Unleash the Power of Innovation
with IBM Rational
Solutions for Power

Milano, 1 Luglio 2010

Massimo Caprinali

Rational Client Technical Professional

La soluzione IBM Rational per la Sicurezza

2009 IBM CIO Survey: Risk Management e Compliance sono considerati fra gli elementi piu' importanti del piano strategico dalle aziende a livello mondiale

Source:
IBM Global CIO Study 2009;
2345 clienti in 78 paesi e
19 settori

NOTE: CIOs were asked to select all applicable answers to the question, "What kind of visionary plans do you have for enhanced competitiveness?"

La sfida di oggi: rendere sicuro un pianeta più intelligente

IBM

The Opportunity – smarter planet

Globalizzazione e dislocazione globale delle risorse

Accessi a flussi di informazioni in tempo reale

Milioni di device mobili che accedono al Web

Nuove forme di collaborazione

Unleash the Power of Innovation with
IBM Rational Solutions for Power

Applicazioni non protette mettono a rischio dati sensibili e compliance

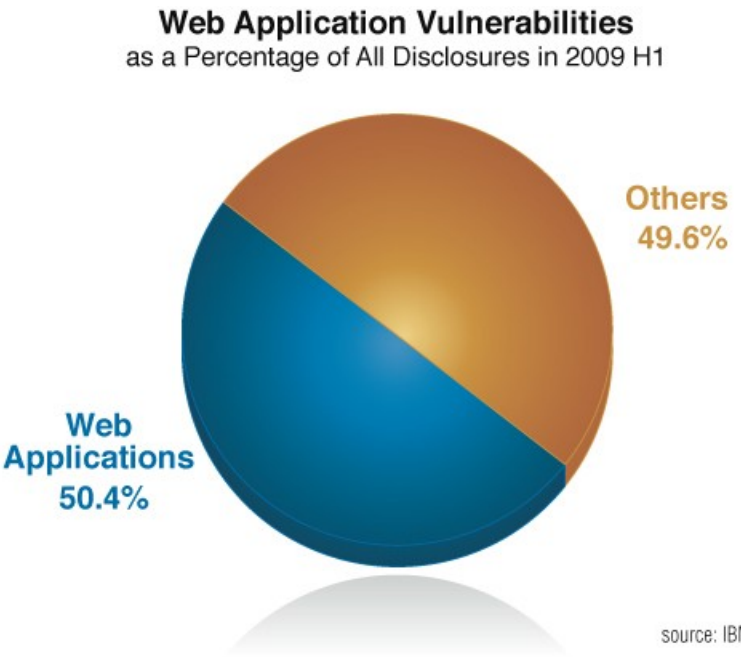
IBM

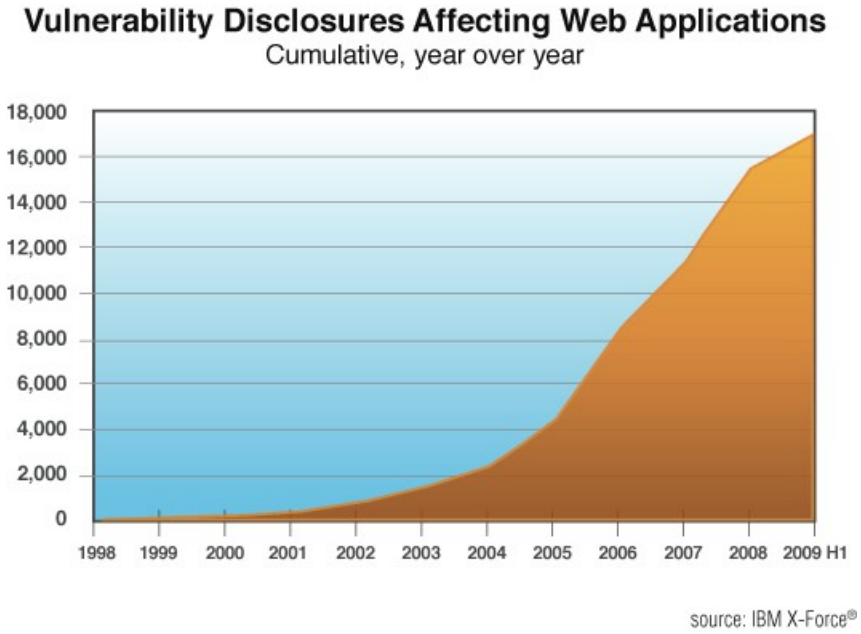
Rischi e Minacce	Costi di una Violazione di Sicurezza	Compliance Demands
Il furto di Informazioni Sensibili è la 2a motivazione per gli attacchi delle Applicazioni Web	▪ Il Costo medio di una violazione della sicurezza è di 6.6 milioni di dollari ▪ Notifica ai propri clienti ($202 per record) ▪ Multe (fino a $15 million) ▪ Perdita d'immagine ed azioni legali ▪ Sconvolgimento delle operazioni di business	Costi di non conformità alle regolamentazioni (es. Multe per il non rispetta della PCI DSS)

Source: Web Incidents Hacking Database 2008 Annual report

Le vulnerabilità delle applicazioni web continuano a dominare

- **50.4%** di tutte le vulnerabilità sono vulnerabilità applicative
- SQL injection e Cross-Site Scripting sono testa a testa in una gara per il primo posto

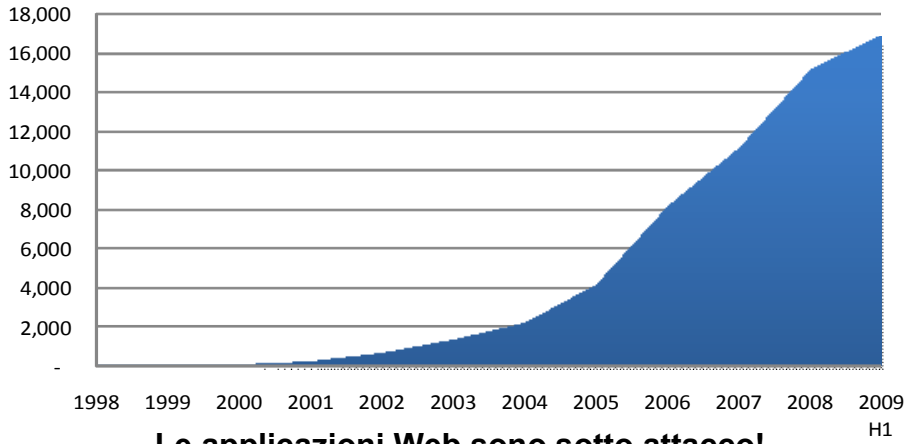




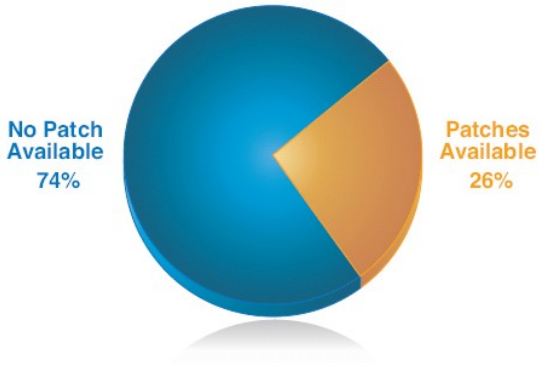
Gli Hackers continuano a concentrarsi sulle Applicazioni Web

… perché sono facili punti di accesso e ci sono informazioni "prezione" scambiate dai processi di business eseguiti dalla applicazioni

Vulnerabilità delle applicazioni Web in aumento



Percentuale di vulnerabilità delle applicazioni Web Disponibile con Patch



Le applicazioni Web sono sotto attacco!

