IBM Software Group

Web Application Security mit IBM Rational AppScan

Alexander Nenz

IBM Rational Software Group

Watchfire Sales Manager Germany

Troopers 2008, München 23.-24.04.08

Agenda

Warum “Web Application Security”?

Sicherheitslücken

Unsere Lösung “Rational AppScan”

Demo Appscan

Q&A

Der Mythos “Wir sind sicher”

Wir haben Firewalls

Wir lassen jedes Jahr ein Audit durchführen

Wir haben SSL Verschlüsselung

Wir haben Netzwerk-Scanner

Die Realität

“Hacker haben persönliche Informationen von 26.000 Mitarbeitern gestohlen.”

ComputerWorld, June 22, 2006

“Zwischen Juli 2005 und Juni 2006 wurde festgestellt, dass 69 % aller Web Applikationen angreifbar sind.”

Gartner

“64 % aller Entwickler sind nicht sicher, ob sie die Fähigkeit haben, sichere Applikationen zu schreiben.”

Microsoft Developer Research

“70 % aller Unternehmen wenden heute keine Sicherheitstechniken in der Softwareentwicklung an.”

Aberdeen Group, May 2007

Kosten fehlender Security

Hackers breach LexisNexis, grab info on 32,000 people

By Paul Roberts
IDG News Service, 03/09/05

Hackers have compromised databases belonging to LexisNexis and stolen information on at least 32,000 people, according to a statement Wednesday from LexisNexis' parent company, Reed Elsevier PLC.

The hackers stole passwords, names, addresses, Social Security and drivers license numbers of legitimate customers of the company's Seisint division. Seisint collects data on individuals that is used by law enforcement and private companies for debt recovery, fraud detection and other services.

LexisNexis identified the incidents in a review of security procedures and warned that there may be more incidents of data theft, Reed Elsevier said. The incident is eerily familiar to recent revelations about similar compromises at Seisint competitor ChoicePoint, which acknowledged in February that hackers had access to data on 145,000 people.

Reed Elsevier did not immediately respond to requests for comment.

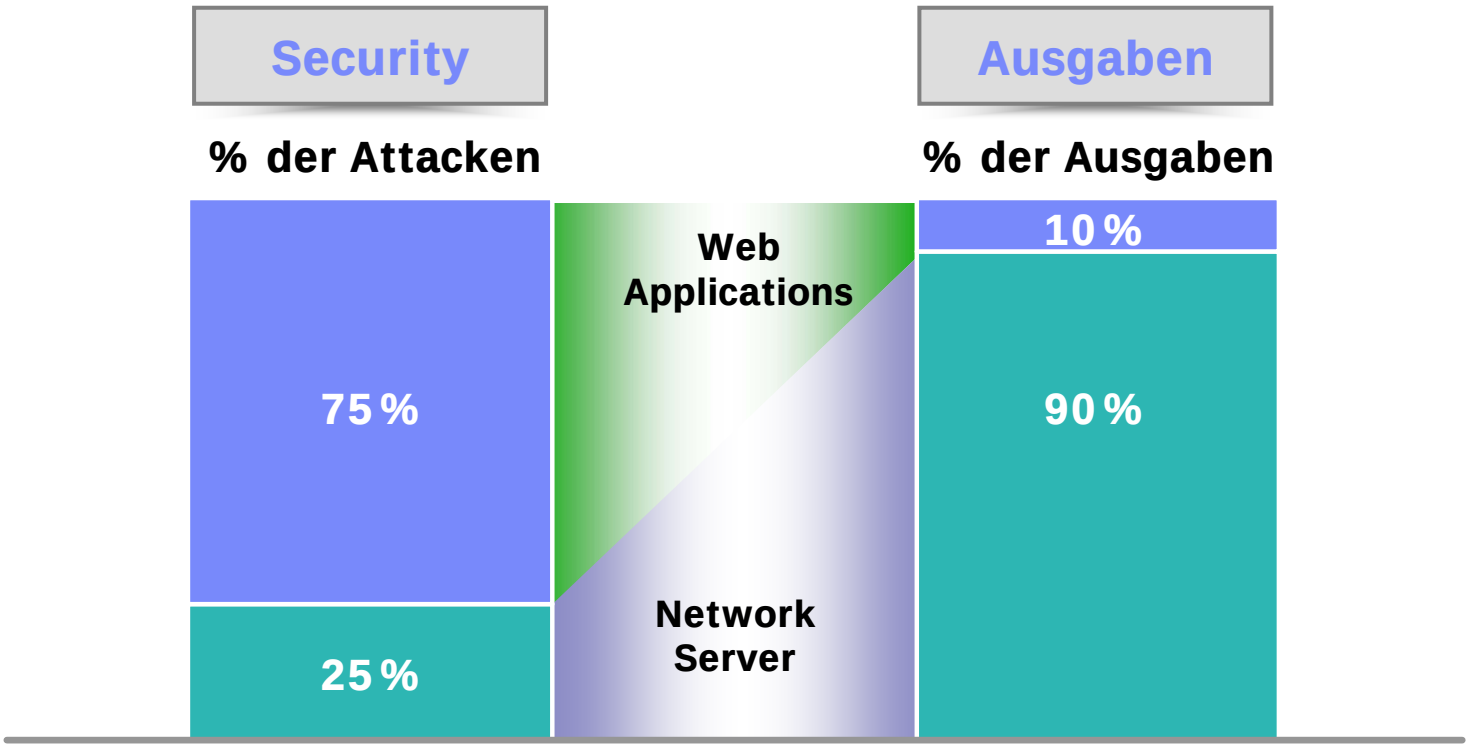
LexisNexis, which acquired Seisint of Boca Raton, Fla., in September for $775 million, expressed regret for the incident and said it is notifying the individuals whose information may have been accessed and will provide them with credit monitoring services.

The U.S. Secret Service is actively involved in an investigation of the incident, but declined to give any details about the case through spokesman Jonathan Cherry.

