Session 9 : Rational

Nicolas Berney
Rational Account Manager

Smart Decisions for
a Smarter Planet

LEARN NEW IDEAS TO STAY AHEAD
OF THE MARKET!

Scanner automatiquement les vulnérabilités des applications Web et du code source avec **Rational AppScan**

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

1 IBM Software Solutions Day

vous faire connaître les dernières évolutions de l’offre software

650 Collaborateurs IBM pour vous aidez en Suisse Romande

5 Familles de produits: Tivoli, WebSphere et Rational pour la fondation d’architecture services « SOA», Information Management pour la gestion des données et finalement Lotus pour la collaboration.

Smart Decisions for
a Smarter Planet

LEARN NEW IDEAS TO STAY AHEAD
OF THE MARKET!

IBM®

Agenda

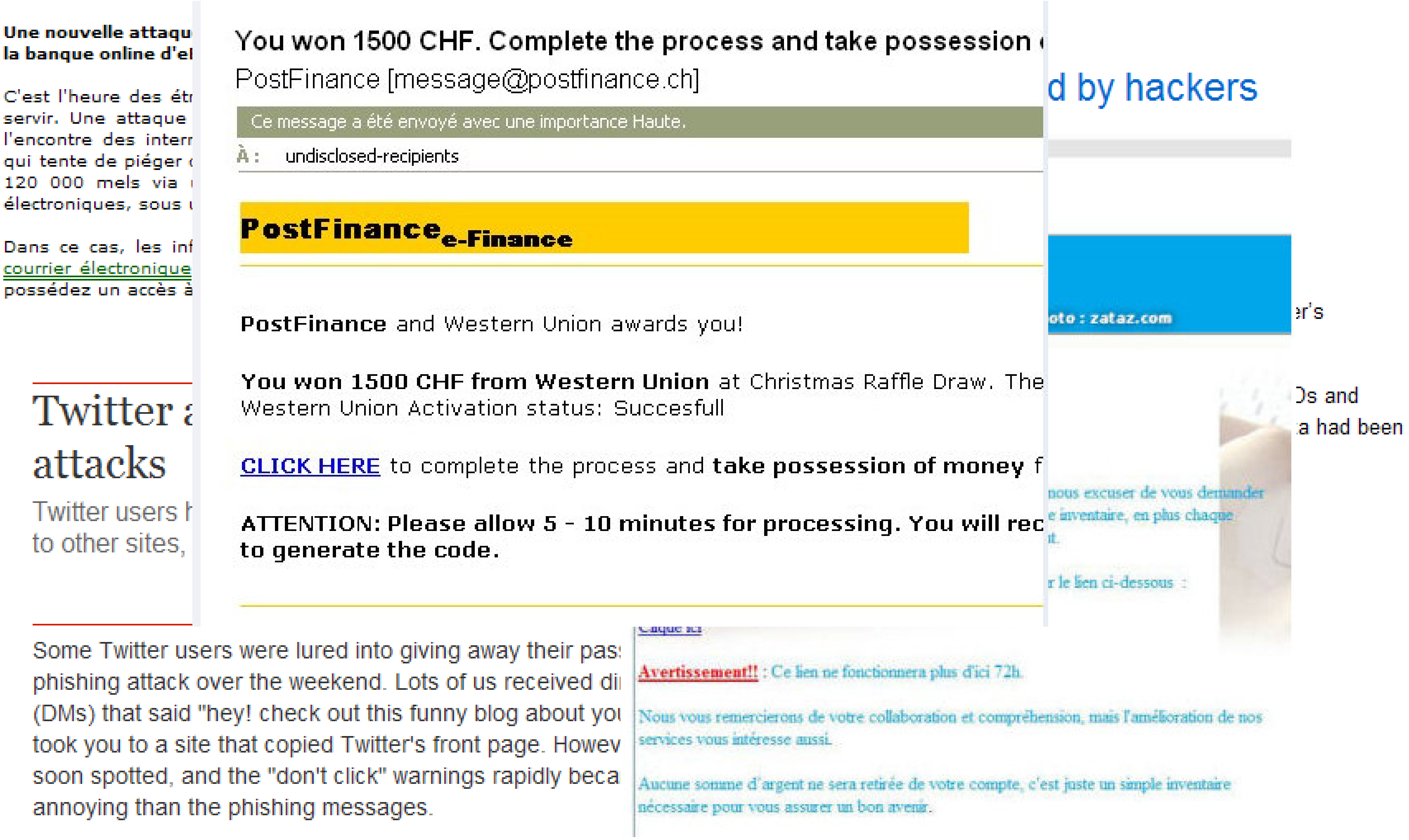
- **Should we worry about our application security?**

- **Security maturity**

- **Automatic Security Scanning**
  Rational AppScan → Demo

- **Resources**

Do we get attacked?



Une nouvelle attaqu
la banque online d'el

C'est l'heure des étr
servir. Une attaque
l'encontre des interr
qui tente de piéger
120 000 mels via
électroniques, sous

Dans ce cas, les inf
courrier électronique
possédez un accès à

Twitter a
attacks

Twitter users h
to other sites,

Some Twitter users were lured into giving away their pas
phishing attack over the weekend. Lots of us received di
(DMs) that said "hey! check out this funny blog about you
took you to a site that copied Twitter's front page. Howev
soon spotted, and the "don't click" warnings rapidly beca
annoying than the phishing messages.

You won 1500 CHF. Complete the process and take possession

PostFinance [message@postfinance.ch]

Ce message a été envoyé avec une importance Haute.

À : undisclosed-recipients

PostFinance e-Finance

PostFinance and Western Union awards you!

You won 1500 CHF from Western Union at Christmas Raffle Draw. The
Western Union Activation status: Succesfull

CLICK HERE to complete the process and **take possession of money** f

**ATTENTION: Please allow 5 - 10 minutes for processing. You will rec
to generate the code.**

d by hackers

oto : zataz.com

er's

Ds and
a had been

nous excuser de vous demander
e inventaire, en plus chaque
t.

r le lien ci-dessous :

