

## Näin xss-aukoilla on hyökätty

31.3.2008 14:44 — Aleksis Moisio [aleksi.moisio@sanoma.fi](mailto:aleksi.moisio@sanoma.fi)

Haavoittuvuus Danske Bankin verkkopankissa paljasti xss-ongelmavyyhden. Maailmalla xss-haavoittuvuuksien avulla on varastettu esimerkiksi pankkitunnuksia ja luottokorttien numeroita.

**Viime viikolla** paljastunut [Sampo Pankin tietoturva](#) haavoittuvuus on nostanut cross-site scripting- eli xss-haavoittuvuudet tapetille.

Suomalaiset tietotekniikan harrastajat ovat paljastaneet [vastaavia haavoittuvuuksia](#) myös muiden pankkien, yritysten, valtionhallinnon ja median verkkosivuilta.

Kyseessä on kaikkea muuta kuin uusi ilmiö.

- Samaa tekniikkaa on hyödynnetty jo vuosikausia ennen kuin koko xss-termi yleistyi, TietoEnatorilla työskentelevä tietoturvaneuvonantaja **Tomi Tuominen** sanoo.

Tuominen kertoo kuulleensa vastaavista haavoittuvuuksista ensimmäistä kertaa vuonna 1997.

- Se, että haavoittuvuuksia löytyy näin monelta sivulta kertoo omaa tarinaansa ohjelmistokehittäjien arjesta. Kovien aikataulupaineiden alla tietoturva ei aina ole päällimmäisenä mielessä, Tuominen sanoo.

**Hieman yksinkertaistettuna** xss-hyökkäyksissä on kyse siitä, että sivuston syötteentarkistus on toteutettu puutteellisesti.

Huolimattomasti toteutetulla sivulla käyttäjä saattaa pystyä muokkaamaan sivuston ulkonäköä esimerkiksi syöttämällä omaa koodiaan sivulla pyörivän hakukoneen hakulausekkeisiin.

Puutteellinen syötteentarkistus voi altistaa sivuston monille erilaisille hyökkäyksille, joista xss on vain yksi esimerkki.

Se, että joltain sivulta löytyy xss-aukko, ei ole itsessään vielä katastrofi, Tuominen muistuttaa. Tietyillä herkkää tietoa käsittelevillä sivuilla haavoittuvuus avaa kuitenkin suuret mahdollisuudet väärinkäytöksille.

*Digitoday* listasi törkeimpiä esimerkkejä siitä, mihin kaikkeen verkkosivujen xss-haavoittuvuuksia on maailmalla käytetty.

---

**Banca Fideuram, 2008:** Italialaisen pankin sivuille upotettu kalastelu-sivu onnistui hämäämään useita.

Sen avulla vorot urkkivat pankkitunnuksia ja salasanoja, jotka siirrettiin nopeasti Taiwanissa sijaitsevalle palvelimelle.

**Orkut, 2006:** Yhteisösivusto kärsi niin kutsutusta pysyvästä xss-haavoittuvuudesta, jonka avulla pystyttiin varastamaan vierailijoiden evästetietoja.

Varustettujen evästetietojen avulla hyökkääjä pystyi varastamaan esimerkiksi muiden käyttäjien luomia ryhmiä.

**PayPal, 2006:** Verkkomaksuja välittävän PayPalin sivut kärsivät xss-haavoittuvuudesta.

Sen avulla saatiin kalasteltua luottokorttinumeroita ja henkilökohtaisia tietoja.

**Google, 2005:** Xss-haavoittuvuus antoi voroille mahdollisuuden esiintyä Google.comin muiden käyttäjien nimillä.

**MySpace, 2005:** [Samy-nimeä kantanut xss-mat](#)devisi MySpaceen luodusta profiilisivusta toiseen kulovalkean tavoin. Virus levisi 20 tunnin aikana yli miljoonalla käyttäjälle.

<http://www.digitoday.fi/tietoturva/2008/03/31/nain-xss-aukoilla-on-hyokatty/20089020/66>