



IBM Rational AppScan

Web Uygulamaları Güvenliđi & IBM Rational AppScan

Mehmet ađrı ELİBOL
Rational Ürün Teknik Satıř Uzmanı
cagrie@tr.ibm.com

Gündem

- Web Uygulamaları Güvenliği
 - Genel Bakış
 - Endüstriyel Durum
- Uygulama Güvenliği Açıkları
 - WASC, OWASP ve The OWASP Top Ten
 - 2 Yüksek Seviyeli Atağı İnceleme
- IBM Rational AppScan Ailesinin Ürünlerinin Tanıtımı
- Sorular ve Cevaplar

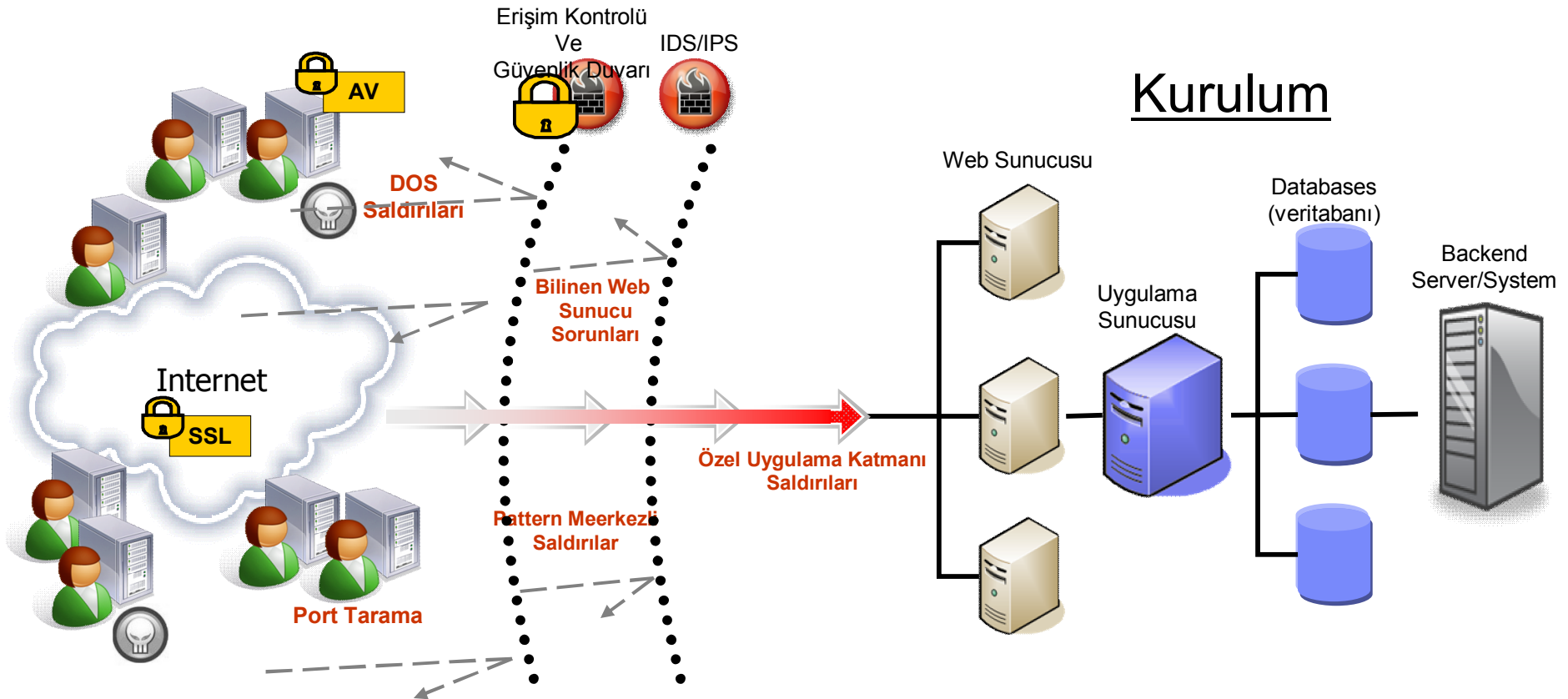


IBM Rational AppScan

Uygulama Güvenliđi

Endüstriyel Durum

Basit Güvenlik Görünümü



Saldırı Gerçekleri

**LexisNexis
Veri Açığı**

— Washington Post
Feb 17, 2008

**IndiaTimes.com
Kötü Amaçlı Yazılım**

— InformationWeek