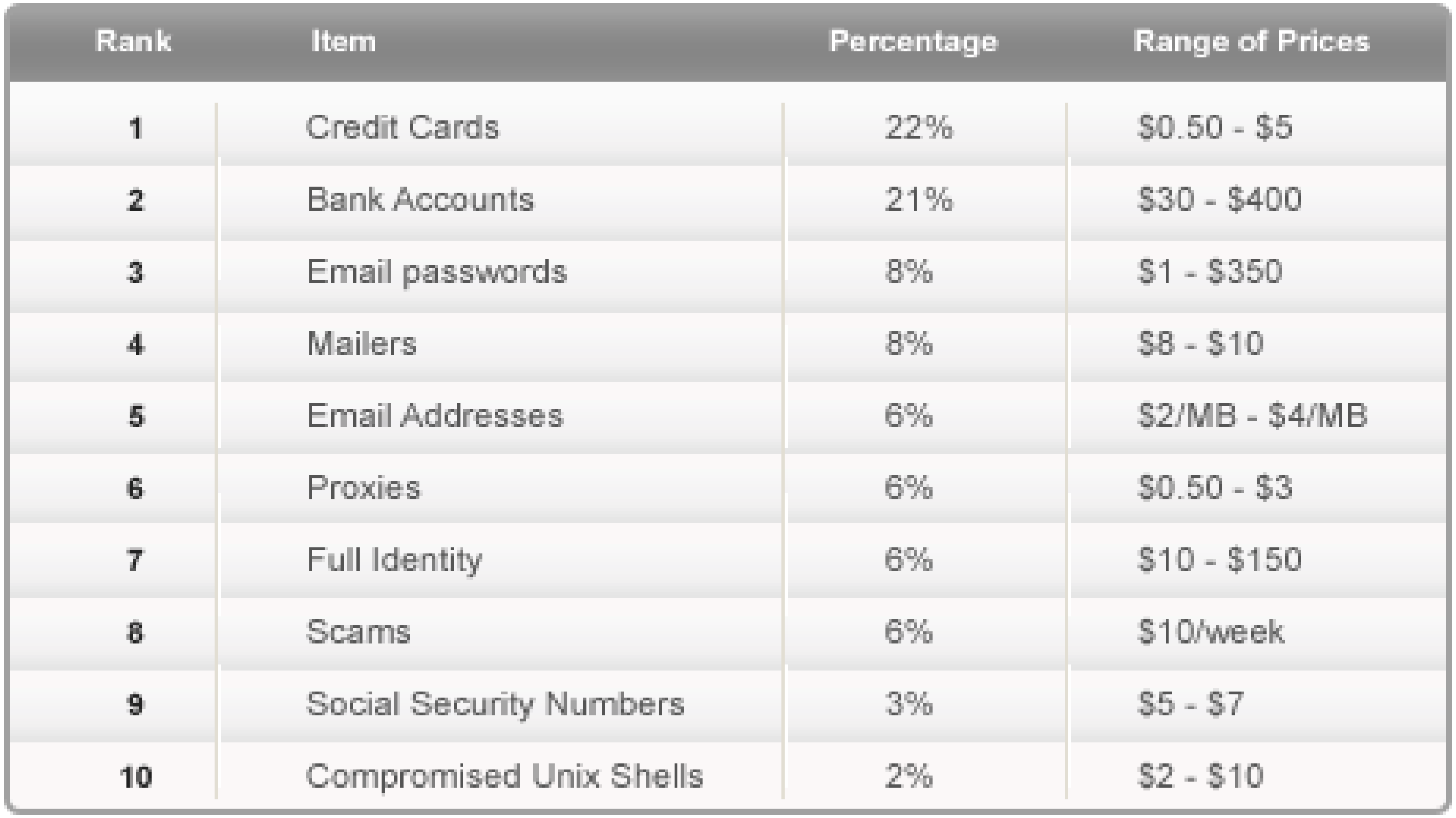
Cliquez ici

Avertissement!! : Ce lien ne fonctionnera plus d'ici 72h.

Nous vous remercierons de votre collaboration et compréhension, mais l'amélioration de nos services vous intéresse aussi.

Aucune somme d'argent ne sera retirée de votre compte, c'est juste un simple inventaire nécessaire pour vous assurer un bon avenir.

Breakdown of goods available for sale on underground economy servers



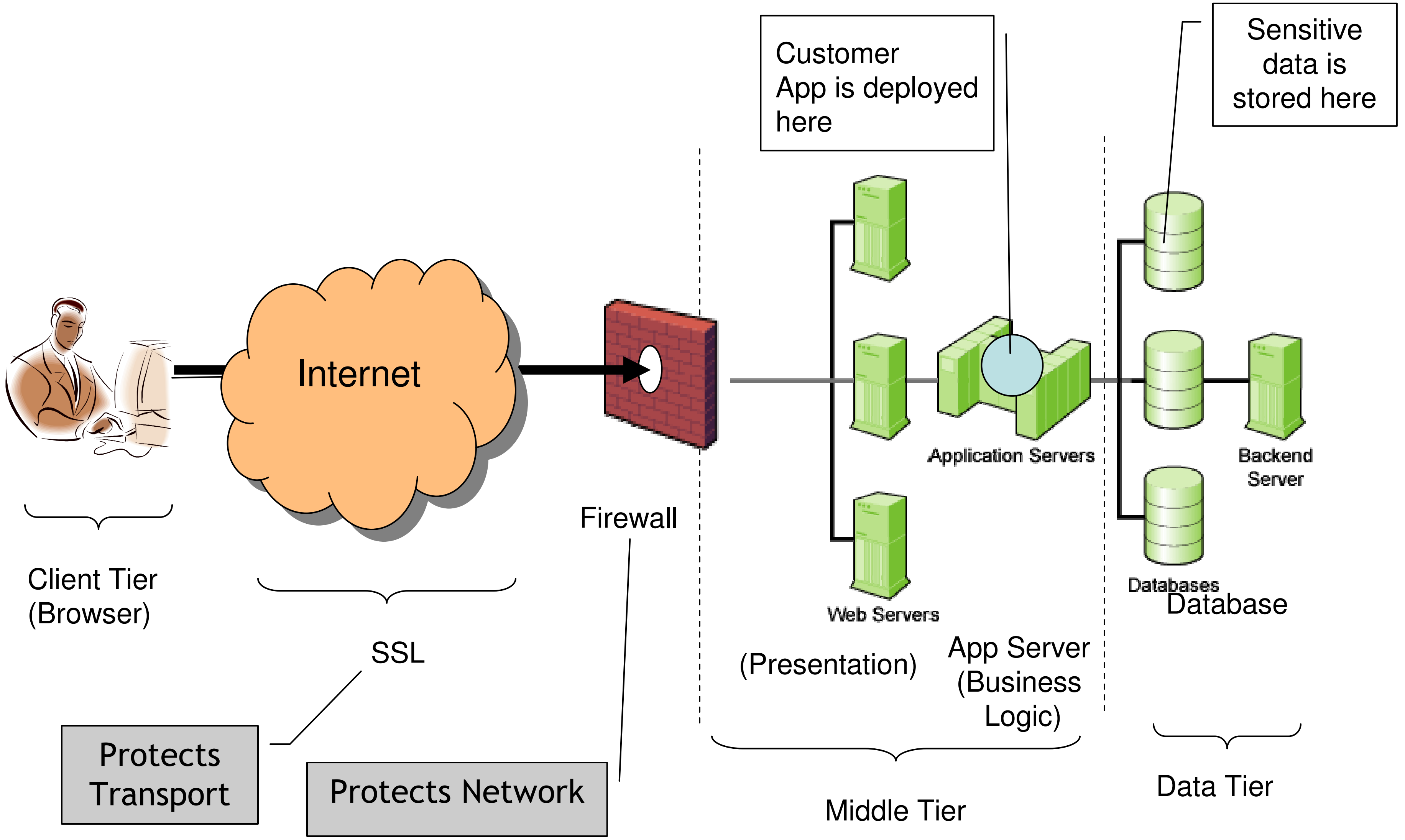
Rank	Item	Percentage	Range of Prices
1	Credit Cards	22%	$0.50 - $5
2	Bank Accounts	21%	$30 - $400
3	Email passwords	8%	$1 - $350
4	Mailers	8%	$8 - $10
5	Email Addresses	6%	$2/MB - $4/MB
6	Proxies	6%	$0.50 - $3
7	Full Identity	6%	$10 - $150
8	Scams	6%	$10/week
9	Social Security Numbers	3%	$5 - $7
10	Compromised Unix Shells	2%	$2 - $10

