aina testata tietoturvariskien kartoittamiseksi sekä tietoturva-aukkojen ennaltaehkäisemiseksi. Verkkosivuston testaus voidaan jakaa kahteen kategoriaan. Frontend testaukseen, joka keskittyy verkkosivuston käyttäjäpuolen testaamiseen sekä Backend testaukseen, joka keskittyy taustan testaamiseen eli tietokannan testaamiseen.

Verkkosivustojen testaus auttaa vähentämään ja ennaltaehkäisemään tietoturvariskejä sekä tietoturvahaavoittuvuuksia. Verkkosivuston sekä tietokannan testauksessa olisi aina hyvä tarkistaa, että käyttöliittymä näyttäytyy

ja toimii kuten se on suunniteltu sekä varmistaa, että testauksen taustapuoli palauttaa asianmukaiset tiedot sekä toimii tietoturvallisesti.

7.1 Frontend käyttöliittymätestaus

Käyttöliittymätestaus (Frontend), voidaan myös kutsua toiselta nimeltään Graafiseksi käyttöliittymätestaukseksi, on tapa testata käyttäjäpuolen toiminnallisuutta verkkosivustolla. Käyttöliittymätestaukseen yleensä sisältyy kaikki sellaiset kohteet, jotka ovat jollain tavalla käyttäjälle näkyvillä olevia elementtejä ja tietoja. (Hamilton 2021.)

Frontend-testaus sisältää esimerkiksi lomakkeiden, kaavioiden, raporttien sekä verkkosivuston valikoiden testauksen. Näiden lisäksi verkkosivustolla voidaan testata esimerkiksi tekstikenttiä, kalentereita, sivun navigointia ja painikkeita sekä koko verkkosivuston yleisilmettä ja käyttäytymistä. (Hamilton 2021.)

7.2 Backend taustatestaus

Backend-testauksella yleisesti ottaen tarkoitetaan tietokannan testausta. Tietokannan tietoturvan testauksella selvitetään tietokantatietojen eheys sekä johdonmukaisuus. Tietokannan testauksella voidaan selvittää, miten tietokanta reagoi erilaisissa tilanteissa sekä testata tietokannan suoriutumiskyky tietokantaa stressaavilla kyselyillä. Tietokantatestaus tietoturvan näkökulmasta on tärkeää siksi, että auttaa välttämään tietojen katoamista, tallentaa keskeytetyt tapahtumatiedot sekä estää luvattoman pääsyn tietokantatietoihin. (Hamilton 2021.)

Toimivan tietokantasuojainfrastruktuurin näkökulmasta olisi siis tärkeää testata tietokannan suoriutuminen myös todellista hyökkäystä vastaan. Tietokannan testaus tai ”hakkerointi” vie lähemmäksi hyökkääjän ajattelutapaan ja voi auttaa löytämään tietoturvahaavoittuvuuksia, joita on mahdollisesti voitu unohtaa ottaa huomioon tietoturvaa suunniteltaessa. (eSecurity Planet 2021.)

7.3 Virtuaalisen Showroom-ympäristön testaus

Virtuaalisen Showroom-ympäristön tietoturvan testaaminen suoritettiin tutkimustyön pohjalta laaditun kyselyn avulla. Selvitystyössä laadittiin kysely verkkosivustoa ylläpitäville kehittäjille. Selvitystyön tarkoituksena oli saada selville millä tavoin tietoturva on otettu huomioon virtuaalisessa Showroom-ympäristötoteutuksessa. Selvitystyössä haluttiin saada selville, millaisia asioita verkkosivustolla on otettu huomioon tietoturvan näkökulmasta.

Selvitystyössä saatuja tuloksia hyödynnettiin tämän opinnäytetyön luvun 8 tarkastelussa, Virtuaalisen Showroom-ympäristön tietoturvatoteutus. Seuraavassa luvussa tarkastellaan virtuaalisen Showroom-verkkosivuston kyselyssä saatuja tuloksia. Selvitystyössä käytetty kysely on tämän opinnäytetyön liitetiedostona.

8 Virtuaalisen Showroom-ympäristön tietoturvatoteutus

Verkkosivustojen kehittämisen ja ylläpidon kannalta on tärkeää huolehtia verkkosivuston tietoturvan täyttymisestä. Verkkosivustolla olisi hyvä olla huomioituna vähintään perusasiat tietoturvan näkökulmasta. Perustietoturvalla varmistetaan sellainen tietoturvataso, jolla verkkosivustoa voidaan ylipäätään käyttää tietoturvallisesti.

