

Innovate2011

The Premier Software and Product Delivery Event

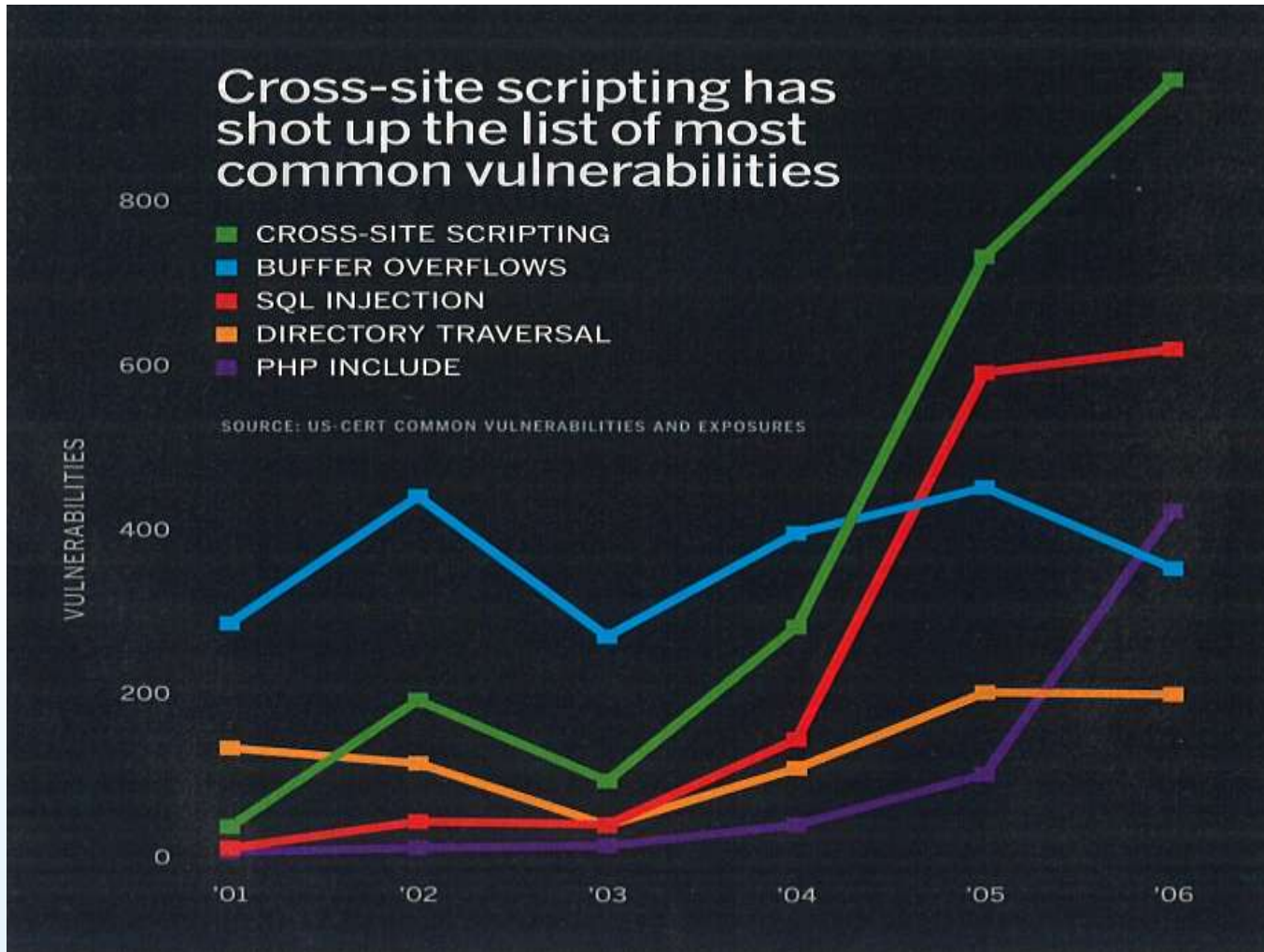


Asegurando sus Aplicaciones: Hackeo Ético

Miguel A. Dzay Lemus
Rational IT Specialist
IBM Software México, Rational



Los Hackers se están Enfocando en las Aplicaciones Web



