Sovellustietoturvallisuus

Petteri Arola
OWASP Chapter Leader
Nixu Oy
petteri.arola@owasp.org

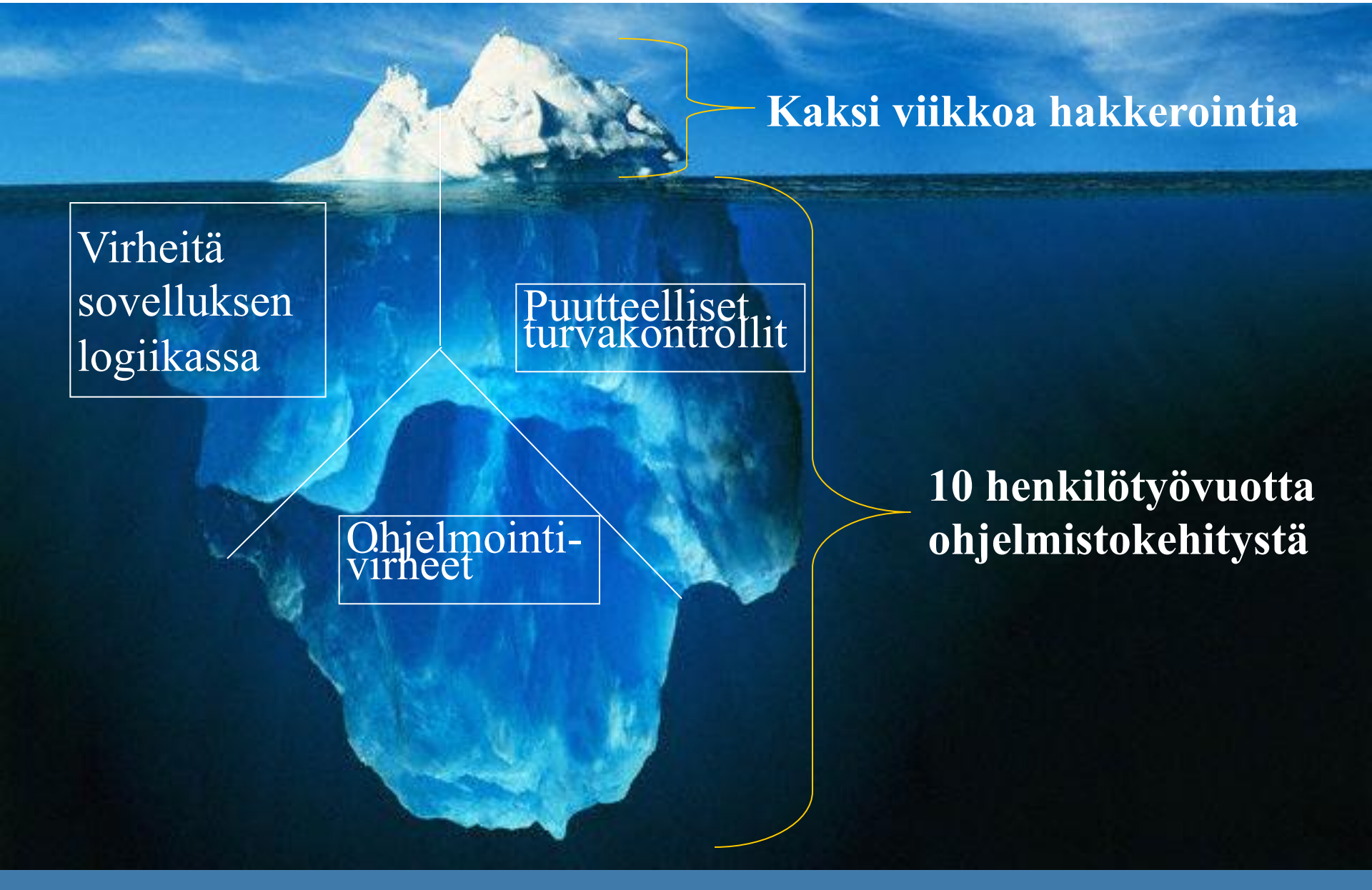
OWASP
7.2.2012

The OWASP Foundation
http://www.owasp.org

Sovellustietoturvallisuus

- Miksi sovellukset ovat haavoittuvia?
- OWASP

Karu todellisuus



Sovellukset ovat hyökkäysten etulinjalla

- Sovellukseen on yhä helpompi päästä käsiksi, sovellushaavoittuvuudet ovat hyökkäysten aloituspiste
- Haavoittuvuuksia on helppo hyödyntää -> Mahdollisuuksia on lukuisia -> Hyökkäykset ovat tuloksekkaita
- Verkon suojaukset ovat hyödyttömiä nykypäivän sovellusturvallisuusuhkiin

