**2 Yleisimmät web-sovellusten tietoturva uhat**

Web-sovelluksiin kohdistuu nykypäivänä monia erilaisia uhkia, joita vastaan yritykset joutuvat taistelemaan päivittäin. Tätä voisi ajatella eräänlaisena kissa ja hiiri -leikkinä. Kun uusi haavoittuvuus löydetään, pitää se paikata mahdollisimman nopeasti ilman, että haavoittuvuudesta aiheutuu suurta vahinkoa yritykselle tai yrityksen asiakkaille.

2.1 Kolme suurinta tietoturvauhkaa

Yleisin tietoturvauhka on käyttäjä [1]. Tähän voi jokainen vaikuttaa omalla käyttäytymisellä. The Open Worldwide Application Security Project, eli lyhyemmin OWASP, on koonnut vuoden 2021 yleisimpiä haavoittuvuuksia listaksi. [2]

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, viiva

Kuvaus luotu automaattisesti

Kuva 1 OWASP top-10 tietoturva haavoittuvuudet 2017 ja 2021

2.2 Broken access control

Access control, suomeksi valtuuksien tarkistus, valvoo, että web-sovelluksen käyttäjä ei pysty toimimaan yli hänelle annettujen oikeuksien web-sovelluksen sisällä. Viallinen valtuuksien tarkistus johtaa yleensä luvattomien tietojen paljastumisen, muokkaamisen tai tuhoamisen mahdollisuuteen käyttäjälle. Tältä voi välttyä oikeanlaisella suunnittelulla projektin alkuvaiheessa ja myöntää käyttäjälle vain ne oikeudet, jotka ovat vain välttämättömiä.

2.3 Cryptographic failures

Salaustekniikan epäonnistuminen koskee arkaluotoisen tiedon, esimerkiksi salasanojen, luottokortin tietojen tai henkilökohtaisten tietojen, huonoa salausta tai salauksen puuttumista. Tähän kehittäjä voi vaikuttaa muistamalla salata kaikki arkaluontoinen data säilyttäessään sitä ja myös siirtäessä sitä, pitämällä huolen ettei evästeet tallenna arkaluontoista dataa ja olla käyttämättä vanhentunutta teknologiaa datan siirroissa.

2.4 Injection

Injektiohyökkäyksistä yleisimmät ovat SQL-injektio, NoSQL-injektio ja object-relational mapping, lyhyemmin ORM [3]. Structured query language, lyhennettynä SQL, on kyselykieli, jota käytetään ohjelmoinnissa tietokantoihin tallennettuihin tietoihin pääsemiseksi. SQL-injektio kuuluu yhteen vanhimmista verkkosovellushaavoittuvuuksista. SQL-injektio on hyökkäys, jossa virheellistä SQL-koodia hyväksikäyttäen voidaan manipuloida, lukea tai jopa poistaa arkaluontoisia tietoja tietokannasta. Mitä keskitetympää tieto on, sitä pahempaa jälkeä injektiohyökkäykset saavat aikaa. Näitä hyökkäyksiä vastaan voidaan suojautua esimerkiksi käsittelemällä käyttäjän syöttämä data ennen kuin sillä haetaan tietoja verkkosivuston käyttämästä tietokannasta.[4]

Lähteet

[1 Suomen asiakastieto Oy https://www.asiakastieto.fi/omatieto/fi/artikkelit/20221012160000]

[2 OWASP <https://owasp.org/www-project-top-ten>]

[3 OWASP [https://owasp.org/Top10/A03\_2021-Injection/#description](https://owasp.org/Top10/A03_2021-Injection/" \l "description)]

[4 NordVPN <https://nordvpn.com/fi/blog/sql-injektio/>]

[5