



# Hoe bouw je veilige applicaties met Lotus Notes?

Ferdinand Vroom CISSP  
30 November 2007

**Zeker zijn van elkaar**

## **Missie**

- 'Nationale-Nederlanden helpt als toonaangevende, geïntegreerde financiële dienstverlener op innovatieve wijze haar klanten hun ambities te realiseren.'
- Zij doet dat door actief en oplossingsgericht financiële concepten aan te bieden en uit te blinken door een excellente kwaliteit van dienstverlening.'

# Agenda

1. Laatste stand van web applicatie kwetsbaarheden
2. Introductie in (web) applicatie beveiliging
3. Aanpassing van het software ontwikkelproces
4. (web) Applicatie tests en tools
5. Conclusies

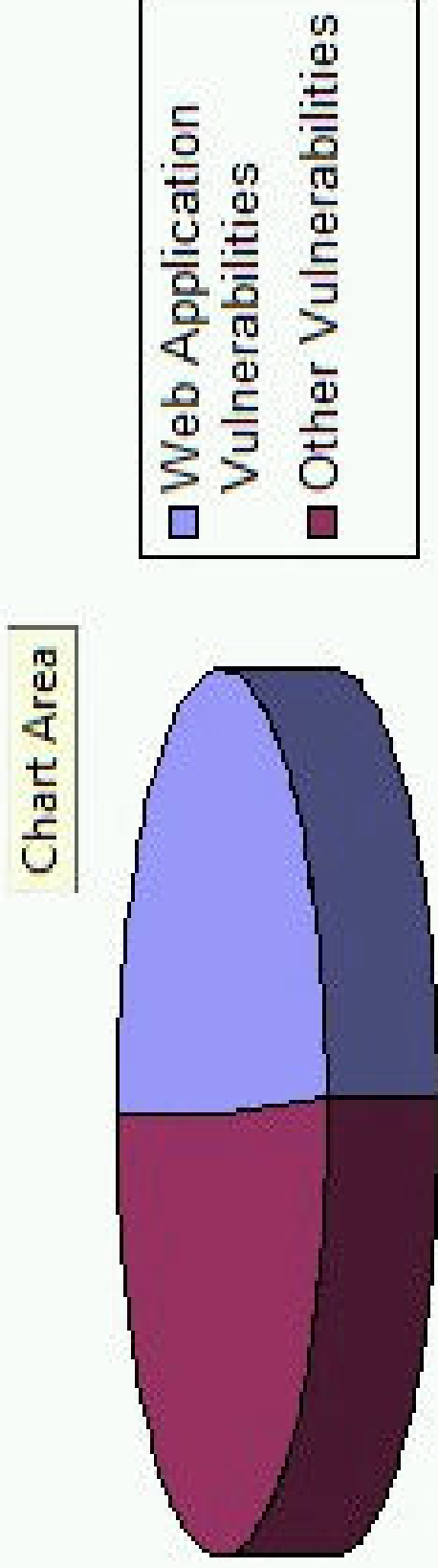
## **Laatste stand van web applicatie kwetsbaarheden**

“Daft users and insecure web apps dominate threat index” – The Register 27 November 2007

“Web application vulnerabilities in open-source as well as custom-built applications account for almost half the total number of vulnerabilities being discovered in the past year” – SANS Institute 28 November 2007

