SQL-injektio

- OWASP Appsec series
- Tapauksia
  - http://www.computerworld.com/s/article/9080580/Huge_Web_hack_attack_infects_500_000_pages

Hyökkääjän tavoitteita

- Komentojen suoritus
  - Järjestelmäkomennot
  - Tietokantakomennot
- Tieto
  - Taulukot ja sarakkeet
  - Lukumäärät
  - Taustalla oleva järjestelmä

(C) Marko Helenius

SQL-injektion torjunta

- Toteutukseen vaikuttaa ohjelmointikieli
  - ohjelmointikielten piirteiden huomioiminen
  - ohjelmointikielen valinta
- Syötteen parametrisointi (parametrised statements)
  - Syötettä ei tulkita SQL-koodiksi.
  - Käytettävä, jos vain mahdollista.
- Syötteen tarkistus ja suodatus (escape / validate)
  - Pyritään varmistamaan, että syöte ei sisällä mitään haitallista.

(C) Marko Helenius

SQL-injektion torjunta

- ”Stored procedures” eli tallennetut proseduurit
  - Torjunta riippuu tarpeesta käyttää SQL:ää
- Kyselyjen laillisuus
- Dynaamisen SQL:n välttäminen
- Merkistökoodauksen huomioiminen
  - Varaudutaan siihen, että haitallinen syöte voi olla eri merkistökoodauksella kuin alun perin oli varauduttu ja saattaa siten läpäistä validoinnin.

Tietokannan turvaaminen

- Tietokantaohjelmien erityispiirteet
  - haavoittuvuudet
  - Tarpeettomat ominaisuudet voidaan ottaa pois käytöstä.
  - virheloki
- Virheilmoitukset
  - hyökkääjän saama informaatio
  - Sokea hyökkäys (blind sql injection) on edelleen mahdollinen.

(C) Marko Helenius

Tietokannan turvaaminen

- Käyttöoikeuksien rajoitukset
  - vähimpien oikeuksien periaate
    - tietokannan sisällä
    - prosessien oikeudet
- Salaus
- Ylläpito sisältää mm.
  - päivitykset
  - varmuuskopiointi
  - ennakointi, toipumissuunnitelma
  - seuranta, lokitiedot
  - turva-asetukset

(C) Marko Helenius

Tietokannan turvaaminen

- Tietokantaohjelmien erityispiirteet
  - haavoittuvuudet
- Tarpeettomat ominaisuudet voidaan ottaa pois käytöstä
- Käyttöoikeuksien rajoitukset
- Testaus
  - Tyypillisimpien tapaukset voidaan helposti kokeilla tai automatisoida
  - Valmiita testiohjelmia löytyy.

(C) Marko Helenius

Cross Site Scripting

Tallennettu (stored)

- Hyökkääjän syöte jää sivulle
- Esim. Hyökkääjä syöttää lomakkeeseen javascript-koodia, joka jää palvelimelle
- Käyttäjän tullessa palvelimelle, koodi suoritetaan selaimessa

Heijastettu

- Haavoittavan sivuston kautta hyökätään

(C) Marko Helenius

Cross Site Scripting

Heijastettu

- Haavoittavan sivuston kautta hyökätään
- Esim. käyttäjän avatessa sähköpostin kutsutaan haavoittuvan palvelimen otsikkoriviä ja syötetään omaa koodia käyttäjälle -> Myös CSRF (Cross Site Request Forgery) mahdollinen

(C) Marko Helenius

Cross Site Scripting

DOM (Domain Object Model)

- https://www.owasp.org/index.php/DOM_Based_XSS

(C) Marko Helenius