Qentinel
SOFTWARE QUALITY ASSURANCE

Tietoturvatestaus

24.3.2010

Teemu Vesala

Aluksi

- Saa keskeyttää
- Saa kysyä
- Saa olla eri mieltä

Minä

- Teemu Vesala, 35-wee, nörtti, perheellinen
- Teemu.vesala@qentinel.com
- Laatukonsultti, Qentinel, 1.1.2007-
  - Tekninen asiantuntija
- Aikaisemmin koodaajana
  - C/C++ (Serveri-softaa, NT kernel, web, Windows, *nix), J2EE, Perl, PHP
- Harrastukset
  - Kirjoittaminen, lukeminen, oppiminen, ~~D&D~~ Pathfinder, nörtteily

Qentinel

- Erikoistunut ohjelmistojen testaukseen ja projektien laadunvarmistukseen
- Riippumaton asiantuntija-organisaatio
- Alan aktiivinen kehittäjä
- Yksityisomistuksessa
- N. 60 työntekijää

Rakenne

- Mitä tietoturva on
- Mitä tarkoitetaan turvallisella ohjelmistolla
- Mitä tietoturvan testaus on
- Käytännössä

Miksi testata?

- Varastetut luottokortti nro:t
- Palvelin levittää haittaohjelmia
- Phishing
- Tietoa katoaa
- Palvelu on poissa käytöstä
- Imago kärsii
- ....

=> Rahan menetys

Miksi murretaan

- Taloudellinen hyöty
- Poliittinen motiivi
- Ilkeily
- Kilpailu

Todellista

Laudalta hakkeroimaan, se oli kyttä jutun alkuu, toiset selvis, toiset ei käyttänytkää proxyy

Et taida tietää mitä demareissa tapahtu, miltä näytti ku Urpilaisen saitti oli haxattu

Entä se ku jonne raidissa pärisi, proxyttomalle sivuilla onnettomuus tapahtu

Raavittiin kasaan, accoja, passuja, poliisit keräs hies, laudalta IPeitä

Kyberterroristi säädöistä rikosrekisteri, uudet päiväsakot, ihan vitun jepa

Viljamin veli osaa pari hyvää hakkeri kikkaa, sata paskoi meemuja, Iltalehti flippaa

nyymijengis passut kiersi ringis, vanhahomoista kukaan niit ei sendis

Urpilaisen sivuilla lapoa ja ES, Heinäluoman sivuilla avaruuskulttuuri on jo täällä

Esan kanssa Vauva.fi rölläsin, nyt hakkeroin demareita ja esa onki poliisi

Uutiset tuli ja alko feimii olla, KEULIN HAKEE ES MAKEN MOPOLLA XXXX--DDDD

gr33tzit 80k paasun & urpilaisen & heinäluoman häkkereille<3

Anonyymi: awfsnad.txt

Ja mitä sai aikaan?

- Otsikoita 22.-23.3.2010
- 127000 tunnus-nimi-sähköposti-salasana-riviä
- Salasanat kryptaamatta
- Sanoman tappiot?
- Ihmisten työt salasanojen vaihtamiseen?
- Mahdollisesti muita tietomurtoja (mm. Kapsin ssh-palvelin?)

Mitä tietoturva on?

- Luottamuksellisuus
- Eheys
- Vastuullisuus
- Kiistämättömyys
- Autenttisuus
- Saavutettavuus

- Yksityisyys?

TUPAS-tunnistautuminen

- Pankkien tarjoama vahva tunnistautuminen
- Turvallisuus
- Yksityisyyden suoja
  - https://munpalvelu.com/return/nordea/return?=&....B02K_CUSTNAME=NORDEA+%2F+DEMO&B02K_KEYVERS=0001&B02K_ALG=01&B02K_CUSTID=010100-123D&....

PCI-DSS:n näkymä

- Luottokorttifirmojen vaatima standardi
- Suojaa
- Rajoita
- Valvo
- Testaa

Tietoturvan eri tasot

- Ihmiset, ohjeet, säännöt
- Infrastruktuuri
- Sovellus

Turvallinen ohjelmisto

- (secure) software must be able to resist most attacks, tolerate as many as possible of those attacks it cannot resist, and contain the damage and recover to a normal level of operation as soon as possible after any attacks it is unable to resist or tolerate.
  - Goertzel et al: Software security assurance: State of the art (SOAR), IATAC, 2007