## Laatste stand van web applicatie kwetsbaarheden

### 4396 Total Vulnerabilities Reported in SANS @RISK Data From November 2006 - October 2007



Zeker zijn van elkaar

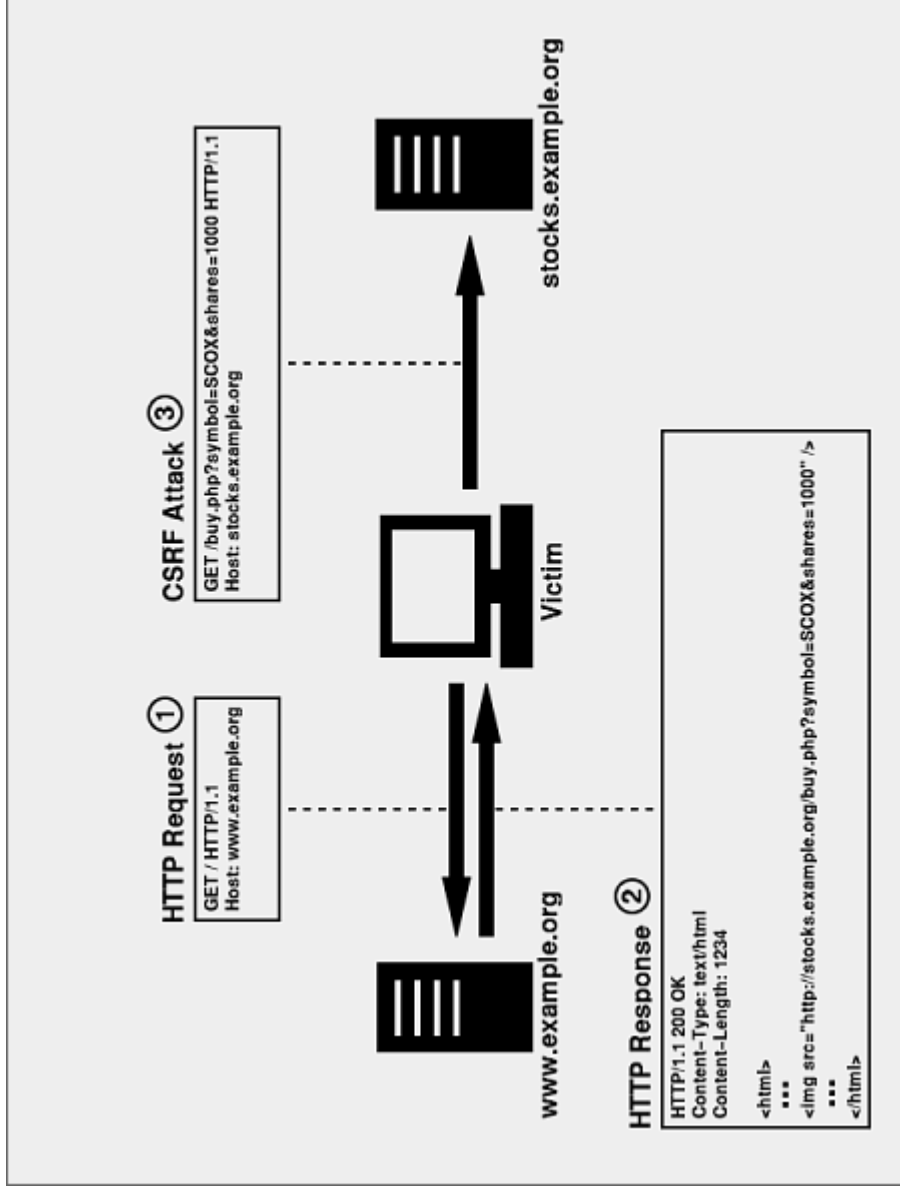
## Laatste stand van web applicatie kwetsbaarheden

### ■ Soorten XSS

1. Aanval op lokaal uitgevoerde html e/o script
2. “Non- persistent”, aanval waarbij html e/o script in een dynamische pagina wordt geïnjecteerd
3. “Persistent”, aanval waarbij html e/o script op een server wordt opgeslagen en vervolgens door niets vermoedende gebruikers wordt bekeken

