



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.

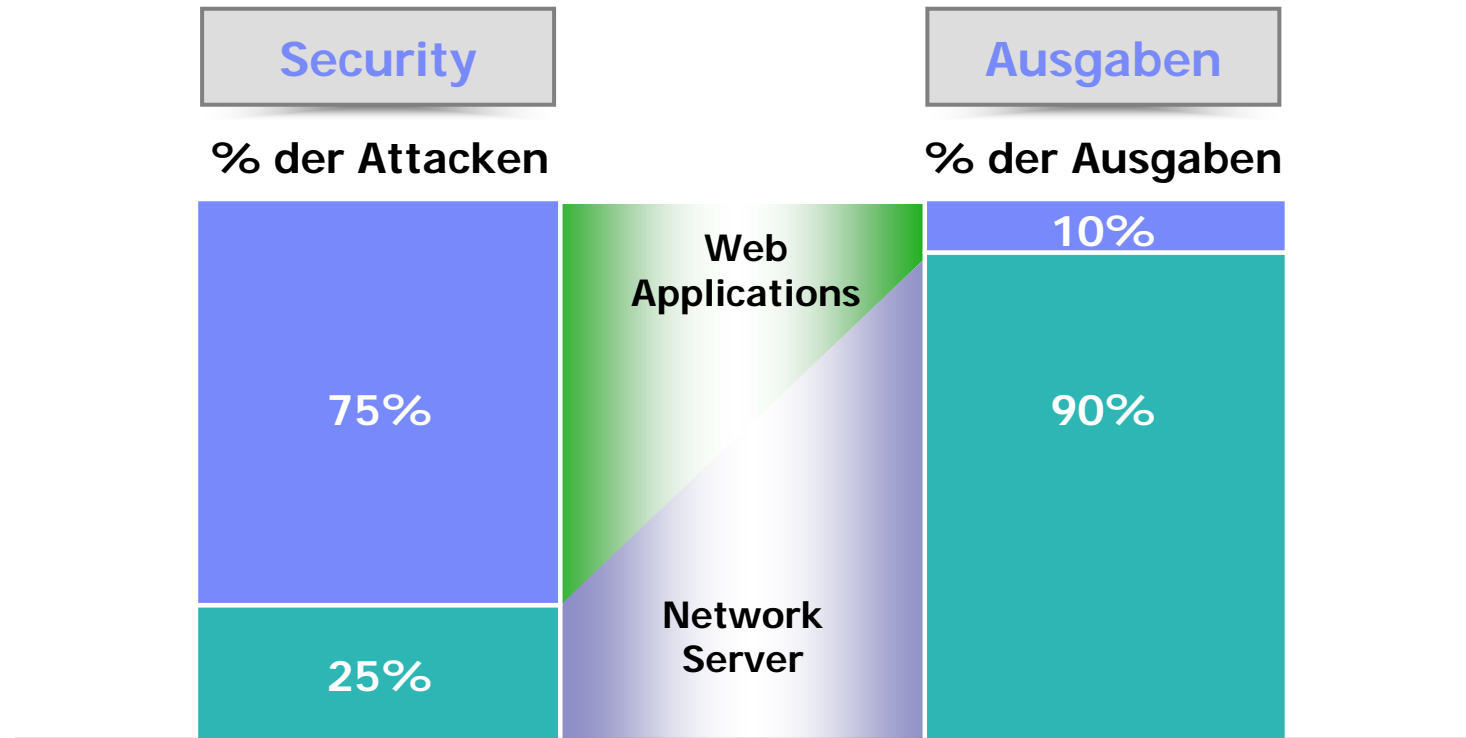
Like ChoicePoint, Seisint collects Social Security numbers, credit card numbers and other sensitive information. "Multistate Anti-Terrorism Information System"



