Opinnäytetyösuunnitelma

NodeJS sivustojen yleisimmät haavoittuvuudet ja niiden korjaaminen

Insinööri opinnäytetyö

Tieto- ja viestintätekniikka

hyväksymislukukausi 2025

Niilo Ikonen

Koulutus Koulutuksen nimi

Tekijä Nimi Vuosi 20xx

Työn nimi Opinnäytetyön nimi

Ohjaaja Nimi

Kirjoita tiivistelmään opinnäytetyösi pääasiat kokonaisin virkkein. Kerro työsi tavoite, tausta, keskeinen sisältö, tulokset, johtopäätökset, yhteenveto jne. Muista tuoda esille myös mahdollinen toimeksiantaja.

Tiivistelmän pituus on 1 sivu.

Avainsanat Kirjoita 3−5 työtäsi kuvaavaa avainsanaa. Käytä hyväksesi esim. yleistä asiasanastoa (YSA)

Sivut XX sivua ja liitteitä XX sivua

DP Name of the Degree Programme

Author Name Year 20xx

Subject Name of the Thesis

Supervisors Names

Start writing here. The abstract summarises the main contents of your thesis in complete sentences. It should include the aim(s), background, main contents, the outcome(s), and the conclusion of the thesis. Do not forget to mention the commissioner of your thesis if you have one.

The abstract should be no more than one page in length.

Keywords Write 3−5 keywords describing your thesis.

Pages XX pages and appendices XX pages

Sisällys

[1 Tutkimuskysymys 1](#_Toc191488568)

[2 Tutkimuksen tavoite 1](#_Toc191488569)

[3 Aiheen rajaaminen 1](#_Toc191488570)

[4 Taustateoria 2](#_Toc191488571)

[5 Tutkimusmenetelmät 2](#_Toc191488572)

[6 Aikataulu 3](#_Toc191488573)

[Lähteet 4](#_Toc191488574)

# Tutkimuskysymys

Mitä yleisiä heikkouksia nettisivuilla on, miten niitä voidaan hyväksikäyttää ja paikata. Minkälaisia seurauksia ”huonosti” toteutetulla ohjelmistolla on.

# Tutkimuksen tavoite

Työn tavoitteena on tehdä React nettisivu, jossa käyttäjät voivat tehdä tekstipohjaisia postauksia. Ensiksi toteutan sivun niin, että siinä on OWASP Top 10 Web Application Security Risks ongelmia (ei kaikkia). Tarkoituksena on esittää, miten sivustoon hyökätään ja miten sitä voidaan korjata. Lopputuloksena pitäisi olla sivusto, jossa ei ole ilmiselviä aukkoja.

# Aiheen rajaaminen

Nettisivulle luodaan käyttäjät, jotka voivat tehdä postauksia. Postauksia voidaan kommentoida, ja postauksia sekä kommentteja voidaan tykätä. On mahdollista olla myös järjestelmänvalvoja käyttäjiä, joilla on enemmän oikeuksia. Sivustolle luodaan yksinkertainen tietokanta, josta löytyvät käyttäjät, postaukset ja postauksien kommentit.

Sivuston etusivulla on ensimmäiset 20 postausta. Jokaista postausta kohden näkyy viimeisimmät kaksi kommenttia. Avaamalla postauksen voidaan nähdä enemmän kommentteja. Käyttäjiä klikkaamalla voidaan nähdä käyttäjän aiemmat postaukset ja ne postaukset, joihin käyttäjä on kommentoinut. Sivuston alapuolella voi hakea seuraavat 20 postausta.

Sivustolla on yksinkertainen rekisteröitymislomake, jossa tarvitaan käyttäjätunnusta, salasanaa ja sähköpostia.

Kuva 1. tietokannan ER kaavio.

Kuva, joka sisältää kohteen teksti, diagrammi, numero, Samansuuntainen

Tekoälyn generoima sisältö voi olla virheellistä.

Jokaisista haavoittuvaisuutta ei toteuteta, sillä joihinkin haavoittuvuuksiin tarvitaan nettisivulta enemmän ominaisuuksia, eikä siihen riitä aika. Haavoittuvuuksien jokaista hyväksikäyttötapaa ei käydä tarkemmin läpi.

# Taustateoria

React on itselleni jokseenkin tuttu, sillä olen suorittanut Helsingin yliopiston FullStack Open kurssin. Aion hyödyntää React:in dokumentaatiota ja kyseisen kurssin kurssimateriaalia virkistääkseni mieltäni.

Olen suorittanut kurssin ReactJS:stä ja se on minulle jokseenkin tuttu. Aion kuitenkin käyttää Reactin dokumentaatiota sekä mahdollisesti Helsingin yliopiston FullStack Open kurssin kurssimateriaalia virkistääkseni mieltäni.

Haen tietoa NodeJS ja npm perustoiminnasta niiden omista dokumentaatioista.

Haen tietoa yleisistä haavoittuvuuksista OWASPin artikkeleista. Haavoittuvuuksien toteuttamiseen haen GitHubista ja artikkeleista koodia, jota lainata/työstää omaan käyttöön. Haavoittuvuuksien paikkaamiseen käytän mm. OWASP:n NodeJS Security Cheat Sheet:iä.

# Tutkimusmenetelmät

En tiedä vielä

# Aikataulu

Mahdollinen aikataulu

Suunnitteluvaihe valmis mahdollisimman pian. Toteutusvaihe valmiina 31.3. ja viimeistelyvaihe valmis 30.4.

9.5. järjestetään loppuseminaari.

Lähteet

Node.js haavoittuvuusblogi <https://nodejs.org/en/blog/vulnerability>

Npm left-pad incident <https://en.wikipedia.org/wiki/Npm_left-pad_incident>