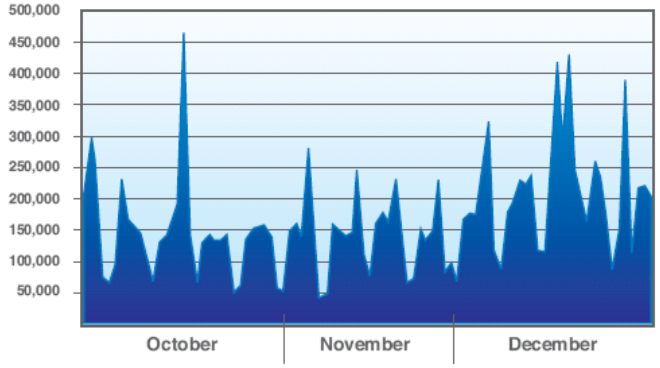


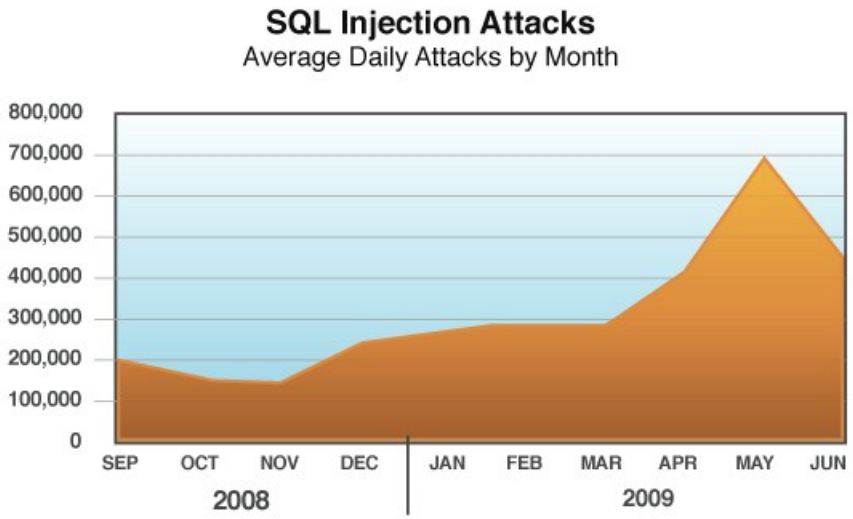
Figure 21: SQL Injection Attacks Monitored by IBM ISS Managed Security Services, Q4 2008

- **In Q4 2008, IBM MSS attesta milioni di attacchi SQL Injection in tutto il mondo**
- **Gli Hacker puntano alle applicazioni web per rubare dati ridirigere siti legittimi a siti dannosi**
- **90% delle vulnerabilità scoperte nel 2008 sono are utilizzabili remotamente**
- **Gli Hacker adottano tecniche molto complesse e malevoli per rubare le informazioni**
- **Il numero di attacchi automatizzati sui Web Server sono stati senza precedenti (30x negli ultimi 6 mesi)**

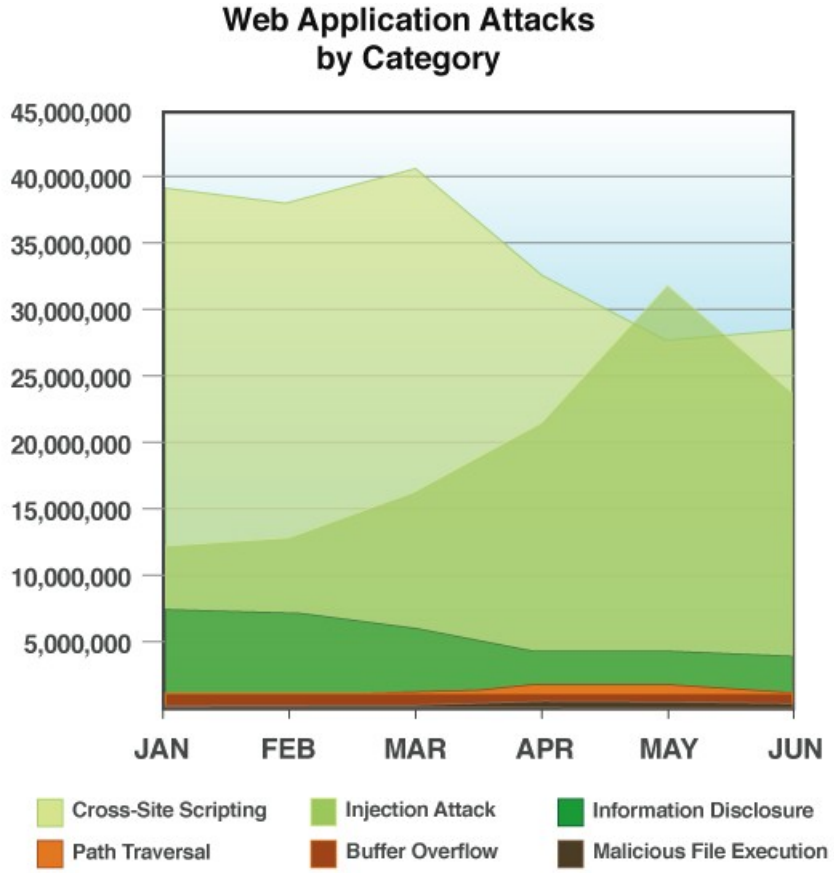
Source: 2008 IBM ISS X-Force Annual Report

Attacchi Cross Site Scripting ed Injection Continuano a Dominare

- **90%** degli attacchi di injection sono relativi ad SQL
- I toolkit che automatizzano continuano a prosperare nel 2009
- Gli attacchi di SQL injection continuano a crescere, **50%** in più tra Q1 2009 e Q4 2008 e quasi il doppio tra Q2 e Q1