Motivadores del Mercado

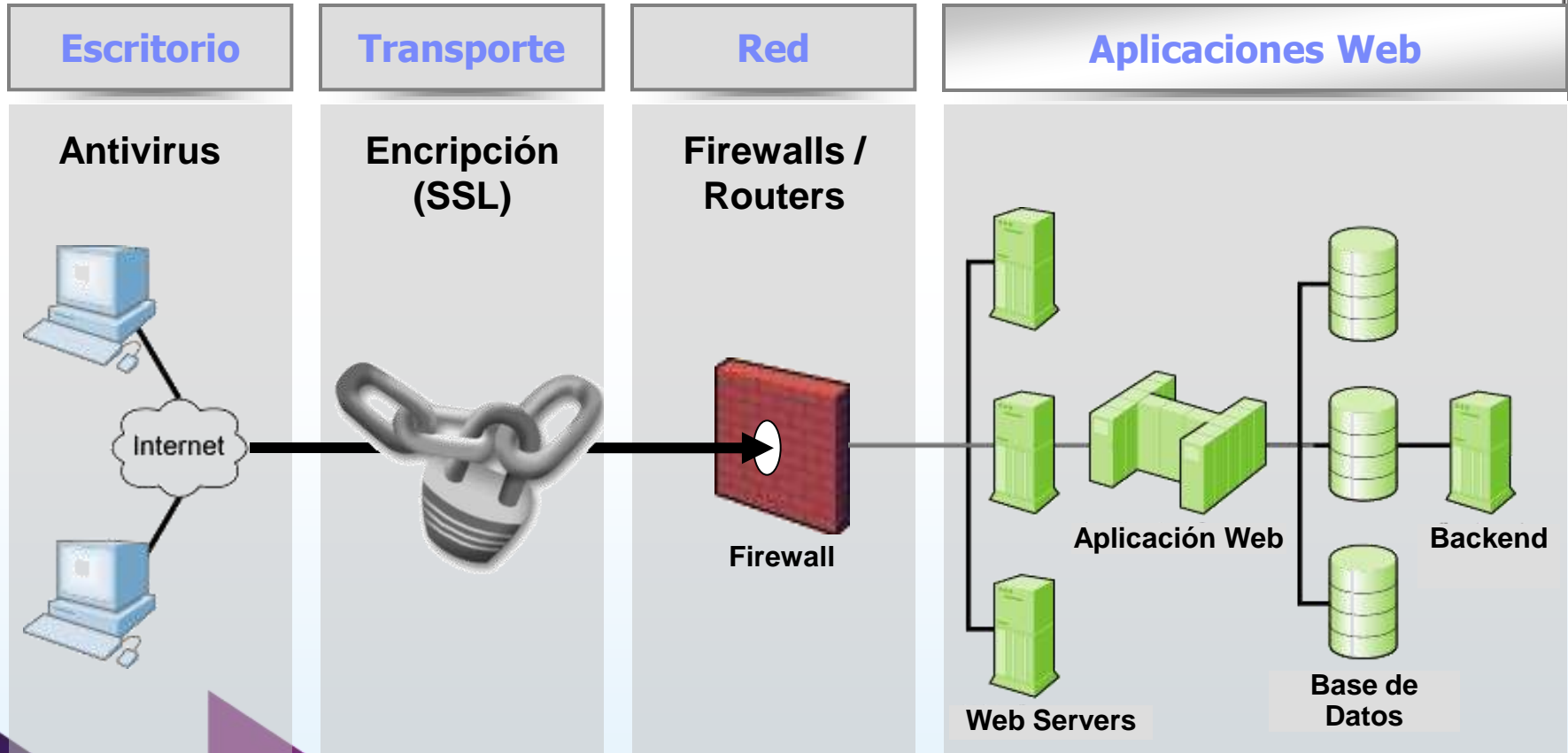
- **Cumplimiento de Regulaciones**
 - eCommerce: PCI-DSS, PA-DSS
 - Sarbanes Oxley
 - ISO 27001
 - ISO 27002
 - y más....



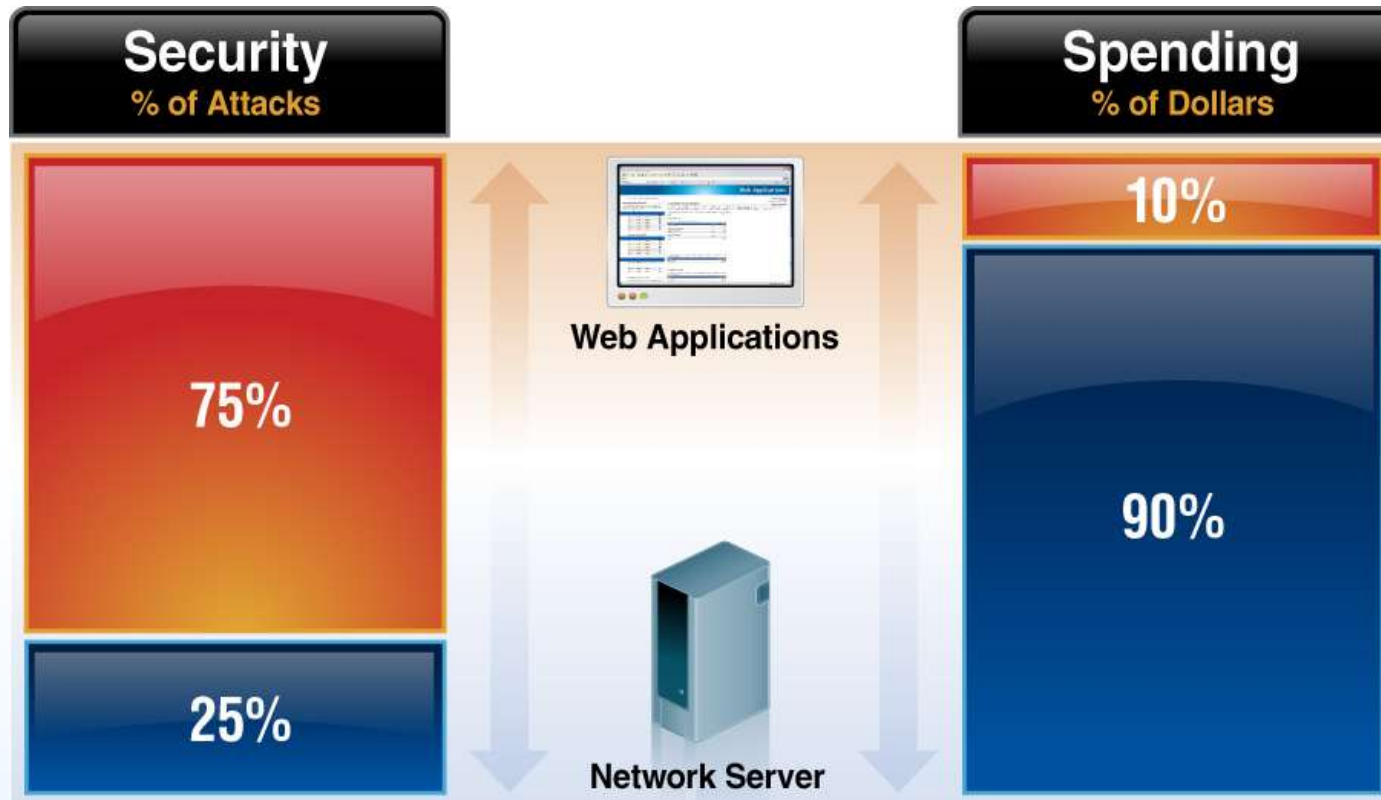
Hackers Break Into Playstation Network
2011