Ohjelmiston elinkaari – perinteinen tapa

1. Asiakas tarvitsee ohjelman
2. Toimittajan ohjelmistokehittäjä ohjelmoi jotain joka näyttäisi toimivan
3. Sen pituinen se

Sovellushaavoittuvuuden elinkaari – perinteinen tapa

1. Haavoittuvuustutkija/ tietoturvakonsultti/”lonely hacker” löytää haavoittuvuuden
2. Haavoittuvuus ilmoitetaan ohjelmistotoimittajalle ja haavoittuvuuskoordinaattorille (CERT)
3. Haavoittuvuuskoordinaattori valvoo, että haavoittuvuus tulee joskus korjattua

...

N. Toimittaja julkaisee korjauksen

N+1. Sen pituinen se

Mitä tapahtui vaiheessa N?

1. Vikatiketti avataan
2. Ohjelmoija korjaa bugin
3. Tiketti suljetaan

Sama juttu seuraavassa kuussa…

Ja seuraavassa kuussa...

Mikä on pielessä?

“Meidän ei tarvitse huolehtia sovellusturvallisuudesta, koska…"

- Meillä on palomuuri ja SSL käytössä
- Kehittäjä: “kysyt väärältä henkilöltä, meidän tietoturva-hemmo hoitaa nämä asiat”
- Tietoturvahemmo: “kysyt väärältä henkilöltä, koska meidän ohjelmistokehittäjät hoitavat nämä asiat”
- Sovellusta ostava henkilö: “tottakai meidän sovellustoimittajan huomioi tässä sovelluksessa tietoturva-asiat ilman eri vaatimusta, sehän on selvä”
- Sovellustoimittaja: “me teemme tämän sovelluksen täsmälleen vaatimusten mukaisesti”
- Meidän sovelluskehitysvälineet huolehtivat sovelluksen turvakontrolleista

Miksi sovellusturvallisuus on yleisesti niin heikossa jamassa?

- Koko sovellusturvallisuuskäsite on epäselvä ja se edelleen mielletään jonkun toisen ongelmaksi
- Ala on vielä kohtuullisen nuori ja kehittymätön -> yleinen tietoisuus sovellusturvallisuudesta ja siihen liittyvistä parhaista käytännöistä on vähäistä
- Sovellusten ostajat eivät vielä osaa vaatia sovellustoimittajilta toteutuksia, jossa sovellusturva-asiat olisi huomioitu riittävällä tasolla
- Ohjelmistokehityksen ammattilaisia kouluttavissa oppilaitoksissa ei opeteta sovellusturvallisuutta

Kenen pitäisi huolehtia sovellusten tietoturvasta?

- Eilen
  - Mikä sovellustietoturva?
- Tänään
  - “Tietoturvahemmo”
- Huomenna (?)
  - Jokainen: ohjelmistokehittäjät, sovellusarkkitehdit, sovellusten ostajat, sovellustoimittajat