Seuraavissa kappaleissa tarkastellaan luvun 5 tutkimustyössä saatujen tulosten sekä luvun 7 pohjalta saatujen kyselytulosten pohjalta niitä asioita, joita olisi hyvin tärkeää ottaa huomioon verkkosivuston tietoturvatoteutuksessa. Saatuja tuloksia tarkastellaan Virtuaalisen Showroom-verkkosivuston näkökulmasta. Kyselyssä saatujen tulosten pohjalta laadittiin tarkistuslista tietoturvan jatkokehitykseen sekä suunnitteluun.

8.1 Tarkistuslista

Tähän tarkistuslistaa on poimittu verkkosivustojen tietotuvallisuuden kannalta tärkeitä tietoturva-asioita. Tarkistuslista on laadittu tietoturvan varmistamiseen, sekä suunnitteluun virtuaalisella Showroom-verkkosivustolla. Tarkistuslistaan on poimittu tärkeitä tietoturva-asioita tutkimustyön sekä kehittäjille lähetetyn kyselyn ja kyselystä saatujen tulosten pohjalta. Virtuaalisen Showroom-verkkosivuston tietoturvaa voitaisiin jatkokehityksessä tarkistaa sekä varmistaa seuraavien tietoturva-asioiden osalta.

- Suojaa verkkopalvelin palomuurilla
- Pidä eri tarkoituksiin tarkoitettujen ympäristöjä eri palvelimilla
- Käytä erillisiä käyttäjätunnuksia erillisillä verkkosivustoilla
- Rajaa eri ympäristöjen käyttöoikeuksia
- Anna vain tarpeelliset käyttöoikeudet
- Sijoita tietokanta aina omalle palvelimelle
- Pidä tietokantapäivitykset aina ajan tasalla
- Seuraa tietokantapalvelimen verkkoliikennettä sekä lokeja
- Käytä palomuureja verkkosivustolla
- Määritä sallitut palvelimet sekä lokit verkkosivustolle
- Seuraa ja dokumentoi palvelimilla tapahtuvia muutoksia
- Huolehdi tietokannan tehokkaasta valvonnasta
- Käytä vain vahvoja salasanoja
- Päivitä palvelimet aina ajankohtaisilla tekniikoilla
- Käytä DoS ja DDoS-hyökkäysten havaitsemiseen palvelutuotteita
- Sisällytä pyyntöihin CSRF-istuntotunniste
- Varmista parametriset kyselyt sekä validointiprosessi
- Varmista koodituloj en poissuodatus HTML ja JavaScript

8.2 Selvitystyössä käytetyt menetelmät

Selvitystyössä käytettyinä menetelminä toimivat tutkimustyö sekä sen pohjalta laadittu tietoturvakysely verkkosivuston kehittäjille ”liite 1”. Verkkosivuston kehittäjille laadittiin tutkimustyön pohjalta saadun tiedon perusteella kysely virtuaalisen Showroom-verkkosivuston tietoturvatoteutuksesta. Selvitystyön tarkoituksena oli saada selville, miten tietoturva on huomioitu virtuaalisella Showroom-verkkosivustolla. Kyselystä saatujen tulosten pohjalta pystyttiin tarkastelemaan, toteutuivatko verkkosivustolla samat tietoturvasuositukset kuin tutkimustyöstä saaduissa tuloksissa.

8.3 Selvitystyöstä saadut tulokset

Verkkosivuston tietoturvan varmistusta ja suojausta käsiteltiin tämän opinnäytetyön luvussa 5. Tutkimustyössä saatiin selville, että tietoturvallisen verkkosivuston keskiössä on aina huolellinen verkkopalvelimen suojaamien. Verkkopalvelin on koko verkkoinfrastruktuurin tärkein osa ja sen suojaaminen on erittäin tärkeässä roolissa koko verkkosivuston tietoturvan näkökulmasta.

Tietoturvallisella verkkosivustolla olisi hyvin tärkeää myös huolehtia erillisen tietokantapalvelimen käyttämisestä sekä suojata kaikki käytössä olevat palvelimet palomuureilla. Tietokannan pääsyvalvonnan seuraaminen sekä kehittyneiden kyberuhkien torjuminen on tärkeää huomioida tietoturvallisen verkkosivuston tietoturvasuunnittelussa.

Showroom-verkkosivuston tietoturvan selvittämisen lähetettiin laadittu kysely verkkosivuston kehittäjille. Kyselyn pohjalta selvitystyössä saatiin selville, että ainakin virtuaalisen Showroom-verkkosivuston verkkopalvelin oli suojattu omalla palomuurillaan. Showroom-verkkosivustolla oli käytössä Karelia-ammattikorkeakoulun oma verkkopalvelin, jolle oli valmiiksi asennettuna Windows-palomuuri.