Feb 17, 2008

**Mac blogları XSS ile
Hacklendi**

The Register, Feb 17, 2008

**Çinli Hacker 18M
Bilgileri Çaldı**

— HackBase.com, Feb
10, 2008

**Ekvator
Cumhurbaşkanlığı
Websitesi Hacklendi**

— The Indian, Feb 11, 2008

**Yunan Bakanlığında
Hacker Saldırıları**

— eKathimerini, Jan 31, 2008

**Hacker Davidson
İstemci Verilerini Çaldı**

— Falls Tribune, Feb 4 2008

**Ücretsiz MacWorld
Expo Platinum Pass**

— CNet, Jan 14, 2008

6 Aşamada Hackleme

— Wikipedia, Feb 9 2007

**Hacker
Pennsylvania gvmnt 'i
Alasağı Eder**

AP, Jan 6, 2008

**Drive-by Pharming in
the Wild**

— Symantec, Jan 21 2008

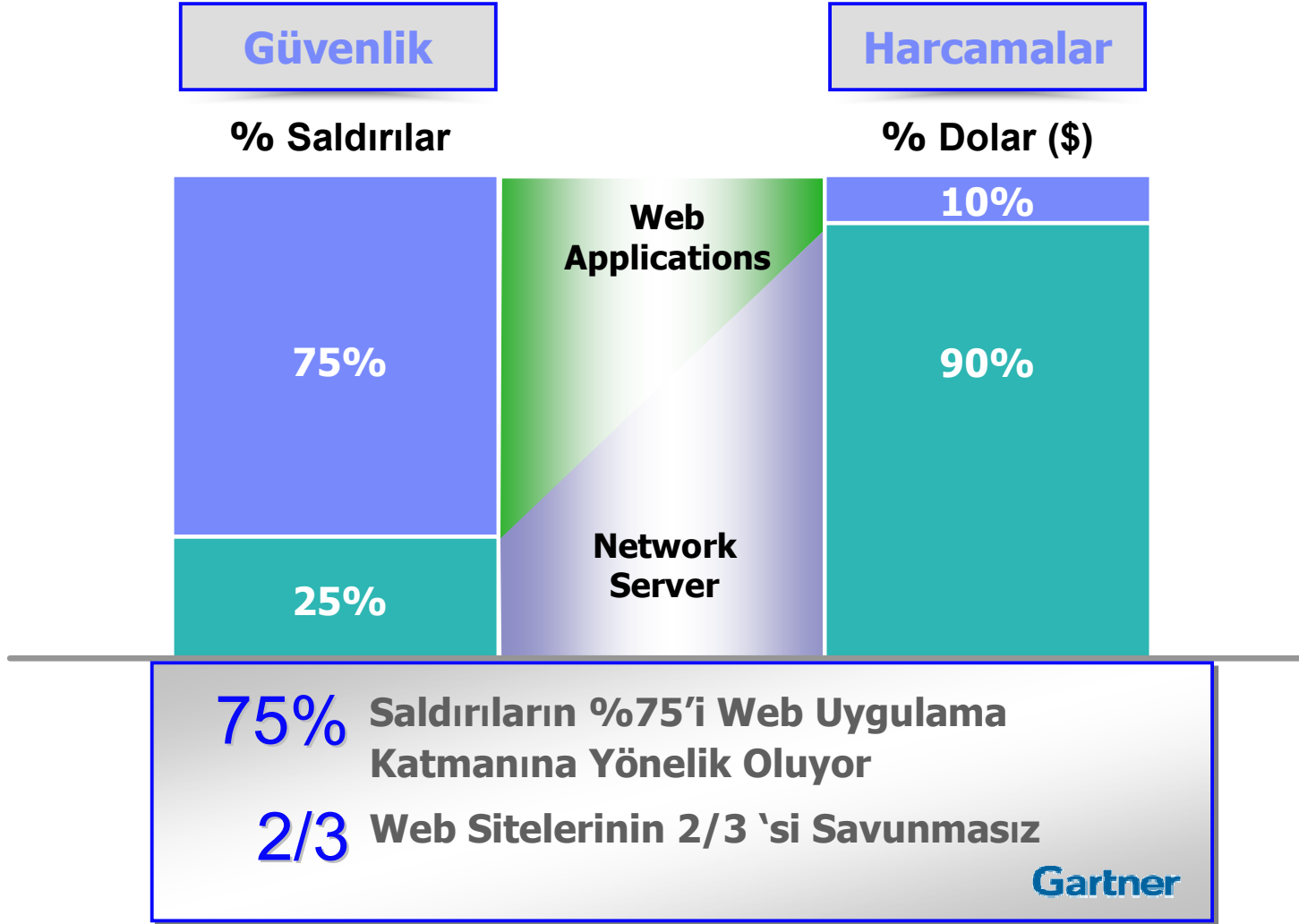
**RIAA wiped off the
Net**