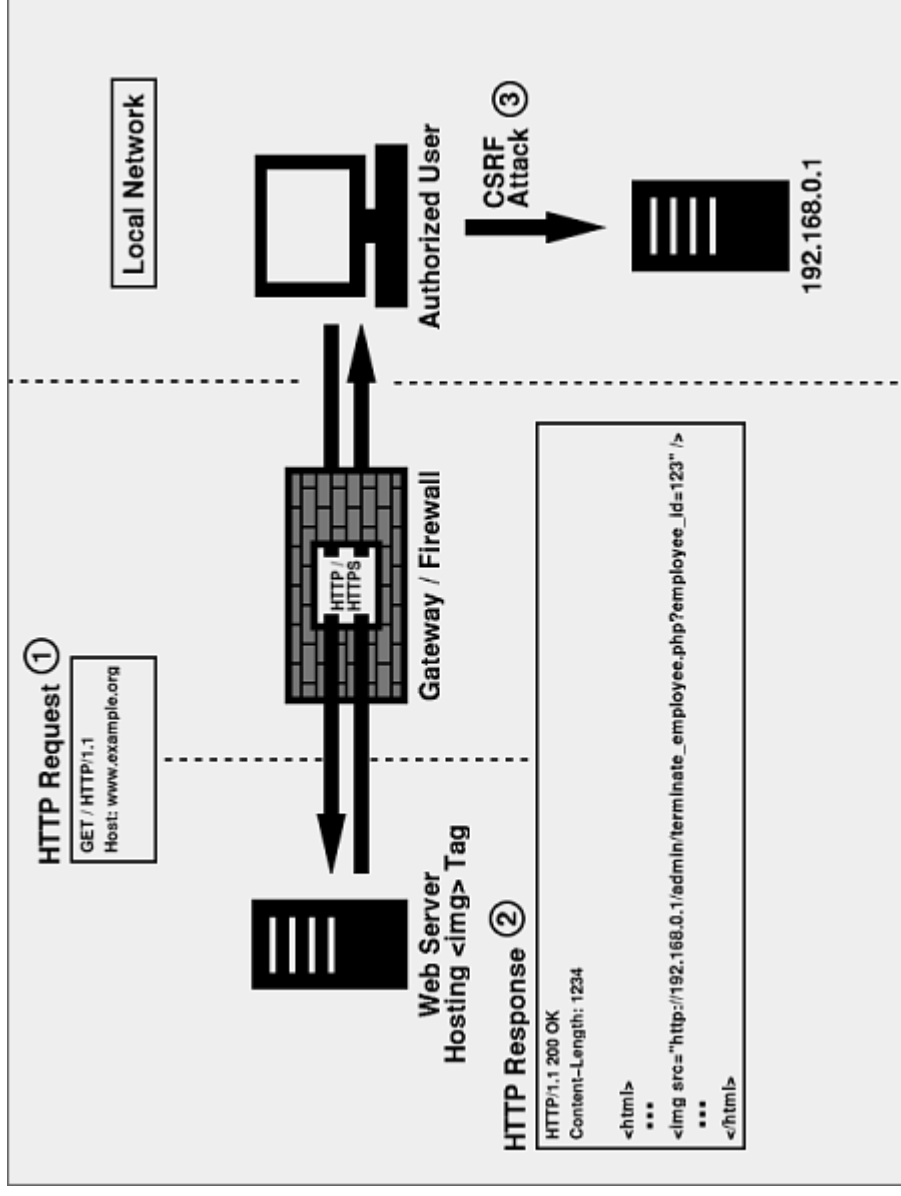
# Laatste stand van web applicatie kwetsbaarheden

