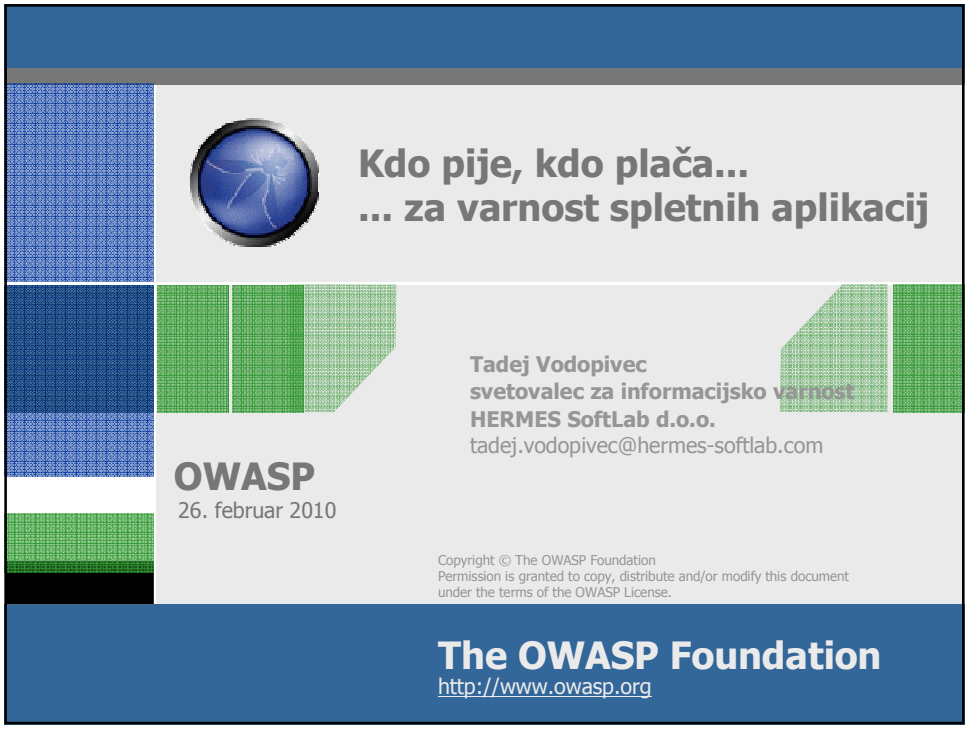


Kdo pije, kdo plača...
... za varnost spletnih aplikacij

Tadej Vodopivec
svetovalec za informacijsko varnost
HERMES SoftLab d.o.o.
tadej.vodopivec@hermes-softlab.com

OWASP
26. februar 2010

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

Agenda

- SDLC i SDL
- Poslovni modeli
- Analiza
- Načrtovanje
- Implementacija
- Testiranje
- Prenos v produkcijsko okolje
- Vzdrževanje in podpora
- Agilni življenjski cikli

SDLC – Software Development Life Cycle

Analiza

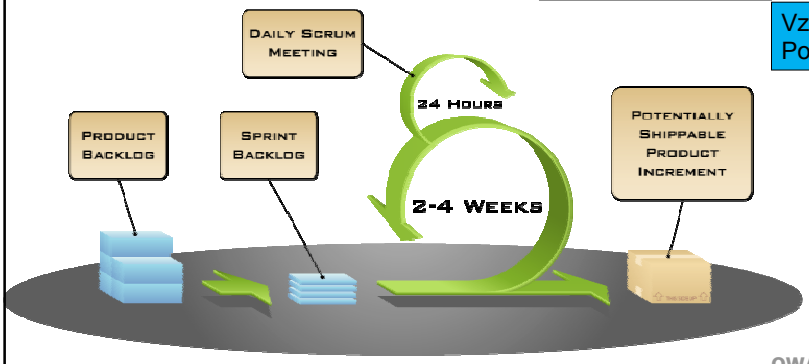
Načrtovanje

Implementacija

Testi

Prenos v produkcijo

Vzdrževanje & Podpora



SDL – Security Development Lifecycle

- Formalen pristop Definiran s strani Microsofta

Training	Require-ments	Design	Impleme-ntation	Verifi-cation	Release	Response
• Core Security Training	• Establish Security Requirements • Create Quality Gates / Bug Bars • Security & Privacy Risk Assesment	• Establish Design Requirements • Analyze Attack Surface • Threat Modelling	• Use Approved Tools • Deprecate Unsafe Functions • Static Analysis	• Dynamic Analysis • Fuzz Testing • Attack Surface Review	• Incident Response Plan • Final Security Review • Release Archive	• Execute Incident Response Plan

Agenda

- SDLC i SDL
- **Poslovni modeli**
- Analiza
- Načrtovanje
- Implementacija
- Testiranje
- Prenos v produkcijsko okolje
- Vzdrževanje in podpora
- Agilni življenjski cikli

Poslovni modeli

- Razvoj po naročilu
- Razvoj za trg
- Free Open Source
- SaaS

Agenda

- SDLC i SDL
- Poslovni modeli
- **Analiza**
- Načrtovanje
- Implementacija
- Testiranje
- Prenos v produkcijsko okolje
- Vzdrževanje in podpora
- Agilni življenjski cikli

Analiza

- Prepoznavanje varnostnih zahtev
- Definicija varnosti
- Zakonodaja in relevantni predpisi
- Tveganja
- Avtentikacija, faktorji in seje
- Verifikacija operacij/transakcij
- Računalniki -> mobilni telefoni
- Konflikti poslovnih interesov – postavimo prioritete
- Pregled specialista