— The Register, Jan 20 2008

**Dolandırıcılar
İtalyan Bankasını
Çarptı**

— Netcraft, Jan 8
2008

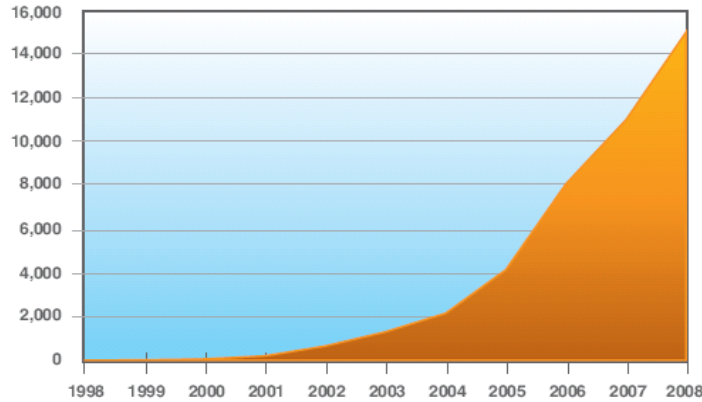
Uygulama Katmanı Açıkları: Genel



Kaynaklar: Gartner, Watchfire

Hackerlar Web Uygulamalarına Odaklanmaya Devam Ediyorlar ... çünkü web uygulamaları en kolay giriş noktalarıdır ve uygulamaların yürütümünde veri değişiminin önemi göz ardı edilemez.

Web Uygulamalarında Güvenlik Açıklarındaki Artış



Web uygulamaları Saldırı Tehtidi Altında!

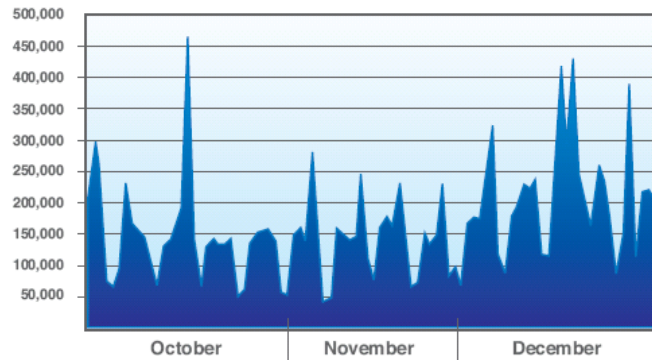
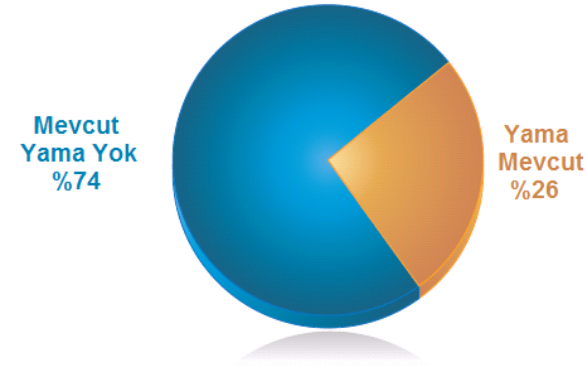


Figure 21: SQL Injection Attacks Monitored by IBM ISS Managed Security Services, Q4 2008