Source: Symantec Corporation – Internet Security Threat Report Volume XII

Top 10 list - Open Web Application Security Project

Application Threat	Negative Impact	Example Impact
Cross Site scripting	Identity Theft, Sensitive Information Leakage, …	Hackers can impersonate legitimate users, and control their accounts.
Injection Flaws	Attacker can manipulate queries to the DB / LDAP / Other system	Hackers can access backend database information, alter it or steal it.

High Level Web Application Architecture Review



Customer App is deployed here

Sensitive data is stored here

Internet

Firewall

Client Tier (Browser)

SSL

Protects Transport

Protects Network

(Presentation)

App Server (Business Logic)

Database

Middle Tier

Data Tier

Agenda

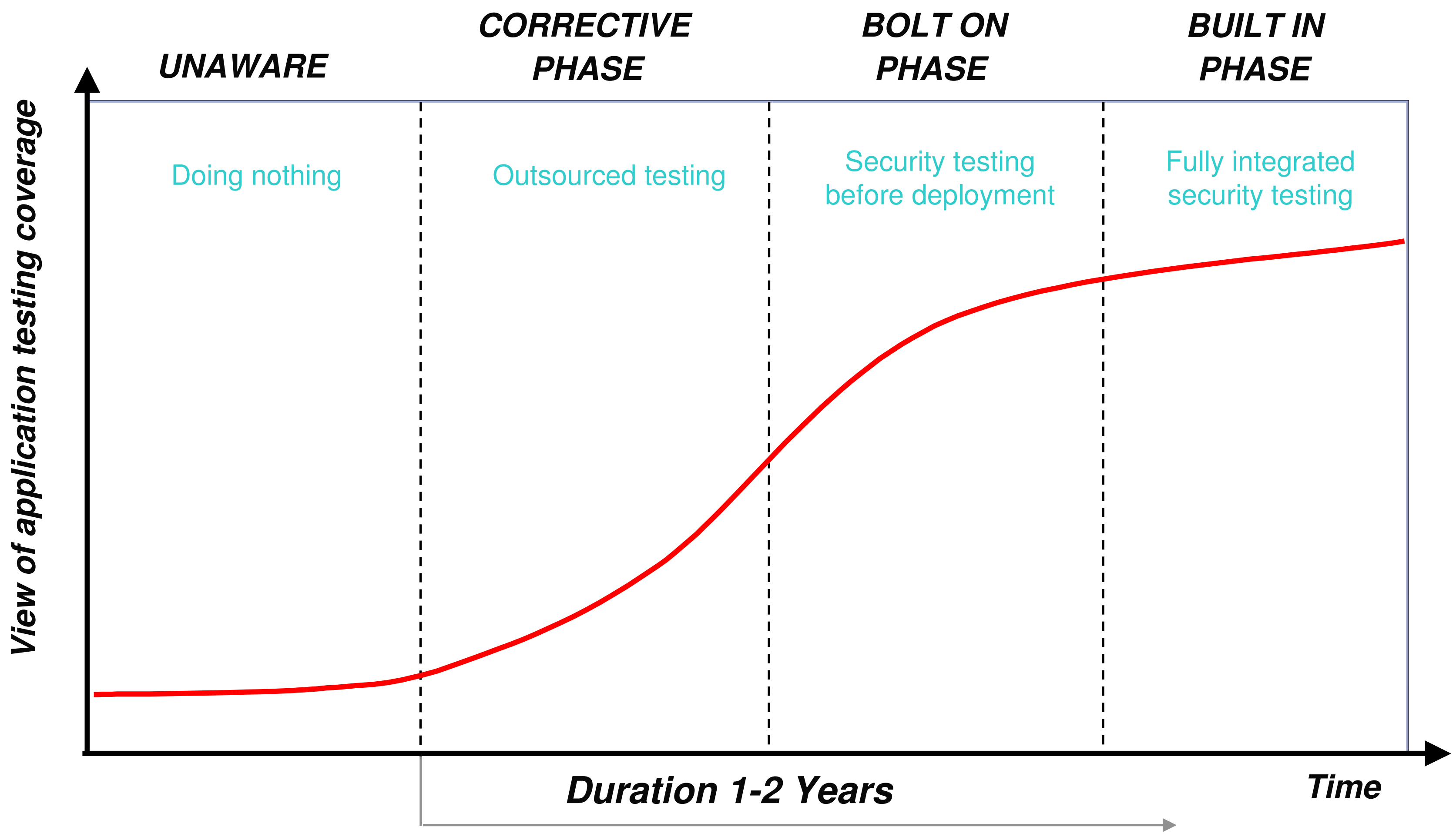
- **Should we worry about our application security?**