Selvitystyössä saatiin selville, että virtuaalisen Showroom-ympäristön tietokantapalvelinta ei ollut sijoitettu omalle palvelimelle, eli tietokantapalvelin ei ole erillään verkkopalvelimesta. Tietokantapalvelin toimi verkkopalvelimen kanssa samalla palvelimella. Kyselystä saatu tulos poikkesi tutkimusaineistossa saaduista suosituksista ja tähän olisi tärkeää kiinnittää huomiota ainakin verkkosivuston jatkokehityksessä. Showroom-sivuston verkkopalvelimen ylläpidosta huolehtivat ne Karelia-ammattikorkeakoulun kehittäjät, joilla on pääsyoikeudet tietokantatietoihin.

Virtuaalisen Showroom-verkkosivuston tietokantana toimi MongoDB tietokanta, joka on NoSQL-tietokanta. NoSQL-tietokannat eroavat perinteisistä tietokannoista yleensä sillä, ettei ne sisällä mitään valmiiksi määriteltyä taulukkorakennetta. Selvitystyössä saadun tiedon perusteella MongoDB-tietokanta ei sijaitse erillisellä tietokantapalvelimella. Tämän vuoksi sitä ei myöskään ole voitu suojata erillisellä tietokantapalomuurilla. MongoDB-tietokanta on suojattu verkkopalvelimen kanssa samalla palomuurilla.

Karelia-ammattikorkeakoulun kehitystiimi huolehtii virtuaalisen Showroom-verkkosivuston tietokantapäivityksistä sekä muista ajankohtaisista toimenpiteistä. Virtuaalisen Showroom-sivuston ylläpitotoimintojen tietoturva on varmistettu kehitystyössä siten, että tietojen muokkaus onnistuu tietokannassa vain tietystä pyynnöstä. Tämä kehittäjien hallinnoima toiminto auttaa suojaamaan ylläpitotietoihin pääsyä tietokannassa.

Kehittäjien suorittamassa virtuaalisen Showroom-verkkosivuston tietokantatestauksessa on selvitetty tietokannan toimivuus. Tiedot välittyvät virtuaalisen Showroom-ympäristön MongoDB-tietokannasta sivustolle sekä käyttäjälle eheänä tekstien sekä kuvien muodossa. Virtuaalisen Showroom-ympäristön suojauksessa on otettu huomioon salasanojen käyttäminen ja kaikkiin tietoihin pääsee ainoastaan kirjaututumalla käyttäjätunnuksella sekä salasanalla.

8.4 Jatkokehityksessä huomioitavaa

Virtuaalisen Showroom-verkkosivuston tietoturvatoteutuksessa oli otettu useita tärkeitä tietoturvallisia asioita huomioon kuten vahvasti suositeltu palomuurien käyttö, käyttöoikeuksien rajaaminen ja vain tarpeellisten käyttöoikeuksien antaminen sekä kirjautumistietojen eli käyttäjätunnusten ja salasanojen käyttäminen. Tietokannan pääsyvalvontaa seurataan sekä verkkopalvelimen uusimmista päivityksistä huolehditaan säännöllisesti. Virtuaalisen Showroom-ympäristön tietoturvatoteutuksen jatkokehityksessä olisi hyvä ottaa vielä tarkemmin huomioon muutamia asioita.

Virtuaalisen Showroom-verkkosivuston tietoturvatoteutuksen selvitystyössä saatiin selville, että verkkosivuston tietoturvaa voitaisiin parantaa vielä jatkokehityksessä enemmän esimerkiksi sijoittamalla verkkosivuston tietokanta omalle tietokantapalvelimelleen. Erillinen tietokantapalvelin auttaa pitämään tietokantatiedot suojassa ja rajaa selkeästi paremmin pääsyä tietokantatietoihin.

Virtuaalisen Showroom-verkkosivuston selvitystyössä saatiin myös selville, että jatkokehityksessä verkkosivustolla voitaisiin paremmin suunnitella ja ennakoida suojautuminen kehittyneitä kyberuhkia vastaan ja kartoittaa niiden mahdollista vaikutusta verkkosivustoon. Kehittyneitä kyberuhkia voi olla vaikeaa ennustaa etukäteen, mutta niitä vastaan voidaan suojautua huolellisella tietoturvasuunnittelulla.