Source: 2008 IBM ISS X-Force Annual Report

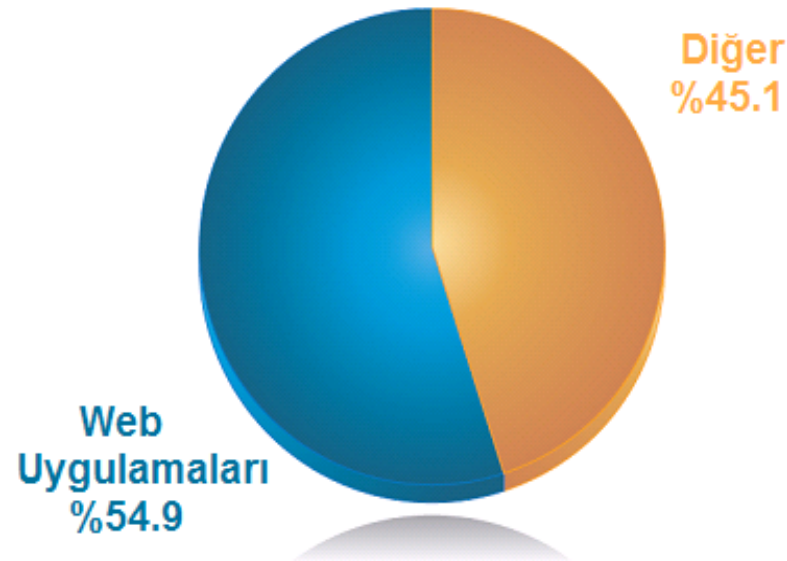
Web Uygulamaları Güvenlik Açıkları Yüzdesi (yamalarla birlikte)



- 2008 yılında IBM Mss milyonlarca SQL Injection Saldırılarına Tanık Olmuştur
- Hackerların Hedefledikleri Çaldıkları Verilerle Yasal, Meşru Siteleri Zararlı Sitelere Yönlendirmektedir
- 2008 Açıklamalarına Göre Güvenlik Açıkları %90 Oranında Uzaktan Ele Geçirilebilir Vaziyettedir
- Hackerler Son Derece Karmaşık Ve Kötü Niyetli Teknikleri Verilerinizi Çalmak İçin Kullanır
- Web Sunucuları Üzerindeki Saldırıları Son 6 Ay İçinde Eşi Görülmemiş Derecede Artış Göstermiştir(30 kat)

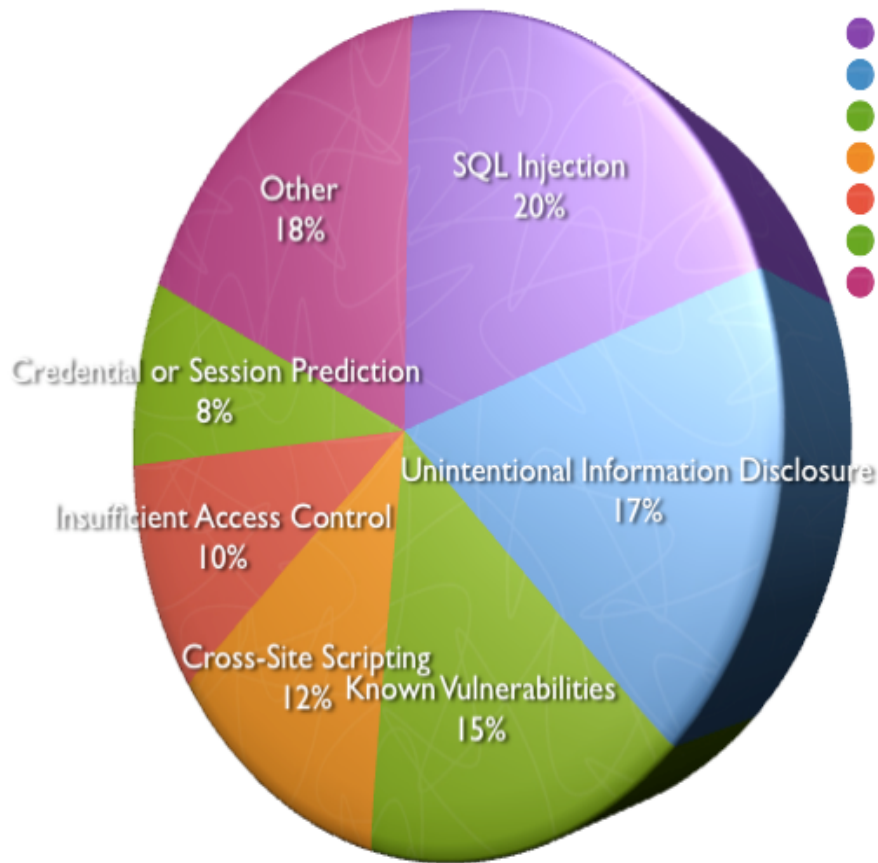
Web Tehditleri En Büyük Rolü Oynamakta

- Web Uygulama Açıkları
 - 2008 Yılı için Web Uygulamalarında %54.9 Oranında Korunmasızlık Görülmektedir



2007 Web Hackleme Olayları Veritabanı (WASC Projesi)

Hackerlar hangi saldırıları kullanır?