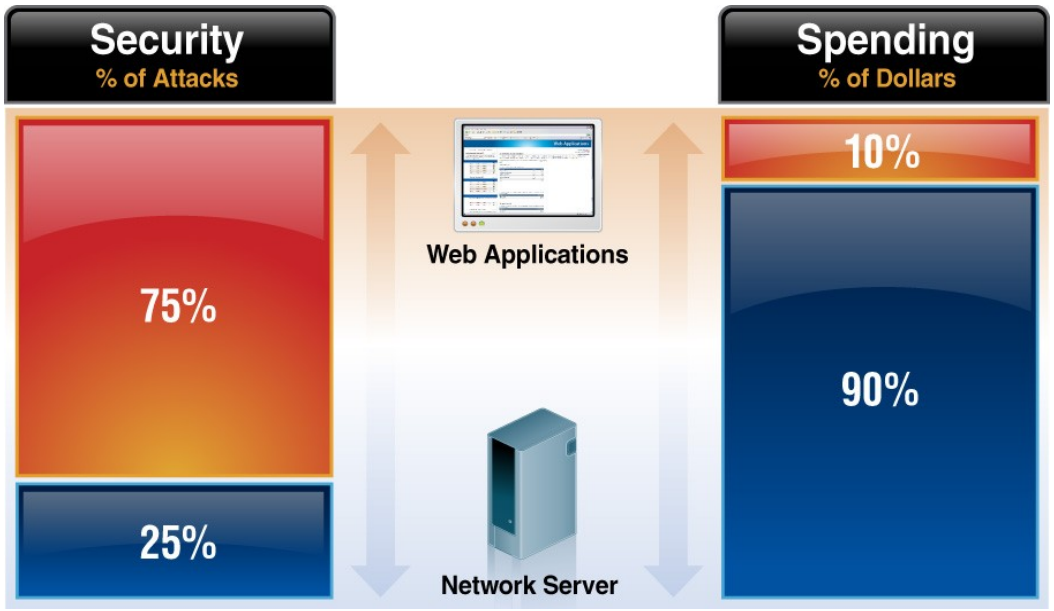
source: IBM X-Force®



source: IBM X-Force®

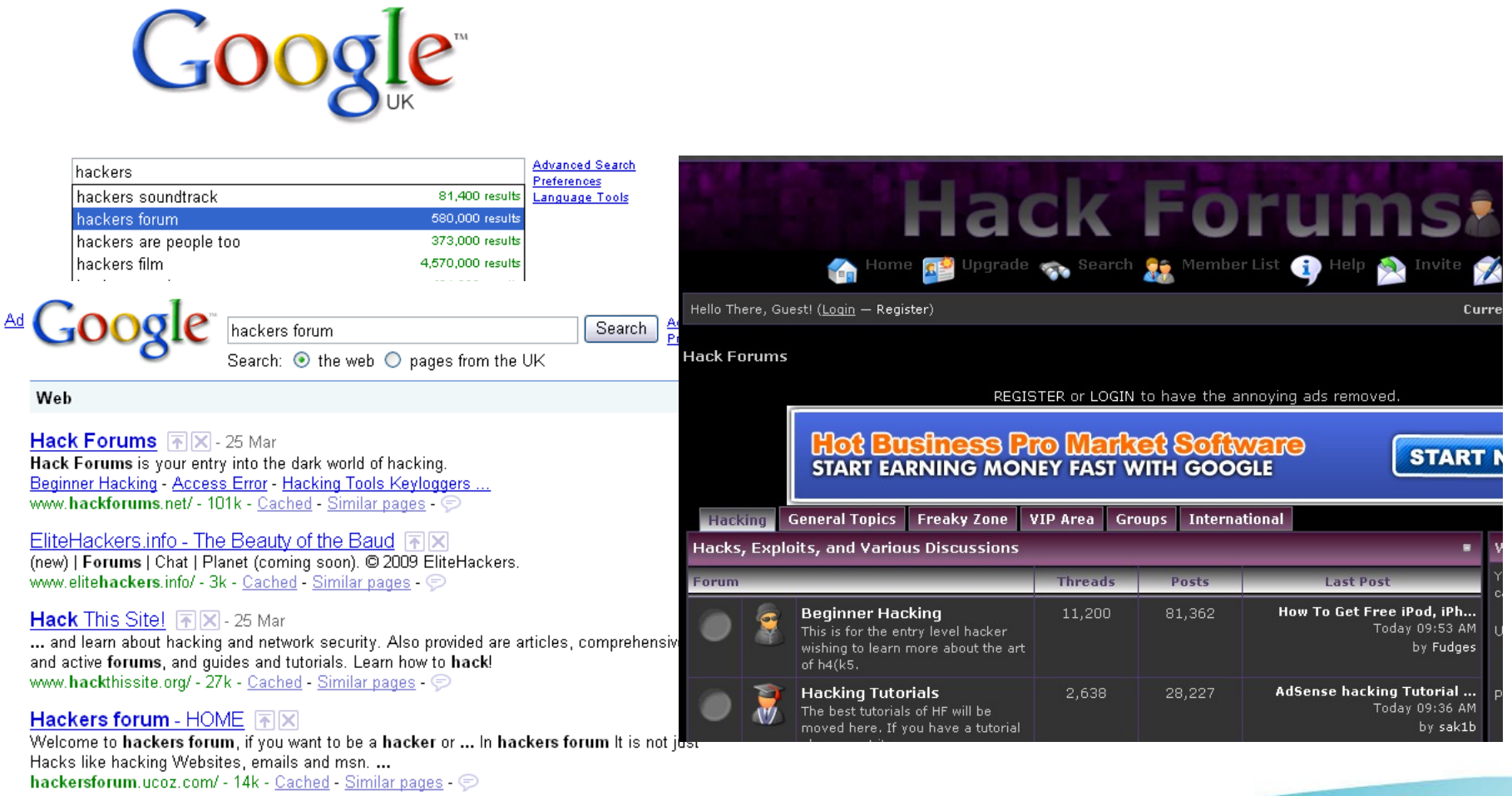
La soluzioni tradizionali non possono affrontare tutte le esigenze di sicurezza del Web

- **Vulnerability scanners**
  - I tradizionali scanner non coprono le applicazioni Web
- **Penetration testing**
  - Efficace nel trovare le vulnerabilità, ma non scalabile per un test continuo
  - Non si concentrano sulla remediation
- **Network firewall e IPS**
  - Protezione generica per le applicazioni Web così che molte applicazioni web custom non sono coperte
  - Gran parte delle soluzioni IPS si concentrano sugli exploit e non sulle vulnerabilità delle applicazioni Web
- **Web application firewall**
  - Costosi da mantenere e gestire
  - Possono essere efficaci, ma difficili da implementare e ottimizzare.
  - La creazione di regole può impiegare più tempo che correggere la vulnerabilità.



Source: Gartner Inc.

La facilità nel trovare informazioni sulla rete per diventare degli apprendisti hacker



Come si sentono i clienti se questo fosse accaduto a loro?

- Monster.com perse 4.5 milioni di record nel Febbraio 2009
- Il sito web di Panasonic fu attaccato nel Feb 2009 modificando i prezzi a pochi centesimi
- American Express colpita da XSS bugs nel Dic 2008
- Il website di BT fu attaccato da un importante hacker nel marzo 2009
- RBS US si scontrò con un'azione legale da £141m dopo aver ammesso che degli hacker avevano violato i loro sistemi nel Marzo 2009
- Il sito della Sony playstation colpito da un attacco di SQL Injection (Luglio 2008)

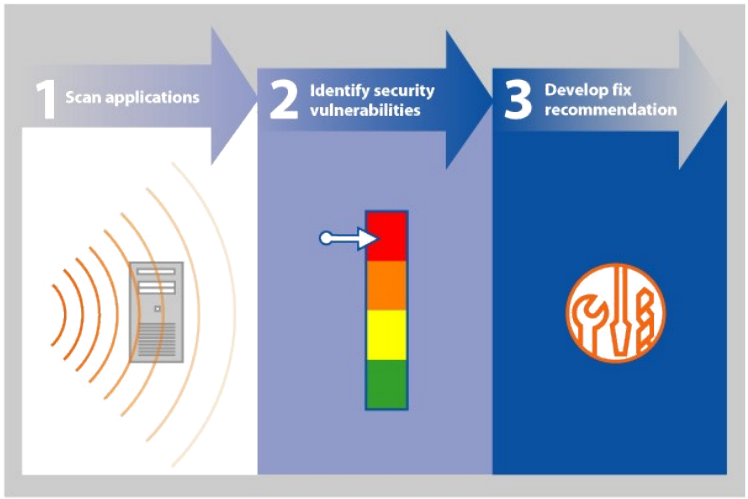
  Che impressione vi fa questo danno? Che danno è per l'immagine del marchio? Vuoi utilizzare questi siti web di nuovo? Chi riceve la telefonata quando ciò accade?

Miglior sicurezza ad un prezzo più basso

Incremento dell'efficienza e facilità di ripetizione attraverso l'automazione

Web application e web service security testing

- ✓ Individuare e correggere le applicazioni web da problematiche di sicurezza e compliance
- ✓ Valutare e porre rimedio alle vulnerabilità di sicurezza
- ✓ Diverse soluzioni per sviluppatori, tester, professionisti della sicurezza e il management
- ✓ **Out of the box Compliance Report**
  - ✓ **PCI DSS compliance**
  - ✓ **Gramm-Leach-Bliley Act (GLBA)**
  - ✓ **Health Insurance Portability and Accountability Act (HIPAA)**
  - ✓ **Children's Online Privacy Protection Act (COPPA)**
  - ✓ **Office of the Comptroller of the Currency (OCC) web linking guidelines**



"Se vi fossero dei seri problemi di sicurezza dei dati, saremmo fuori dal business",
Sakari Kalse, Eläke-Fennia's (Insurance Company).

Eläke Fennia ***ha scelto*** la soluzione di IBM per supportare questo cambiamento. ***IBM non solo riduce il rischio di sicurezza, ma fornisce anche significativi risparmi.***