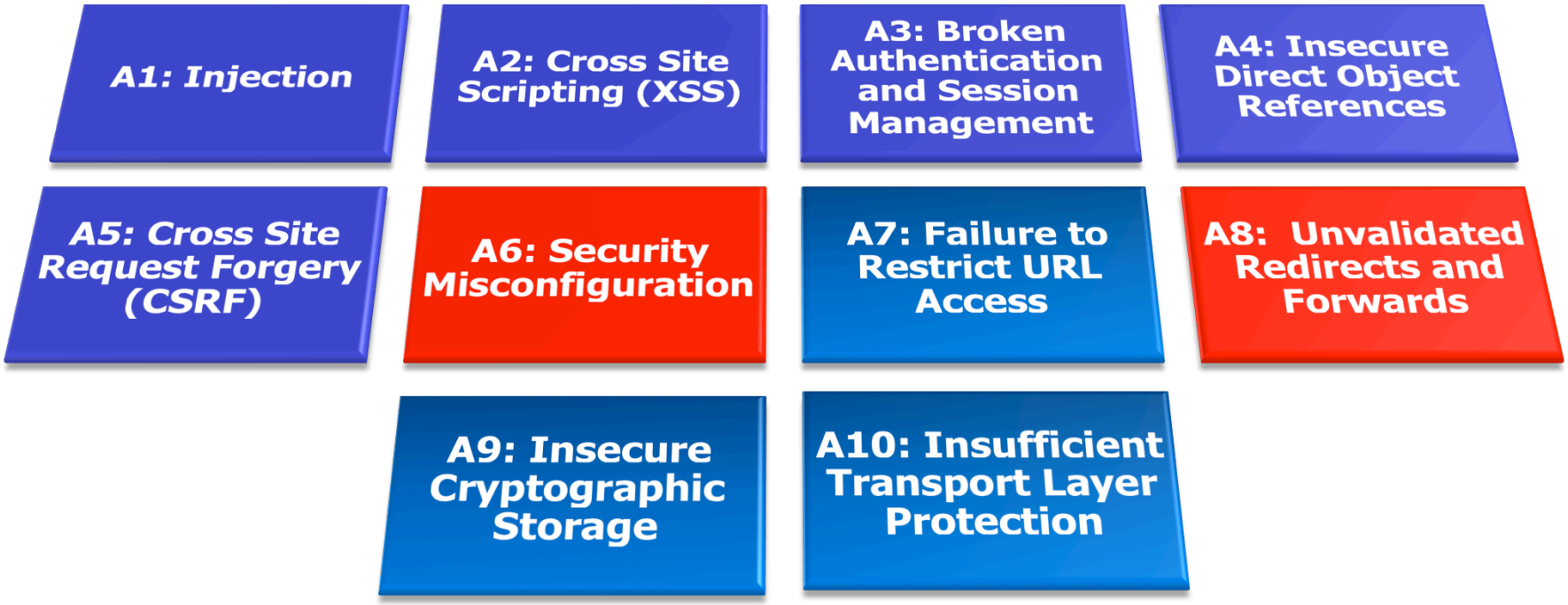
Mikä OWASP on?

- Open Web Application Security Project
- Voittoa tavoittelematon, vapaaehtoisuuteen perustuva “open source” -yhteisö
- Yhteisön tavoitteena on kasvattaa tietoisuutta turvallisen ohjelmistokehityksen menetelmistä kehittää uusia “open source” ratkaisuja turvallisen ohjelmistokehityksen haasteisiin
- Avoin keskustelufoorumi

Hyödynnä OWASPia

- Sovellusturvallisuustietoisuuden kasvattamiseen
  - OWASP Top 10
- Ohjelmistojen ostamiseen
  - OWASP Secure Software Contract Annex
- Ohjelmistojen kehittämiseen
  - Developers guide
  - Code review guide
- Sovellusten tietoturvan varmistamiseen ja testaukseen
  - Testing guide
  - ASVS
- Building security in
  - OpenSAMM