- SQL Injection
- Unintentional Information Disclosure
- Known Vulnerabilities
- Cross-Site Scripting
- Insufficient Access Control
- Credential or Session Prediction
- Other

- SQL Enjeksiyon
- Kasıtlı Olmayan Bilgi Dağıtımı
- Bilinen Güvenlik Açıkları
- Çapraz Site Oluşturma
- Yetersiz Erişim Kontrolü
- Kimlik ve Oturum Tahmini
- Diğerleri

** <http://www.webappsec.org/projects/whid/>

Bir Uygulama Güvenliđi İhlalinin Maliyeti

- Medya İlgisi/ Marka Zararı
- Stok Fiyatlarındaki Ani Düşüşler
- İletişim/Takip Servisi Maliyetleri
- Yasal ücretler (Belirtilen 3-4 Milyon Dolar)
- Denetimler
- Yeni Güvenlik Harcamaları
- Müşteri Davaları
- Müşteri Kayıpları



IBM Rational AppScan

Web Uygulama Saldırıları: Özel Saldırılar

Altyapı ve Uygulama Güvenliği Konuları

	Altyapı Güvenlik Açıkları	Uygulamalara Özel Güvenlik Açıkları
Hata Sebebi	3^{ncü} Parti Yazılımın Güvenliksiz Geliştirilmesi ve Deploy edilmesi	Bize Ait Güvensiz Geliştirilen Uygulamalar
Güvenlik Açığının Olduğu Yer	3 ^{ncü} Partinin Altyapısı (web server, OS, etc.)	Uygulama Kodları , Sıklıkla Application Server Üzerinde Bulunur
Giriş Metodları	Bilinen Güvenlik Açıkları	Şüpheli Bileşenler, Bilgi Sızıntısı
Tarama/Bulma	Yama Yönetim Sistemi	Uygulama Güvenliği Taranır
	Dahili/Harici Denetimler, Otomatik Taramalar	
Ne Yapılabilir?	Yamaları Yükle, Güvenilir 3 ^{ncü} Parti Yazılımlar Kullan	Eğitim & Tarayıcılar (Yazılım Yaşam Döngüsü Boyunca)

WASC

- Web Application Security Consortium (WASC)
 - Amaç:
Geliştirmek, Sahip Çıkmak Ve Web Uygulamaları Güvenliği İçin Standartları Desteklemek

- Resmi Web Sitesi: www.webappsec.org

- Web Güvenliği Tehdit Sınıflandırma Projesi

http://www.webappsec.org/projects/threat/v1/WASC-TC-v1_0.pdf

Amaç:

- Bir Web Sitesinin Güvenliği İçin Tehditleri Tanımlamak ve Organize Etme
- Endüstri Standardında, Terminolojiyi, Çıkan Neticelelere Göre Geliştirmek.

OWASP (The Open Web Application Security Project)

Açık Web Uygulama Güvenliği Projesi

Amaç:Yazılımların Güvensizliğinin Nedenini Bulmaya Ve Mücadele Etmeye Adanmıştır.

- Resmi web sitesi : www.owasp.org
- OWASP in zirvedeki 10 projesi:
- http://www.owasp.org/index.php/OWASP_Top_Ten_Project
- Amaç:
 - Kritik Web Uygulamaları Açıkları Hakkında geniş Bir Fikir Birliği Sağlayabilmek.
 - Web Uygulama Güvenliği Konularında Bilinçlendirmek.