Virtuaalisen Showroom-verkkosivuston jatkokehityksessä olisi tärkeää tarkastella tarkemmin verkkosivuston tietoturvaa. Tässä opinnäytetyössä laadittiin tutkimustulosten sekä laaditun kyselyn pohjalta tarkistuslista, jonka tarkoituksena olisi olla jatkokehityksessä apuna verkkosivuston tietoturvan tarkistamiseen sekä suunnitteluun. Tarkistuslistan avulla voitaisiin tarkastella niitä tietoturva-asioita, joiden avulla voidaan parantaa Virtuaalisen Showroom-verkkosivuston tietoturvaa.

9 Yhteenveto

Opinnäytetyössä tarkasteltiin tietoturvatoteutusta virtuaalisella Showroom-verkkosivustolla. Tutkimustyön sekä kehittäjille lähetetyn tietoturvakyselyn avulla saatiin selville virtuaalisen Showroom-ympäristön tämänhetkinen tietoturva. Selvitystyön pohjalta, laadittiin tarkistuslista verkkosivuston jatkokehitykseen tietoturvan jatkosuunnittelua sekä tarkistamista varten.

Selvitystyössä saatujen tulosten perusteella Showroom-verkkosivuston tietoturva oli hyvällä perustasolla. Verkkosivuston jatkokehityksessä voitaisiin kiinnittää enemmän huomiota nimenomaan vahvojen salasanojen käyttämiseen sekä miettiä tietokannan sijoittamista omalle tietokantapalvelimelle. Verkkosivuston tietoturvasuunnittelussa olisi myös hyvin tärkeää miettiä mahdollisten kehittyneiden kyberuhkien vaikutusta verkkosivustoon sekä tietokantaan. Olisi tärkeää miettiä, miten kehittyneiltä kyberuhkilta voitaisiin suojautua sekä miten pahimmassa tapauksessa kyberuhista voitaisiin toipua.

Verkkosivuston sekä tietokannan suojaamiseen ei ole yhtä ainoaa oikeaa tapaa, mutta on olemassa paljon yleisiä suosituksia verkkosivustojen tietoturvallisuuteen liittyen. Verkkosivuston tietoturvaa olisi hyvin tärkeää ylläpitää ja kehittää. Tietoturva ei ole koskaan täysin valmis, sillä tietoturva päivittyy uusimilla tekniikoilla ja tiedoilla jatkuvasti. Ajankohtaisimmat tietoturvasuositukset ja menetelmät löytyvät parhaiten internetistä sekä tietoturvan palveluntarjojilta.

Paras tapa suojata verkkosivusto sekä tietokanta tietoturvauhkia vastaan on huolehtia huolellisesta tietoturvasuunnitellusta sekä ennakoida mahdolliset tietoturvahaavoittuvuudet. Selvitystyössä saadut tietoturvan perustasot voidaan varmistaa jokaisella dynaamisella verkkosivustolla. Vahvojen salasanojen käyttäminen, palomuurilla suojautuminen sekä palvelimien tehokas ylläpito ja valvonta ovat tehokkaita keinoja suojata verkkosivustoa sekä tietokantaa.

Lähteet

AppliCure Technologies. 2021. Database Security Best Practices. http://www.applicure.com/blog/database-security-best-practice. 06.12.2021.

Cyblance Technologies. 2021. Different Techniques to Secure the Data in the Web Development. https://www.cyblance.com/responsive-design/different-techniques-to-secure-the-data-in-the-web-development/. 06.12.2021.

Ferguson, K. & Loshin, P. 2021. What is denial-of-service attack?. TechTarget. https://searchsecurity.techtarget.com/definition/denial-of-service. 06.12.2021.

Geeksforgeeks. 2019. What is the difference between Front-End and Back-End Web Development?. https://www.geeksforgeeks.org/what-is-the-difference-between-front-end-and-back-end-web-development/. 06.12.2021.

Geeksforgeeks. 2021a. Web Development. https://www.geeksforgeeks.org/web-development/. 06.12.2021.

Geeksforgeeks. 2021b. How can I start to learn Web Development?. https://www.geeksforgeeks.org/can-start-learn-web-development/. 06.12.2021.

Hamilton, T. 2021. Database (Data) Testing Tutorial with Sample Test Cases. Guru99. https://www.guru99.com/data-testing.html. 06.12.2021.

Javapoint. 2021. What is database?. https://www.javatpoint.com/what-is-database. 06.12.2021.

Jiping, X., Lifeng, X., Jian, Z. & Tao, H. 2012. Web and Database Security. Intechopen. https://www.intechopen.com/chapters/37306. 06.12.2021.

