Beveiligingsaspecten van webapplicatie ontwikkeling

9-4-2009

Wouter van Kuipers
Informatiekunde
Radboud Universiteit Nijmegen
w.vankuipers@student.ru.nl

Inhoud

- Het onderzoek
- Literatuurstudie
- Interviews
- Sourcecode analyzer
- Best practices
- Conclusie

Wouter van Kuipers - w.vankuipers@dacon.nl

Achtergrond

- **Opleidingen**
  - *MBO Informatica*
  - *HBO Communicatie systemen*
  - *WO Informatiekunde*
- **Werkervaring**
  - *Freelance PHP programmeur*
  - *Dacon*

Wouter van Kuipers - w.vankuipers@dacon.nl

Het onderzoek

- **Waarom dit onderwerp**
  - *Vooropleiding*
  - *Werkervaring*
  - *Veranderingen in de softwaremarkt*
- **Het doel**
  - *Oplossingen bieden aan ontwikkelbedrijven*

Wouter van Kuipers - w.vankuipers@dacon.nl

'Vijf Nederlandse banken hebben zelfde xss-lek'

Artikelgereedschap

Gepubliceerd: Vrijdag 20 maart 2009
Auteur: Loek Essers

Vijf Nederlandse banken zijn sinds begin maart kwetsbaar voor xss-aanvallen. Slechts twee banken ondernamen actie na waarschuwing van een hacker.

Volgens ict'er Zarco Zwier zijn vijf Nederlandse banken vatbaar voor cross site scripting aanvallen. Het gat is te gebruiken via de zoekfuncties van de verschillende websites.Het gaat om ABN AMRO, Aegon bank, Delta Lloyd, Binck Bank, Fortis en ING.

Begin maart blogde de hacker over het lek en stelde hij de banken via e-mail op de hoogte. Daarop ondernamen alleen ING

Bron: webwereld.nl

Wouter van Kuipers - w.vankuipers@dacon.nl

Klantendatabase Kaspersky door hacker gestolen

08-02-2009, 11:06 door **Redactie**
Reacties: 8

Een Italiaanse hacker beweert de website van de Russische virusbestrijder Kaspersky Lab te hebben gehackt, waarbij hij onder andere toegang tot de klantendatabase had. Via SQL-injectie lukte het de aanvaller om toegang tot de database van de Amerikaanse website te krijgen. Daarin stond informatie over gebruikers, activatiecodes, lijsten met bugs, beheerders, gegevens over de webshop en nog veel meer. Als bewijs zijn er verschillende screenshots geplaatst, hoewel de aanvaller geen persoonlijke informatie online zette. "Voor deze keer zal ik, voor redenen die ik niet hoef uit te leggen, geen screenshots met persoonlijke informatie of activatie codes publiceren." Wel heeft hij de lijst met database tabellen online gezet en dat is een behoorlijke lijst.

Bron: security.nl

Wouter van Kuipers - w.vankuipers@dacon.nl

Hackers plunderen weer database Monsterboard

24-01-2009, 10:05 door **Redactie**
Reacties: 11

Weer zijn aanvallers erin geslaagd de database van vacaturesite Monsterboard te plunderen, in 2007 was het ook al twee keer raak. Tevens wisten de hackers ook in te breken bij USAJOBS.gov, waar Monster de database van beheert. De vacaturesite waarschuwt haar gebruikers dat de aanvallers gebruikersnamen, wachtwoorden, e-mailadresssen, namen, telefoonnummers en "beperkte demografische gegevens" wisten te stelen. "Zoals het geval is bij vele bedrijven die grote databases met informatie beheren, is Monster het doelwit geworden van illegale pogingen om toegang te verkrijgen tot en/of het halen van informatie uit haar database."