Like ChoicePoint, Se… g Social Security numbers, cre… behind the "Multistate Anti-Terr… id public

- Mediale Aufmerksamkeit
- Beschädigung der Marke
- Stark sinkende Aktienkurse
- Hohe Kommunikationskosten
- Gesetzliche Strafen
- Verstärkte Audits
- Klagewelle von Kunden
- Verlust von Kunden.

Ausgabenverteilung für Security



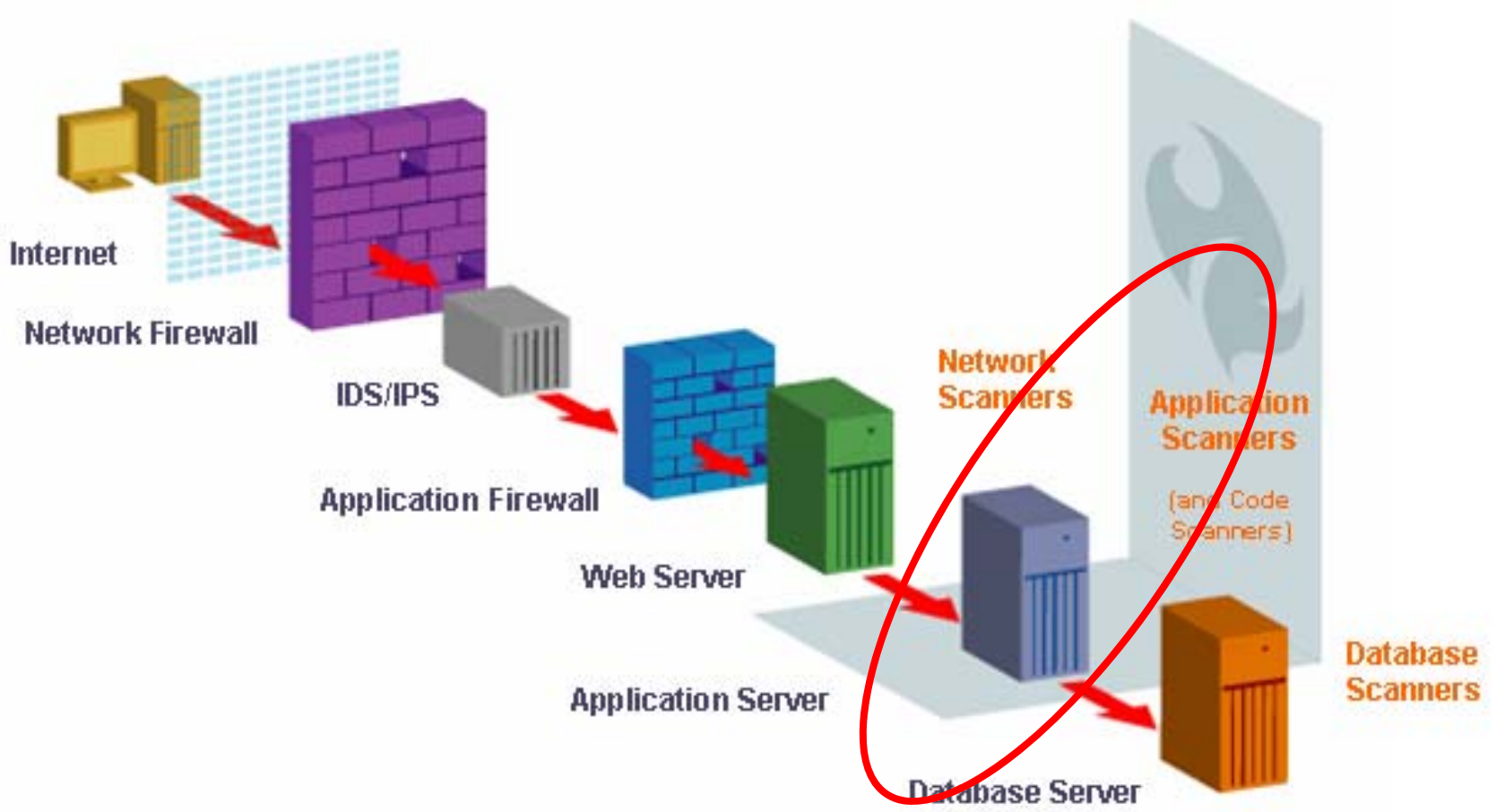
75% aller Attacken auf Informationssicherheit finden im Web Application Layer statt

2/3 aller Web Applicationen sind gefährdet.