- **Security maturity**

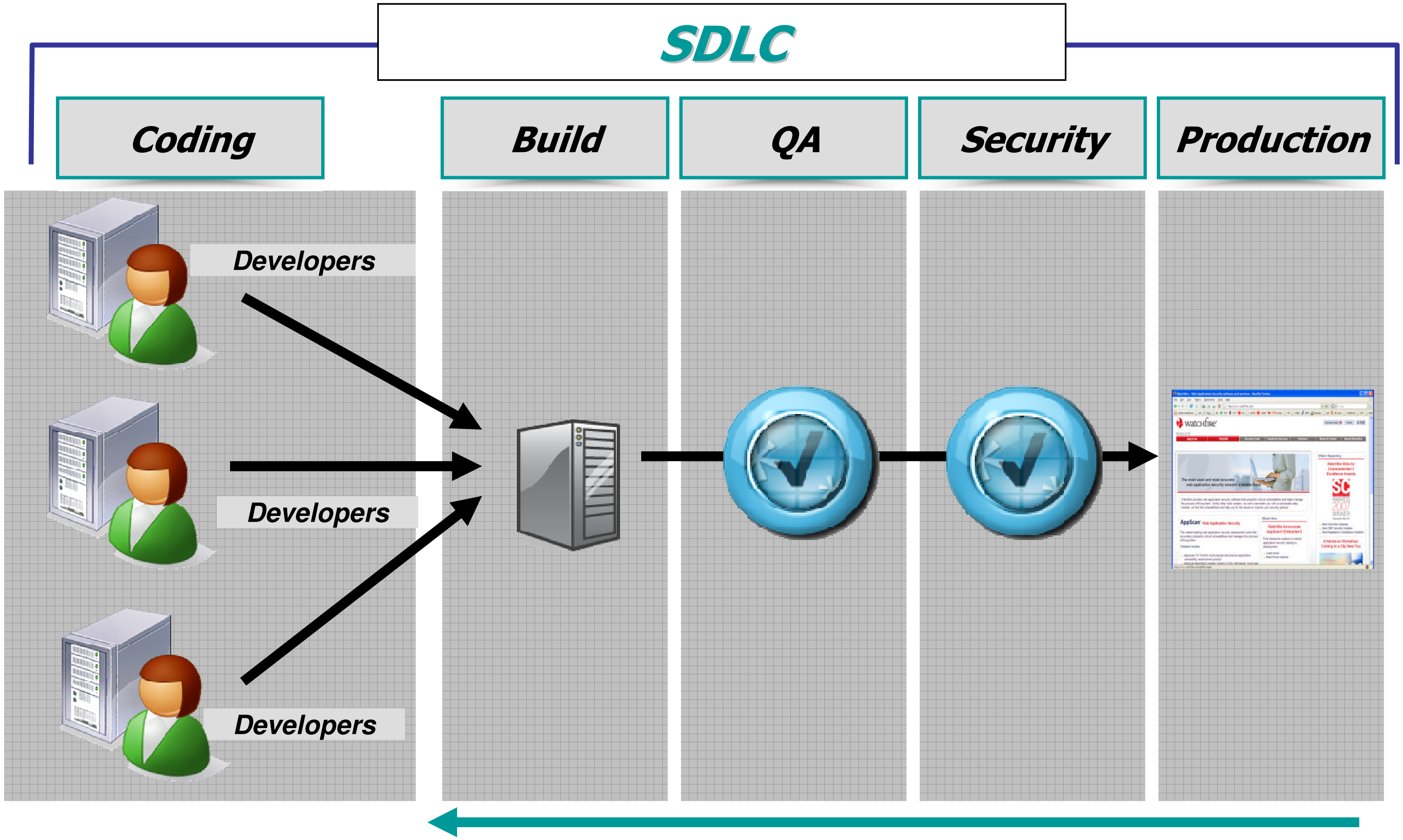
- **Automatic Security Scanning**
  Rational AppScan → Demo