g Social
behind the
and public

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

Ausgabenverteilung für Security



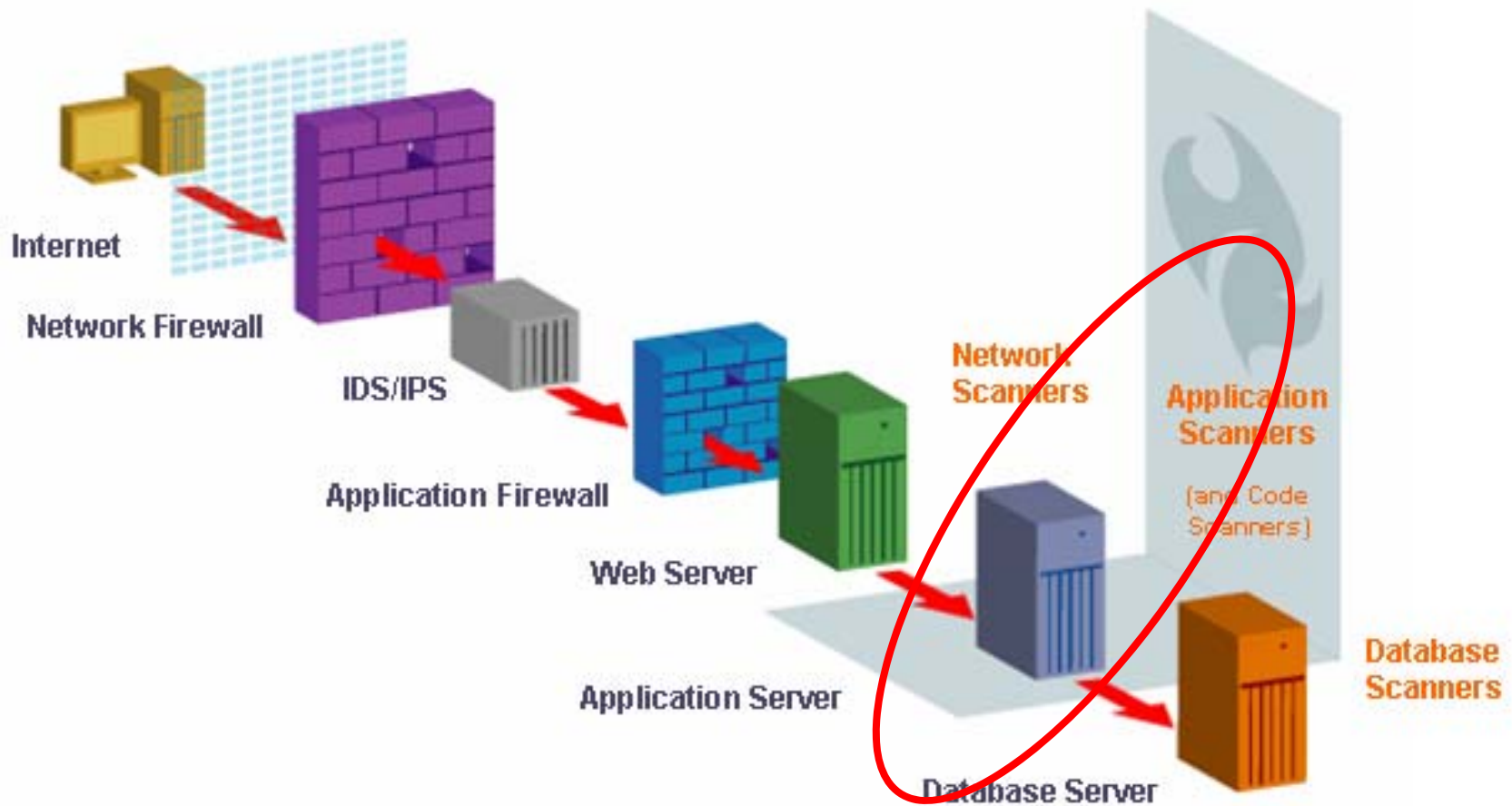
75% aller Attacken auf Informationssicherheit finden im Web Application Layer statt

2/3 aller Web Applications sind gefährdet.