Gartner

Sources: Gartner, Watchfire

Einordnung der „Application Security“

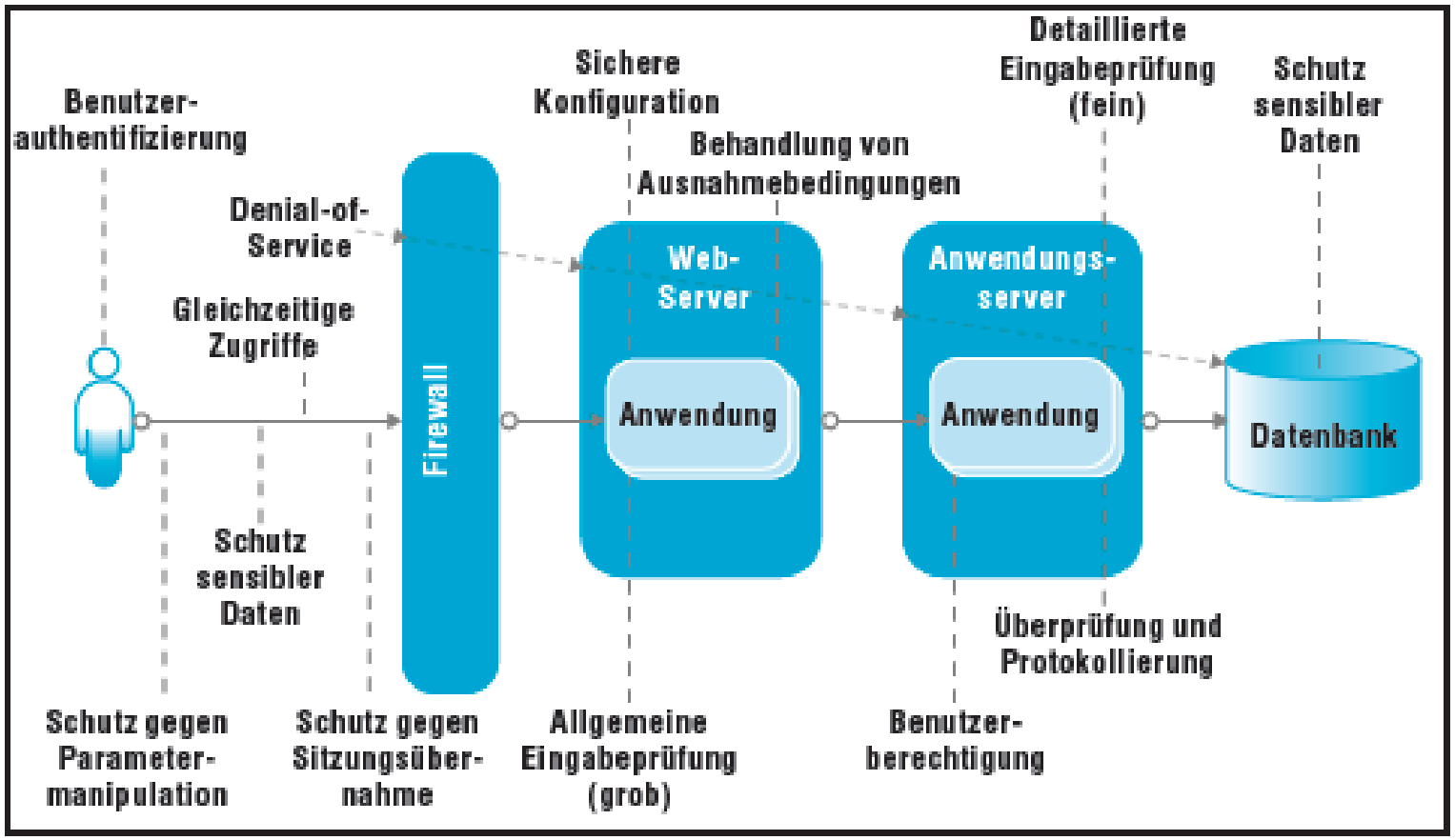


(IDS=Intrusion Detection System, IPS=Intrusion Prevention System)

Warum ist “Application Security” so wichtig?

- **Web Applikationen stehen an erster Stelle der Hacker Attacken**
  - 75% aller Attacken betreffen die Applikationsschicht (Gartner)
  - “XSS” und “SQL Injection” stehen an erster und zweiter Stelle der Attacken
- **Die meisten Sites sind angreifbar**
  - 90% aller Seiten sind angreifbar durch Applikations-Attacken (Watchfire)
  - 78% der einfach anwendbaren Attacken betreffen Web Applikationen (Symantec)
  - 80% aller Unternehmen werden bis 2010 mit Sicherheitsvorfällen konfrontiert werden (Gartner)
- **Web Applikationen sind für Hacker höchst interessant**
  - Zugriff auf persönliche Daten, Kundendaten, Unternehmensdaten, Kreditkarten usw.
- **Compliance Anforderungen werden verletzt**
  - Basel II, Datenschutzgesetze, SOX, Payment Card Industry (PCI) Standards, GLBA, HIPPA, FISMA.

Was muss “Application Security” leisten?



Agenda

Warum “Web Application Security”?

Sicherheitslücken

Unsere Lösung “Rational AppScan”

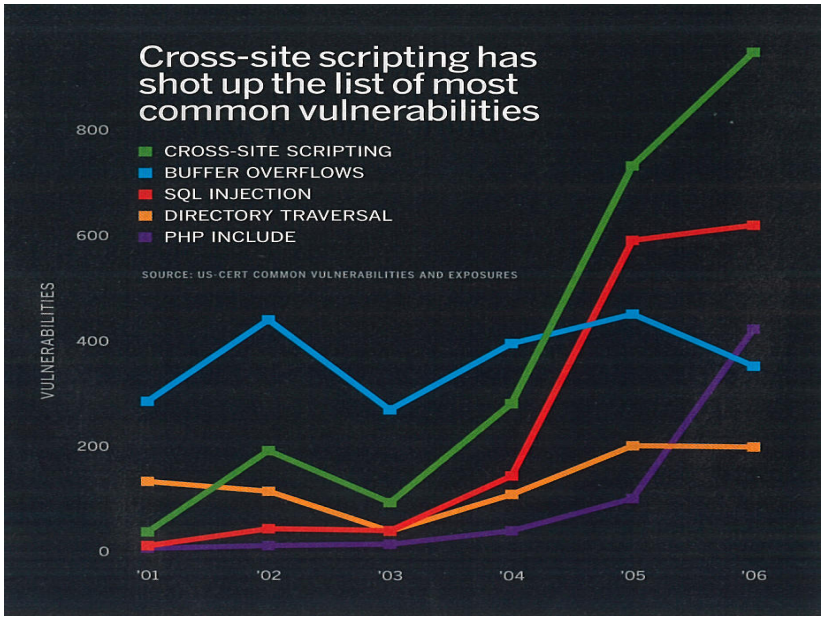
Demo Appscan

Q&A

Hacker Attacken …

- Vortäuschen einer anderen Identität (Impersonation)
- Aneignung von Berechtigungen (Elevation of Privilege).
- Manipulation von Daten während der Übertragung (Tampering)
- Einlesen von Informationen (Information Disclosure)
- Löschen des Nachweises einer getätigten Transaktion (Repudation)
- Verursachen einer Serverüberlastung (Denial-of-Service).