Bron: security.nl

Wouter van Kuipers - w.vankuipers@dacon.nl

Het onderzoek

- **Achtergrond**
  - *Computer applicaties*
  - *Het World Wide Web*
  - *Webapplicaties → Web 2.0*

- **PHP Hypertext preprocessor**
  - *Marktaandeel 33%*
  - *Laagdrempelig*
  - *Ontwikkelgemak ten kosten van security*

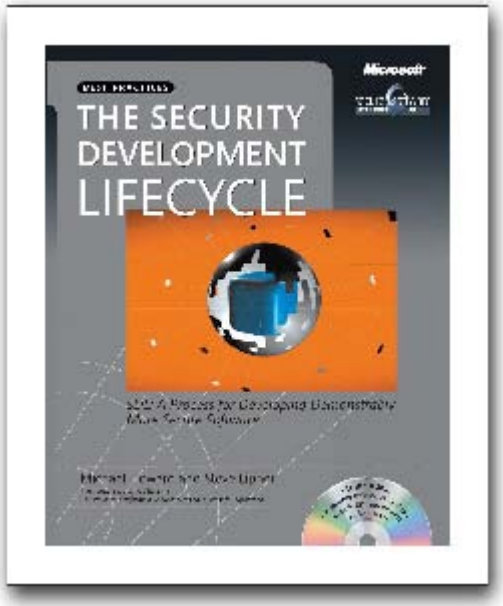
Wouter van Kuipers - w.vankuipers@dacon.nl

Interviews

- **Kleine bedrijven**
  - *Ontwikkelaar verantwoordelijk voor eigen werk*
  - *Geen geld/tijd voor persoonlijke ontwikkeling*
- **Grote bedrijven**
  - *Duidelijke verantwoordelijkheden*
  - *Scholing goed geregeld*
- **Overigen**
  - *Code testen (JAVA)*
  - *Awareness bij het management*

Wouter van Kuipers - w.vankuipers@dacon.nl

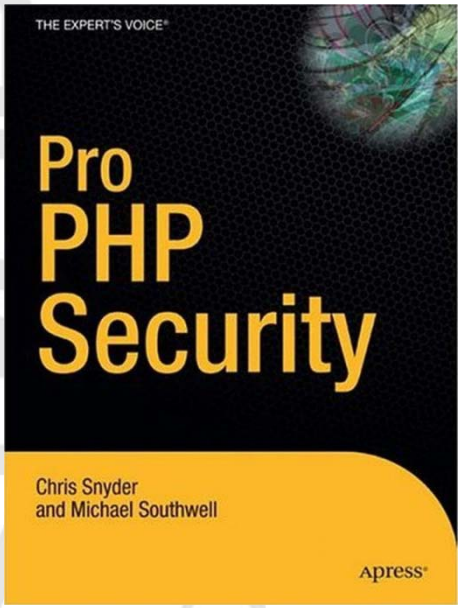
Literatuurstudie

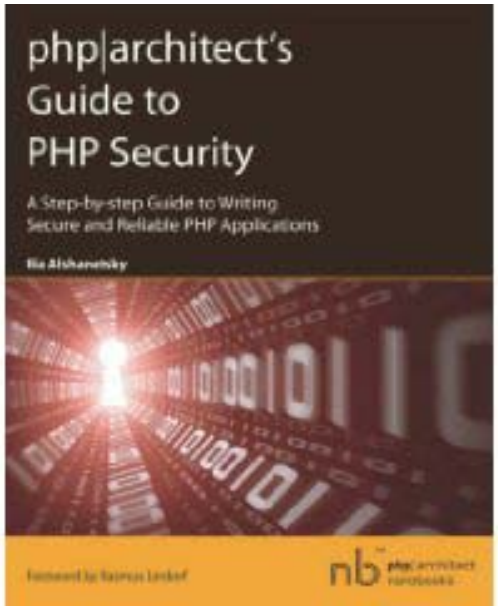


- **Oplossingen als Microsoft SDL**
  - *Totaalpakket aan oplossingen*
  - *Geschikt voor grote bedrijven*