Gartner

Sources: Gartner, Watchfire

Einordnung der „Application Security“



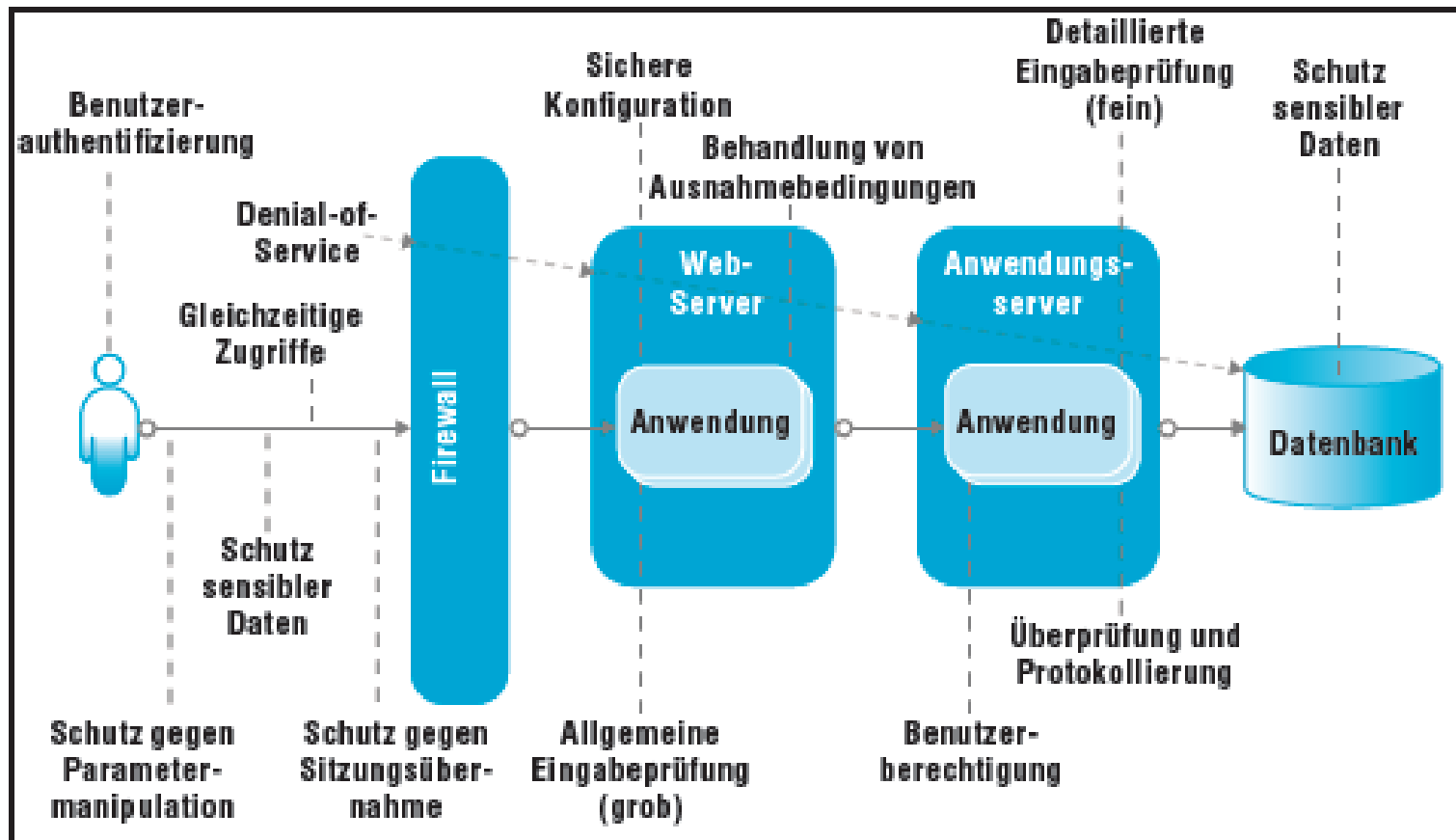
(IDS=Intrusion Detection System, IPS=Intrusion Prevention System)

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 ...