Kärkkäinen, H. 2020. Vastaamoon kohdistui kaksi tietomurtoa- näin kymmenientuhansien suomalaisten tiedot varastettiin. Ilta-Sanomat. https://www.is.fi/digitoday/tietoturva/art-2000006700584.html. 06.12.2021.

Lanigan, T. 2020. How to Protect a Database: All About Data Security Today. Dataversity. https://www.dataversity.net/how-to-protect-a-database-all-about-data-security-today/#. 06.12.2021.

Open Web Application Security Project. 2021. SQL Injection. The OWASP Foundation. https://owasp.org/www-community/attacks/SQL_Injection#. 06.12.2021.

Paul, R. 2021. Database Security: 7 Best Practices & Tips. eSecurity Planet. https://www.esecurityplanet.com/networks/database-security-best-practices/. 06.12.2021.

Pohjois-Karjalan Maakuntaliitto. 2019. https://www.pohjois-karjala.fi/pohjois-karjalan-ja-japanin-naganon-metsabiotalousyhteistyon-kehittaminen. 06.12.2021.

Portswigger. 2021a. Cross-site scripting (XSS). https://portswigger.net/web-security/cross-site-scripting. 06.12.2021.

Portswigger. 2021b. Cross-site request forgery (CSRF). https://portswigger.net/web-security/csrf. 06.12.2021.

Portswigger. 2021c. SQL injection. https://portswigger.net/web-security/sql-injection. 06.12.2021.

Pratt, M. 2021. Cyber-attack. Techtarget. https://searchsecurity.techtarget.com/definition/cyber-attack. 06.12.2021.

Positive Technologies. 2019. How to prevent SQL injection attacks. https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-injection-attacks/. 06.12.2021.

Scott, S. 2018. 30 years ago, the world's first cyberattack set the stage for modern cybersecurity challenges. The Conversation. https://theconversation.com/30-years-ago-the-worlds-first-cyberattack-set-the-stage-for-modern-cybersecurity-challenges-105449. 06.12.2021.

Sirkin, J. 2021. SQL (Structured Query Language). Techtarget. https://searchdatamanagement.techtarget.com/definition/SQL. 06.12.2021.

Synopsys. 2021. Cross-Site Request Forgery. https://www.synopsys.com/glossary/what-is-csrf.html. 06.12.2021.

Sanastokeskus TSK. 2018. Kyberturvallisuus. https://termipankki.fi/tepa/fi/haku/kyberturvallisuus. 06.12.2021.

Tapala, K. 2016. Mitä webkehitys on?. Karhu Helsinki. https://www.karhuhelsinki.fi/blogi/mita-web-kehitys. 06.12.2021.

Trendmicro. 2021. Cross-site scripting (XSS). https://www.trendmicro.com/vinfo/us/security/definition/cross-site-scripting-(xss). 06.12.2021.

Kysely

Tietokanta- ja verkkosovelluspalomuurit

Kuinka monta ja minkälaisia palomuureja verkkosivustolla on käytössä?
Onko tietokannalla oma palomuuri?

Tietokantapalvelin

Sijaitseeko tietokanta omalla tietokantapalvelimella? Jos ei niin miksi?
Kuka ylläpitää tietokantapalvelinta ja huolehtii ajankohtaisista päivityksistä?

Verkkopalvelin

Kuka hallinnoin Verkkopalvelinta (lokeja ja päivityksiä)?
Millä tavalla verkkopalvelin on suojattu?

Tietokannan suojaus

Miten tietokannan tietovierailu eli käyttäjän laillinen pääsyoikeus oikeaan tietoon on toteutettu/rajattu? Miten sitä seurataan ja hallinnoidaan?
Miten tietokannan tietojen palauttaminen on varmistettu? Palautuvatko haetut tiedot tietokannasta turvallisesti ja täydellisinä?

Tietokannan suojauksen testaus

Onko verkkosivuston tietokantaa koitettu ”hakkeroida” tai testata jollain tavalla? Jos on niin miten ja minkälaisia tuloksia saitte?

Kehittyneet tietoturvauhat

Miten verkkosivustolla on varauduttu yleisimpiin ja kehittyneisiin tietoturvauhkiin? Onko niihin varauduttu? Jos ei niin miksi.
Tietokannan näkökulmasta?
Koko verkkosivuston näkökulmasta? (Denial of service attack, Cross site scripting, Cross site request forgery ja SQL injection. Muuta?)

Muu tietoturva

Millä muulla tavalla verkkosivuston ja tietokannan tietoturva on otettu huomioon?