OWASP UYGULAMA SALDIRILARINDA TOP 10

Uygulama Tehditleri	Olumsuz Etkisi	Örnek Durum
Cross Site Scripting	Kimlik Hırsızlığı, Hassas Bilgi Sızıntısı	Saldırganlar Meşru kullanıcıları ve Kontrol Hesaplarını Taklit Ederler
Injection Kusurları	Saldırgan DB / LDAP / Diğer Sistemleri Manipüle Edebilir	Saldırganlar Veritabanındaki Verilere Ulaşabilir, Değiştirebilir veya Çalabilir
Kötü Amaçlı Dosya Yürütümü	Server Üzerinde Komutlar İle Tam Kontrol Sağlayabilirler	Sitenin Tüm Etkileşimleri Hacker Tarafından Değiştirilir
Güvensiz Referans Nesnesi	Saldırganlar Özel Dosya ve Kodlara Erişebilirler	Özel Dosyanın İçeriği Web Uygulamasına Döner
Cross Site İsteğinde Sahtecilik	Saldırgan Web Uygulamalarında 'KÖR' Eylemleri Güvenli Bir Kullanıcı Gibi Çağırabilir	Hacker Banka Hesabına Para Transferi İçin Kör İstek Yollar
Bilgi Sızıntısı Ve Yanlış Veri İşleme	Saldırganlar Sistem Bilgilerini Detaylarıyla Elde Edebilirler	Kötü Niyetli Sistem Yazılımları Saldırı Tiplerinin Gelişimine Neden Olur
Hatalı Kimlik Doğrulama & Oturum Yöneticisi	Korunamayan Oturum İçerikleri yada Geçersiz Oturum Açılması	Hacker Kurban Üzerinden Oturumu 'Zorlayabilir' , Oturum Verileri Çalıntı Olabilir
Güvensiz Kriptografik Depolama	Zayıf Şifreleme Teknikleri Şifrenin Kırılmasına Neden Olabilir	Gizli Bilgiler (TC No, Kredi Kartı Bilgileri) Kötü Niyetli Çözülebilir
Güvensiz İletişim	Hassas Bilgi Güvensiz Kanal Üzerinden Şifresiz Gönderildi	Hacker Kullanıcıyı Taklit Edebilmek için Şifresiz Kimlik Bilgilerini Kullanabilir
Kısıtlı URL Erişimi	Hacker Yetkisiz Kaynaklara Ulaşabilir	Hacker Bir Sonraki Sayfaya Zorla Erişebilir ve İçeriğe Göz Atabilir

Injection Akışları

▪ Nedir ?

- Kullanıcı Tarafı Bilgiler (veriler) Bir Komut Parçası, Sorgu Veya Data(veri) Şeklinde Yorumlayıcıya Yollanır.

▪ Ne Gibi Etkileri Vardır?

- **SQL Injection** – Erişim/Modifiye/DB İçinde Veri Silme
- **SSI Injection** – Server Üzerinde Yürütülen Komutlar ve Hassas Verilere Erişim
- **LDAP Injection** – Kimlik Doğrulama
- **XPath, MX (Mail), HTML Injection** (Cross Site Script), **HTTP Injection** (HTTP Cevabını Ele Geçirme)

SQL Injection

Kullanıcı Girişi Gömülü Olabileceği Gibi Önceden Tanımlı da Olabilir (SQL Cümleleri İle):

```
query = "SELECT * from tUsers where
userid='" + iUserID + "' AND
password='" + iPassword + "'";
```

hackbook

Username:

Password:

Remember me

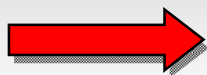
[Forgot Password?](#)



UserID	Username	Password	Name
1824	jsmith	demo1234	John Smith

- Hacker Girdileri(Verileri) Orjinal Veriyi Değiştirir, Bir Örnekle:

```
- iUserID = ' or 1=1 --
```



UserID	Username	Password	Name
1	admin	\$#kaoeFor56	Administrator

SQL Injection Algilama (Black Box)

hackbook

Username:

Password:

Remember me

Login

[Forgot Password?](#)

Login

File Edit View History Bookmarks Tools Help

https://login.hackbook.com/login.php

hackbook

Hackbook Login

Everyone Can Join

Sign Up

An Error Has Occurred

Summary: Syntax error (missing operator) in query expression 'username = '' AND password = 'foobar'.

Error Message Details:

System.Data.OleDb.OleDbException: Syntax error (missing operator) in query expression 'username = '' AND password = 'psaok'. at System.Data.OleDb.OleDbCommand.ExecuteNonQueryForSingleResult(tagDBPARAMS dbParams, Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteNonQuery(Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteReader(CommandBehavior behavior, Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteReaderInternal(CommandBehavior behavior, String method) at System.Data.OleDb.OleDbCommand.ExecuteReader(CommandBehavior behavior) at System.Data.OleDb.OleDbCommand.System.Data.IDbCommand.ExecuteReader(CommandBehavior behavior) at System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior) at System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior) at System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, String srcTable) at Altoro.Authentication.ValidateUser(String userName, String password) in

**SELECT * from tUsers where
userid='' AND password='foobar'**

Email:



PERSONAL

- [Deposit Product](#)
- [Checking](#)
- [Loan Products](#)
- [Cards](#)
- [Investments & Insurance](#)
- [Other Services](#)

SMALL BUSINESS

- [Deposit Products](#)
- [Lending Services](#)
- [Cards](#)
- [Insurance](#)
- [Retirement](#)
- [Other Services](#)

INSIDE ALTORO MUTUAL

- [About Us](#)
- [Contact Us](#)
- [Locations](#)
- [Investor Relations](#)
- [Press Room](#)
- [Careers](#)

Online Banking Login

Username:

Password:



MY ACCOUNT	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
----------------------------	--------------------------	--------------------------------	--------------------------------------

I WANT TO ...