## ■ Cross Site Request Forgery



## Laatste stand van web applicatie kwetsbaarheden

### ■ Cross Site Request Forgery (local)



## Laatste stand van web applicatie kwetsbaarheden

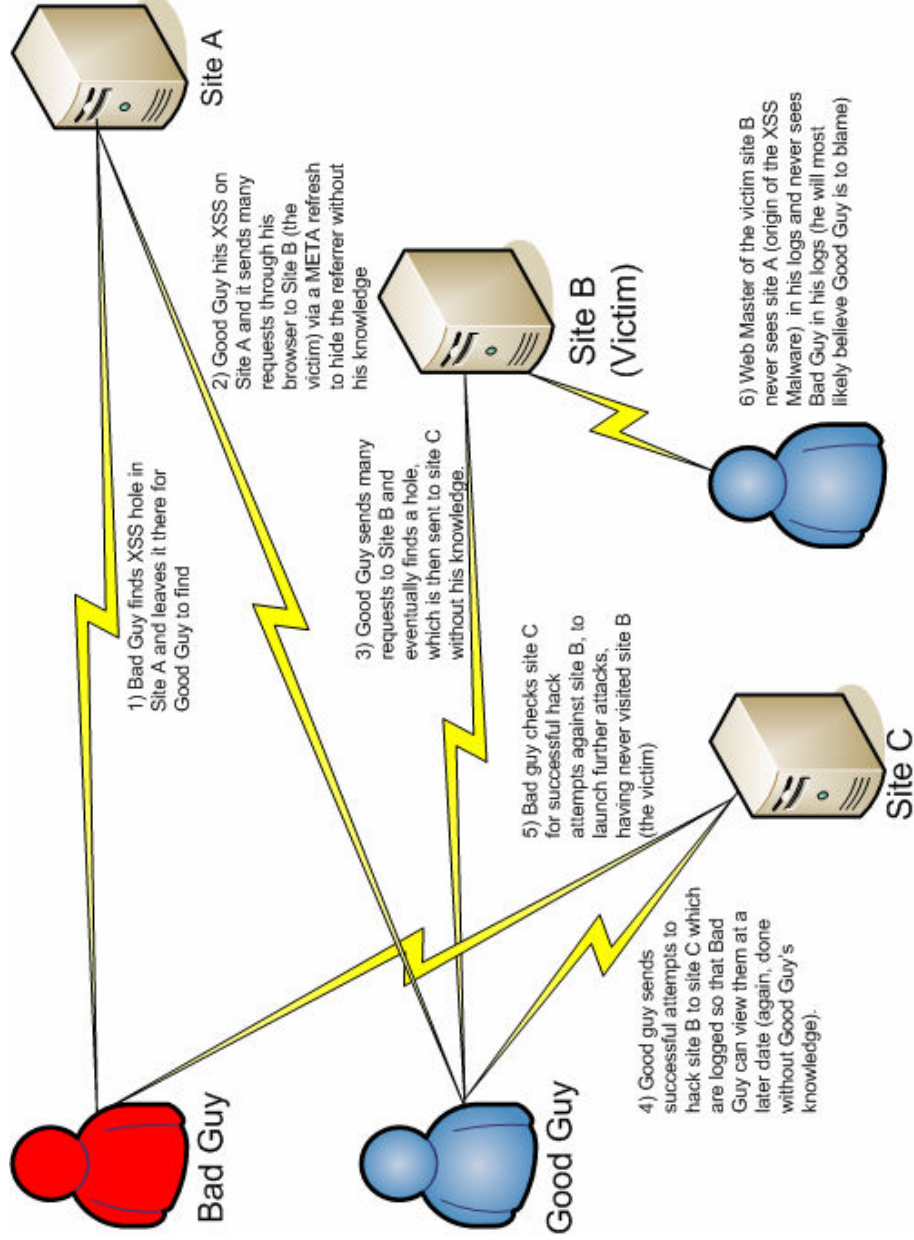
- Acrobat PDF XSS (Cross Site Scripting)

[http://www.snug.nl/home/snugnew.nsf/view/doc/\\$FILE/SNUG%2020060905.pdf#bla=javascrpt:alert\('XSS'\)](http://www.snug.nl/home/snugnew.nsf/view/doc/$FILE/SNUG%2020060905.pdf#bla=javascrpt:alert('XSS'))

- Lotus Domino Web Access XSS
  - XSS aanval in de naam van een attachment in DWA
  - LDAP deamon
  - SMTP/ IMAP
  - Etc.