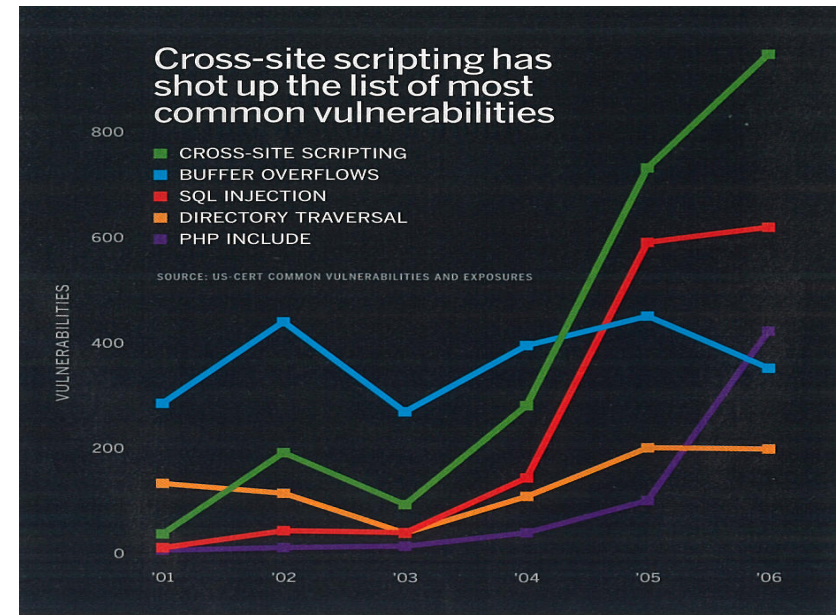
- Vortäuschen einer anderen Identität (Impersonation)
- Aneignung von Berechtigungen (Elevation of Privilege).
- Manipulation von Daten während der Übertragung (Tampering)
- Einlesen von Informationen (Information Disclosure)
- Löschen des Nachweises einer getätigten Transaktion (Repudation)
- Verursachen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

