TURUN YLIOPISTO
Informaatioteknologian laitos

LEINIÖ, TIMO: Web-sovellusten turvallisuus

Diplomityö, 102 s.
Ohjelmistotekniikka
Tammikuu 2010

Web kasvaa koko ajan. Nykyään webiin pääsee käsiksi joka puolelta maailmaa monenlaisilla laitteilla. Web ei sisällä enää vain staattista sisältöä, vaan suurin osa sisällöstä on dynaamista, jota webin käyttäjät voivat lisätä, muokata ja poistaa. Web ei sisällä enää niinkään web-sivuja vaan täysiverisiä web-sovelluksia, joiden toimintalogiikka voi olla erittäin monimutkaista. Tämän lisäksi monet sovellukset sisältävät tietoa, jotka ovat vain tiettyjen käyttäjien nähtävillä. Tällaisten toiminnallisuuksien myötä sovellusten turvallisuus on noussut erittäin ajankohtaiseksi aiheeksi.

Yritykset käyttävät todella paljon web-sovelluksia oman toimintansa tarkasteluun. Yrityksen sisäinen tieto ei kuitenkaan saa päästä ulkopuolisten käsiin. Sovelluksia turvataan monenlaisilta hyökkäyksiltä. Hyökkääjä voi päästä käsiksi arkaluontoiseen tietoon muun muassa murtamalla todentamisen, istunnon hallinnan tai saanninvalvonnan. Tämän estämiseksi ohjelmistosuunnittelijoiden ja -arkkitehtien tulisi olla tietoisia monenlaisista turvallisuusasioista.

Tässä tutkielmassa tarkasteltiin, mitä kaikkea web-sovelluksen turvallisuudessa tulisi ottaa huomioon. Tämän lisäksi työssä muodostettiin lista, jonka avulla voidaan suorittaa sovelluksen turvallisuustestaus. Listan avulla suoritettiin turvallisuustestaus Sofokus Oy:n Sofokus iManager™ web-sovelluksen sisäiselle kehitysversiolle. Testauksen perusteella lista on hyödyllinen, sillä sovelluksesta löydettiin muutamia tietoturva-aukkoja. Havaitut tietoturva-aukot on korjattu sovelluksesta jo tämän työn valmistuessa.

Avainsanat: web-sovellus, web-turvallisuus, todentaminen, istunto, saanninvalvonta

UNIVERSITY OF TURKU
Department of Information Technology

LEINIÖ, TIMO: Web Application Security

Master's Thesis, 102 p.
Software Engineering
January 2010

Web is growing all the time. You can access web nowadays everywhere in the world with many different kind of devices. Web content is not anymore just static, it is mostly dynamic and web users can add, edit and delete it. Web doesn't contain just web sites anymore but genuine web applications that can have complex functionality. Furthermore many of these applications contain information that can be seen by only certain users. This kind of functionality has raised web application security as an important topic.

Corporations use web applications to examine their business. Corporation's information should not be available to outsiders. Web applications are secured from a wide range of attacks. An attacker may access delicate information by breaking authentication, session handling or access control. Web architects and designers should know many security issues so that they can prevent such attacks.

In this M.Sc.(Tech) thesis it was examined what kind of aspects should be considered regarding web security. Moreover a list, that could be used when testing an application's security, was created. The list was used while testing a development version of Sofokus iManager™ web application that is being developed by Sofokus Inc. The list was found useful because it revealed a few security threats. Those security threats have been fixed by the time this thesis was finished.

Keywords**:** web application, web security, authentication, session, access control