Wouter van Kuipers - w.vankuipers@dacon.nl

Literatuurstudie





- **PHP oplossingen**
  - *Lost slechts een deel van het probleem op*
  - *Geschikt voor kleinere bedrijven*

Literatuurstudie

- **Informatie op het internet**
  - *Lastig te vinden*
  - *Lastig te beoordelen*

Wouter van Kuipers - w.vankuipers@dacon.nl

Sourcecode analyzer

- **Fortify 360**
  - *Sourcecode Analyzer (SCA)*
  - *Real-time Analyzer (RTA)*
  - *Program Trace Analyzer (PTA)*
  - *ASP.NET, C#.NET, VB.NET, C/C++, JAVA, PLSQL/TSQL, PHP en VB*

Wouter van Kuipers - w.vankuipers@dacon.nl

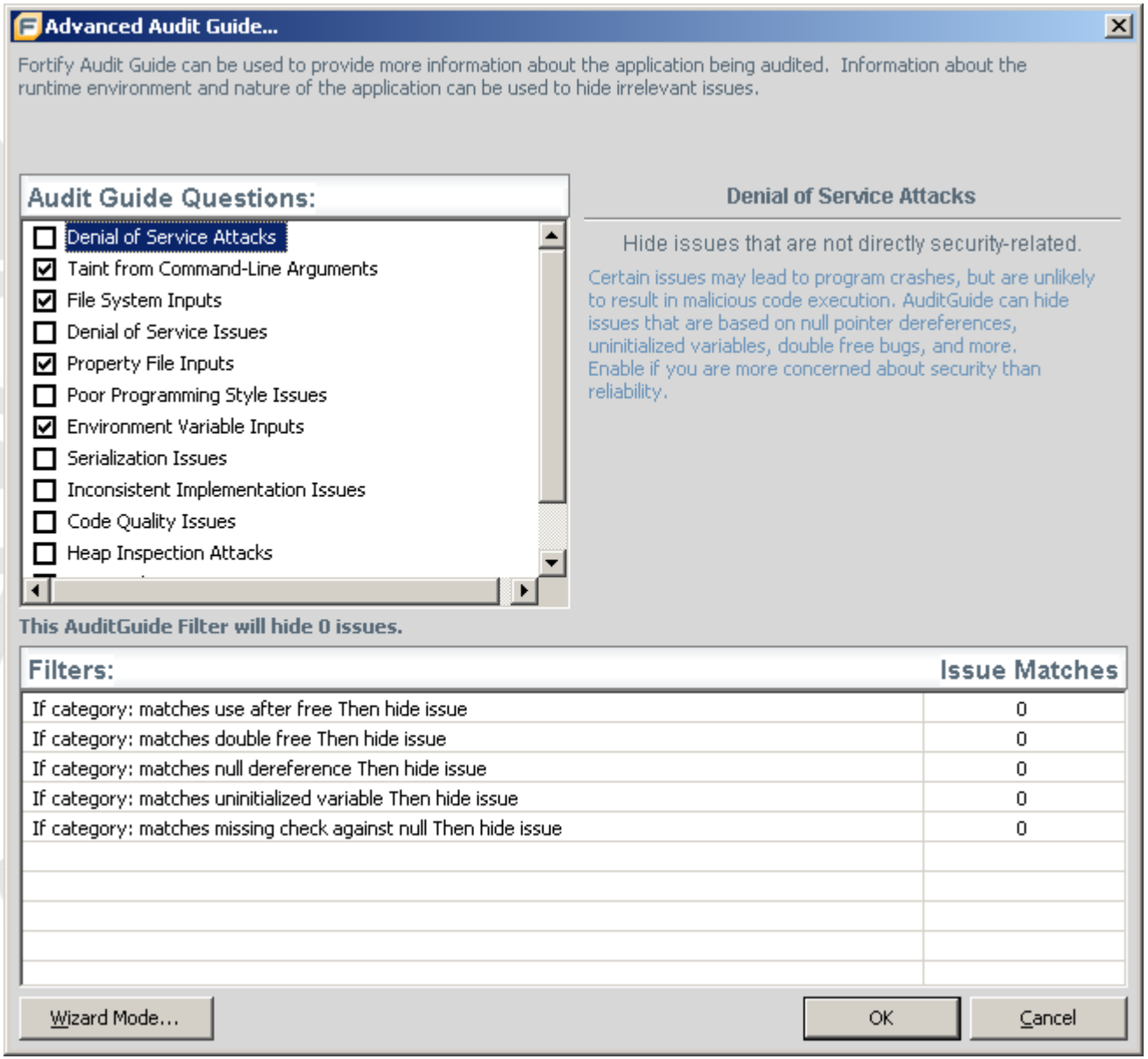
Sourcecode analyzer

Wouter van Kuipers - w.vankuipers@dacon.nl

Sourcecode analyzer

- **Doel**
  - *Analyseren van de broncode op problemen*

Wouter van Kuipers - w.vankuipers@dacon.nl

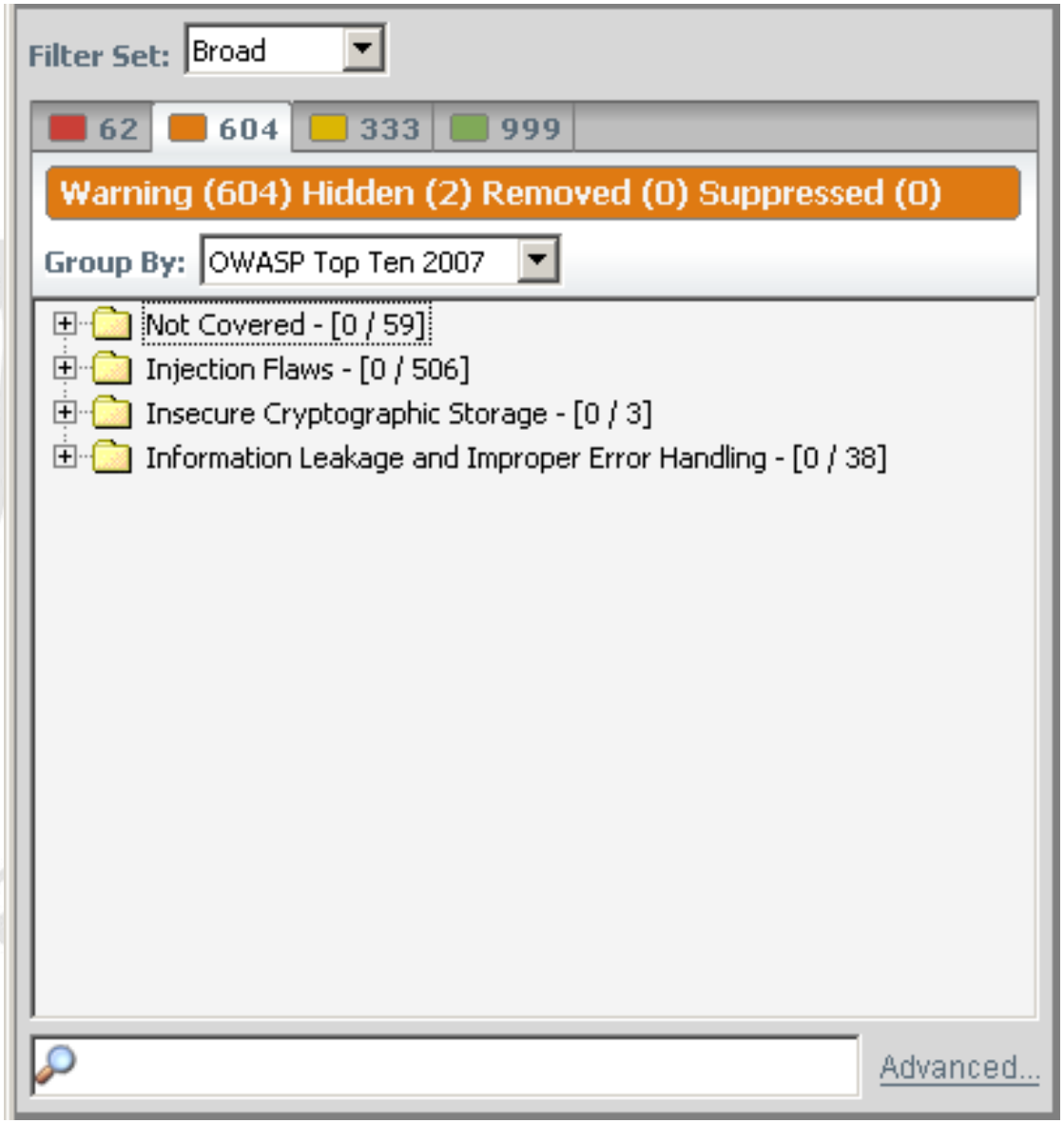


Wouter van Kuipers - w.vankuipers@dacon.nl

Sourcecode analyzer

- **Doel**
  - *Ordenen van gevonden problemen*