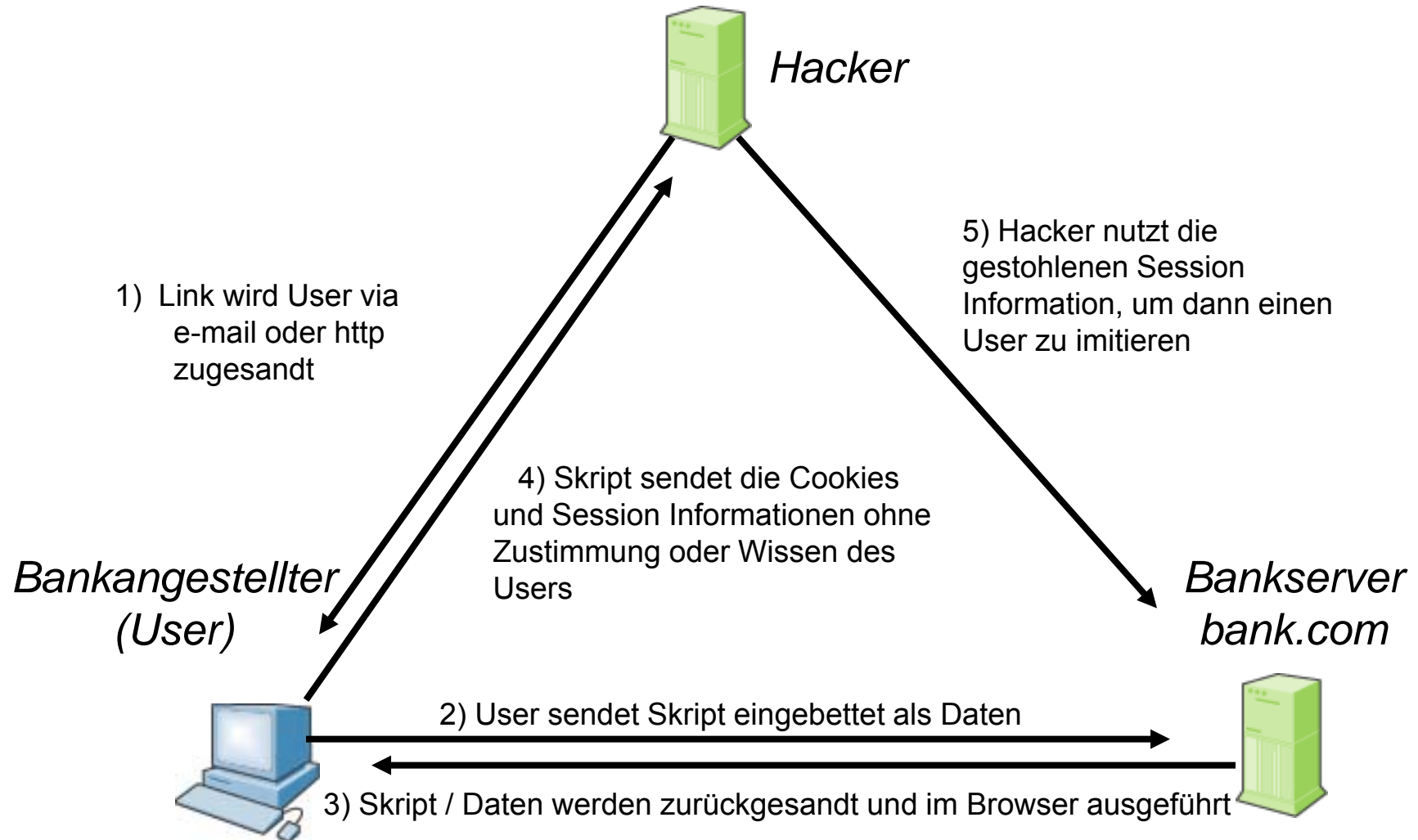
- **Was ist das?**

- ▶ 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

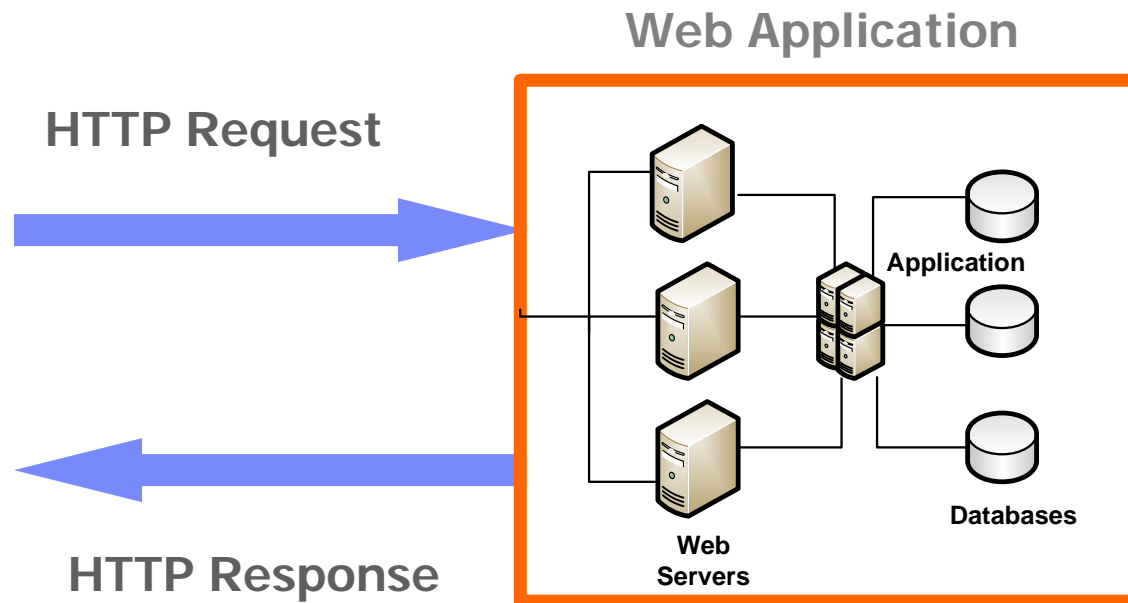
- **IBM's Watchfire AppScan was a no-brainer** for the Editor's Choice award. Not only was it the only entry to fulfill the original purpose of the review--Ajax scanning--it met or exceeded the best features of all the other products without any of the accompanying problems. We recommend it for any company concerned about Web 2.0 security.
- http://www.informationweek.com/news/security/showArticle.jhtml;jsessionid=MXWOI PW2FRNQOQSNDLOSKH0CJUNN2JVN?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