La Seguridad de Aplicaciones Requiere de un Acercamiento Diferente



La Realidad



75% De todos los ataques están dirigidos al Web

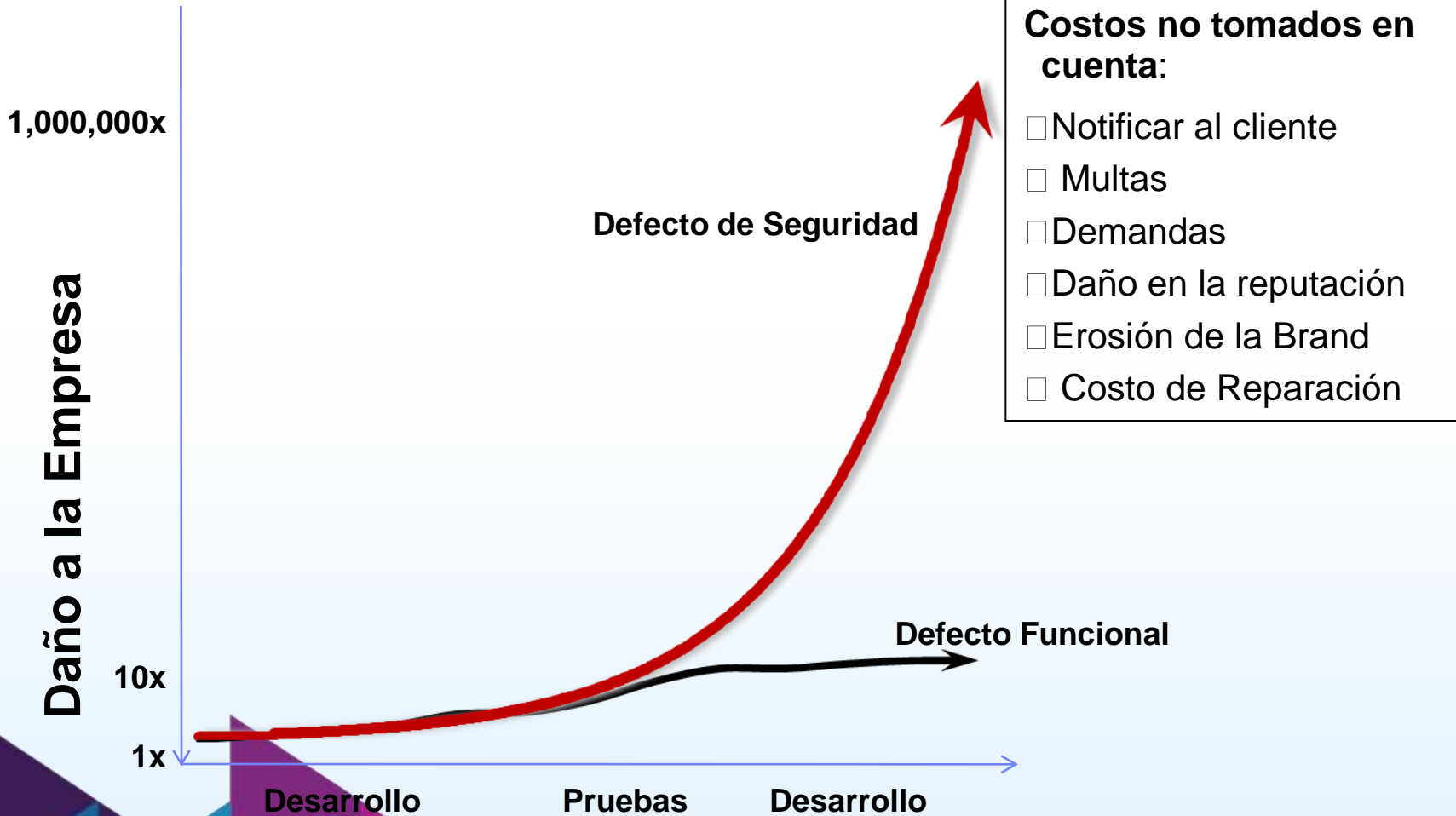
2/3 De todas las aplicaciones son vulnerables

Innovate2011



**Gartner
Software. Everywhere.

Costos de las diferentes fuentes de defectos



¿Por que son las aplicaciones tan vulnerables?