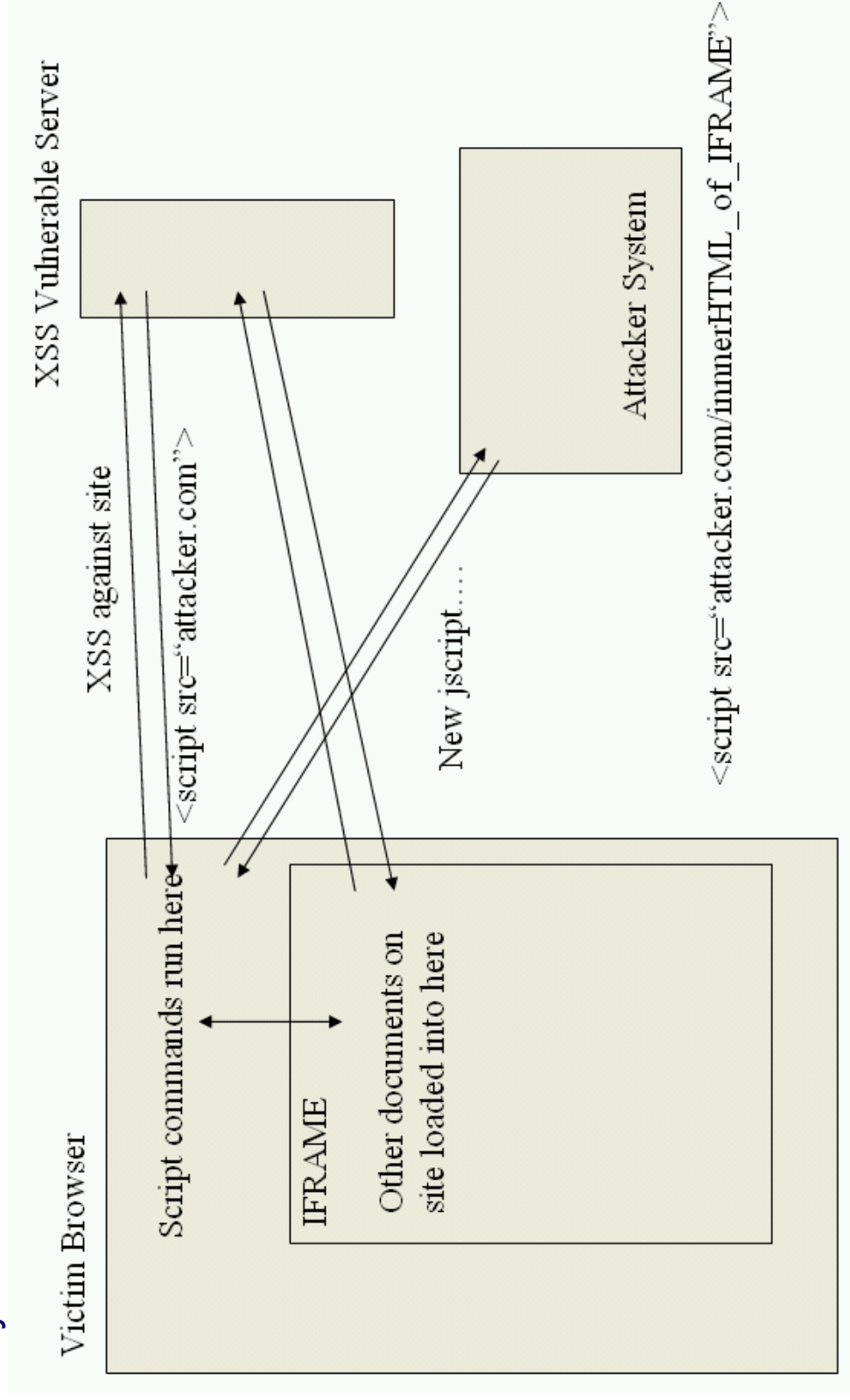
# Laatste stand van web applicatie kwetsbaarheden