Unleash the Power of Innovation with
IBM Rational Solutions for Power

Security Testing nel Ciclo di Vita del Software

SDLC

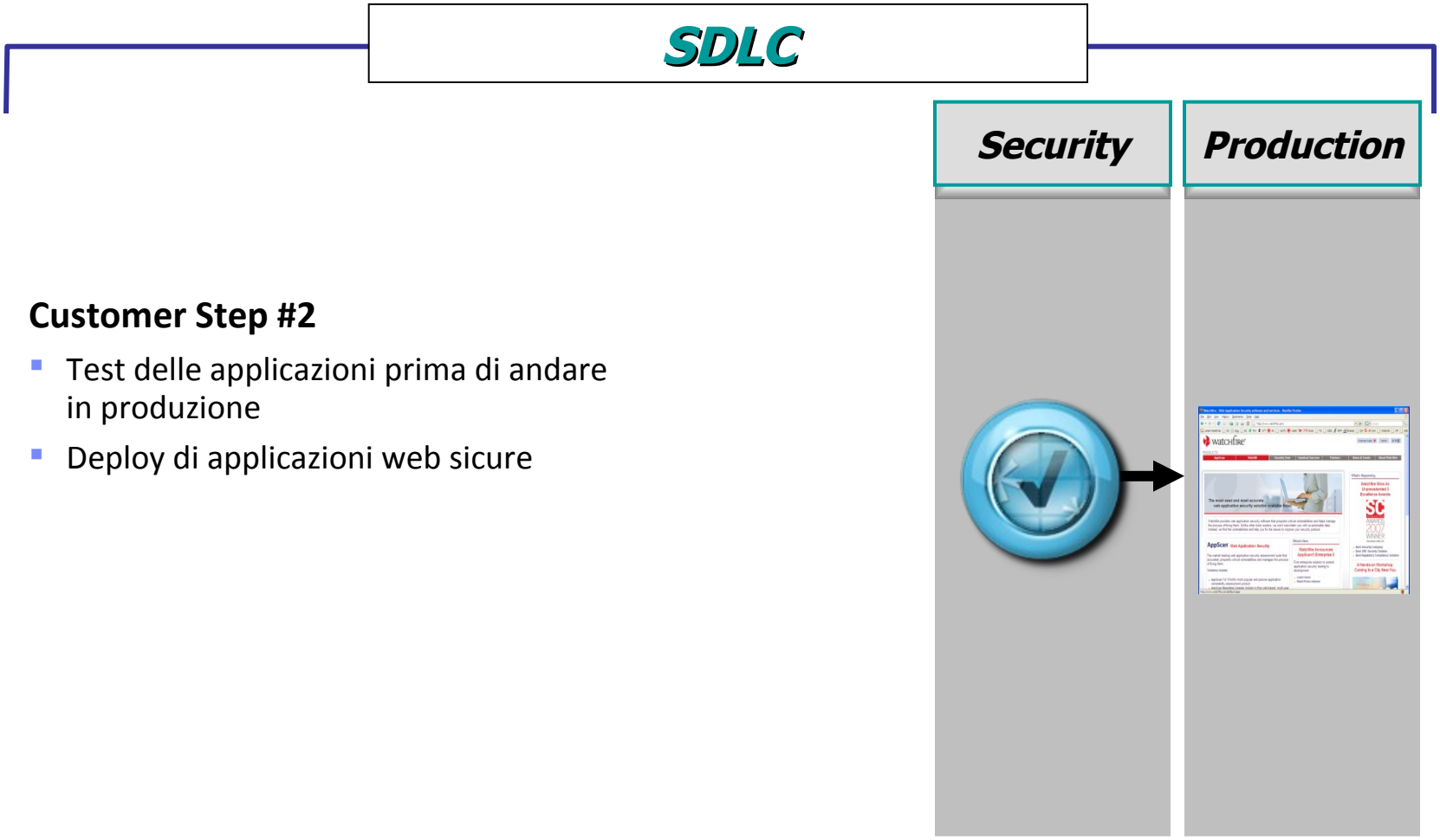
Production

Customer Step #1

- Test applicazioni già rilasciate
- Eliminare le vulnerabilità in applicazioni live

Application Security Testing Maturity

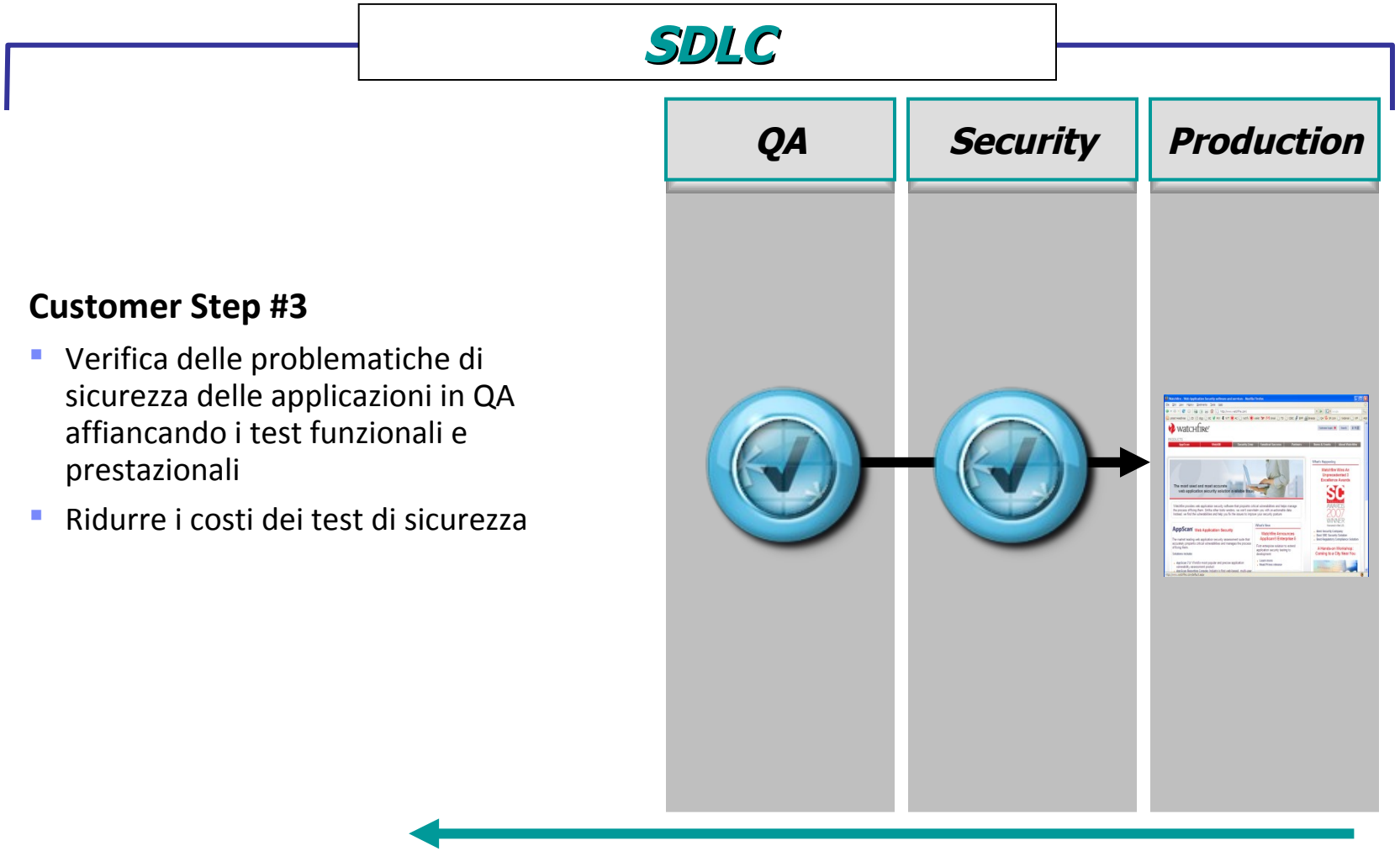
Security Testing nel Ciclo di Vita del Software



Customer Step #2

- Test delle applicazioni prima di andare in produzione
- Deploy di applicazioni web sicure

Security Testing nel Ciclo di Vita del Software

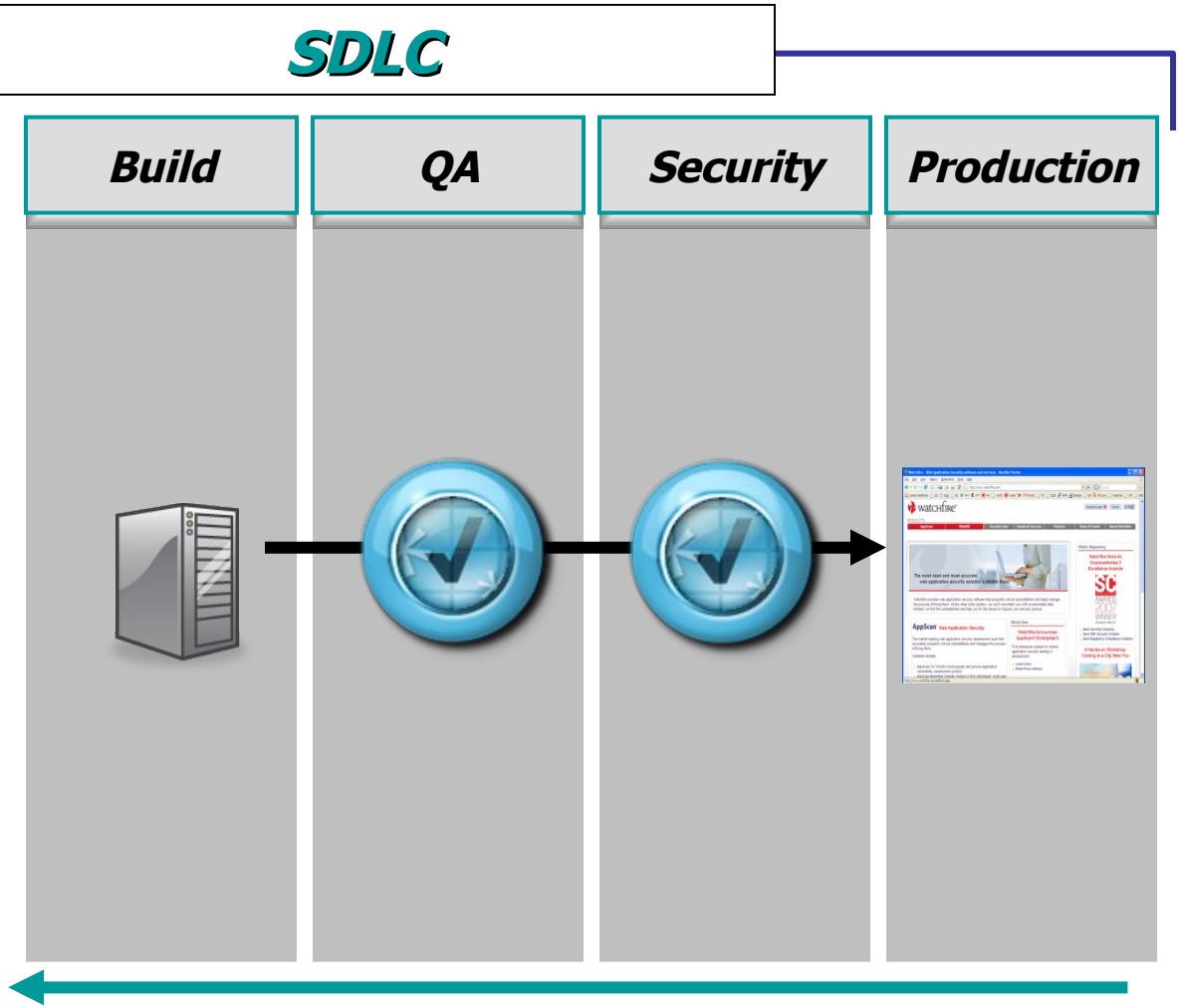


Customer Step #3

- Verifica delle problematiche di sicurezza delle applicazioni in QA affiancando i test funzionali e prestazionali
- Ridurre i costi dei test di sicurezza