- ❑ A los desarrolladores se les exige que entreguen funcionalidad en tiempos y costos pero no se les pide que desarrollen aplicaciones seguras
- ❑ Los desarrolladores no tienen prácticas de desarrollo seguro
- ❑ Las aplicaciones son cada vez más complicadas y con más interconexiones



Volúmenes grandes de aplicaciones continúan siendo liberadas llenas de defectos de seguridad...



¿Como funciona Rational AppScan?

Automatiza la detección y Análisis de Vulnerabilidades en Aplicaciones Web



Revisa las Aplicaciones



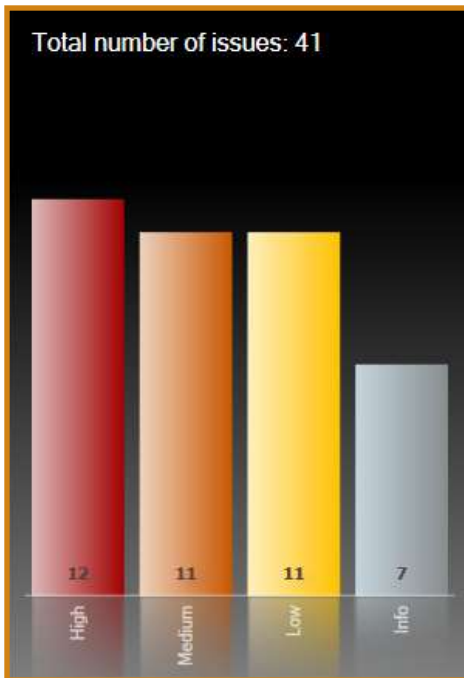
Analiza
(identifica problemas)



Reporta
(detalles & acciones a tomar)



Resultados Fácil de Entender – Problemas y Prioridades



Arranged By: Severity | Highest on top

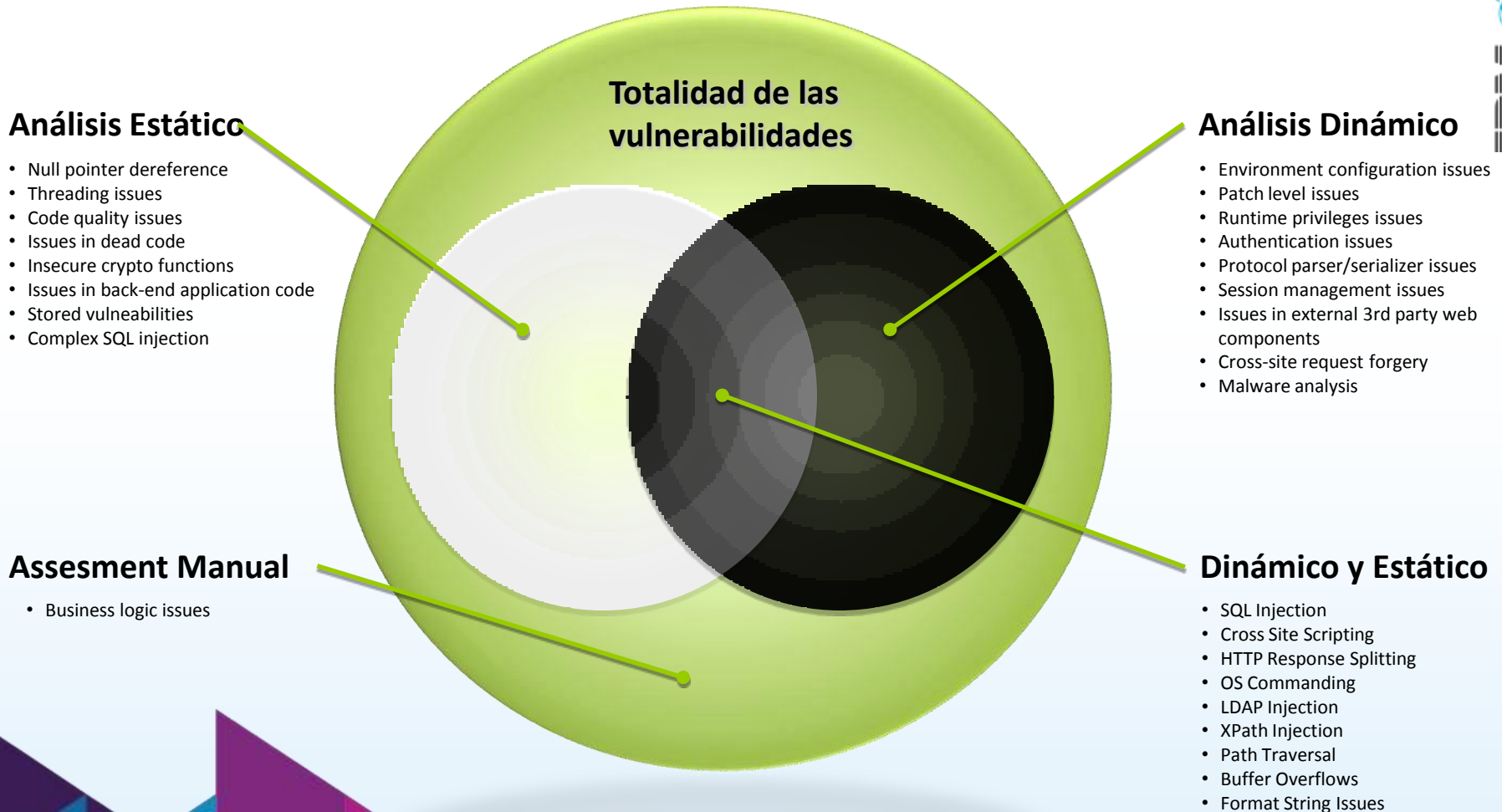
41 Security Issues (137 variants) for 'My Application'