- [View Account Summary](#)
- [View Recent Transactions](#)
- [Transfer Funds](#)
- [Search News Articles](#)
- [Customize Site Language](#)

Hello, John Smith

Welcome to Altoro Mutual Online.

View Account Details:

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

Click [Here](#) to apply.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.

1. Cross Site Scripting (XSS)

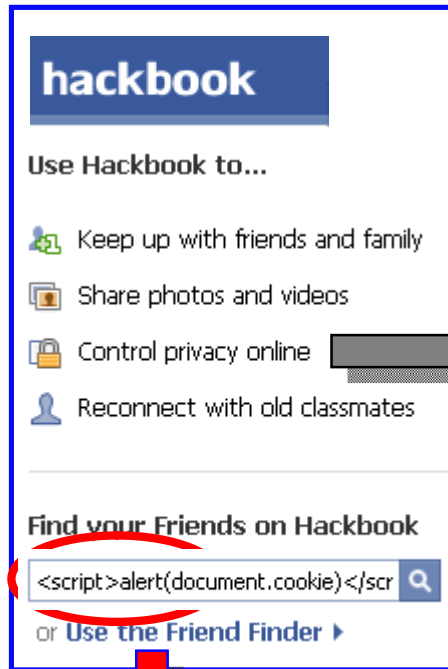
■ Nedir ?

- Geri Dönen HTML İçinde Zararlı Program Yankılanır, Ve Güvenilir Modda Çalışır

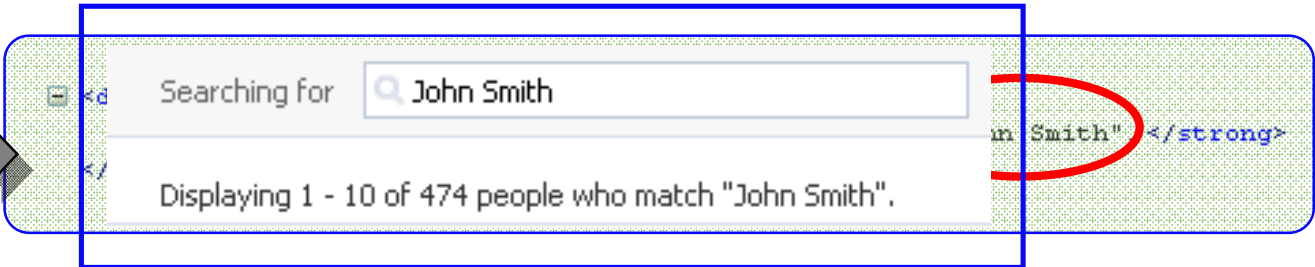
■ Ne Gibi Etkileri vardır ?

- Çalınmış Oturum Verileri(Token) (Tarayıcı Güvenliği Atlatılabilir)
- Sayfa İçeriği Bütünüyle Taviz Verebilir
- Gelecek Sayfa Tarayıcıda Tehlikeye Atılabilir

Neden & Nerede XSS Kullanılır ?