Agenda

- SDLC i SDL
- Poslovni modeli
- Analiza
- **Načrtovanje**
- Implementacija
- Testiranje
- Prenos v produkcijsko okolje
- Vzdrževanje in podpora
- Agilni življenjski cikli

Načrtovanje

- Preprečevanje tehničnih ranljivosti
- Spletne storitve, AJAX, Pametni odjemalci
- Varnostne kontrole naj bodo na strežniku!
- Zahteve za produkcijsko okolje
  - platforma (Adobe Flash, AIR, Silverlight, Java FX...) – upoštevamo tudi zgodovino ranljivosti platforme
  - vključeni programski produkti
- Digitalno podpisovanje programske opreme, pri prenosih prek interneta, tudi npr. samodejnih posodobitvah
- Pozorno pri banalnih zadevah: SSL in ne-SSL
  - http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf
- Pregled specialista

Agenda

- SDLC i SDL
- Poslovni modeli
- Analiza
- Načrtovanje
- **Implementacija**
- Testiranje
- Prenos v produkcijsko okolje
- Vzdrževanje in podpora
- Agilni življenjski cikli

Implementacija

- Doslednost
- Podprtost z orodji
- Izobraževanje razvijalcev
- Pregledi kode (ročni, avtomatski)
  - Neodvisnost
- Unit testi
- Dokumentacija
- Don't believe in miracles, rely upon them
  - ljudje vs. metodologija

Agenda

- SDLC i SDL
- Poslovni modeli
- Analiza
- Načrtovanje
- Implementacija
- **Testiranje**
- Prenos v produkcijsko okolje
- Vzdrževanje in podpora
- Agilni življenjski cikli

Testiranje

- Varnostno testiranje
  - preverjanje vseh varnostnih zahtev
  - pozitivno in negativno - "misuse cases"
- Neodvisnost
- Security Functional Requirements vs. Security Assurance Requirements

Agenda

- SDLC i SDL
- Poslovni modeli
- Analiza
- Načrtovanje
- Implementacija
- Testiranje
- **Prenos v produkcijsko okolje**
- Vzdrževanje in podpora
- Agilni življenjski cikli

Prenos v produkcijsko okolje

- veliko možnosti da pokvarimo varnost
- pomembno je dokumentirati varnostne predpostavke / zahteve za produkcijsko okolje

Agenda

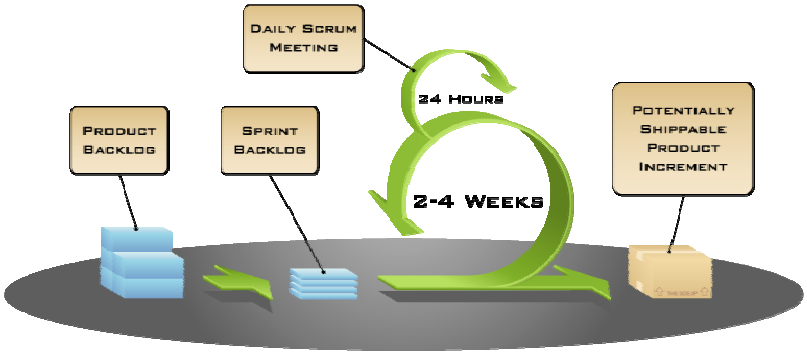
- SDLC i SDL
- Poslovni modeli
- Analiza
- Načrtovanje
- Implementacija
- Testiranje
- Prenos v produkcijsko okolje
- **Vzdrževanje in podpora**
- Agilni življenjski cikli

Vzdrževanje in podpora

- Izziv: spremembe v okolju
  - novo odkrite ranljivosti vključenih produktov
  - novo odkrite ranljivosti platforme
  - novo odkrite ranljivosti protokolov
  - nove vrste napadov se realizirajo
- Spremljanje zunanjih dogodkov
- Financiranje sprememb
- Stabilna aplikacija
  - zaradi sprememb v okolju spoznamo, da je (postala bolj) ranljiva
- Vzdrževanje nivoja varnosti

Agilni življenjski cikli in SDL

- http://www.blackhat.com/presentations/bh-dc-10/Sullivan_Bryan/BlackHat-DC-2010-Sullivan-SDL-Agile-wp.pdf



Agilni življenjski cikli in SDL

- Every-Sprint Requirements
  - če jih izpustimo, se "podre" varnost izdelka
- Bucket Requirements
  - manj kritične
  - 3 buckets
    - testi (fuzzers & other tools)
    - pregledi (review) design-a
    - response planning
  - v vsakem sprintu ena iz vsakega "ajmarja"
- One-time requirements
  - Baseline threat model
  - druge zahteve, katerih izpolnitev je smiselna 1x v projektu
    - določitve odgovornih za varnost, varstvo osebnih podatkov, izbira razvojne platforme, vključenih produktov

Re-use

- pozorno – po komponentah npr.
  - specifikacije – posamezne
  - building block – specifičen
- ovrednotiti tveganje za re-use

- Naravno stanje spletne aplikacije je ne-varno – varnost potrebno ustvariti s pravilno vloženim delom, ki ga mora nekdo plačati ali darovati
  - Naročnika tipično varnost zanima, ko občuti zlorabo, prej ne
  - Uporabnika tipično varnost zanima, ko občuti zlorabo, prej ne
  - Ponudnika tipično varnost zanima, ko lahko z njo kaj zasluži

Kdo pije, kdo plača...
... za varnost spletnih aplikacij

Tadej Vodopivec
svetovalec za informacijsko varnost
HERMES SoftLab d.o.o.
tadej.vodopivec@hermes-softlab.com

OWASP
26. februar 2010

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