- [-] **Cross-Site Scripting (7)**
 - [+] <http://demo.testfire.net/bank/customize.aspx> (2)
 - [+] <http://demo.testfire.net/bank/login.aspx> (1)
 - [+] <http://demo.testfire.net/comment.aspx> (2)
 - [+] <http://demo.testfire.net/search.aspx> (1)
 - [+] <http://demo.testfire.net/subscribe.aspx> (1)
- [+] **HTTP Response Splitting (1)**
- [+] **SQL Injection (3)**

The screenshot shows a security scanner interface with a list of issues on the left and a detailed view of a Cross-Site Scripting issue on the right. The detailed view includes the following information:

- Severity:** High
- Type:** Application Head Test
- WASC Threat Classification:** Client-side Attacks, Cross-site Scripting
- CVE Reference(s):** N/A
- Security Risk:** It is possible to steal or manipulate customer session and cookies, which may be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user.
- Possible Causes:** Sanitization of hazardous characters was not performed correctly on user input.
- Technical Description:** The Cross-Site Scripting attack is a privacy violation that allows an attacker to capture a legitimate user's credentials and to impersonate that user when interacting with a specific website. The attack hinges on the fact that the web site contains a script that returns a user's input (usually a parameter value) in an HTML page, without first sanitizing the input. This allows an input consisting of JavaScript code to be executed by the browser when the script returns this input in the response page. As a result, it is possible to both link to the site where one of the parameters consists of malicious JavaScript code. This code will be executed by a user's browser in the site context, granting it access to cookies that the user has for the site, and other windows in the site through the user's browser. The attack proceeds as follows: The attacker lures the legitimate user to click on a link that was produced by the attacker. When the user clicks on the link, the browser's