- **Resources**

Application Security Maturity Model



Security Testing Within the Software Lifecycle



SDLC

Coding

Build

QA

Security

Production

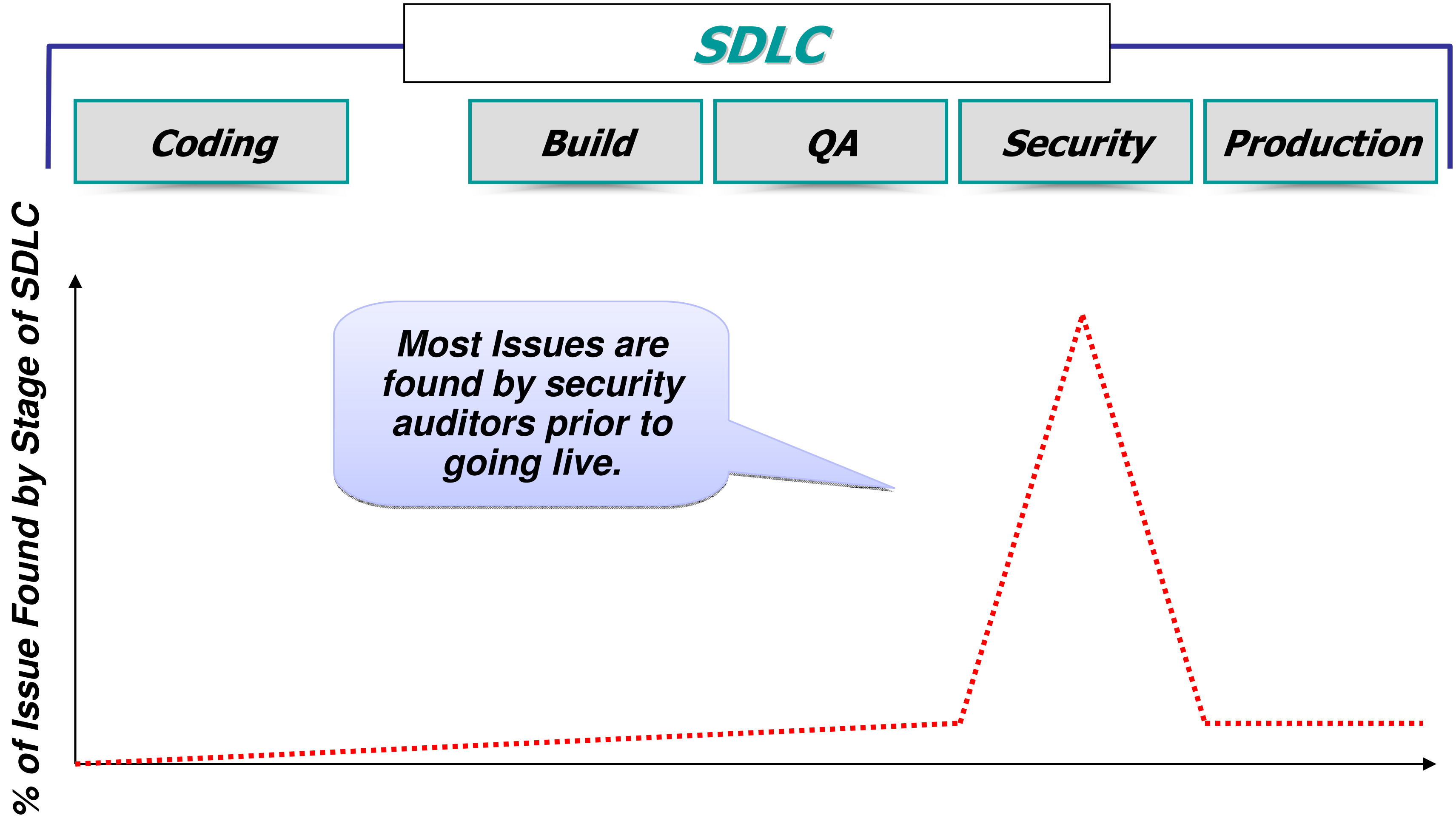
Developers

Developers

Developers

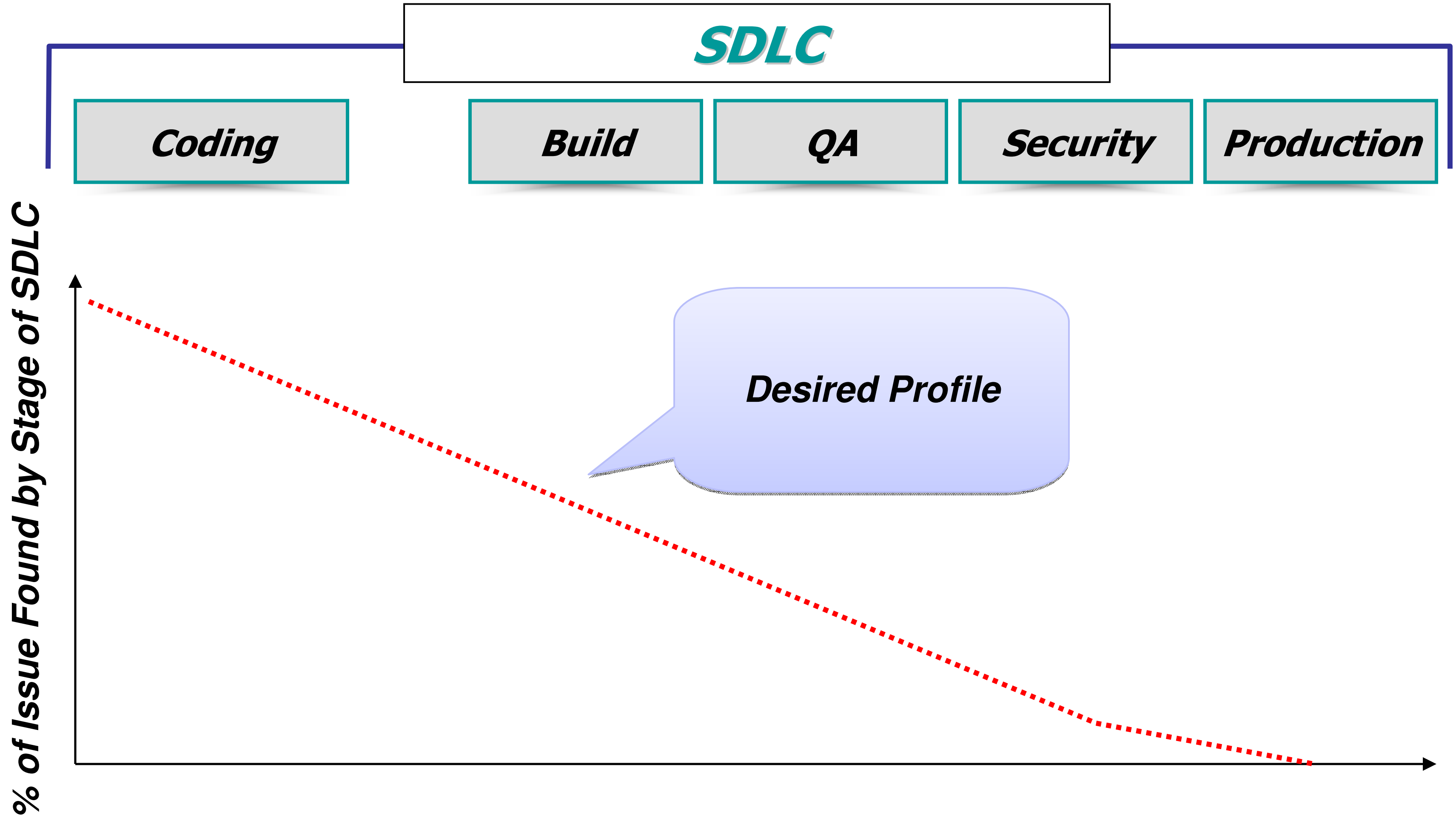
Application Security Testing Maturity

Security Testing Within the Software Lifecycle



Most Issues are found by security auditors prior to going live.

Security Testing Within the Software Lifecycle



Agenda

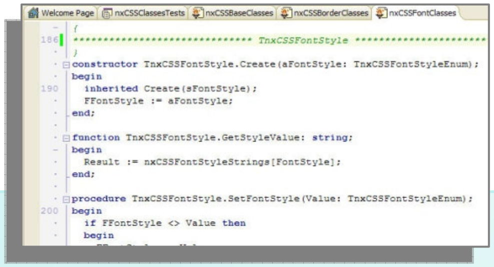
- **Should we worry about our application security?**
- **Security maturity**
- **Automatic Security Scanning**
  Rational AppScan → Demo
- **Resources**

Security Testing Technologies...

Combination Delivers a Comprehensive Solution

Static Code Analysis = Whitebox

Scanning source code for security issues



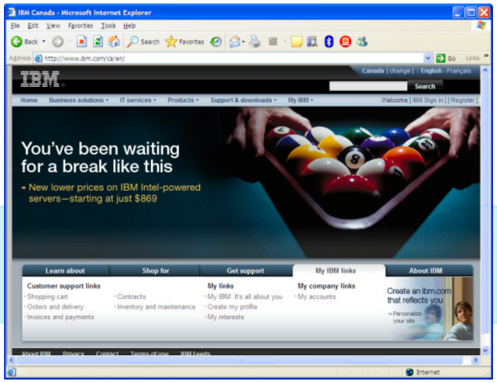
```
{
****************************** TnxCSSFontStyle **********************
}
constructor TnxCSSFontStyle.Create(aFontStyle: TnxCSSFontStyleEnum);
begin
  inherited Create(sFontStyle);
  FFontStyle := aFontStyle;
end;

function TnxCSSFontStyle.GetStyleValue: string;
begin
  Result := nxCSSFontStyleStrings[FontStyle];
end;

procedure TnxCSSFontStyle.SetFontStyle(Value: TnxCSSFontStyleEnum);
begin
  if FFontStyle <> Value then
  begin
```

