



SWG Partner Academy

Rational – Mehr Sicherheit für Ihre Webanwendungen und Hacker haben keine Chance

3. Tag, Donnerstag den 09.10.2008

Michael Bleichert
Rational Channel Manager Germany
Michael.Bleichert@de.ibm.com

IBM Rational Sales Presentation

Watchfire provides web application vulnerability and web compliance testing solutions to help enterprises **reduce risk and the costs** associated with online security and compliance breaches.



Security



Privacy



Quality



Standards



Compliance

Web Application Security, Quality and Compliance

Angriffe auf Anwendungsebene

- **Angriffe auf Webanwendungen**
- **Angriffe auf die Authentifizierung**
 - Brute Force / Dictionary Angriff
 - Angriffe auf die Authentifizierung
 - SQL Injection
 - Cross Site Scripting (XSS)
 - Command Execution
 - Input Validation / Encodings

Angriffe auf die Authentifizierung

- **Brute Force**
 - Durchprobieren aller möglichen Kombinationen einer bestimmten Zeichenmenge

- **Dictionary Angriff**
 - Durchprobieren aller Benutzernamen und Passwörter basierend auf Wörterlisten

- **Es existieren Programme für nahezu alle Protokolle / Anwendungen**
 - telnet, snmp, pop, ssh, http, ...

Angriffe auf Webanwendungen

■ SQL Injection

- Bezeichnet eine Technik SQL Code in eine Anwendung einzuschleusen (injizieren), der so von der Anwendung nicht vorgesehen war
- Ermöglicht je nach Zugriffs-Rechte Struktur bis zu vollem Zugriff auf das Datenbank System bzw. das zugrundeliegende Betriebssystem
- Das Problem entsteht wenn Benutzereingaben vertraut wird oder diese nicht hinreichend validiert werden, und in SQL Statements einfließen

Angriffe auf Webanwendungen

■ **Cross Site Scripting**

- Ähnlich wie bei SQL Injection wird bei Cross Site Scripting (XSS) Skript oder HTML Code in eine Anwendung eingebettet
- Ermöglicht Ausführung von Code im Kontext einer Anwendung
- Wird die Web Seite von einem Benutzer aufgerufen wird, im Falle von Skript Code, dieser Code auf dem Client ausgeführt

■ **Ermöglicht Angriffe auf**

- Die Web Site
- Die Benutzer der Web Site

Cross Site Scripting

- **„persistentes“ Cross Site Scripting**
 - Skriptcode wird persistent auf dem Server gespeichert und bei anderen Nutzern ausgeführt
 - Gästebücher
 - Foren
 - Weblogs

- **„nicht persistentes“ Cross Site Scripting**
 - Skriptcode wird nicht auf dem Server gespeichert
 - Skriptcode wird mit der Anfrage (Query) mitgesendet
 - Suchen (search.asp?q=suchbegriff)
 - Personalisierte Seiten (welcome.php?name=helmut)

Schwachstellen erkennen

- **Penetration Tests**

- **Regelmäßiges Audit der Systeme**
 - Logfiles
 - Vulnerability Scanner -> IBM Rational Appscan

Why application security?

Many application owners think,

- **... it's sufficient to secure only the infrastructure**
- **... their applications are secure, because they use based on standards**
- **...the data within their applications is not interesting enough for attackers**