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

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)

Security Issues

Remediation Tasks

Application Data

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

Die Disziplinen von Rational AppScan



Security



Privacy



Quality



Standards



Compliance

1

Scan

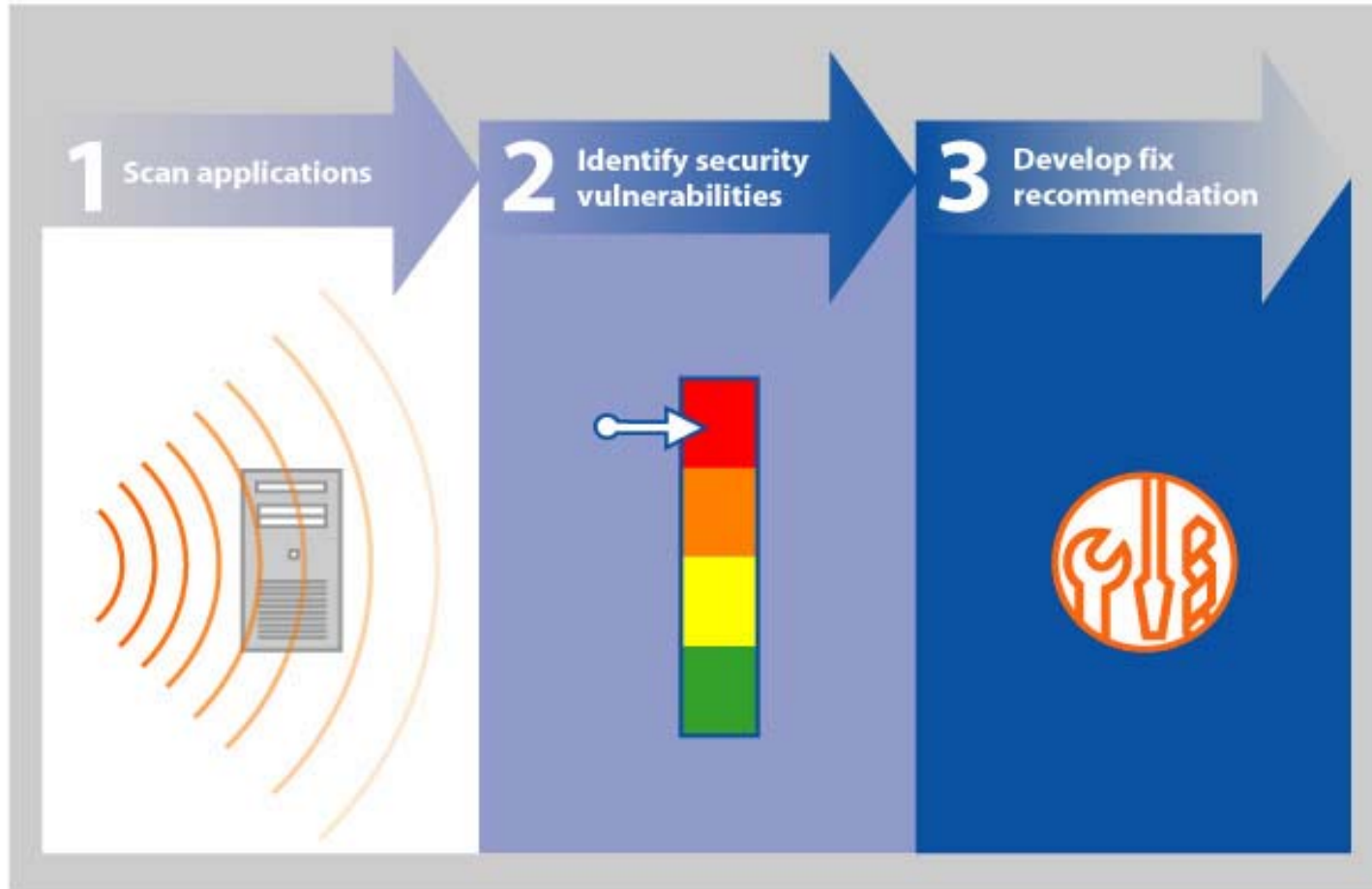
2

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

Rational AppScan Enterprise Edition | Jim (Analyst) | Help | Support | About | Log Out

Training | Jobs & Reports | Administration

Jobs & Reports > Acme Hackme > Analysts

Folders

- Acme Hackme
 - Analysts
 - Frank
 - Jim
 - Developer's
 - Admin
 - Andrew
 - Chris
 - Jennifer
 - Templates

Analysts - Graphical | Last Updated: 9/11/2007 12:56:50 PM

Details | Graphical

Report Pack: All Report Packs [Apply]

Issue Severity History

Issue Management History

Issue Severity by Report Pack

WASC Threat Classification

Recently Viewed

- Analysts
- Applications
- Security Issues (Investment Banking)
- Report Pack Summary (Investment Bank)
- Sarbanes-Oxley Act (SOX) (Investment)
- Activity Log (Test Admin)
- Report Pack Summary (Test Admin)
- Personal Banking

Welche Features bietet “AppScan”?

- Eine Benutzeroberfläche mit wählbaren Ansichten für die Anwendungsbaumstruktur, 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

The screenshot displays the Watchfire AppScan interface. On the left, a tree view shows the application structure under 'My Application (54)', including folders like 'admin (1)', 'bank (41)', and 'images (1)'. The main pane shows a list of security issues, with 'Cross-Site Scripting (5)' selected. A context menu is open over this issue, with the option 'Log Defect to ClearQuest' highlighted. An arrow points from this menu item to a 'Defect Details' dialog box.

The 'Defect Details' dialog box contains the following information:

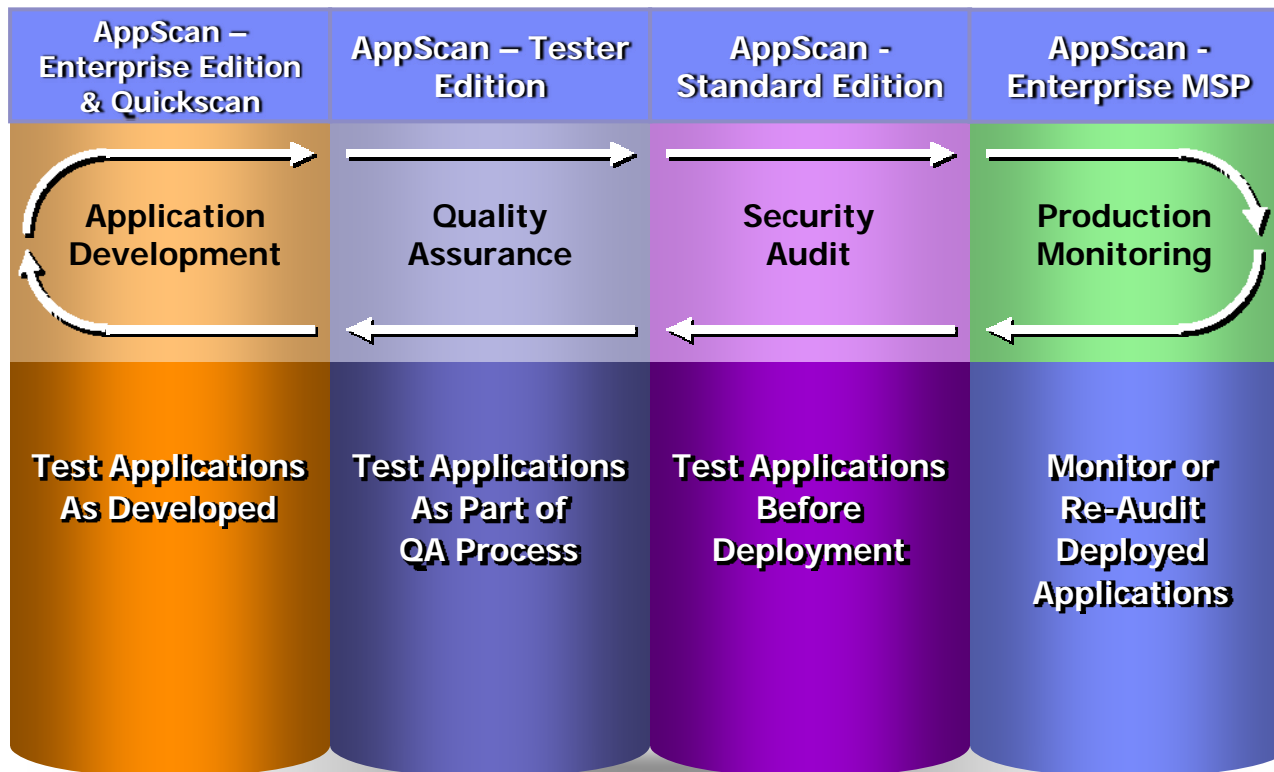
- Credentials:** Username: admin, Password: [empty]
- Defect Details:** Summary: SQL Injection in http://revelation/acmehackme/bank/login.aspx (Parameter passw)
- Configuration:**
 - Project: [dropdown]
 - State: [dropdown]
 - Severity: 1-Critical
 - Priority: solve Immediately
 - Keywords: [dropdown]
 - Symptoms: [dropdown]
 - Owner: engineer
- Description:** SQL Injection, Application-level test, WASC Threat Classification: Command Execution: SQL Injection, Security Risk: It is possible to view, modify or delete database entries and tables.
- Attachments:** Advisory.html, FixRec.html, Variant1-0ri..., Variant1-Tes..., Variant2-0ri..., Variant2-Tes..., Variant3-0ri...

At the bottom of the dialog, there are 'Cancel' and 'Log Defect' buttons.

Rational AppScan Suite

AppScan Enterprise

Web Application Security Testing Across the SDLC



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 Proposition

- 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

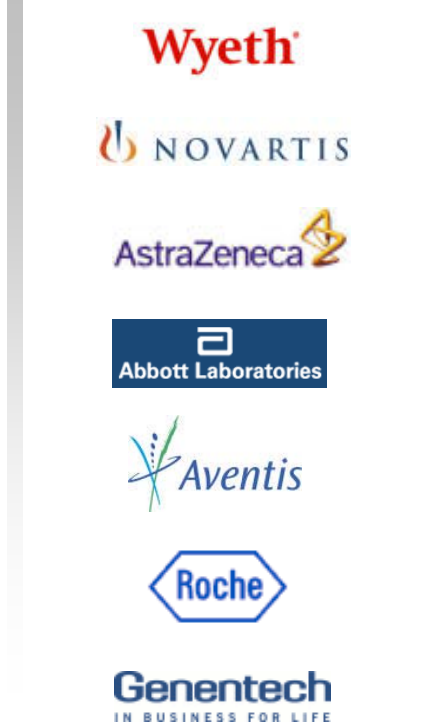
9 der Top 10
größten
US Banken



8 der Top 10
Technologie
Unternehmen



7 der Top 10
Pharma
Unternehmen



Grosse Öffentliche
Kunden



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.



IBM Software Group

Vielen Dank für Ihre Aufmerksamkeit!!!

Kontakt:

Alexander Nenz

Nenz@de.ibm.com