Dynamic Analysis = Blackbox

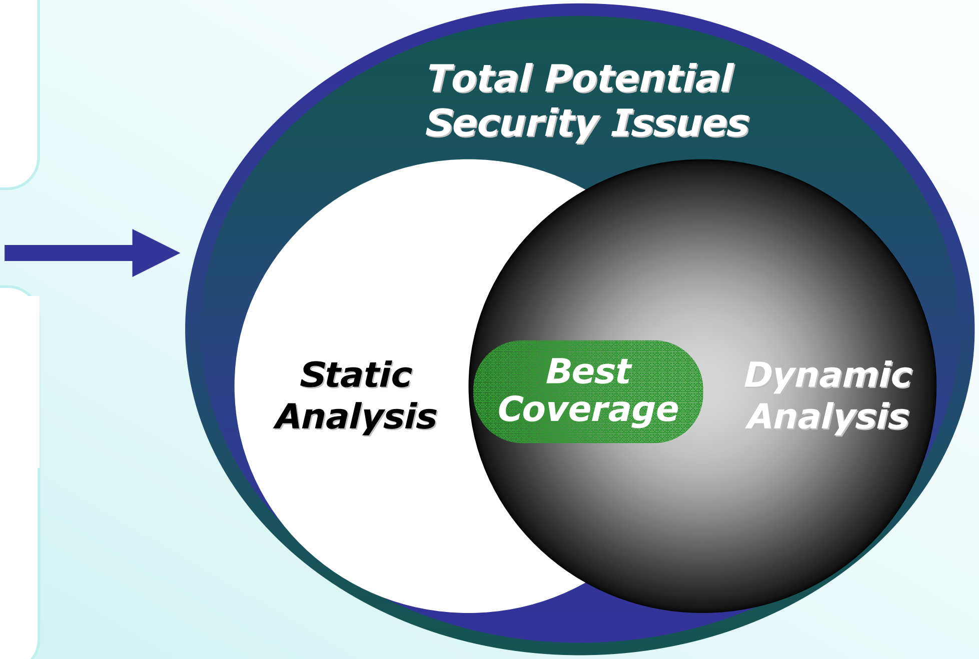
Performing security analysis of a compiled application



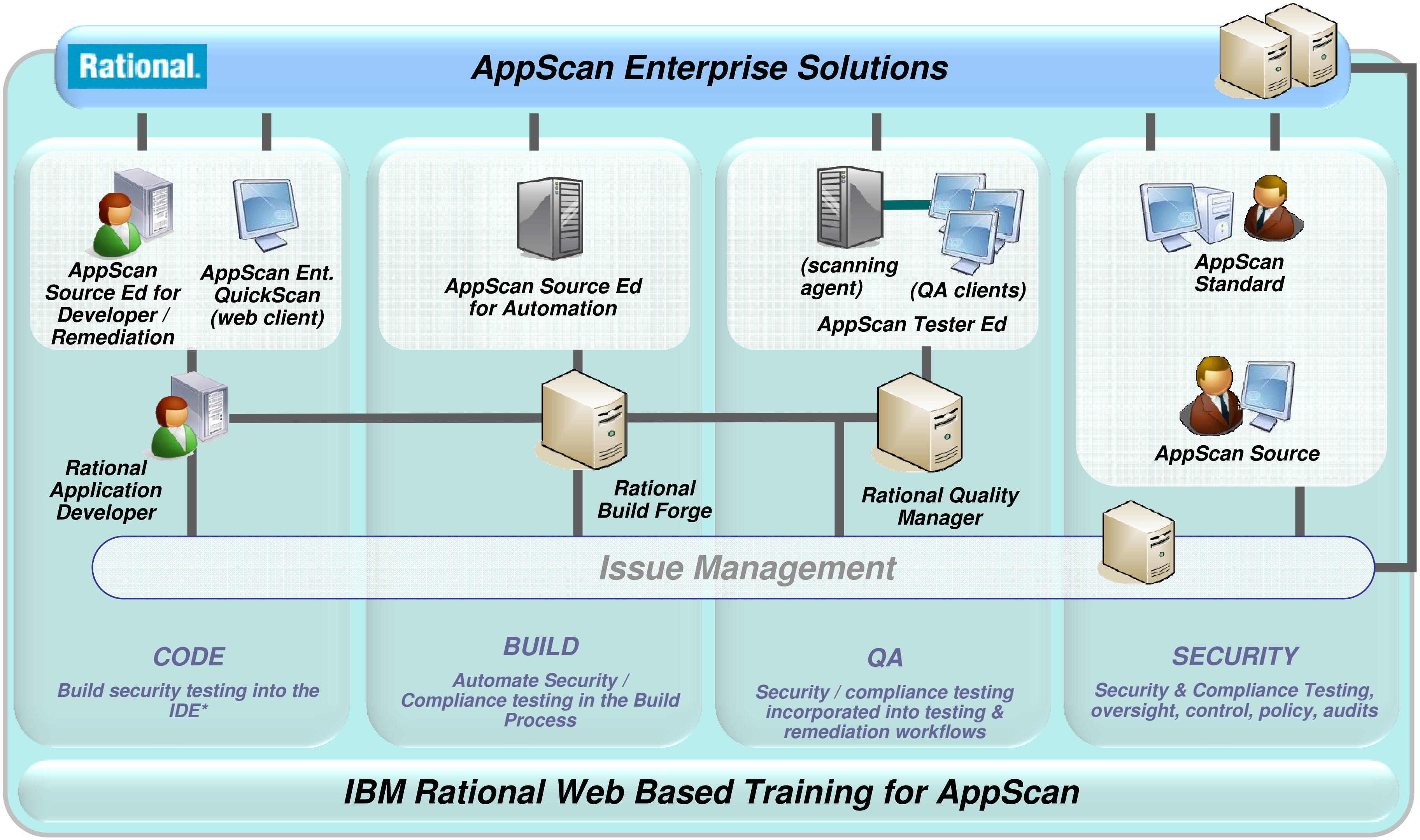
You've been waiting for a break like this