## ■ XSS Proxy



# Laatste stand van web applicatie kwetsbaarheden

- XSS Proxy



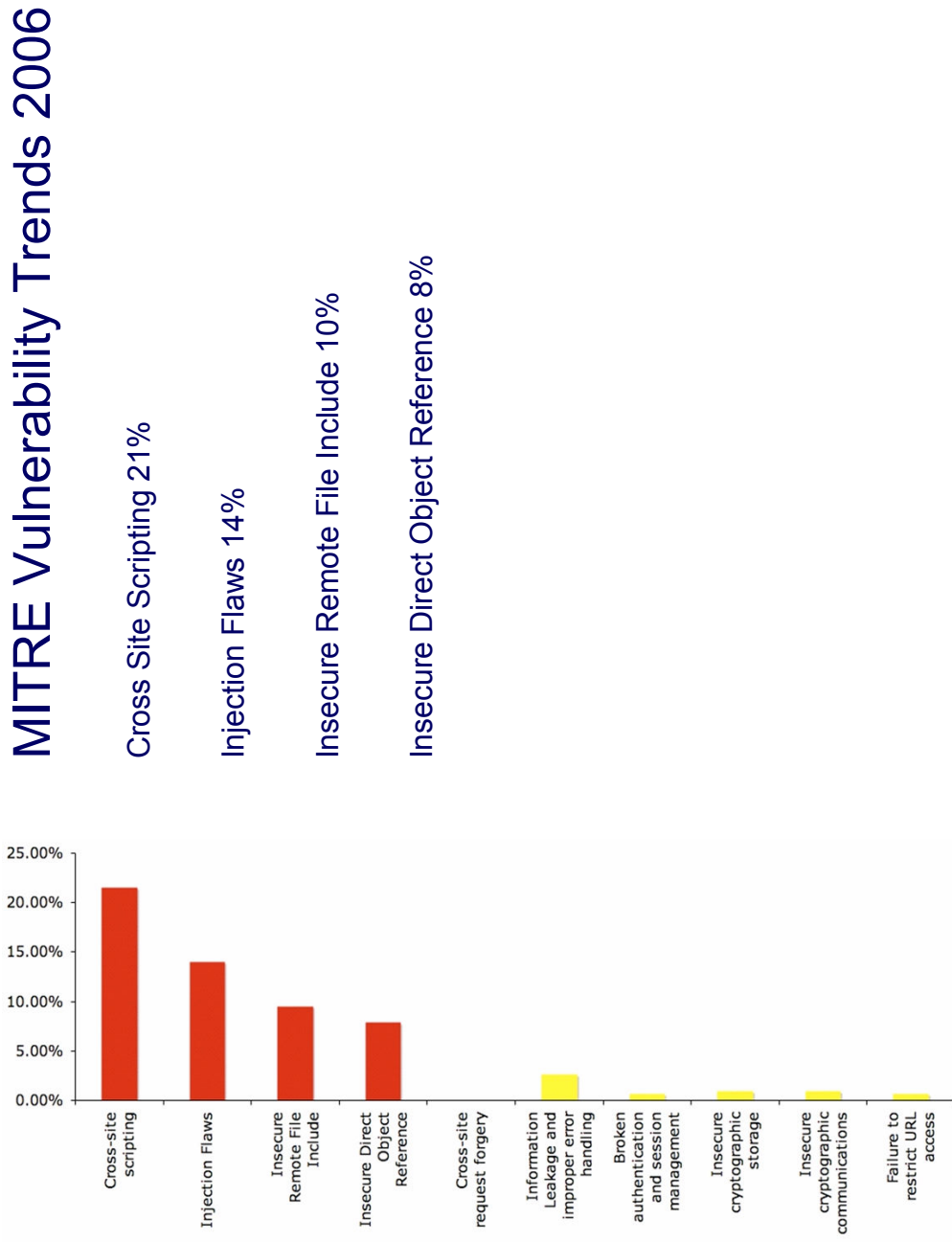
# Agenda

1. Laatste stand van web applicatie kwetsbaarheden
2. **Introductie in (web) applicatie beveiliging**
3. Aanpassing van het software ontwikkelproces
4. (web) Applicatie tests en tools
5. Conclusies

## Introductie in (web) applicatie beveiliging

- OWASP
  - Top ten
    - The OWASP Top Ten provides a powerful **awareness** document for web application security.
  - Guide
    - The Guide is aimed at architects, developers, consultants and auditors and is a comprehensive manual for designing, developing and deploying secure web applications.

# Introductie in (web) applicatie beveiliging



## **Introductie in (web) applicatie beveiliging**

OWASP Top Ten 2004 – 2007

Nieuw in 2007:

- Insecure Remote File Include
- Cross Site Request Forgery
- Insecure Communications

Zie SNUG presentatie van 5 september 2006

## Introductie in (web) applicatie beveiliging

- OWASP Top Ten 2007
- A1 - Cross Site Scripting (XSS)
- A2 - Injection Flaws
- A3 - Malicious File Execution
- A4 - Insecure Direct Object Reference
- A5 - Cross Site Request Forgery (CSRF)
- A6 - Information Leakage and Improper Error Handling
- A7 - Broken Authentication and Session Management
- A8 - Insecure Cryptographic Storage
- A9 - Insecure Communications
- A10 - Failure to Restrict URL Access