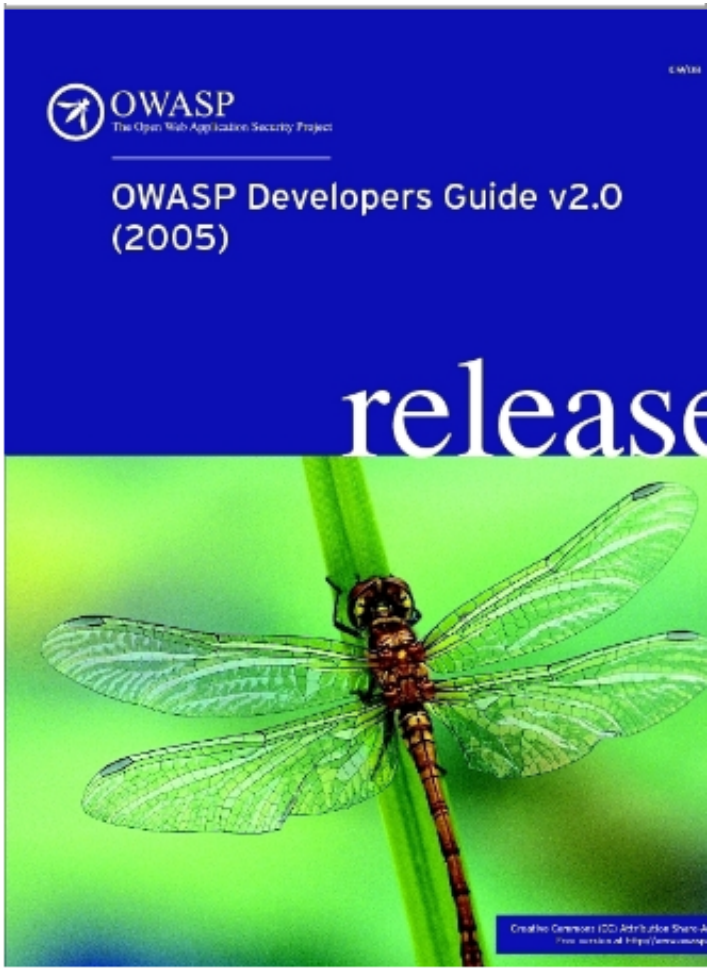
OWASP Top Ten



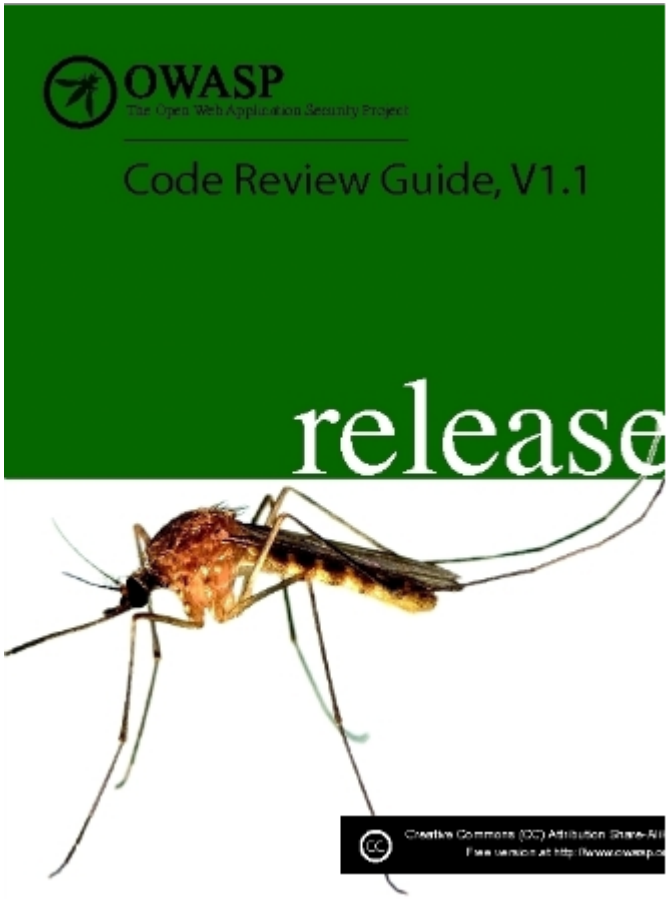
OWASP
The Open Web Application Security Project
http://www.owasp.org