DAST y SAST – Cobertura de issues



Pruebas de Seguridad en el Ciclo de Pruebas



SDLC

Coding

Build

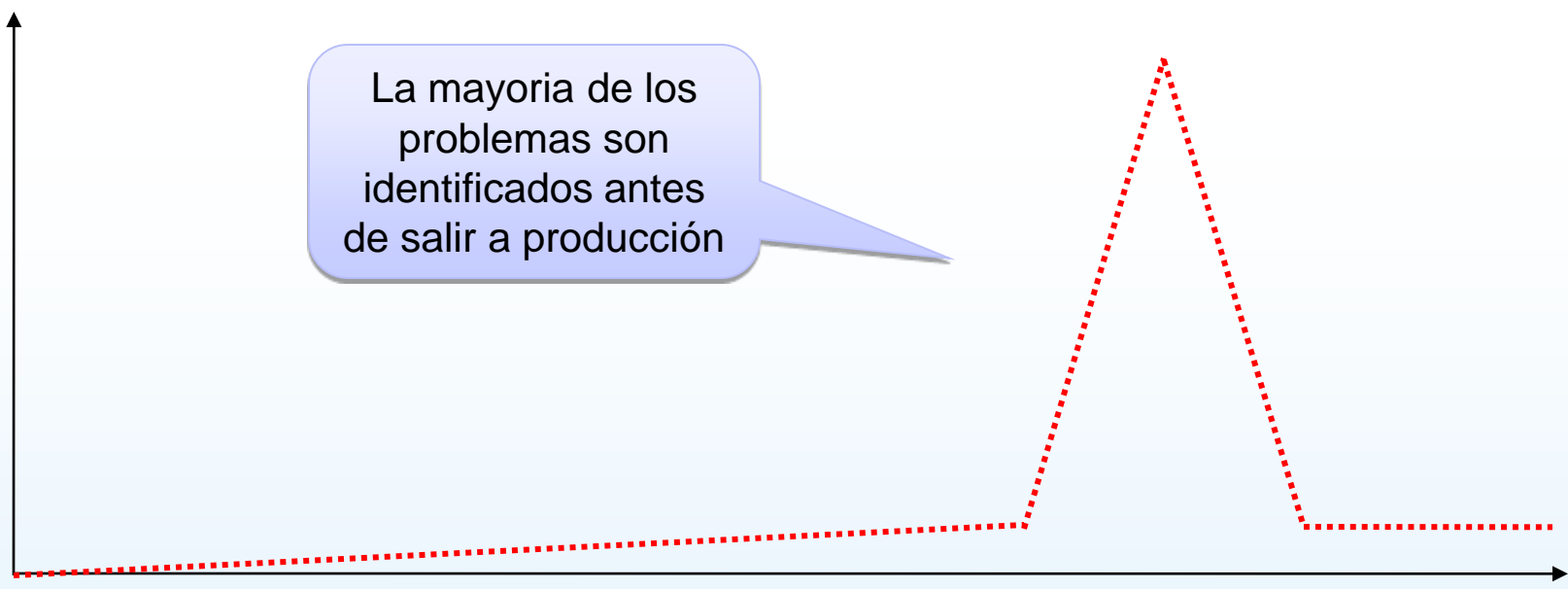
QA

Security

Production

% of Issue Found by Stage of SDLC

La mayoría de los problemas son identificados antes de salir a producción



Pruebas de Seguridad como parte del Ciclo de Desarrollo



SDLC

Coding

Build

QA

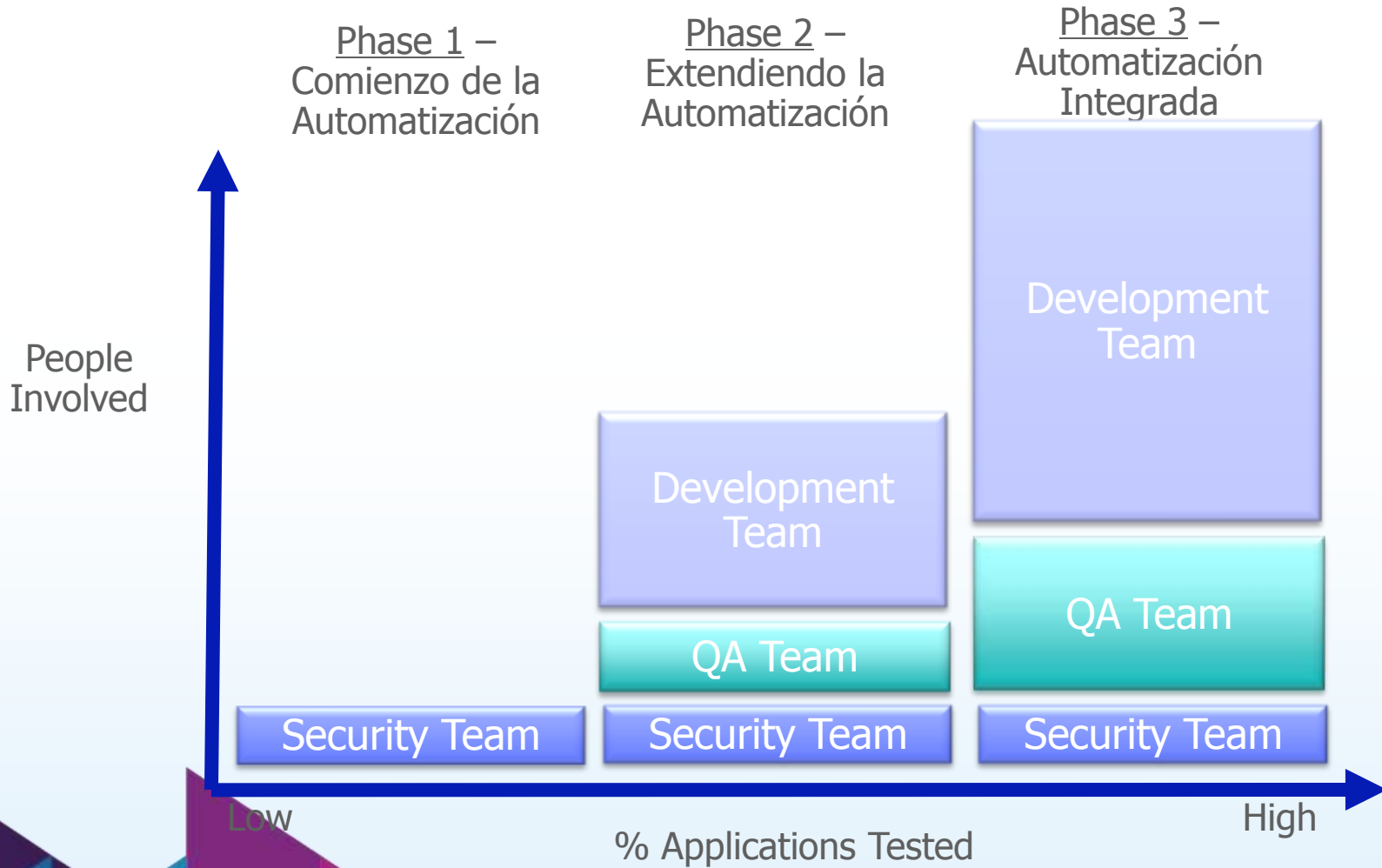
Security

Production

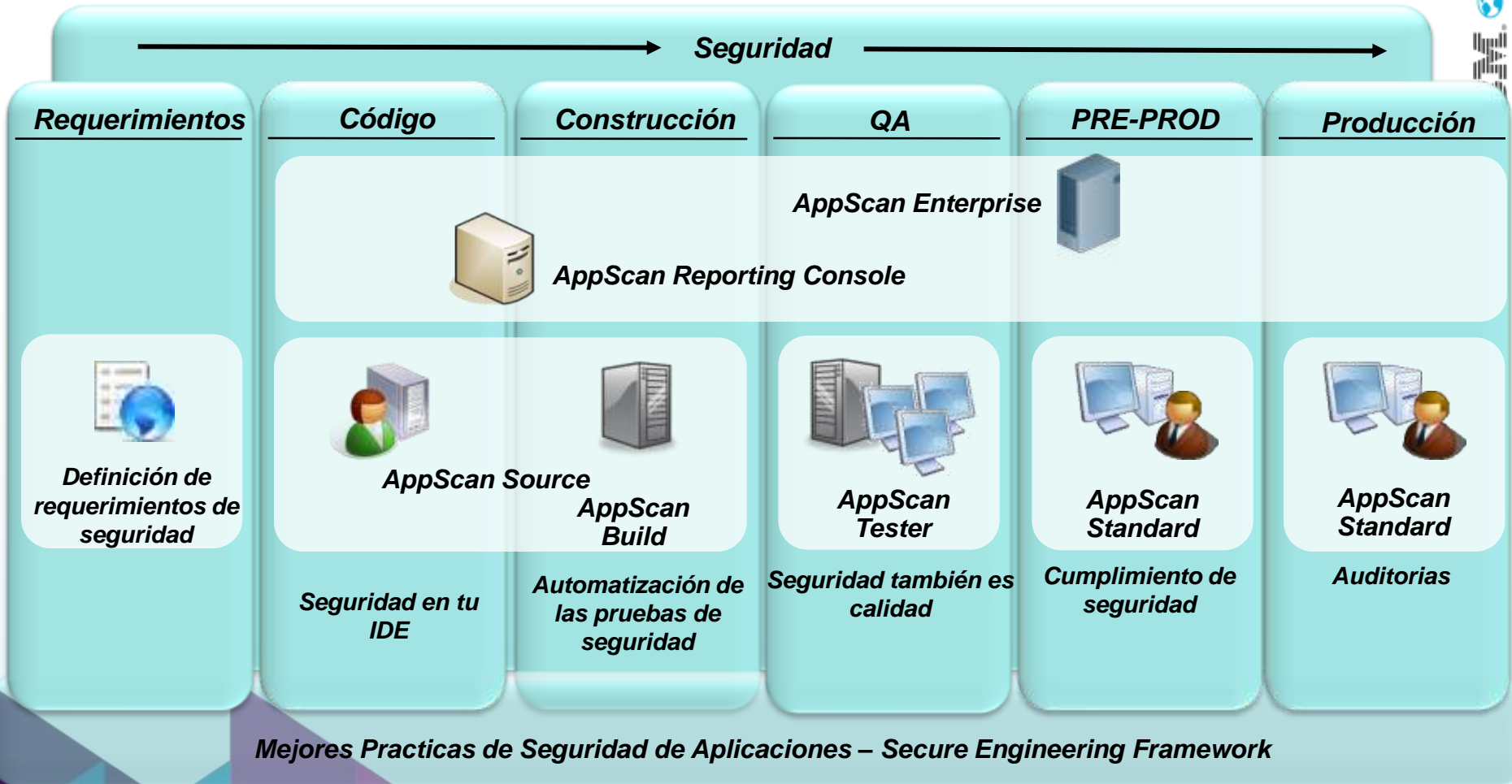
% of Issue Found by Stage of SDLC

Escenario Deseable

La Necesidad de Escalar las Pruebas de Seguridad



Ecosistema IBM Rational AppScan



Innovate2011

 Software. Everywhere.

Issue Correlation

■ Integración con AppScan Enterprise

- ▶ AppScan Source es capaz de exportar directamente hacia la consola de AppScan Enterprise para la correlación de resultados de Caja Negra y Caja Blanca
- ▶ Provee un dashboard centralizado de seguridad y un motor de reporte de tendencia para Caja Negra y Blanca

IBM Rational AppScan Enterprise Edition

Jobs & Reports > Default > Users > Common ASE Service Account > Sample Import > Static Analysis Security Issues

Static Analysis Security Issues

Last Updated: 9/21/2009 8:28:50 AM

Summary Group Show Search Layout


There are 104 issues of 5 different types across 16 files


Vulnerabilities			Type I			Type II		
High	Medium	Low	High	Medium	Low	High	Medium	Low
17	4	5	30			19	4	3

All items

Items 1-25 of 104

Action	Status	Issue	Code Severity	Application	Application V-Density	Project Name	Project V-Density	Source File	Line	File V-Density	Issue Type	Classification