Application Security Testing Maturity

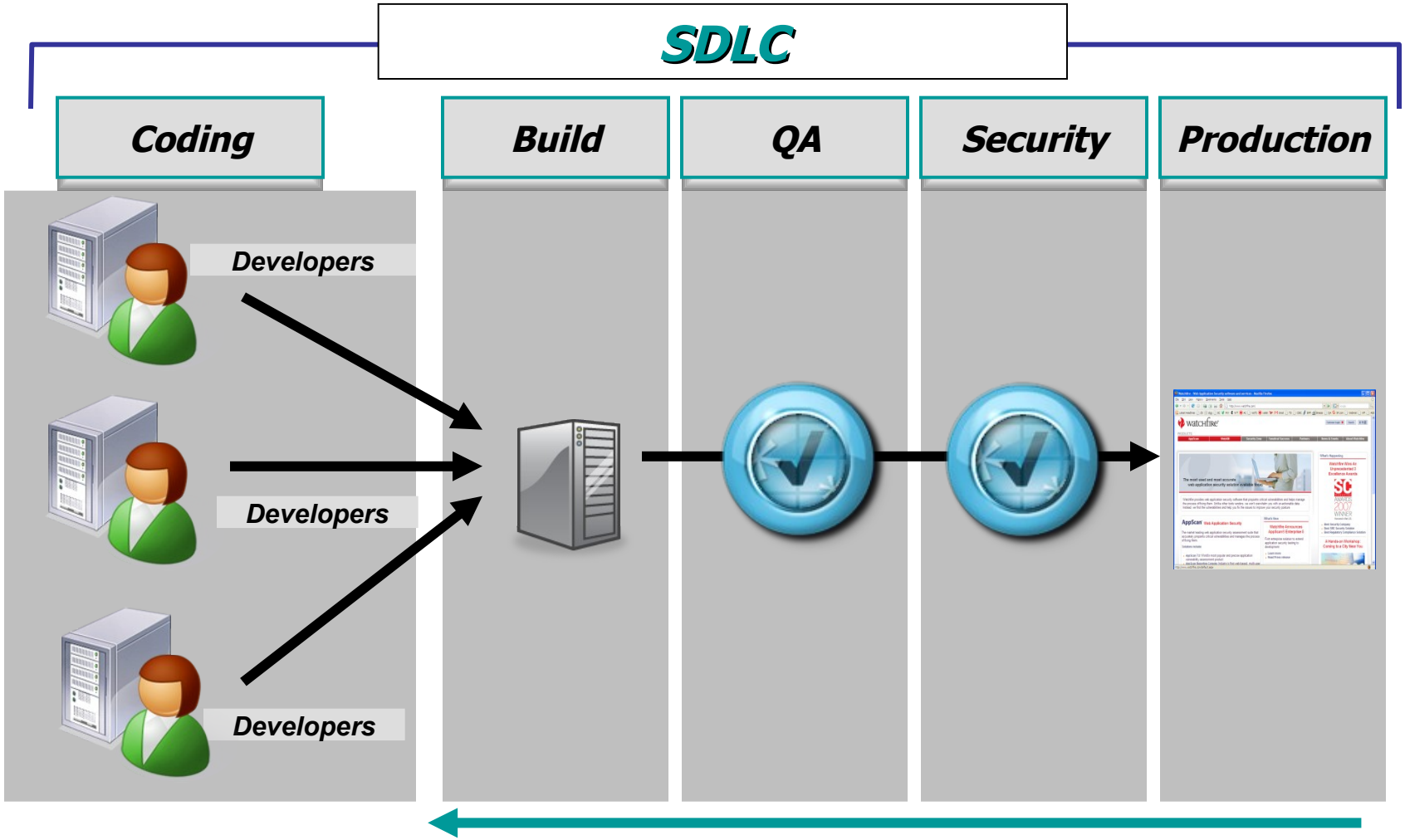
Security Testing nel Ciclo di Vita del Software



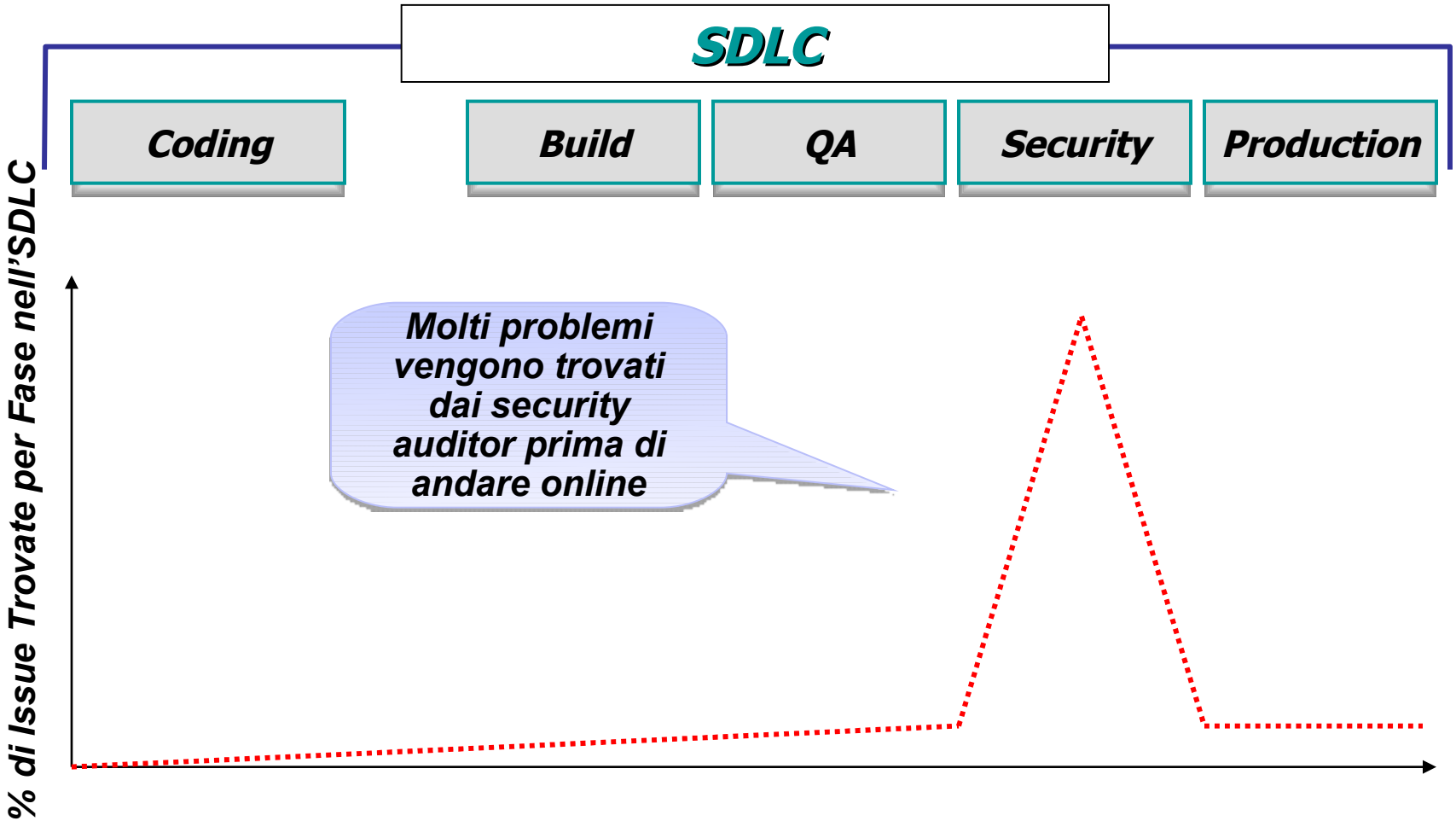
Customer Step #4

- Verifica delle problematiche di sicurezza nello sviluppo identificandole prima
- Ottenere un efficienza ottimale per i test di sicurezza (riduzione dei costi)