Sources of application security breaches

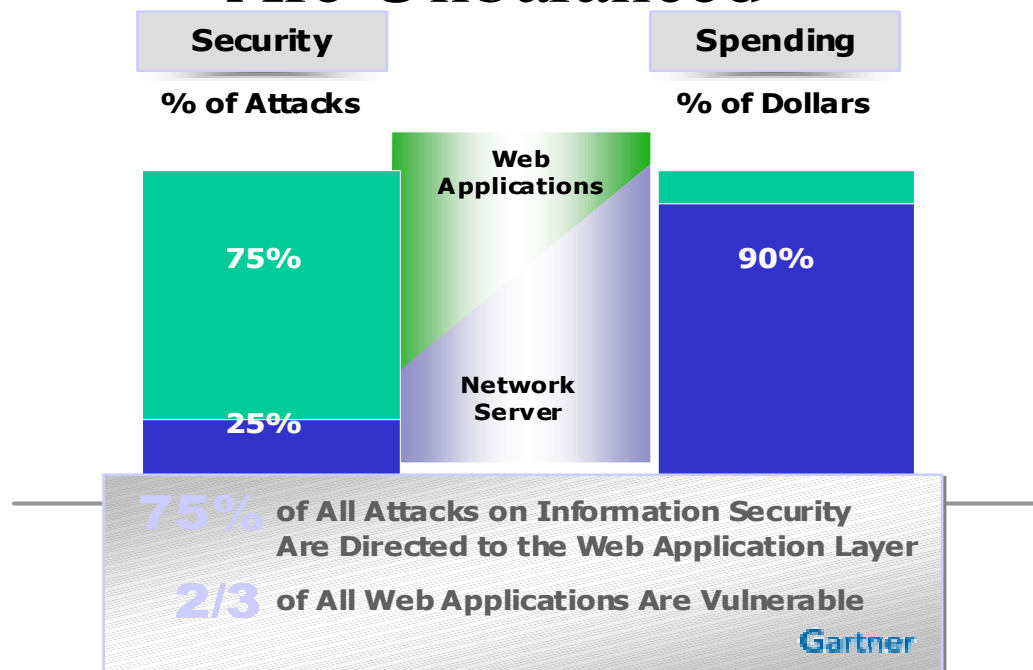
- **Vulnerable forms (bad programming)**
 - Missing input validation
- **Missing user awareness (for example phishing attacks)**
- **Bad architecture / design of web applications**
- **Misconfiguration of infrastructure**
- ...

Warum ist Applikations Sicherheit wichtig?

- **Web applications are the #1 focus of hackers:**
 - 75% of attacks at Application layer (Gartner)
 - XSS and SQL Injection are #1 and #2 reported vulnerabilities (Mitre)
- **Most sites are vulnerable:**
 - 90% of sites are vulnerable to application attacks (Watchfire)
 - 78% percent of easily exploitable vulnerabilities affected Web applications (Symantec)
 - 80% of organizations will experience an application security incident by 2010 (Gartner)
- **Web applications are high value targets for hackers:**
 - Customer data, credit cards, ID theft, fraud, site defacement, etc
- **Compliance requirements:**
 - Payment Card Industry (PCI) Standards, GLBA, HIPPA, FISMA,