… und die Security Lücken



Top Ten des "Open Web Application Security Project" (OWASP)

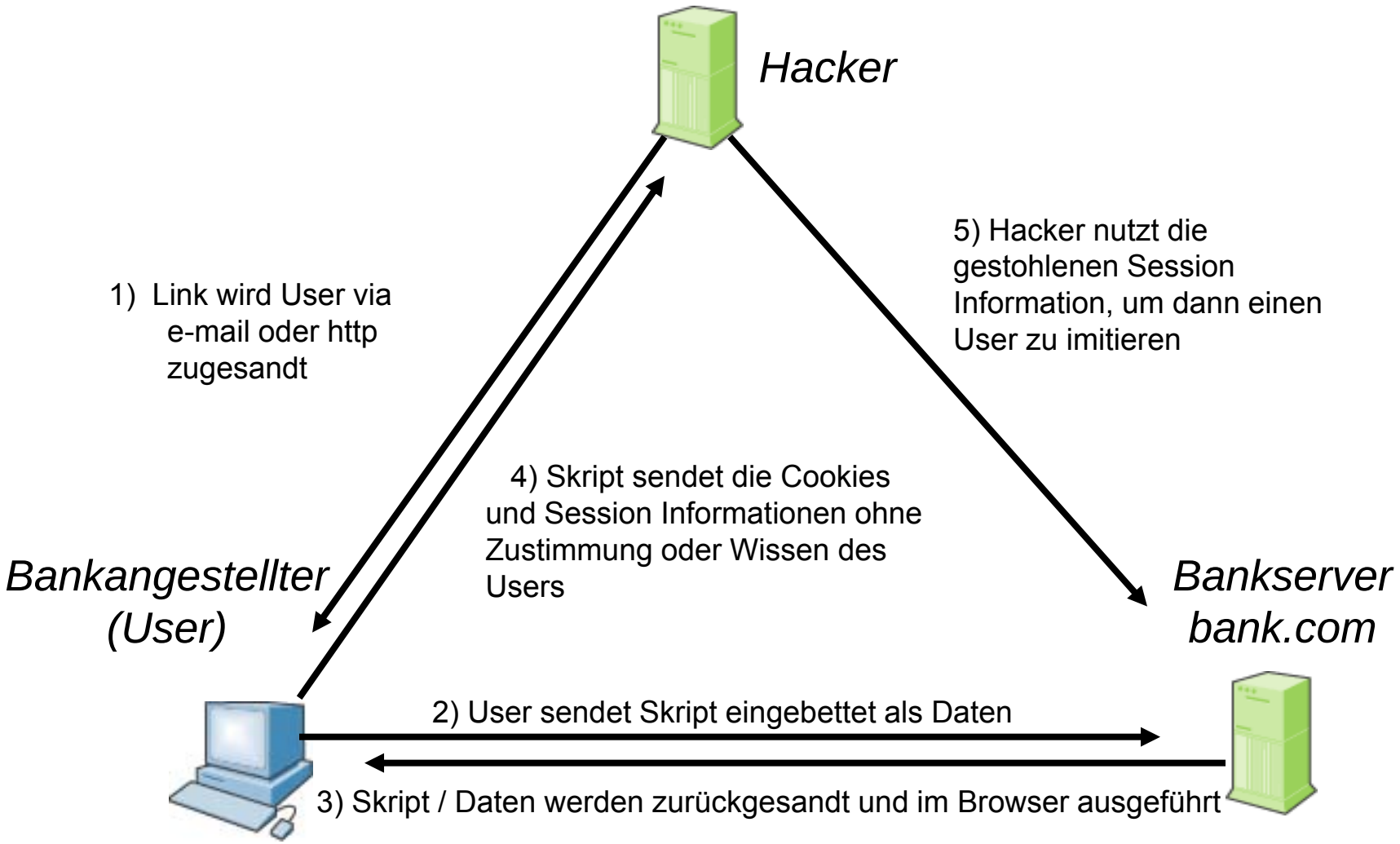
1. **"Cross-Site Scripting" (XSS)**
2. "Injection Flaws"
3. Verstecktes Execute einer Datei
4. Unsichere "Direct Object Reference"
5. Verfälschung eines "Cross-Site Requests"
6. Informationsverlust und falsches "Error Handling"
7. Abgebrochenes Authentication & Session Management
8. Unsichere Kryptografie
9. Unsichere Kommunikation
10. Fehler in der Abwehr eines URL Zugriffes.

1. Cross-Site Scripting (XSS)

- **Was ist das?**
  - Die Bezeichnung „Cross-Site“ leitet sich von der Art ab, wie dieser Angriff Web-Site übergreifend ausgeführt wird.
    - Der Hacker sendet dem Opfer einen präparierten Hyperlink zu, den er zum Beispiel in eine Webseite einbindet oder in einer E-Mail versendet.
    - Mit Hilfe entsprechender Techniken (URL-Spoofing, Kodierung) wirkt der Link unauffällig und vertrauenswürdig
    - Der Link enthält Code, der dann auf dem Client (z.B. im Webbrowser) des Opfers ausgeführt wird.

- **Was wird damit bewirkt?**
  - Mit Hilfe der Ausführung des Codes werden vertrauliche Informationen des Clients und damit des Opfers an den Hacker versandt und/oder manipuliert, z.B.
    - Seiteninhalte, Login Daten, Persönliche Daten aus den Cookies, Session-ID ....
  - Der Hacker bekommt Herrschaft über
    - Jede Aktion der Opfers, Seiteninhalte, Folgeseiten, … bis zur Herrschaft über das System.

XSS – Beispiel Bankanwendung - Prozess



Agenda

Warum “Web Application Security”?

Sicherheitslücken

Unsere Lösung “Rational AppScan”

Demo Appscan

Q&A

Was der Markt sagt...

InformationWeek
DEFINING THE BUSINESS VALUE OF TECHNOLOGY

Powered by techweb NETWORK

- **IBM's Watchfire AppScan was a no-brainer** for the Editor's Choice award. Not only was it the only entry to fulfill the original purpose of the review--Ajax scanning--it met or exceeded the best features of all the other products without any of the accompanying problems. We recommend it for any company concerned about Web 2.0 security.