→ New lower prices on IBM Intel-powered servers—starting at just $869

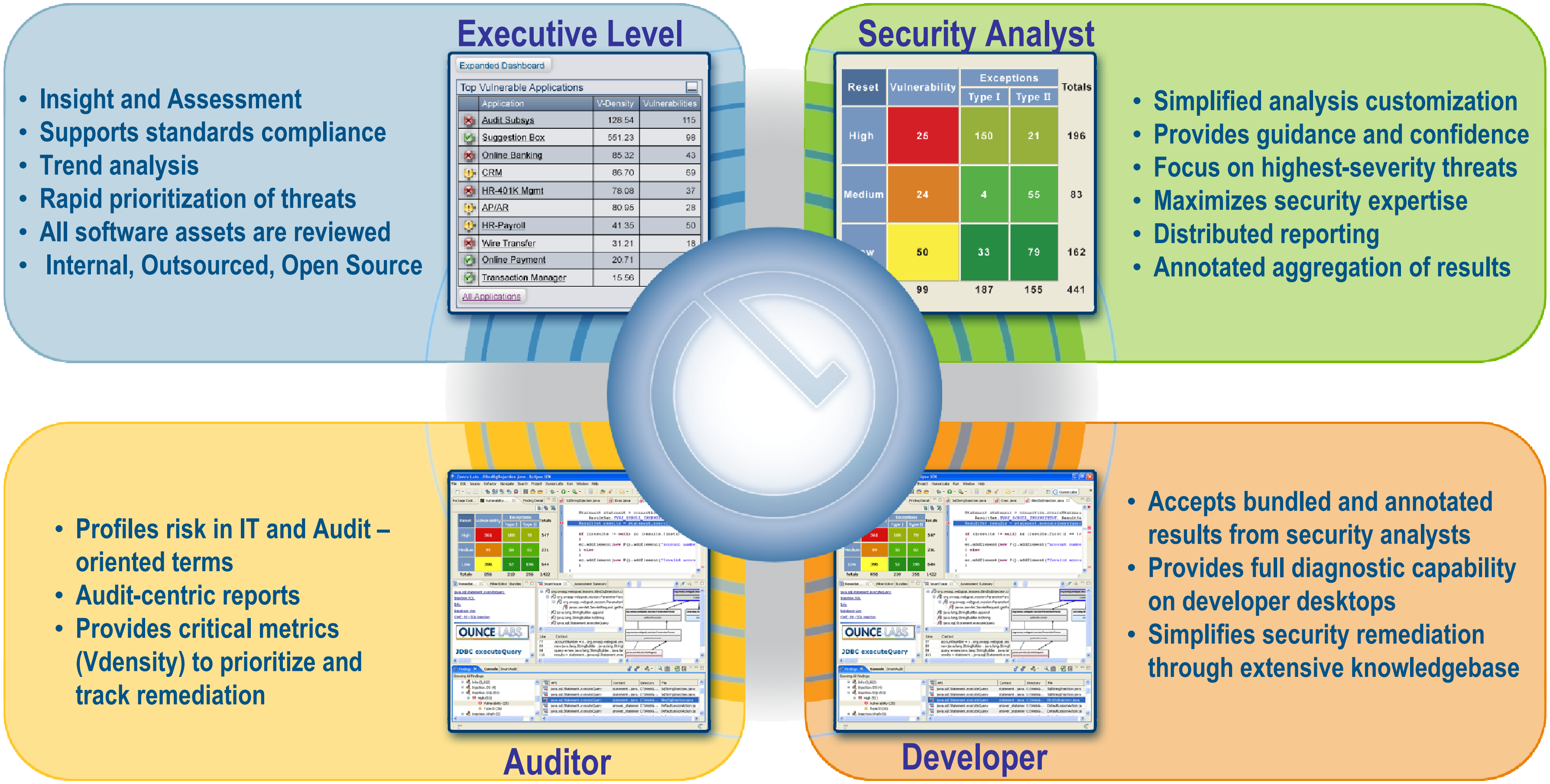
Create an ibm.com that reflects you



IBM Rational AppScan Ecosystem


Rational
AppScan Enterprise Solutions
AppScan Source Ed for Developer / Remediation
AppScan Ent. QuickScan (web client)
AppScan Source Ed for Automation
(scanning agent)
(QA clients)
AppScan Tester Ed
AppScan Standard
AppScan Source
Rational Application Developer
Rational Build Forge
Rational Quality Manager
Issue Management
CODE
Build security testing into the IDE*
BUILD
Automate Security / Compliance testing in the Build Process
QA
Security / compliance testing incorporated into testing & remediation workflows
SECURITY
Security & Compliance Testing, oversight, control, policy, audits
IBM Rational Web Based Training for AppScan

Whitebox: AppScan Source



Executive Level

- Insight and Assessment
- Supports standards compliance
- Trend analysis
- Rapid prioritization of threats
- All software assets are reviewed
- Internal, Outsourced, Open Source

Expanded Dashboard

Top Vulnerable Applications

	Application	V-Density	Vulnerabilities
✗	Audit Subsys	128.54	115
✓	Suggestion Box	551.23	98
✗	Online Banking	85.32	43
!	CRM	86.70	69
✗	HR-401K Mgmt	78.08	37
!	AP/AR	80.95	28
!	HR-Payroll	41.35	50
✗	Wire Transfer	31.21	18
✓	Online Payment	20.71	
✓	Transaction Manager	15.56	

All Applications

Security Analyst

Reset	Vulnerability	Exceptions		Totals
		Type I	Type II	
High	25	150	21	196
Medium	24	4	55	83
ow	50	33	79	162
	99	187	155	441

- Simplified analysis customization
- Provides guidance and confidence
- Focus on highest-severity threats
- Maximizes security expertise
- Distributed reporting
- Annotated aggregation of results

Auditor

- Profiles risk in IT and Audit – oriented terms
- Audit-centric reports
- Provides critical metrics (Vdensity) to prioritize and track remediation

Developer

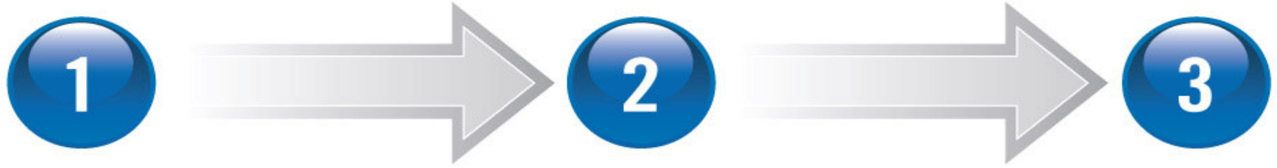
- Accepts bundled and annotated results from security analysts
- Provides full diagnostic capability on developer desktops
- Simplifies security remediation through extensive knowledgebase

Supported technology: Java, JSP, C, C++, C#, ASP.NET, VB .NET, VB 6, Perl and PHP

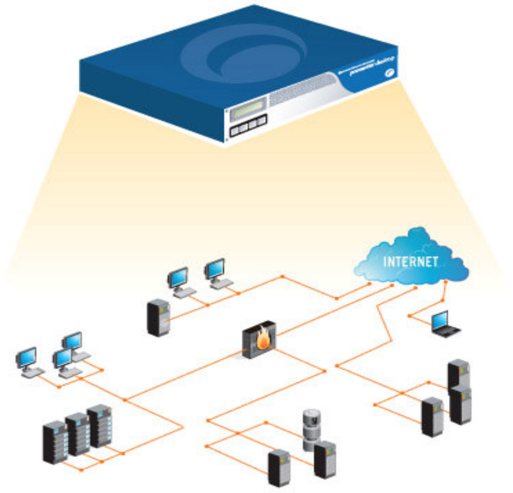
Copyright © 2009 Ounce Labs, Inc. All rights reserved.

Whitebox: How does Rational AppScan work?