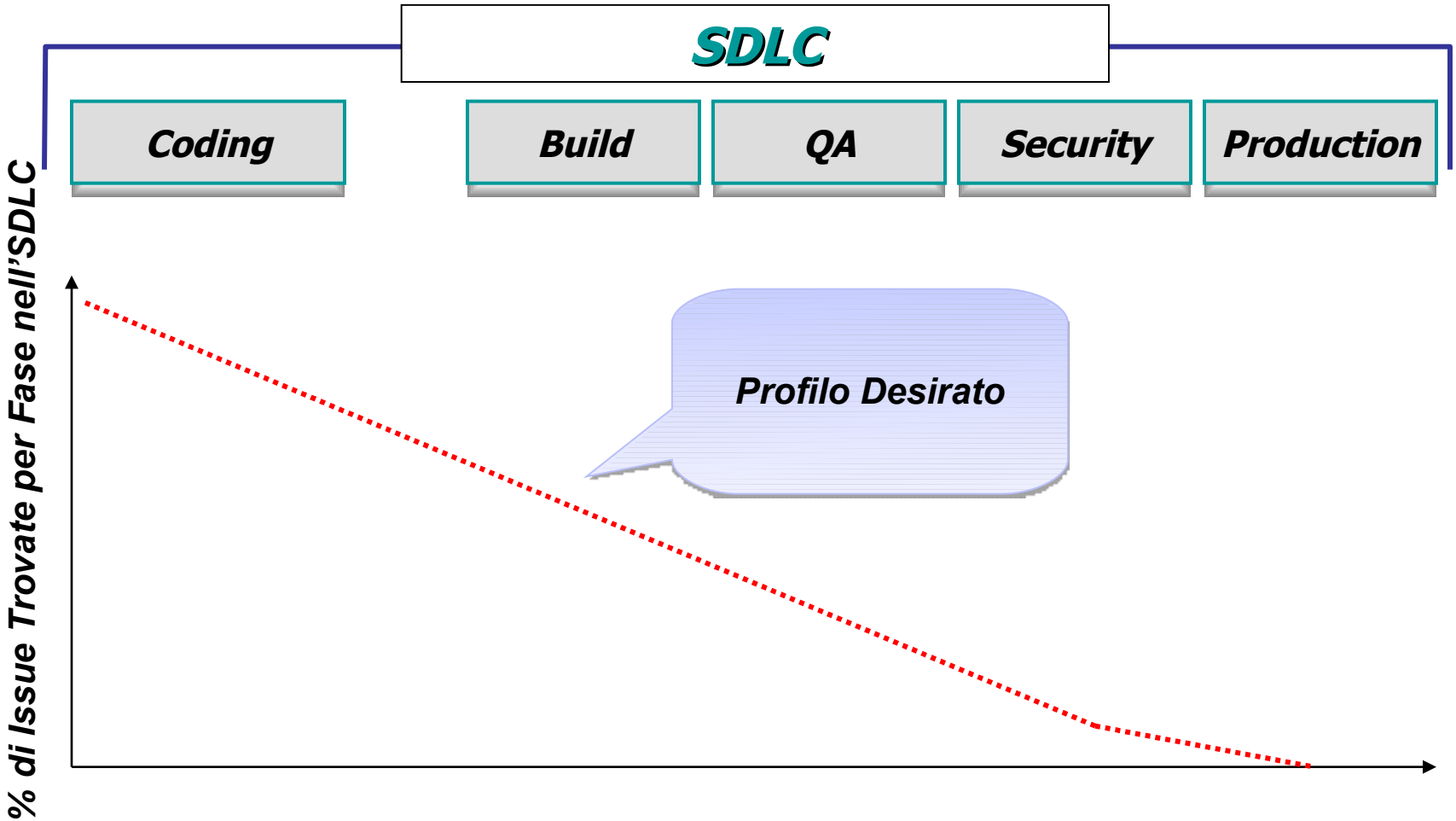
Security Testing nel Ciclo di Vita del Software



Security Testing nel Ciclo di Vita del Software



Security Testing nel Ciclo di Vita del Software



Un ciclo per il Software Sicuro

Fase di Design

- *Tenere in considerazione i requisiti di sicurezza dell'applicazione*
- *Problematiche come i controlli necessari e le best practices sono documentate alla pari dei requisiti funzionali*

Fase di Development

- *Il software è controllato durante la codifica per :*
  - *Vulnerabilità da errori di implementazione*
  - *Conformità ai requisiti di sicurezza*

Fase di Build & Test

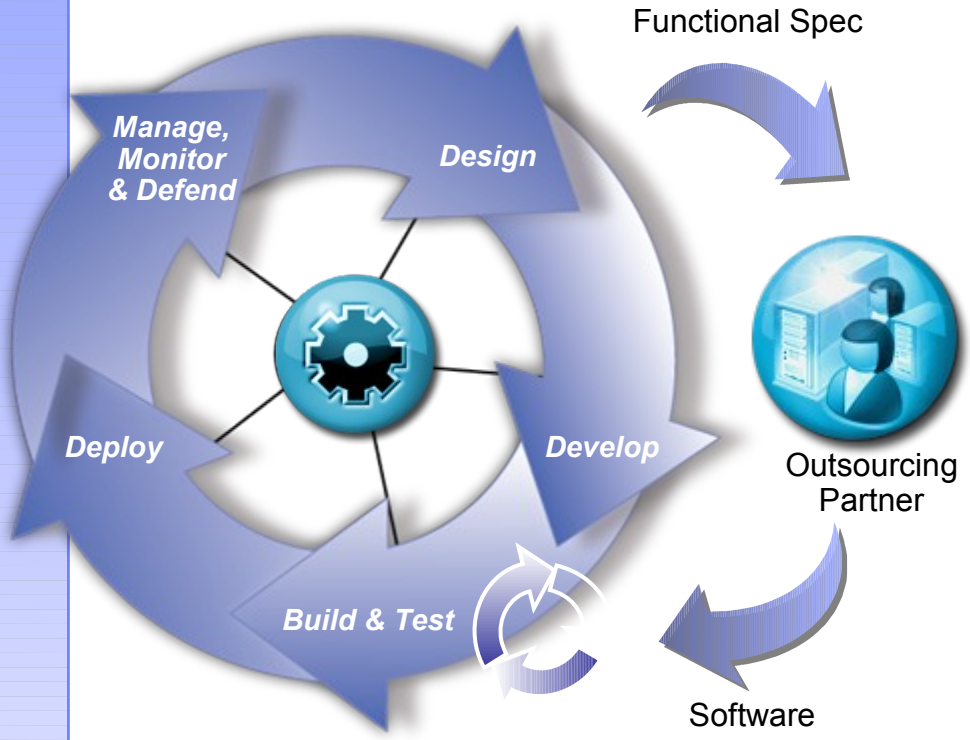
- *Testing alla ricerca di errori e per verificare la conformità ai requisiti di sicurezza per l'intera applicazione*
- *Le applicazioni sono inoltre sottoposte a test di penetrabilità in ambienti di deployment*

Fase di Deployment

- *Configurazione dell'infrastruttura per le policy applicative*
- *Deploy dell'applicazione in produzione*

Fase Operativa

- *Monitorare costantemente le applicazioni per verificando il corretto uso, le vulnerabilità e difendere contro gli attacchi*

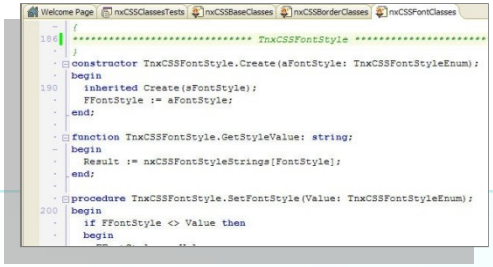


Tecnologie nei Test di Sicurezza...