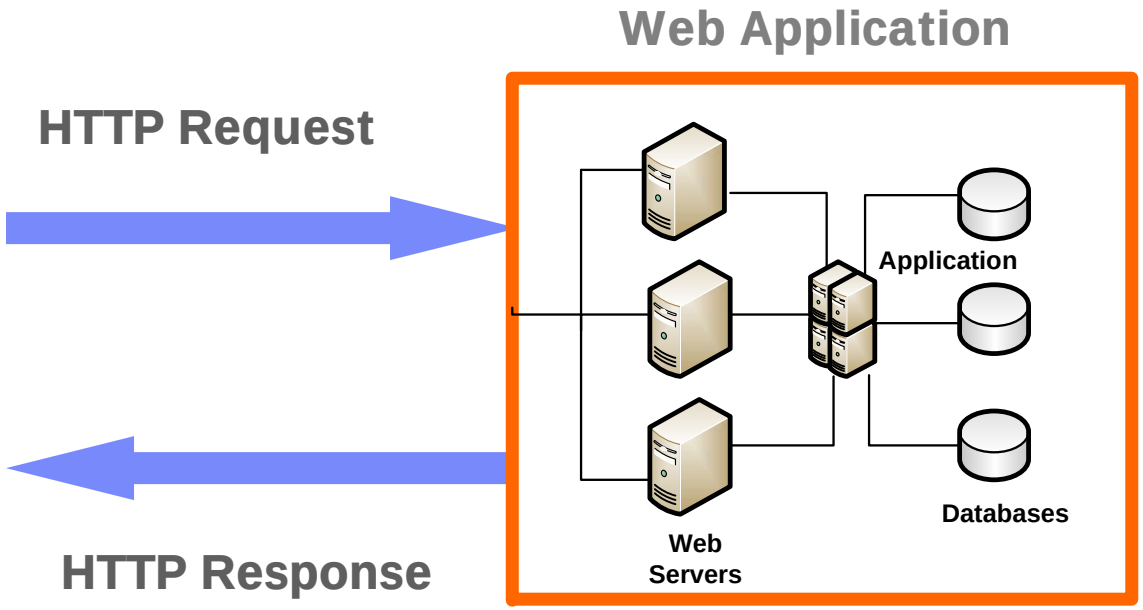
- http://www.informationweek.com/news/security/showArticle.jhtml;jsessionid=MXWOIPW2FRNQOQSNDLOSKH0CJUNN2JVN?articleID=202201216&_requestid=877479

Was ist Rational “AppScan”?

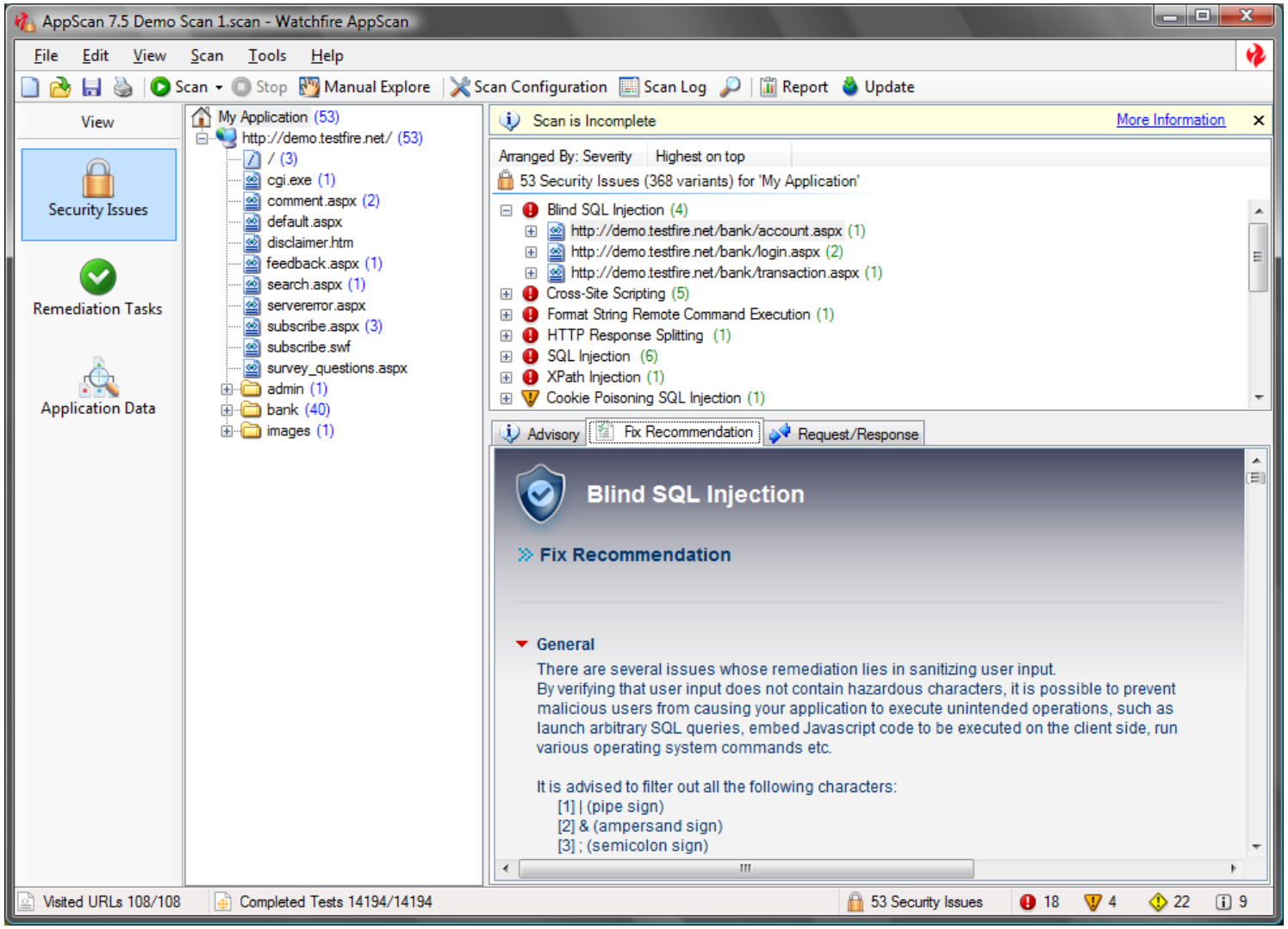
- Ein automatisiertes Testtool zum Aufdecken von Sicherheitslücken in Webanwendungen
- Ein Paket mit Dienstprogrammen, mit dem Tester und Sicherheitsberater Webanwendungen entwickeln und testen und ein Debugging vornehmen können
- Eine Suite mit führenden Sicherheitslösungen für Webanwendungen, die Unternehmen die erforderliche Transparenz und die entsprechenden Kontrollmechanismen zur Verfügung stellt
- Ein Tool für Hackersimulationen unter Berücksichtigung der Top 10 Sicherheitslücken des Open Web Application Security Project (OWASP) und der „Top 20 Vulnerabilities“ des System Administration, Networking, and Security Institute (SANS)
- Ein Informationsdienst zu den neuesten Bedrohungen, die automatisch aktualisiert werden, wenn ein Rational AppScan-Produkt gestartet wird.