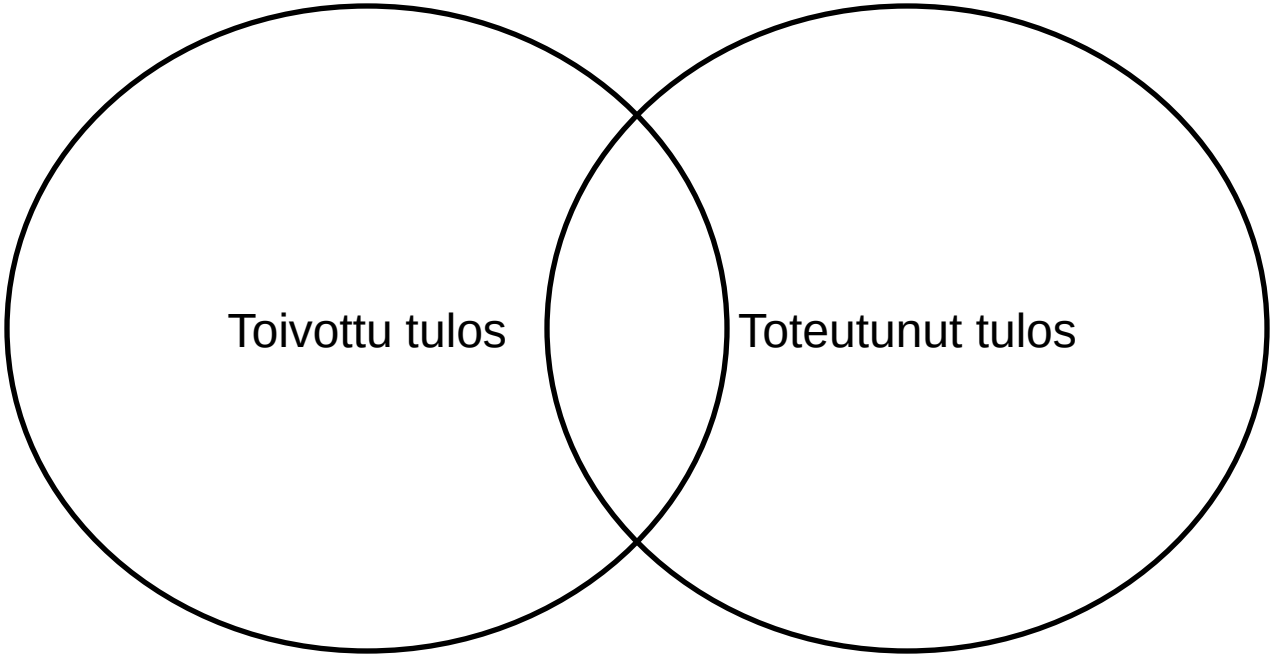
Muodostuminen

- Ei vain testauksesta
- Läpi koko elinkaaren
  - Microsoftin Secure Development Lifecycle
    - Uhkien mallintaminen
    - Suunnittelu ja hyökkäyspinta-alan pienentäminen
    - Koulutus
    - Katselmointi
    - Testaus
    - Jälkihuolto