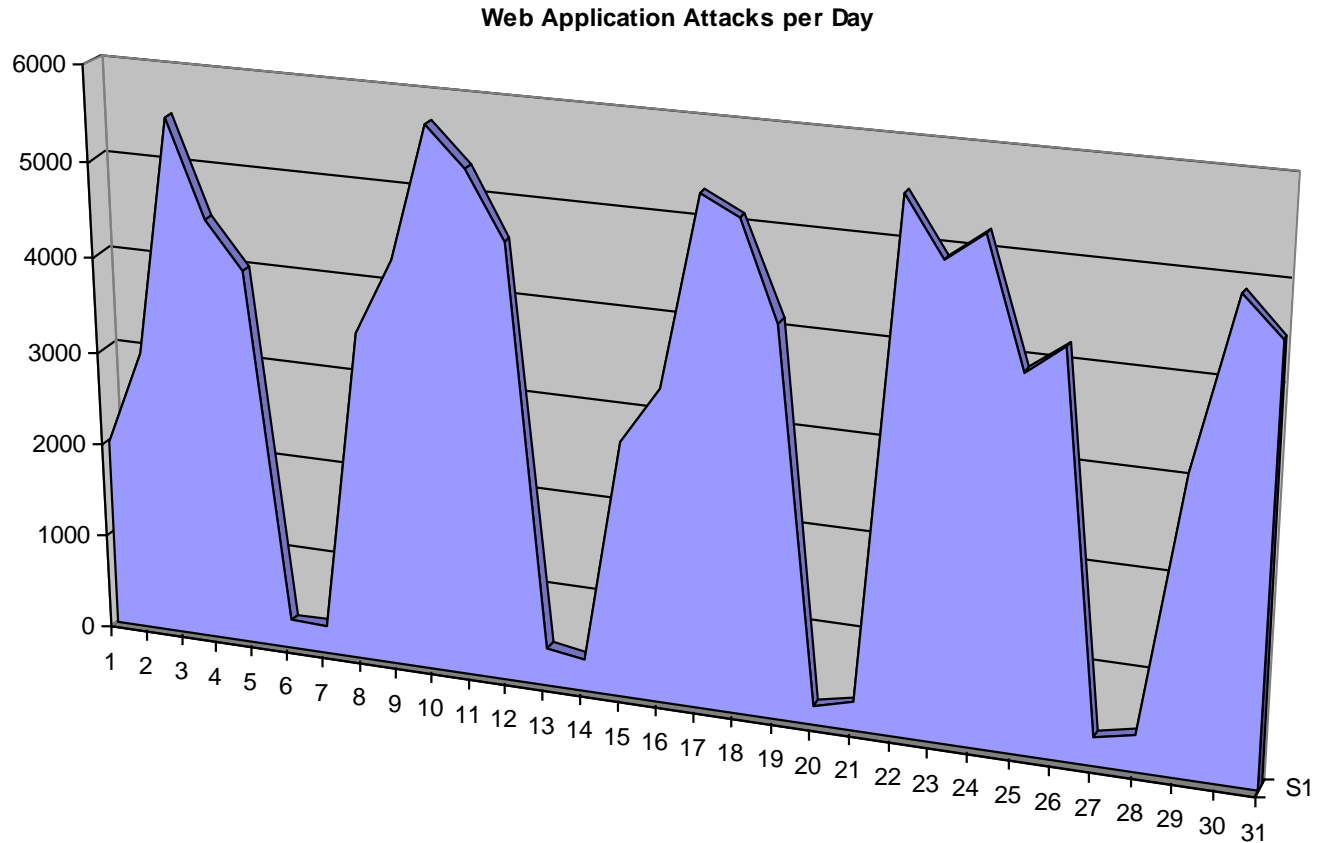
Die Realität

The Reality: Security and Spending Are Unbalanced



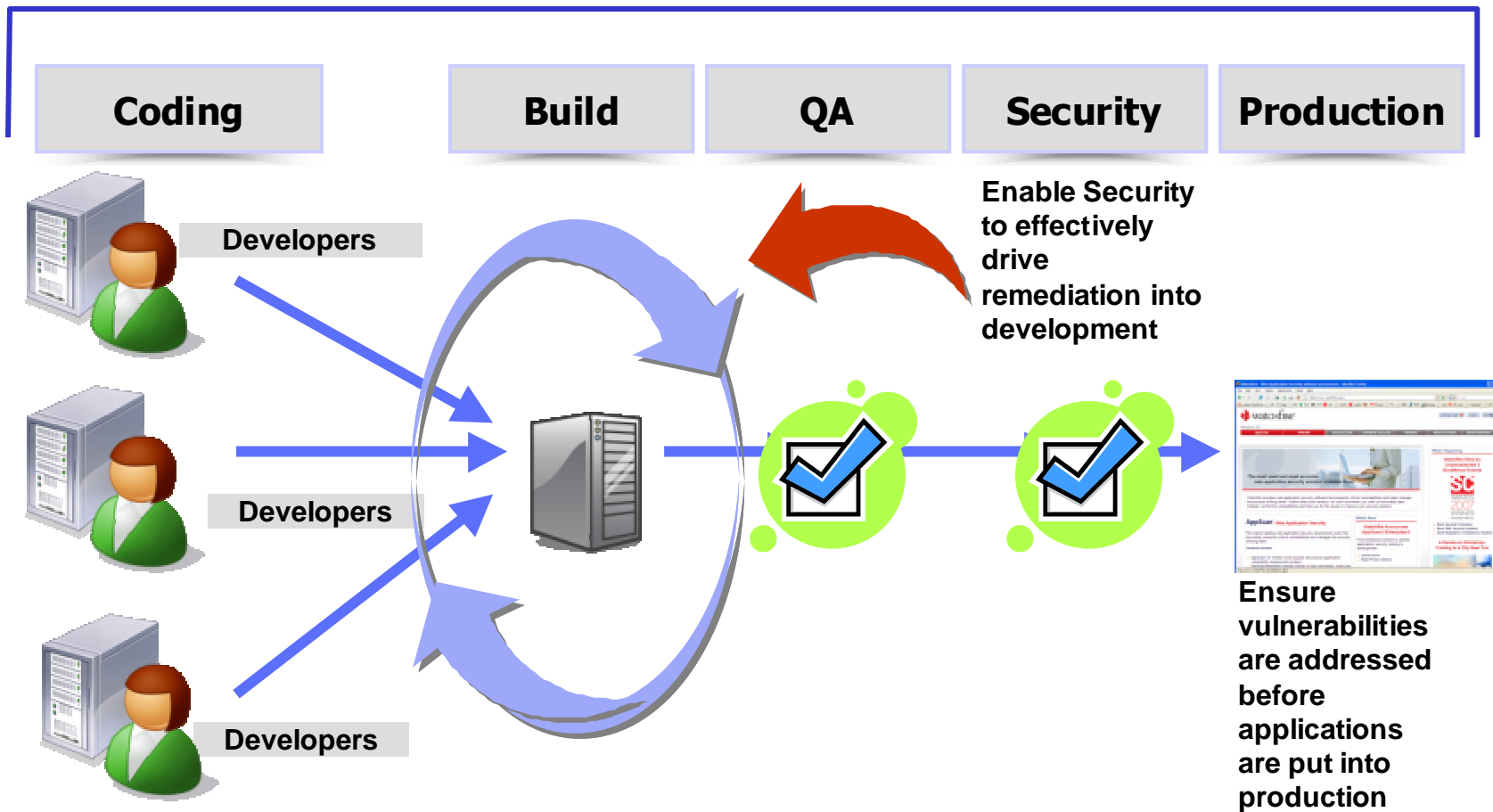
Sources: Gartner, Watchfire

Some more statistics



More than 5000 web application attacks on some days!

Building Security & Compliance into the SDLC



Appscan Highlights

- **Reporting (Developer Reports, Compliance Reports, Delta Analysis, User Defined Reports)**
- **Detailed Remediation Information including code examples**
- **Extendable (User Defined Tests, Complete SDK)**
- **Scriptable (can run from the commandline)**
- **Privilege Escalation Testing (can user A access data of user B)**
- **Can act as proxy server (useful if dedicated clients are used)**
- **Working with the results (for example deleting false positives originating from customized error pages)**
- **Scan Expert (introduced in Version 7.7) helps to determine the right scan configuration**

Beispiel eines Reports



Beis

AppScan 7.5 Demo Scan 1.scan - Watchfire AppScan

File Edit View Scan Tools Help

Scan Stop Manual Explore Scan Configuration Scan Log Report Update

View

- Security Issues
- Remediation Tasks
- Application Data

My Application (53)

- http://demo.testfire.net/ (53)
 - / (3)
 - cgi.exe (1)
 - comment.aspx (2)
 - default.aspx
 - disclaimer.htm
 - feedback.aspx (1)
 - search.aspx (1)
 - servererror.aspx
 - subscribe.aspx (3)
 - subscribe.swf
 - survey_questions.aspx
 - admin (1)
 - bank (40)
 - images (1)

Scan is Incomplete [More Information](#)

Arranged By: Severity Highest on top

53 Security Issues (368 variants) for 'My Application'

- Blind SQL Injection (4)
 - http://demo.testfire.net/bank/account.aspx (1)