Wie arbeitet AppScan?

- Behandelt eine Applikation als Black-Box
- Durchläuft eine Webanwendung und bildet Site Modelle
- Bestimmt die Attacken Szenarien basierend auf der Test Policy
- Testet, indem es modifizierte http Requests an die Applikation sendet und den http Response entsprechend der Validierungsregeln überprüft.



Beispiel eines Scans



Die Disziplinen von Rational AppScan

Security

Privacy

Quality

Standards

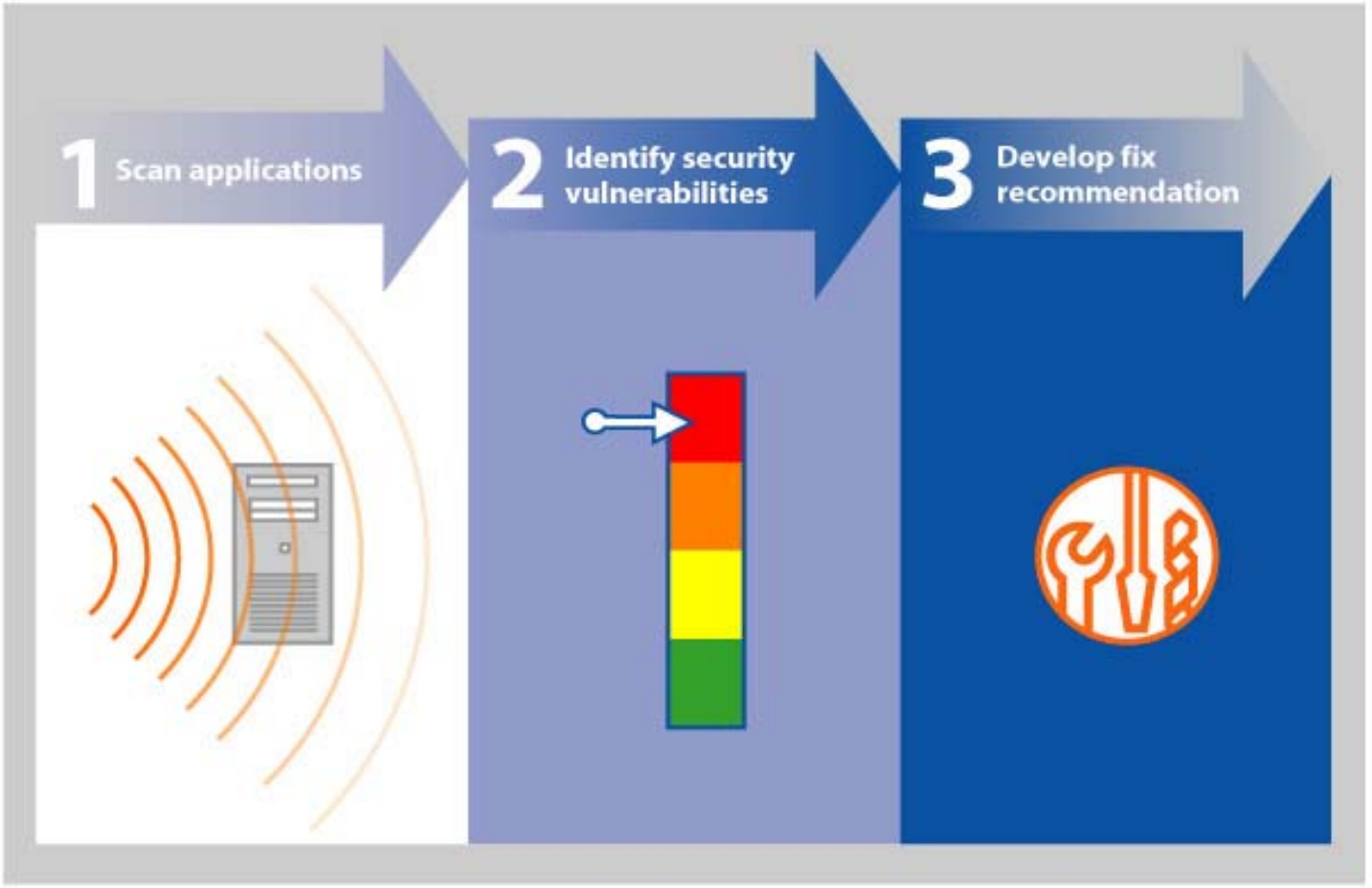
Compliance

1 Scan

2 Analyze

3 Report

AppScan bietet auch Lösungen für die Probleme



Was bietet “AppScan” insbesondere für Führungskräfte?