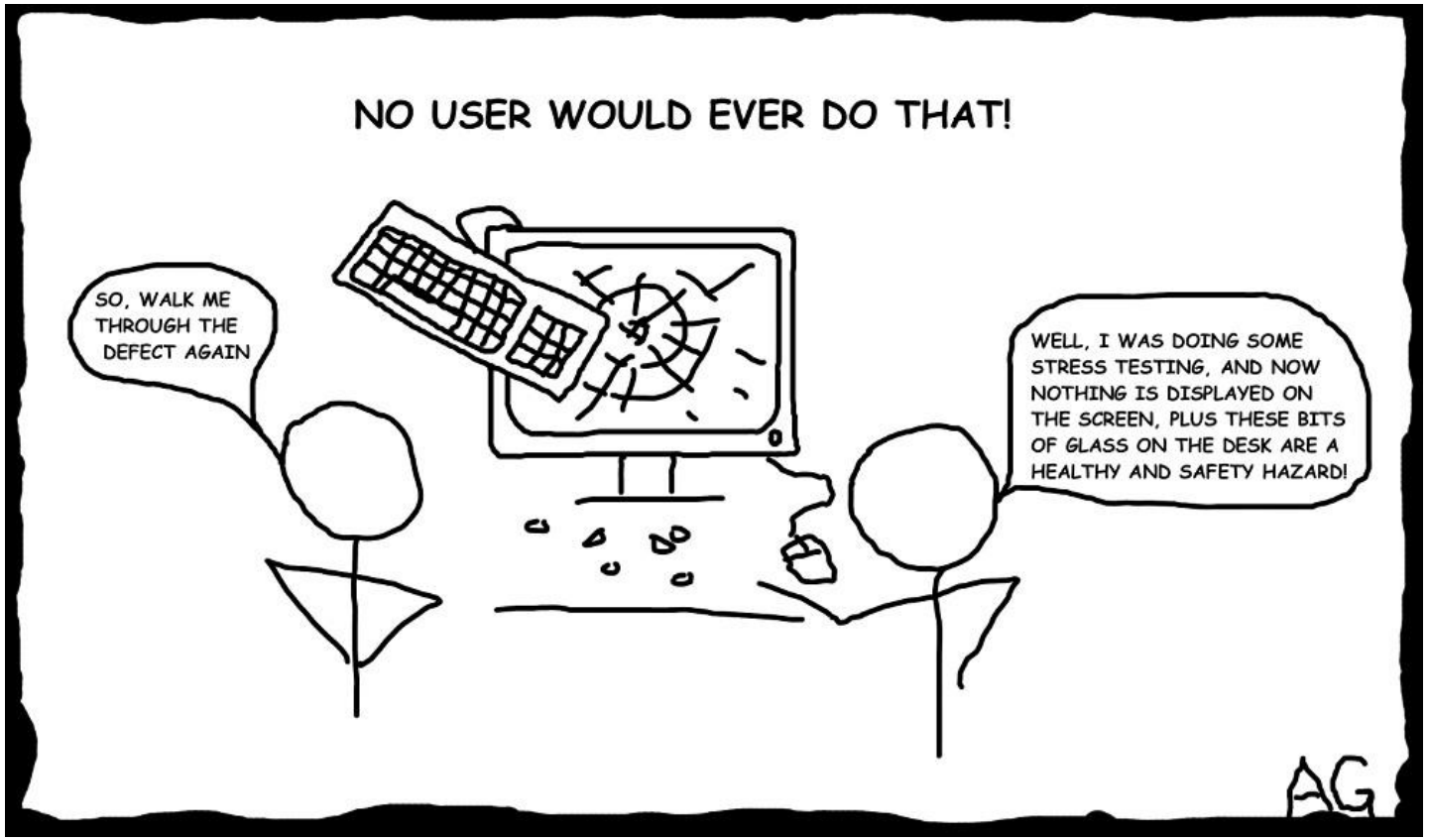
Testauksen kannalta

- Ei-toiminnallinen ominaisuus
- Äääääääääääääääääääääääääääääääääh
- EKSTRA-TOIMINNALLISUUS

