Käytännön tietoturvaa isoilla web-palvelimilla

Henri Salo

1. huhtikuuta 2013

Vuonna 2009 aloin kiinnittää huomiota siihen ilmiöön, etteivät Kapsi Internet-käyttäjät Ry:n jäsenet päivittäneet itse asentamiaan kolmannen osapuolen valmistamia web-sovelluksia.

Tietojärjestelmien sovellusten päivittämättömyys on ollut tietoturvan kannalta iso ongelma jo pitkään.

Kapsilla tämä näkyy haavoittuvuuksien hyväksikäytöllä yleensä tuntemattoman hyökkääjän toimesta.

Usein sivustoja sotketaan ja pahimmassa tapauksessa murrettaan, jolloin hyökkääjä saa pääsyn sivustoa ajavalle palvelimelle komentorivitasolla.

Haavoittuvuuksia käytetään pääsääntöisesti muiden tietojärjestelmiä vastaan hyökkäämiseen, drive-by -hyökkäyksiin JavaScript-koodia injektoimalla sekä esimerkiksi roskapostittamiseen.

Otin tästä itselleni haasteen ja kehitin pyfiscan-nimisen sovelluksen. Pyfiscan nimensä mukaisesti käy käyttäjän määrittelemän hakemiston läpi sekä etsii tietoturva-aukollisia versioita sovelluksista. Sovelluksen tuloksien pohjalta Kapsin jäsenille on sähköpostitettu ja pyydetty päivittämään haavoittuvia sovelluksia. Ennätys on noin 500 päivityksen tasoa viikossa. Sovellusta kehittäessä oma ymmärrykseni web-sovellusten haavoittuvuuksista on kasvanut merkittävästi sekä olen laittanut merkille, että myös jäsenet ovat olleet ahkerampia päivittämään sovelluksia omatoimisesti.

Valitettavasti kaikki jäsenet eivät päivitä sovelluksiaan sähköposteista huolimatta. Projektin aikana olen myös pyytänyt paljon CVE-tunnisteita sekä koordinoinut haavoittuvuuksia. Usein haavoittuvuuden löytäjä ei ilmoita asiasta sovelluksen kehittäjille, vaan haluavat esimerkiksi pelkkää huomiota. Muutaman vuoden aikana on tullut myös useita ilmoituksia haavoittuvuuksista, jotka olen testaamalla todennut virheellisiksi. Tällä hetkellä pyfiscan-sovellus tunnistaa 14 eri sovellusta. Projektiin on osallistunut kolme ihmistä sekä palautetta on tullut isoiltakin toimijoilta. Projektin kotisivut löytyvät osoitteesta: https://code.google.com/p/pyfiscan/.