<input type="checkbox"/>	Open	273*	High	Demo	3826.730249	Demo	3826.730249	bank/que...path.jsp	6	438.38164	Cross-Site Scripting	Subvulnerability
<input type="checkbox"/>	Open	275*	Medium	Demo	3826.730249	Demo	3826.730249	admin/admin.jsp	64	138.324536	Cross-Site Scripting	Subvulnerability
<input type="checkbox"/>	Open	276*	Medium	Demo	3826.730249	Demo	3826.730249	bank/loan.jsp	26	462.482568	Cross-Site Scripting	Subvulnerability
<input type="checkbox"/>	Open	277*	Medium	Demo	3826.730249	Demo	3826.730249	bank/transfer.jsp	86	103.524938	Cross-Site Scripting	Subvulnerability
<input type="checkbox"/>	Open	278*	High	Demo	3826.730249	Demo	3826.730249	dynamic/checkout.jsp	18	1181.499524	Cross-Site Scripting	Subvulnerability
<input type="checkbox"/>	Open	279*	Medium	Demo	3826.730249	Demo	3826.730249	admin/admin.jsp	88	138.324536	Cross-Site Scripting	Subvulnerability
<input type="checkbox"/>	Open	280*	High	Demo	3826.730249	Demo	3826.730249	dynamic/checkoutForm.jsp	17	234.272762	Cross-Site Scripting	Subvulnerability
<input type="checkbox"/>	Open	282*	Medium	Demo	3826.730249	Demo	3826.730249	admin/admin.jsp	64	138.324536	Cross-Site Scripting	Subvulnerability
<input type="checkbox"/>	Open	284*	Medium	Demo	3826.730249	Demo	3826.730249	bank/transfer.jsp	86	103.524938	Cross-Site Scripting	Subvulnerability

Rational AppScan Enterprise 

AppScan Source Ed for Developer 

AppScan Source Ed for Security 



Software. Everywhere.