Wouter van Kuipers - w.vankuipers@dacon.nl



Wouter van Kuipers - w.vankuipers@dacon.nl

Sourcecode analyzer

- **Doel**
  - *Informeren van het management*

Wouter van Kuipers - w.vankuipers@dacon.nl

Sourcecode analyzer

- **Onderzoek**
  - *Automatische analyse door Fortify*
  - *Handmatige analyse resultaten*
  - *Scannen van twee zelf geschreven applicaties*
    - **Content Management Systeem**
    - **Customer Relationship Management System**
    - **30.000 SLOC**

Wouter van Kuipers - w.vankuipers@dacon.nl

Sourcecode analyzer

➔ Tijdsduur

- *Scannen code: 6 minuten*
- *Handmatige analyse problemen CMS: 50 min.*
- *Handmatige analyse problemen CRM: 145 min.*

➔ Resultaten

- *Totaal aantal positives: 421 (CMS 248, CRM 173)*
- *Aantal true positives: 282 (67%)*
- *Aantal false positives: 139 (33%)*

Wouter van Kuipers - w.vankuipers@dacon.nl

Sourcecode analyzer

- **Analyse problemen**
  - *Hoge score op makkelijk te herleiden gevaren*
    - **Hash functies**
    - **Password in comment**
  - *Lage score op lastig te herleiden gevaren*
    - **XSS**
    - **CSRF**
  - *Wat is een probleem?*

Wouter van Kuipers - w.vankuipers@dacon.nl

Probleem?

- # genereer een unieke naam
- $name = md5(time().rand());

- # ask user for password
- Function askPassword(){ ...

Wouter van Kuipers - w.vankuipers@dacon.nl

Sourcecode analyzer

- **Conclusie**
  - *Goede detectie*
  - *Goede aanvulling op bestaande werkwijze*
  - *Snel en goedkoop*
  - *Lastig om andermans code te analyseren → analyseer eigen code*
  - *Programma leidt programmeur op*

Wouter van Kuipers - w.vankuipers@dacon.nl

Conclusie

- Webapplicatie != desktopapplicatie
- Security beleid voor grote bedrijven goed geregeld
- Kleine bedrijven missen
  - *Awareness*
  - *Budget*
  - *Scholing*
- Gebruik SCA's voor analyse
- OWASP
  - *Verzamel bronnen*

Wouter van Kuipers - w.vankuipers@dacon.nl

Bedankt voor uw aandacht

Wouter van Kuipers - w.vankuipers@dacon.nl