http://www.owasp.org/index.php/Top_10

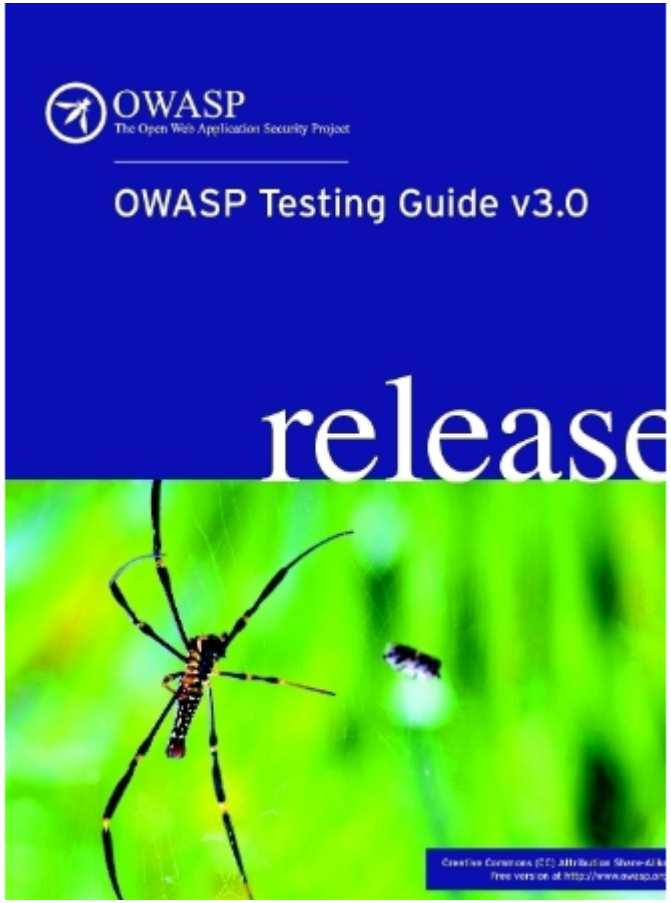
Developer Guide



Code Review Guide



Testing Guide



http://www.owasp.org/index.php/TestingGuide

OWASP Application Security Verification Standard (ASVS)

OpenSAMM


Software Assurance
Maturity Model
A guide to building security into software development
Version - 1.0

OWASP työkalut

- Haavoittuvuus-skannerit
- Staattiset koodianalysaattorit
- Fuzzaustyökalut

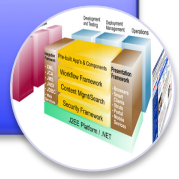
Automaatti-työkalut tietoturvan varmistamiseen

- Pentest työkalut
- Koodikatselmointi-välineet

Työkalut tietoturvan manuaaliseen varmistamiseen

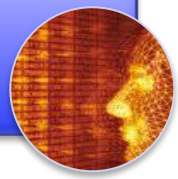
- ESAPI

Tietoturva-arkkitehtuuri



- AppSec kirjastot
- ESAPI referenssitoteutukset

Turvallinen ohjelmointi



- Raportointivälineet

Ohjelmistoturvan hallinta

- Haavoittuvat ohjelmistot
- Oppimisympäristöt
- Live CD

Ohjelmisto-turvallisuuden koulutus

OWASP

Tarvitsetko lisää?

OWASP .NET Project
OWASP ASDR Project
OWASP AntiSamy Project
OWASP AppSec FAQ Project
OWASP Application Security Assessment Standards Project
OWASP Application Security Metrics Project
OWASP Application Security Requirements Project
OWASP CAL9000 Project
OWASP CLASP Project
OWASP CSRFGuard Project
OWASP CSRFTester Project
OWASP Career Development Project
OWASP Certification Criteria Project
OWASP Certification Project
OWASP Code Review Project
OWASP Communications Project
OWASP DirBuster Project
OWASP Education Project
OWASP Encoding Project
OWASP Enterprise Security API (ESAPI)
OWASP Flash Security Project
OWASP Guide Project
OWASP Insecure Web App Project
OWASP Interceptor Project

OWASP JBroFuzz
OWASP Java Project
OWASP LAPSE Project
OWASP Legal Project
OWASP Live CD Project
OWASP Logging Project
OWASP Orizon Project
OWASP PHP Project
OWASP Pantera Web Assessment Studio Project
OWASP SASAP Project
OWASP SQLiX Project
OWASP SWAAT Project
OWASP Sprajax Project
OWASP Testing Project
OWASP Tools Project
OWASP Top Ten Project
OWASP Validation Project
OWASP WASS Project
OWASP WSFuzzer Project
OWASP Web Services Security Project
OWASP WebGoat Project
OWASP WebScarab Project
OWASP XML Security Gateway Evaluation Criteria Project
OWASP on the Move Project
…

OWASP

Tule mukaan

WWW.OWASP.ORG