Automates Application Security Testing

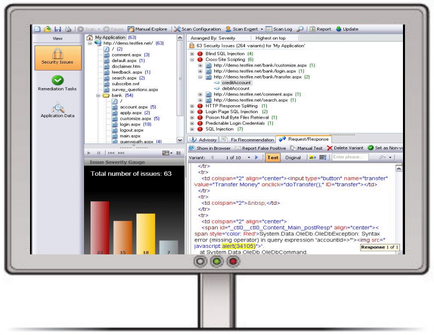


Scan applications



Analyze

(identify issues)



My Application (63)
http://demo.testfire.net/ (63)
/ (2)
comment.aspx (3)
default.aspx (1)
disclaimer.htm
feedback.aspx (1)
search.aspx (2)
subscribe.swf
survey_questions.aspx
bank (54)
/
account.aspx (5)
apply.aspx (2)
customize.aspx (5)
login.aspx (18)
logout.aspx
main.aspx
queryxpath.aspx (4)

Total number of issues: 63

Arranged By: Severity | Highest on top

63 Security Issues (264 variants) for 'My Application'

Blind SQL Injection (4)
Cross-Site Scripting (6)
http://demo.testfire.net/bank/customize.aspx (1)
http://demo.testfire.net/bank/login.aspx (1)
http://demo.testfire.net/bank/transfer.aspx (2)
creditAccount
debitAccount
http://demo.testfire.net/comment.aspx (1)
http://demo.testfire.net/search.aspx (1)
HTTP Response Splitting (1)
Login Page SQL Injection (2)
Poison Null Byte Files Retrieval (1)
Predictable Login Credentials (1)
SQL Injection (7)

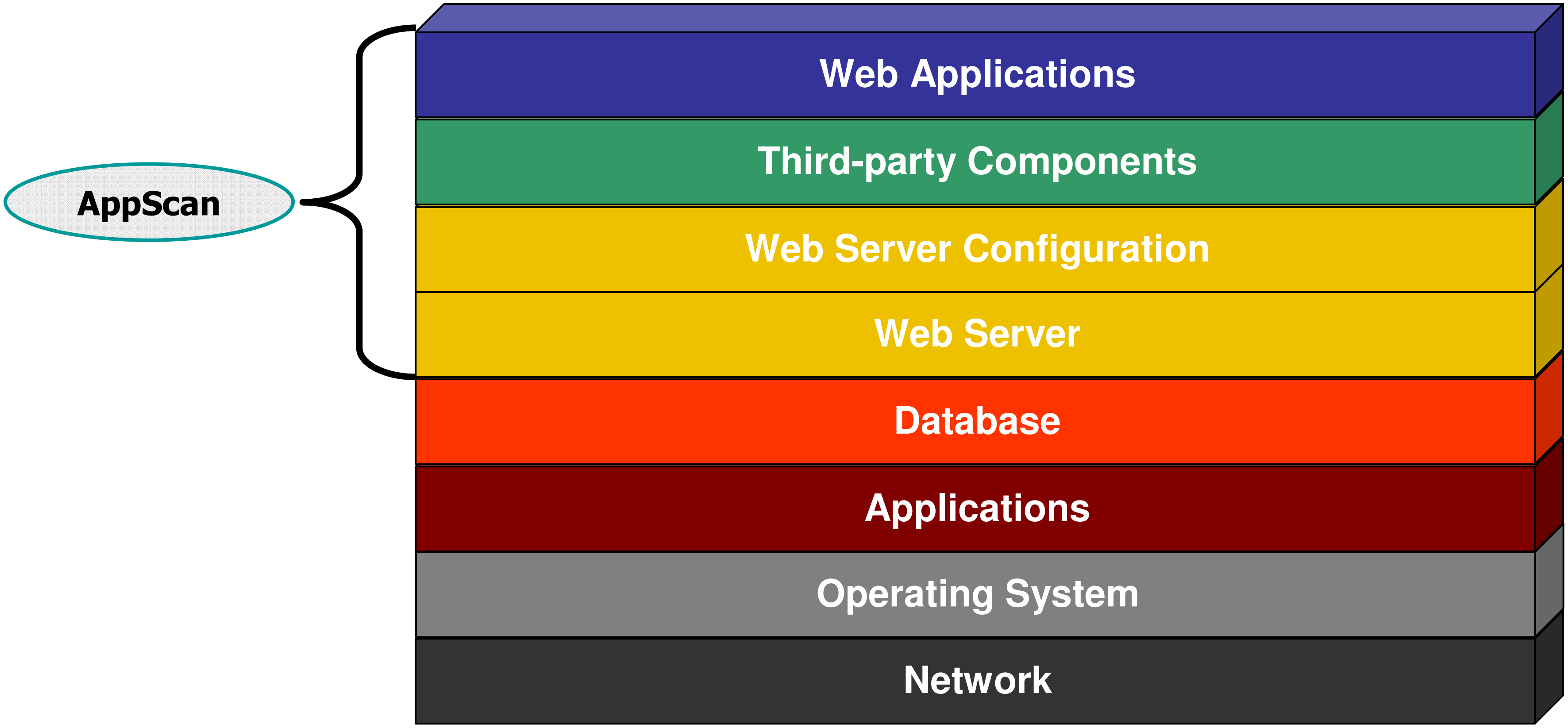
```
  </tr>
  <tr>
    <td colspan="2" align="center"><input type="button" name="transfer"
value="Transfer Money" onclick="doTransfer();" ID="transfer"></td>
  </tr>
  <tr>
    <td colspan="2">&nbsp;</td>
  </tr>
  <tr>
    <td colspan="2" align="center">
    <span id="_ctl0__ctl0_Content_Main_postResp" align="center"><
span style='color: Red'>System.Data.OleDb.OleDbException: Syntax
error (missing operator) in query expression 'accountid=>"'><img src="
javascript:alert(34105)">'.
   at System.Data.OleDb.OleDbCommand.
```

Virtual-SOC Portal

Report

(detailed & actionable)

Whitebox: What does AppScan test for?



Demo: **Rational AppScan**

Agenda

- **Should we worry about our application security?**
- **Security maturity**
- **Automatic Security Scanning**
  Rational AppScan → Demo
- **Resources**

Resources

- Develop secure applications with Rational AppScan
  - http://www-01.ibm.com/software/awdtools/appscan/
- Try AppScan for 30 days
  - http://www-01.ibm.com/software/awdtools/appscan/standard/
- Test web application
  - http://www.altoromutual.com/
- Open Web Application Security Project - Top 10 List
  - http://www.owasp.org/images/0/0f/OWASP_T10_-_2010_rc1.pdf

Conclusion

- Every one gets attacked!
- Security should be part of testing
- Whitebox: AppScan Source
- Blackbox: AppScan Standard