Con l'unione si ottiene una Soluzione Completa

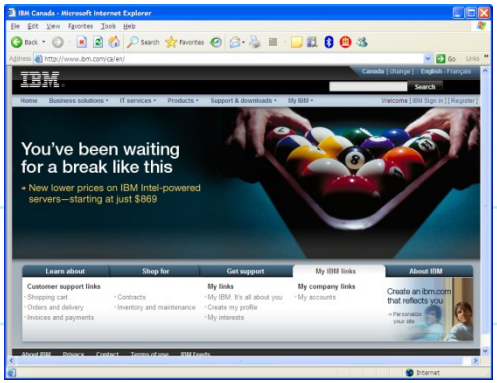
Static Code Analysis = Whitebox

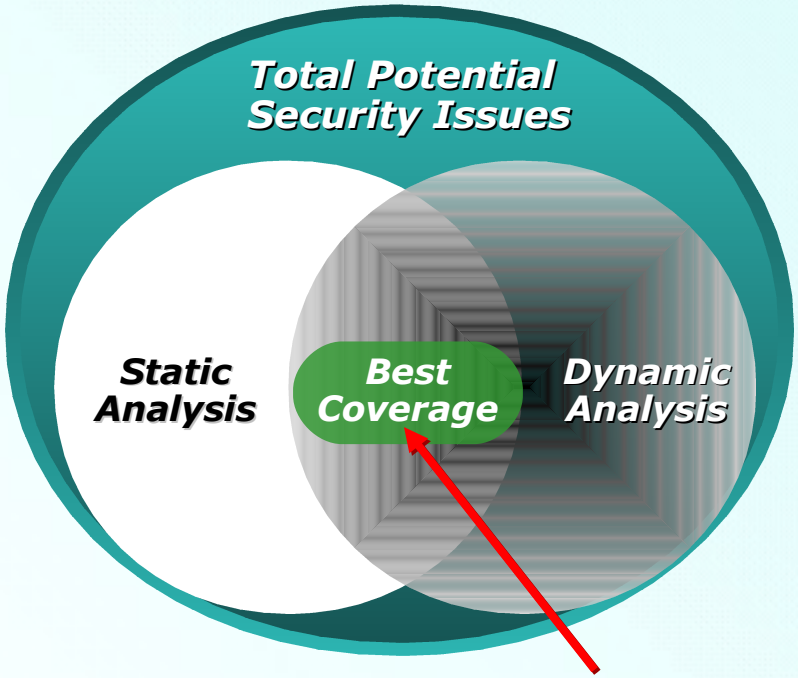
- *Scansione del codice sorgente per problematiche di sicurezza*



Dynamic Analysis = Blackbox

- *Analisi di sicurezza su applicazioni compilate*





NECESSARIE ENTRAMBI!

Unleash the Power of Innovation with
IBM Rational Solutions for Power

IBM Rational AppScan End-to-End Application Security

Dynamic Analysis/Blackbox –

Static Analysis/Whitebox -

SECURITY

REQUIREMENTS	CODE	BUILD	QA	SECURITY	PRODUCTION
Security Requirements Definition	AppScan Source	AppScan Build	AppScan Tester	AppScan Standard	AppScan Standard
Security requirements defined before design & implementation	Build security testing into the IDE	Automate Security / Compliance testing in the Build Process	Security / compliance testing incorporated into testing & remediation workflows	Security & Compliance Testing, oversight, control, policy, audits	Outsourced testing for security audits & production site monitoring

AppScan Enterprise / Reporting Console
(enterprise-wide scanning and reporting)

Application Security Best Practices

Unleash the Power of Innovation with
IBM Rational Solutions for Power

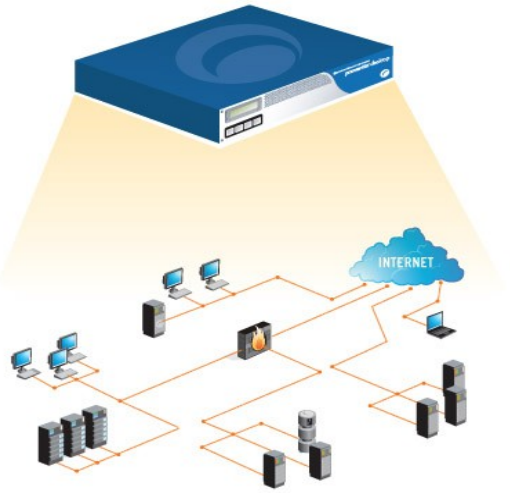
Come funziona Appscan?

Automates Application Security Testing

Identico processo per whitebox e blackbox

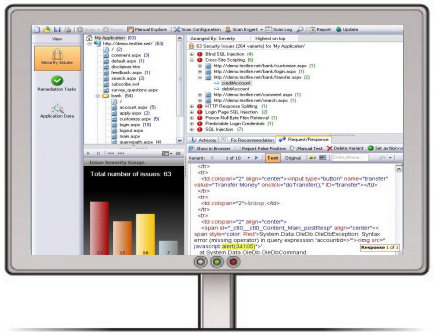
1 → 2 → 3

Scan applications



Analyze

(identify issues)

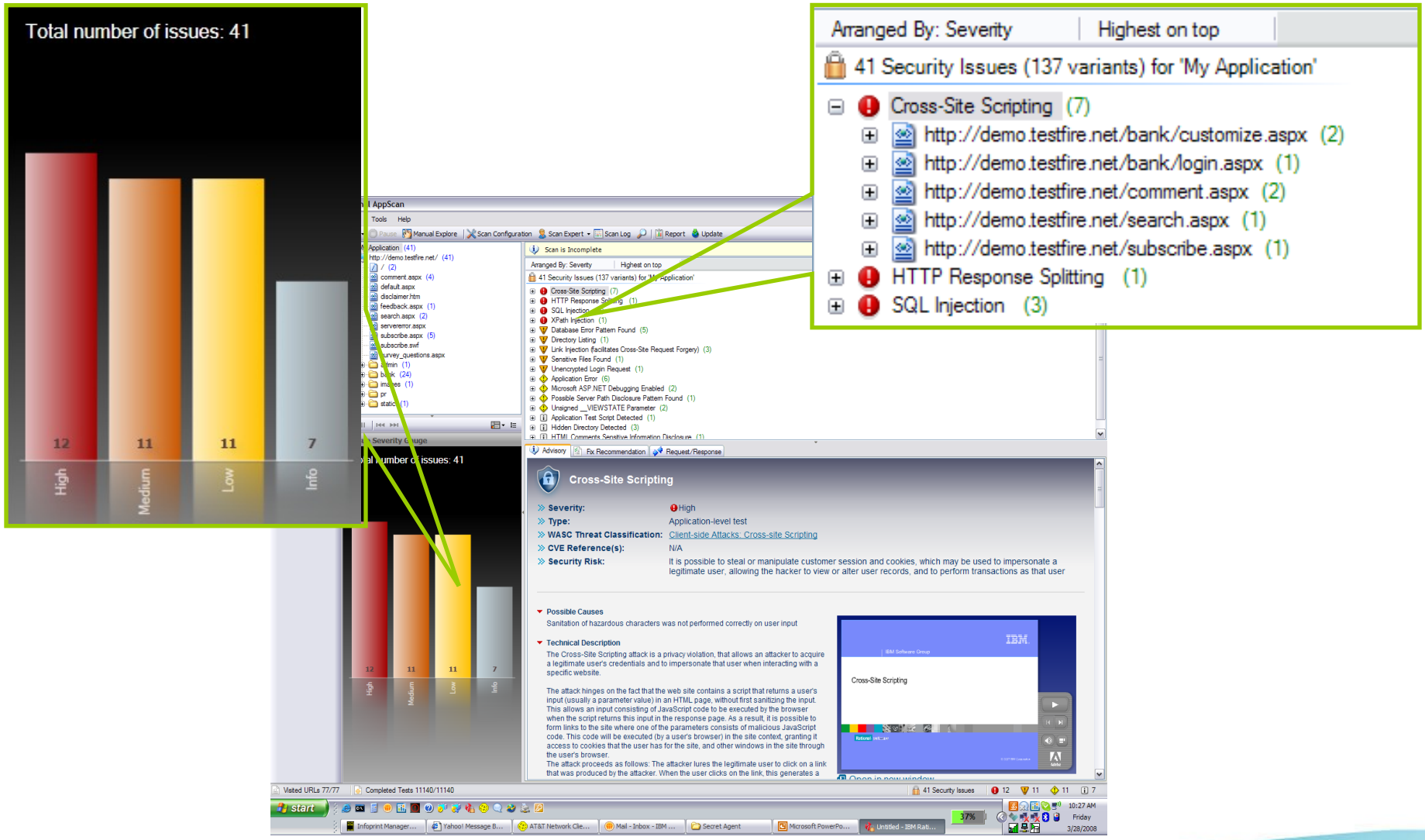


Report

(detailed & actionable)

Unleash the Power of Innovation with
IBM Rational Solutions for Power

Facilità nel comprendere i risultati – Issue e Priorità



Unleash the Power of Innovation with

IBM Rational Solutions for Power

Capire qual'è il problema

Advisory | Fix Recommendation | Request/Response

Cross-Site Scripting

- **Severity:** High
- **Type:** Application-level 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

Sanitation 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 acquire 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 form links 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, this generates a request to the web-site containing a parameter value with malicious JavaScript code. If the web-site embeds this parameter value into the response HTML page (this is the essence of the site issue), the malicious code will run in the user's browser.