# Agenda

1. Laatste stand van web applicatie kwetsbaarheden
2. Introductie in (web) applicatie beveiliging
3. **Aanpassing van het software ontwikkelproces**
4. (web) Applicatie tests en tools
5. Conclusies

## **Aanpassing van het software ontwikkelproces**

- Bewustzijn en opleiding
- Goede voorbeelden
- Risico analyse
- Regels en procedures
- Inspectie en test
- Incident respons

## **Aanpassing van het software ontwikkelproces**

Bewustzijn en opleiding

- OWASP Top Ten & Guide
- HTTP Protocol
- Kwetsbaarheden onderzoeken
- Lotus Domino specifieke trainingen
- Beveiligingstrainingen

## **Aanpassing van het software ontwikkelproces**

Goede voorbeelden

- Templates van IBM Lotus Domino
- OpenNTF
- Teamstudio
- OWASP Guide

## Aanpassing van het software ontwikkelproces

### Risico analyse

- Wat is de impact op de onderneming als er kwetsbaarheden worden gevonden en misbruikt?
  - €
  - Imago
- Application Threat modeling

## Aanpassing van het software ontwikkelproces

### Regels en procedures

- Stel regels op waaraan software moet voldoen
  - Zelfbouw
  - Uitbested
  - Aangekocht
- Procedures voor ontwikkeling en beheer van software
  - Stel procedures op voor het in gebruik nemen van nieuwe versies
  - Stel procedures op voor het oplossen van bugs
  - Stel procedures op voor het oplossen van kwetsbaarheden
  - Gebruik versiebeheerstools e.d.

## Aanpassing van het software ontwikkelproces

### Inspectie en test

- Broncode inspectie
  - Voer broncode inspecties uit
  - Peer reviews
  - Closed code inspection door derde, onafhankelijke partij
- Testen
  - Non- functional requirements
  - Minimaal OWASP Top Ten
  - Begin met testen in de ontwikkelfase
  - Beter nog: test het ontwerp

## **Aanpassing van het software ontwikkelproces**

### **Incident en respons**

- **Zorg ervoor dat is vastgelegd wat te doen als er een incident wordt gemeld**
- **Bepaal de impact**
- **Probeer de schade te beperken**
- **Bepaal een baseline die wel veilig is**
- **Zorg ervoor dat je weet wie welke versie gebruikt**
- **Automatiseer de uitrol van nieuwe versie en patches**

# Agenda

1. Laatste stand van web applicatie kwetsbaarheden
2. Introductie in (web) applicatie beveiliging
3. Aanpassing van het software ontwikkelproces
4. **(web) Applicatie tests en tools**
5. Conclusies

## **(web) Applicatie tests en tools**

- Penetration (Pen) test
- Black/ White Box test

## **(web) Applicatie tests en tools**

### Open source tools

- Paros Proxy
- OWASP Web Scarab

### Commerciële tools

- SPI Dynamics (HP) WebInspect
- IBM Rational AppScan (WatchFire)

# Agenda

1. Laatste stand van web applicatie kwetsbaarheden
2. Introductie in (web) applicatie beveiliging
3. Aanpassing van het software ontwikkelproces
4. (web) Applicatie tests en tools
5. **Conclusies**

# Demo



# Demo

- Hoe gaat een hacker te werk?
- 1. Verkennen
- 2. Scannen en opsommen
- 3. Toegang verkrijgen
- 4. Verhogen van rechten
- 5. Toegang behouden
- 6. Sporen wissen

## Conclusies

- Lotus Domino is een veilig platform
- Ook Lotus Domino heeft kwetsbaarheden
- Blijf op de hoogte van de laatste kwetsbaarheden en zorg ervoor dat ze niet misbruikt kunnen worden op je omgeving
- Pas het ontwikkelproces aan
- Voer beveiligingstests uit
- Denk als een hacker
- Hack zelf eens een applicatie

## Vragen & Antwoorden

[info@ferdinandvroom.nl](mailto:info@ferdinandvroom.nl)