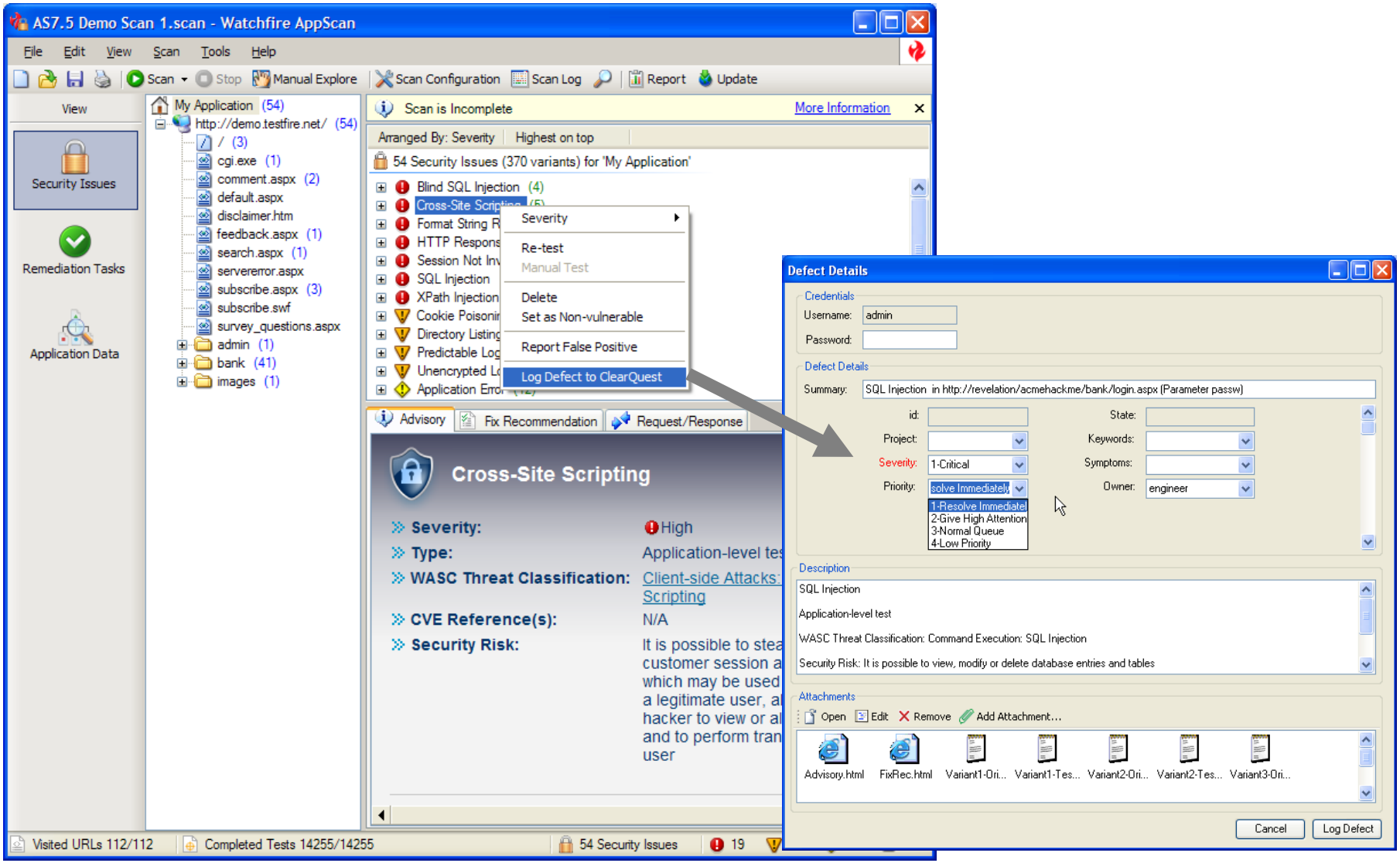
- Zentrale Überwachung und Steuerung der unternehmensweiten Tests zur Ermittlung von Sicherheitslücken bei Webanwendungen.
- Reports und Statusansichten für Führungskräfte (Dashboards)
- Deltaanalyseberichte zur Verdeutlichung der Änderungen zwischen einzelnen Scans, einschließlich korrigierter, anstehender und neuer Sicherheitsprobleme
- Integrierte Trainings-Module für das Verstehen der Sicherheitslücken und der Erläuterung von Scan-Ergebnissen.