Open in new window

Il web-based training integrato facilita lo sviluppo di competenze interne

Cos'è AppScan Source Edition?

- Una soluzione Security Testing attraverso l'analisi statica del codice con il controllo centralizzato delle politiche di sicurezza.
- Consente alle aziende di creare, distribuire e applicare costantemente policy di sicurezza
- Automatizza i test di sicurezza integrando l'analisi statica del codice nel process di build

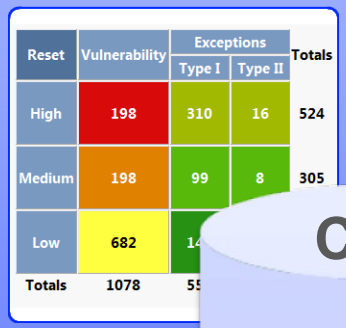
Benefici:

- Aiuta a rinforzare I team di application security, proteggendo i dati confidenziali e migliorando le compliance
- Permette di ridurre il costo effettivo della correzione delle vulnerabilità identificando le problematiche nelle prime fasi del ciclo di sviluppo

IBM Rational AppScan Source Edition Solution

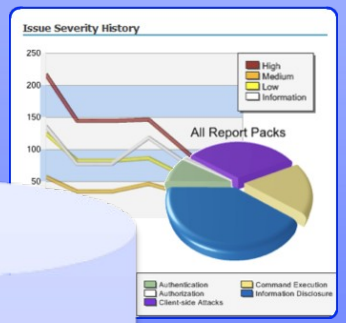
Security

- Configurazione
- Scansione
- Triage dei Risultati
- Gestione policy di sicurezza



Reset	Vulnerability	Exceptions		Totals
		Type I	Type II	
High	198	310	16	524
Medium	198	99	8	305
Low	682	14		
Totals	1078	55		

Reporting Console



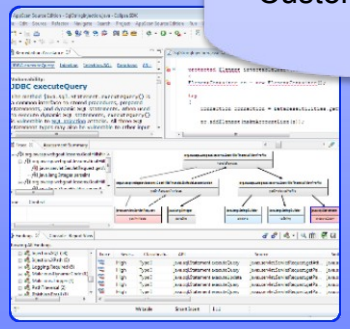
- Tracciamento degli avanzamenti
- Comparazione delle applicazioni
- Personalizzazione Dashboards
- Manage Portfolio Risk
- Combinazione dei risultati BB/WB

Core

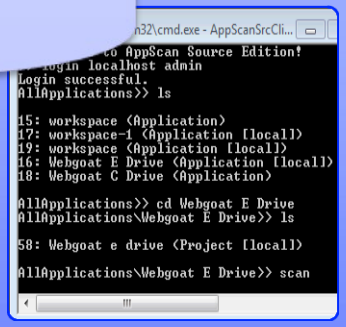
- Knowledgebase
- Assessment Database
- Custom Rules

IDE Plug-Ins

- Esaminare graficamente il flusso dati
- Guida alla risoluzione delle vulnerabilità
- Scansione
- Retest della Fix



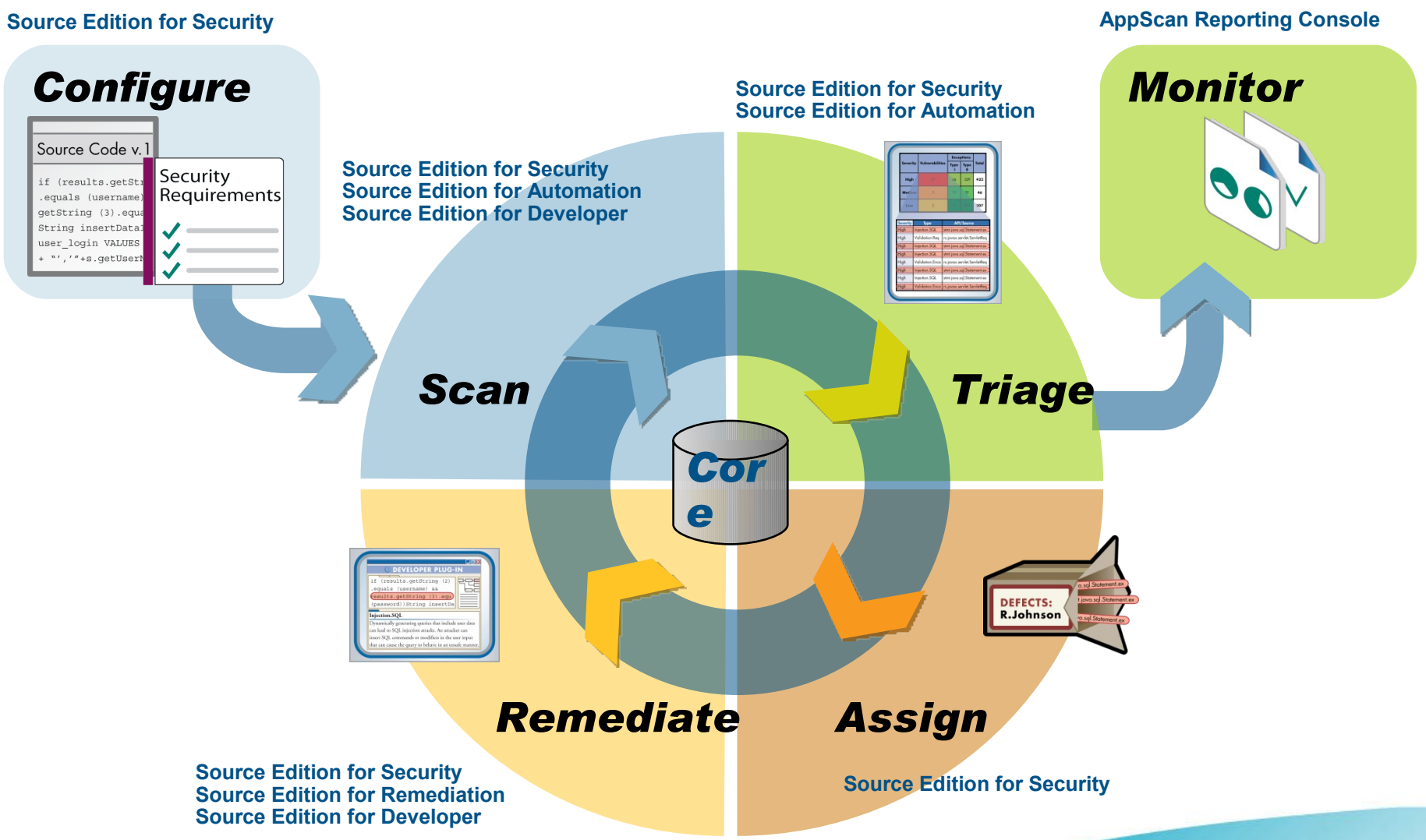
Automation



- Integrazione nella Build
- Automazione delle scansioni
- Integrazione con ANT, Make, Maven
- API per l'accesso ai dati

Unleash the Power of Innovation with
IBM Rational Solutions for Power

AppScan Source Edition Workflow



Unleash the Power of Innovation with
IBM Rational Solutions for Power

Cos'è AppScan Reporting Console?

- Un repository centralizzato per gli assessments sulle applicazioni Web
- Fornisce rapporti dettagliati e di alto livello dei problemi di sicurezza individuati
- Consente agli specialisti di Sicurezza di comunicare le issue identificate allo Sviluppo e al Management

Benefici:

- Offre la visibilità sui rischi di sicurezza e di compliance alle normative
- Consente la comunicazione e la collaborazione tra i diversi soggetti interessati

AppScan Reporting Console Workflows

Management
- Review most common security issues
- View trends
- Assess risk

Compliance Officers
- Review compliance reports

Developers
- View assessment results
- Remediate issues
- Assign issue status

Build automation
- Source code analysis for security issues as part of build verification
- Publish findings for remediation and trending

Tools:
- AppScan Source for Automation
- AppScan Standard Edition CLI

Security specialists
- Conduct security assessments
- Publish findings for remediation and trending

Tools:
- AppScan Standard Edition
- AppScan Source Edition

Unleash the Power of Innovation with
IBM Rational Solutions for Power

Unleash the Power of Innovation with
IBM Rational Solutions for Power