 - http://demo.testfire.net/bank/login.aspx (2)
 - http://demo.testfire.net/bank/transaction.aspx (1)
- Cross-Site Scripting (5)
- Format String Remote Command Execution (1)
- HTTP Response Splitting (1)
- SQL Injection (6)
- XPath Injection (1)
- Cookie Poisoning SQL Injection (1)

Advisory Fix Recommendation Request/Response

Blind SQL Injection

Fix Recommendation

General

There are several issues whose remediation lies in sanitizing user input. By verifying that user input does not contain hazardous characters, it is possible to prevent malicious users from causing your application to execute unintended operations, such as launch arbitrary SQL queries, embed Javascript code to be executed on the client side, run various operating system commands etc.

It is advised to filter out all the following characters:

- [1] | (pipe sign)
- [2] & (ampersand sign)
- [3] ; (semicolon sign)

Visited URLs 108/108 Completed Tests 14194/14194 53 Security Issues 18 4 22 9

Average deal size

| | |
|-------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| IBM Rational AppScan – Standard D61SYLL | € 33,000 floating user license Plug-in can push to ClearQuest or HP Quality Center |
| IBM Rational AppScan – Enterprise D61UYLL | €175,000 up to 5 users €225,000 up to 10 users Additional user price € 2000 Deployment services |
| Start with AppScan - Express No limited functionality D056FLL | € 18,000 authorized user license the size of the deal is related to the impact and in SMB/GB the Website can be highly business critical |



SWG Partner Academy

Kontakt Daten:

Michael Bleichert
Rational Channel Manager Germany
Tel: 0172-8377104
Email: michael.bleichert@de.ibm.com

Vielen Dank für Ihre Aufmerksamkeit!