Beispiel eines Reports

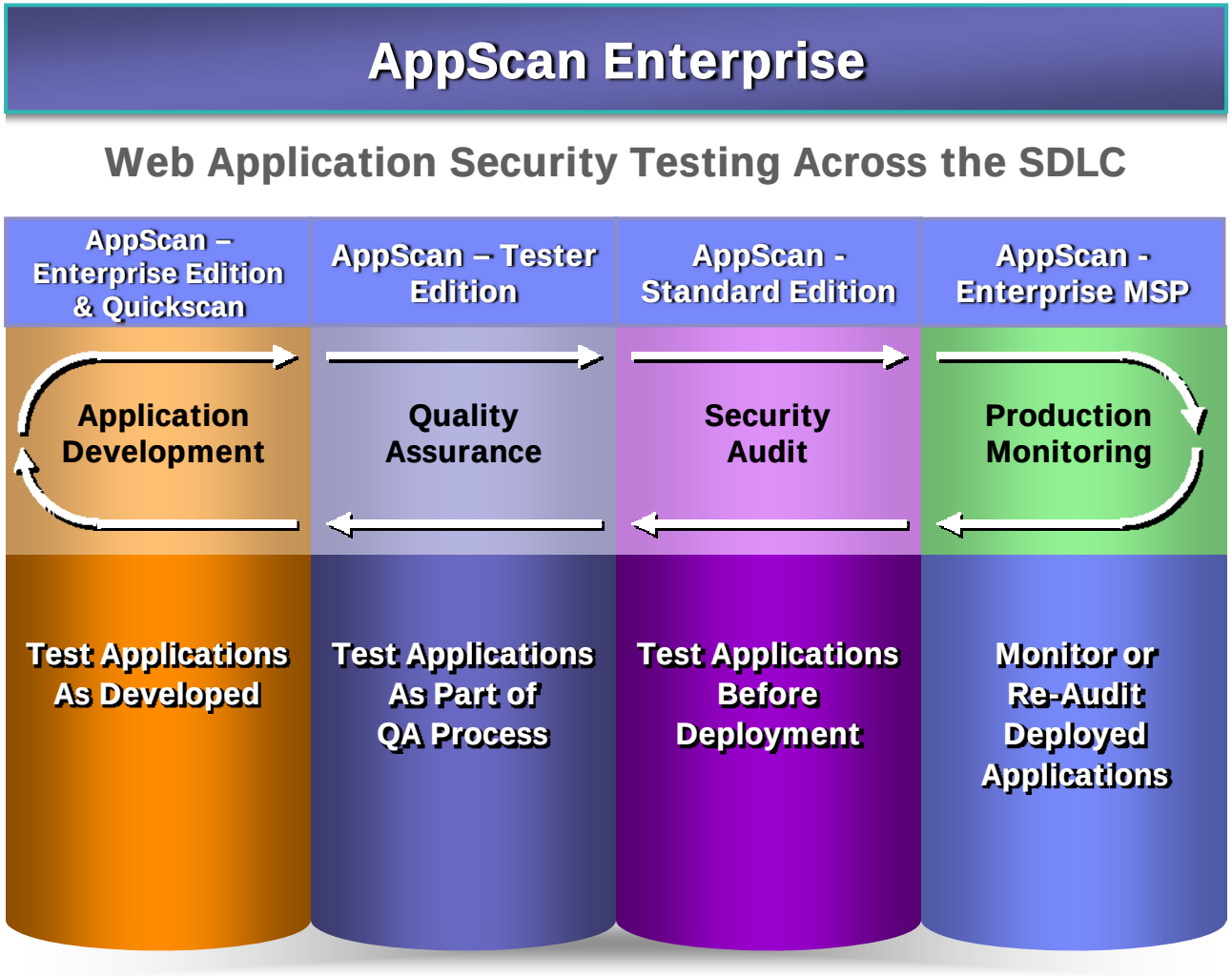
Welche Features bietet “AppScan”?

- Eine Benutzeroberfläche mit wählbaren Ansichten für die Anwendungs-baumstruktur, der gefundenen Sicherheitsprobleme und Korrekturansichten für Entwickler
- Einen anpassbaren Testprozess mit der Möglichkeit, Anwendungsparameter zu analysieren und nur relevante Tests auszuwählen
- Unterstützung komplexer Authentifizierungen wie z. B. gestufte CAPTCHA-Authentication, One-time Passwords, USB-Keys und Smart Cards
- Ansichten mit Echtzeitergebnissen, die es den Benutzern ermöglichen, Probleme schon zu bearbeiten, bevor der Scanvorgang beendet ist
- Suchregeln nach Mustern (Pattern), die bestimmte Sicherheitstests vereinfachen (z. B. im Zusammenhang mit Kreditkarten- oder Sozialversicherungsnummern oder anderen Ziffernfolgen)
- Detaillierte Berichte zu verdächtigen Inhalten, in denen z. B. sensible Daten in html-Kommentaren oder http-Aktivitäten im Zusammenhang mit verrdächtigen Inhalten aufgezeichnet sind.

AppScan kann Defect in Rational ClearQuest einstellen



Rational AppScan Suite



Agenda

Warum “Web Application Security”?

Sicherheitslücken

Unsere Lösung “Rational AppScan”

Woher kommt AppScan? Was ist Watchfire?

- 1996: Watchfire Gründung in Boston
- Entwicklung der Applikation Security Lösung (AppScan)
- 2006: Gartner Marktführer in “Application Security 2006”
- 2007: SC Magazine Award als “Best Security Company”
- Mehr als 800 Referenzen
- 2007: Akquisition durch IBM

#1 in Market Share for Application Security
– Gartner & IDC

Value Propostition

- Automatisches Scannen und Testen und damit Zeitersparnis für Entwickler, Prüfer, Penetrationstester und Consultants
- End-to-End Solution mit dem Ziel, Anzahl der Schwachstellen in Zukunft zu minimieren, andere Anbieter melden lediglich die Schwachstellen
- Umfassendste Lösung für Security und Compliance Reporting (40 verschiedene Templates) und damit auch schnellere Audits.

Watchfire - mehr als 800 Referenzen

9 der Top 10 größten US Banken	8 der Top 10 Technologie Unternehmen	7 der Top 10 Pharma Unternehmen	Grosse Öffentliche Kunden
Bank of America – Higher Standards	IBM	Wyeth	Veteran's Affairs
citi	Microsoft	Novartis	Army
JPMorgan	intel	AstraZeneca	Navy
Wells Fargo	Nokia	Abbott Laboratories	Air Force
Wachovia	Cisco Systems	Aventis	Marines
Washington Mutual	Sony	Roche	Social Security USA Administration
US Bank	Dell	Genentech – In Business For Life	United States Postal Service
SunTrust	Canon		

Hilfreiche Links und Informationen

- Hacking 101
  https://admin.acrobat.com/_a305137129/p74478601/
- Integrating Security into QA's Current Testing Processes
  https://admin.acrobat.com/_a305137129/p68873403
- Moving Application Security Testing into QA
  https://admin.acrobat.com/_a305137129/p68873403/
- AppScan Demo
  http://www.watchfire.com/products/appscan/axfdemo.aspx
- Watchfire Discovers Google Desktop Vulnerability that Hackers Could Exploit to Gain Full System Control
  http://download.watchfire.com/googledesktopdemo/index.htm

… und ein Datenblatt und ein White Paper auf deutsch.

Vielen Dank für Ihre Aufmerksamkeit!!!

Kontakt:

Alexander Nenz

Nenz@de.IBM.com