Innovate2011





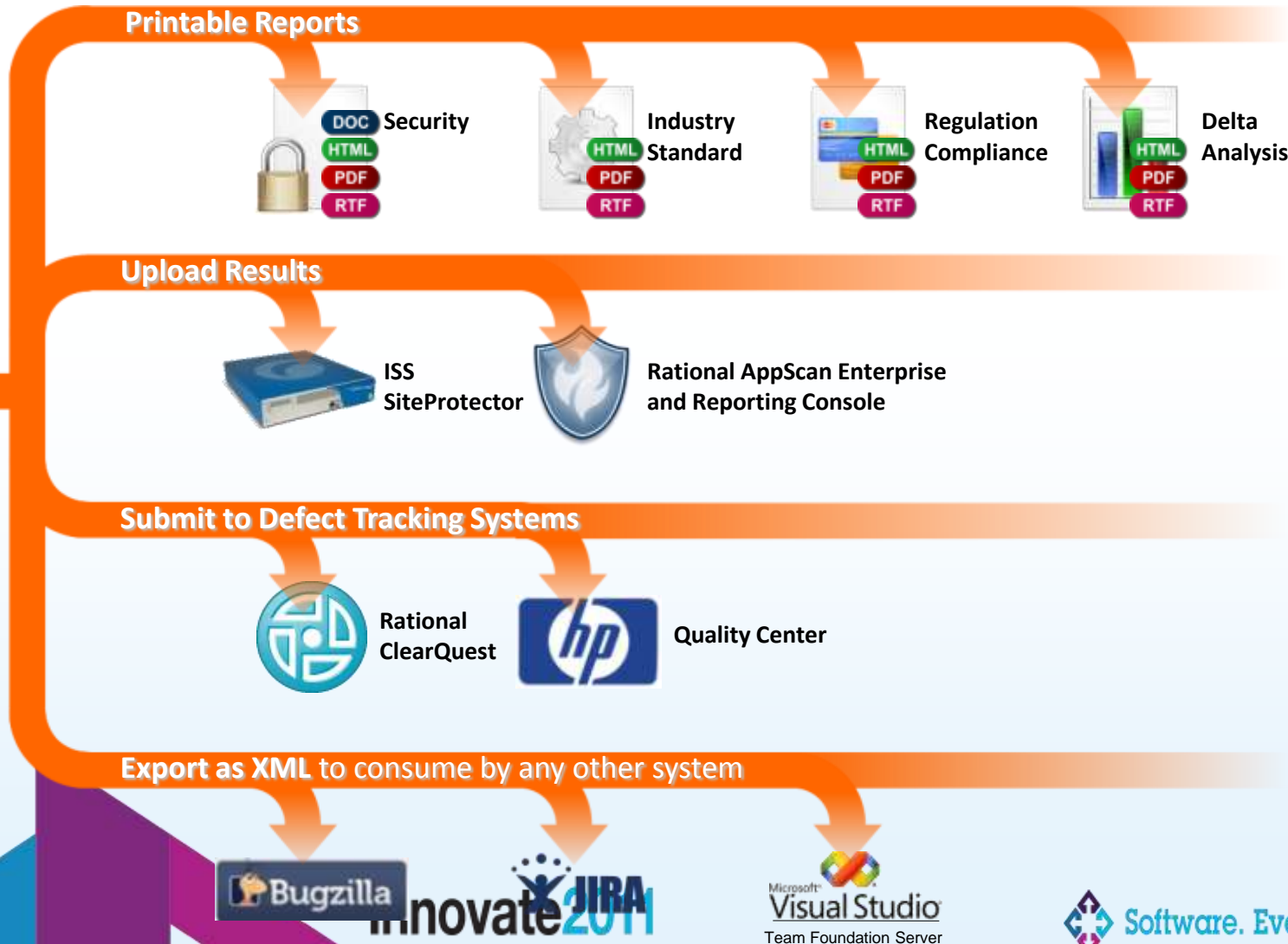
www.ibm.com/software/mx/rational

© Copyright IBM Corporation 2011. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, Rational, the Rational logo, Telelogic, the Telelogic logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

innovate2011

 Software. Everyware.

Capacidades de Reporteo e integracion con DAST





Cross-Site Scripting

- URL: <http://local/altoro/comment.aspx>
- Entity: `comment.aspx`
- Security Risk: It is possible to steal or manipulate customer session and cookies, which may be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

High

CVSS Metrics Scoring (8)



The script AppScan injected seems to be included in the response. If the screen shot below shows a simulation of the pop-up that the injected script produced, this is proof that the application is vulnerable to Cross-Site Scripting. If not, to verify this vulnerability: 1) Open the Request/Response tab and click Show in Browser, and see if a pop-up appears. (Note that some script syntaxes are browser specific, so if the injected alert doesn't pop up, try a different browser (View Source > Save As...).) 2) Check the validity of the alert script(s) in the raw test response.

Rendered Test Response

[Click to View Full Size](#)

The screenshot shows the AltoroMutual website interface. At the top, there is a navigation bar with links for [Sign Off](#), [Contact Us](#), [Feedback](#), and a search box with a [Go](#) button. The main header features the AltoroMutual logo and a banner with images of people and the text "DEMO SITE ONLY". Below the header, there are navigation tabs for "MY ACCOUNT", "PERSONAL", "SMALL BUSINESS", and "INSIDE ALTORO MUTUAL". The "PERSONAL" tab is selected, and the main content area displays a "Thank You" message. A simulated alert box is overlaid on the page, containing a yellow warning icon, the number "8172", and an "OK" button. The text below the alert box reads: "Simulation of the pop-up that will appear when this page is opened in a browser".