Testattava sovellus

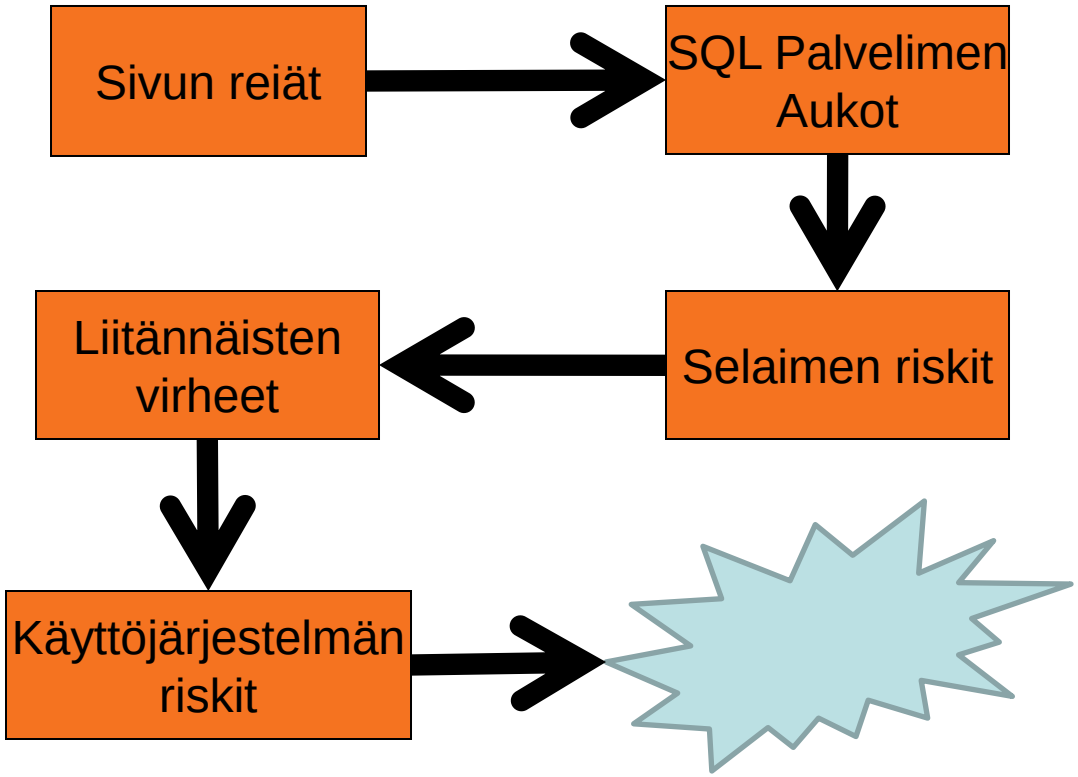


Testausta



http://cartoontester.blogspot.com/

Monitasoisuus



Ei voida täysin testata

- Ympäristön muutos
  - Tänään turvallinen
  - Huomenna – onko sittenkään?
  - Esim. Windowsin Event handling 80-90-lukujen vaihteesta
- Rajallinen aika – rajaton määrä tiloja

Ristiriitaisuuksia

- Laatuvaatimukset voivat olla ristiriitaisia
- Käytettävyys vs. Tietoturva?
- Tietoturva vs. yksityisyys? (TUPAS aiemmin)

Erilaiset testaukset

- Työpöytäsovellukset
  - Tietoa voidaan usein ladata netistä
- Serveri-sovellukset (IMAP, DNS jne.)
- Web-sovellukset

Haasteet

- Kasvava monimutkaisuus
- Laajennettavuus
- Hajautetut järjestelmät
  - Cloud
  - Service Oriented Architecture

Web-sovellusten testaus

- OWASP Security testing
- Selain
- Skannerit

Testaajan palaset

- Ystävällinen viestintä
- Ilkeä viestintä
- Tekninen osaaminen
- Ääretön uteliaisuus
- Kaheli mielikuvitus

Esimerkkejä tarvittavasta

- SQL ja tietokannat
- Koodaus
- Koneen sisusten tuntemus
- Salauksen ja algoritmien ymmärrys
- Muu matemaattinen ymmärrys
- Protokollien hallinta

Esimerkki – Ympäristö

- Testlink 1.8.5 - opensource
- Käyttöjärjestelmänä Ubuntu 9.04
- Testattu loppuvuodesta 2009
  - Niin infra- kuin sovellusvirheitä
- Raportoitu kehittäjille

Tietoturvavaatimukset

- ”Salainen projekti”
  - Erittäin salainen, sisältää sotilasteknologiaa
  - Sopimus kieltää ulkomaisen testauksen
- Turha Web-projekti
  - Asiakkaana Acme Hammers Inc
  - Testaus mahdollisimman halvalla -> ulkoistettu Islantiin
- Admin – myös testipäällikkö molemmissa projekteissa
- Ulkomainen testaaja
  - Oikeus vain Turha Web-projektiin
  - Tarve ryövätä teknologiaa Islannin uudelle armeijalle

Esimerkkien luonne

- Kevyestä kohti tuhoavaa
- XSS
- Evästeet
- XSS+Evästeet
- Cross site request forgery
- SQL injection
- Ja jotain muuta vielä pahempaa

XSS

- Cross site scripting
- Ajetaan kohdedomainin oikeuksilla Javascriptia selaajan koneessa
- Voidaan mm.
  - Tanssittaa Rick Astleytä Tiedon rekrytointisivuilla
  - Varastaa sessio-eväitä
  - Muuttaa sessio-eväitä

Heikko sessioiden käsittely

- Huono satunnaisuus tai liian lyhyt
- Kierrätetään
- Luotetaan liikaa selaimelta tulevaan

XSS+Evästeet

- Kahden aukon yhdistäminen
  -> katastrofaalinen virhe

Cross site request forgery

- Väärennetään kysely näyttämään toisen oikeuksilla tulevalta

SQL Injection

- Ajetaan muuta SQL:ää kuin koodaaja tarkoitti
- Kesä 2008 - yli 20000 sivua saastutettu
  - Levittivät haittaohjelmia
  - Toteutettiin ”sokeasti”
- Saadaan järjestelmä dumppaan mitä lystää

Infrastruktuurivirhe

- Ubuntu 9.04 antaa listata tiedostot
- Latasimme c99.php –shellin serverille
- Uudelleen nimeäminen ei auttanut – löytyi klikkaamalla
- Pystyttäisiin etsimään jopa SQL injektiolla

Linkkejä

- OWASP http://www.owasp.org/
  - Webin tietoturva
- Security Focus http://www.securityfocus.com/
  - Yleinen tietoturva

Yhteystiedot:
info@qentinel.com

Qentinel Oy
Tekniikantie 14, 02150 Espoo
www.qentinel.com

LET THERE BE QUALITY