Kullanıcı Verileri HTML İçine Gömülmüştür



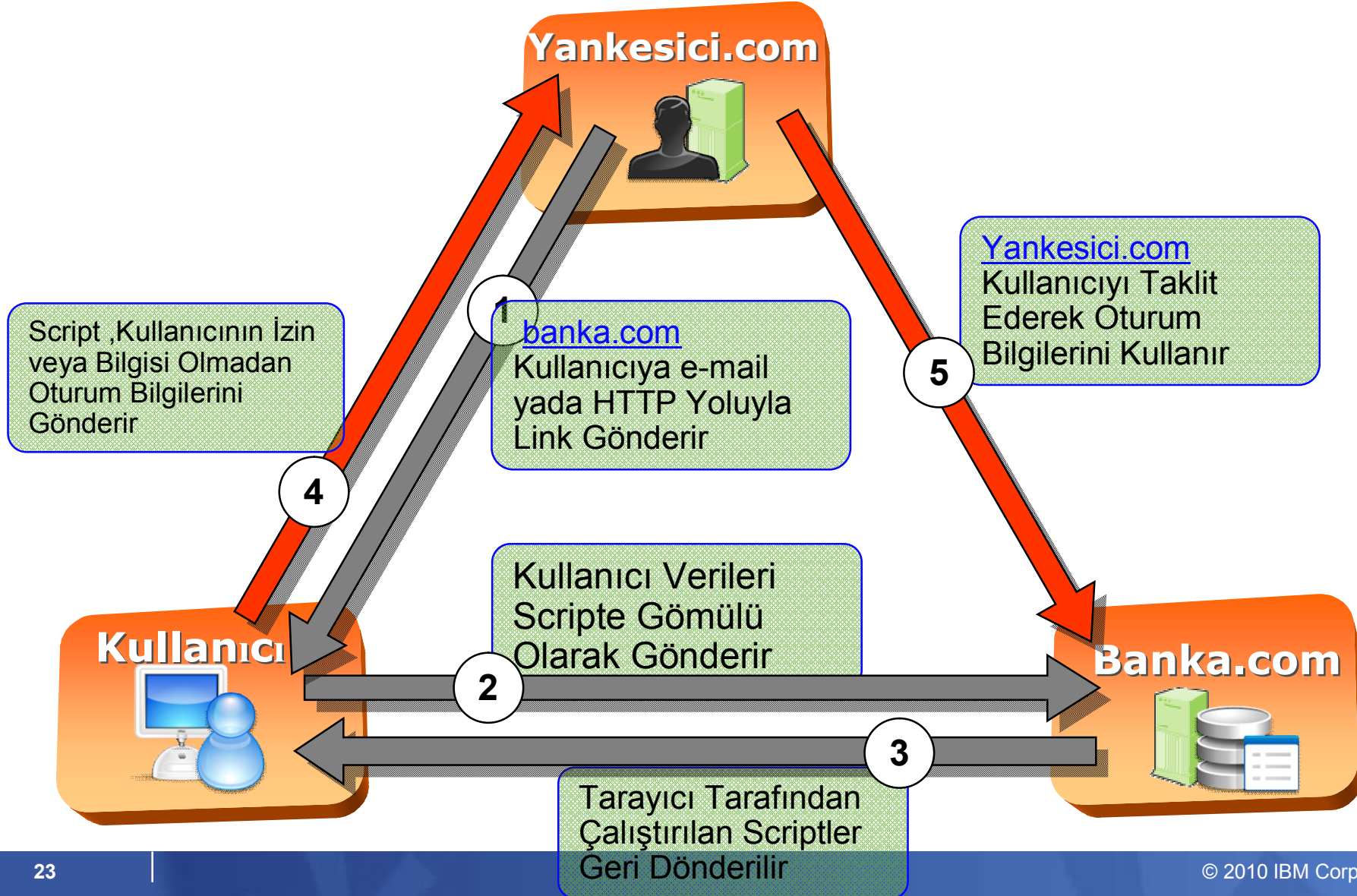
JS Gömülü Olan Sayfa Güvenilir Bir Site Sayfası Gibi Gözükmemektedir

```

<div class="summary">
  <strong>
    Displaying 1 - 10 of 396 people who match
    <script>
      alert (document.cookie)
    </script>
  </strong>
</div>
    
```



Cross Site Scripting – Süreçleri Kullanmak





IBM Rational AppScan

The IBM Rational AppScan Ürün Ailesi

Watchfire (AppScan) Genel Görünümü

■ Watchfire Nedir ?

- Uygulama Güvenliği Ve Uyumu İçin Yazılım Ve Servis Sağlayıcısıdır
- 800'den Fazla Şirket Watchfire'e Güveniyor
- 1996'da Kuruldu, IBM Tarafından Temmuz 2007'de Satın Alındı

**Uygulama
Güvenliğinde 1
Numaralı Pazar
Payına Sahip**
– Gartner & IDC

■ Arkaplan (Tarihçe) :

- Merkezi Boston da Olmak Üzere 190 Çalışanıyla 1996'da Kuruldu
- İlk Uygulama Güvenlik Test Ürünü Oluşturuldu



**En İyi Güvenlik
Şirketi**

Şuan da 800'den Fazla Şirket Watchfire'le Çalışmaktadır

9 of the Top 10 Largest U.S. Retail Banks	8 of the Top 10 Technology Brands	7 of the Top 10 Pharma / Clinical Companies	Multiple Large Government Agencies

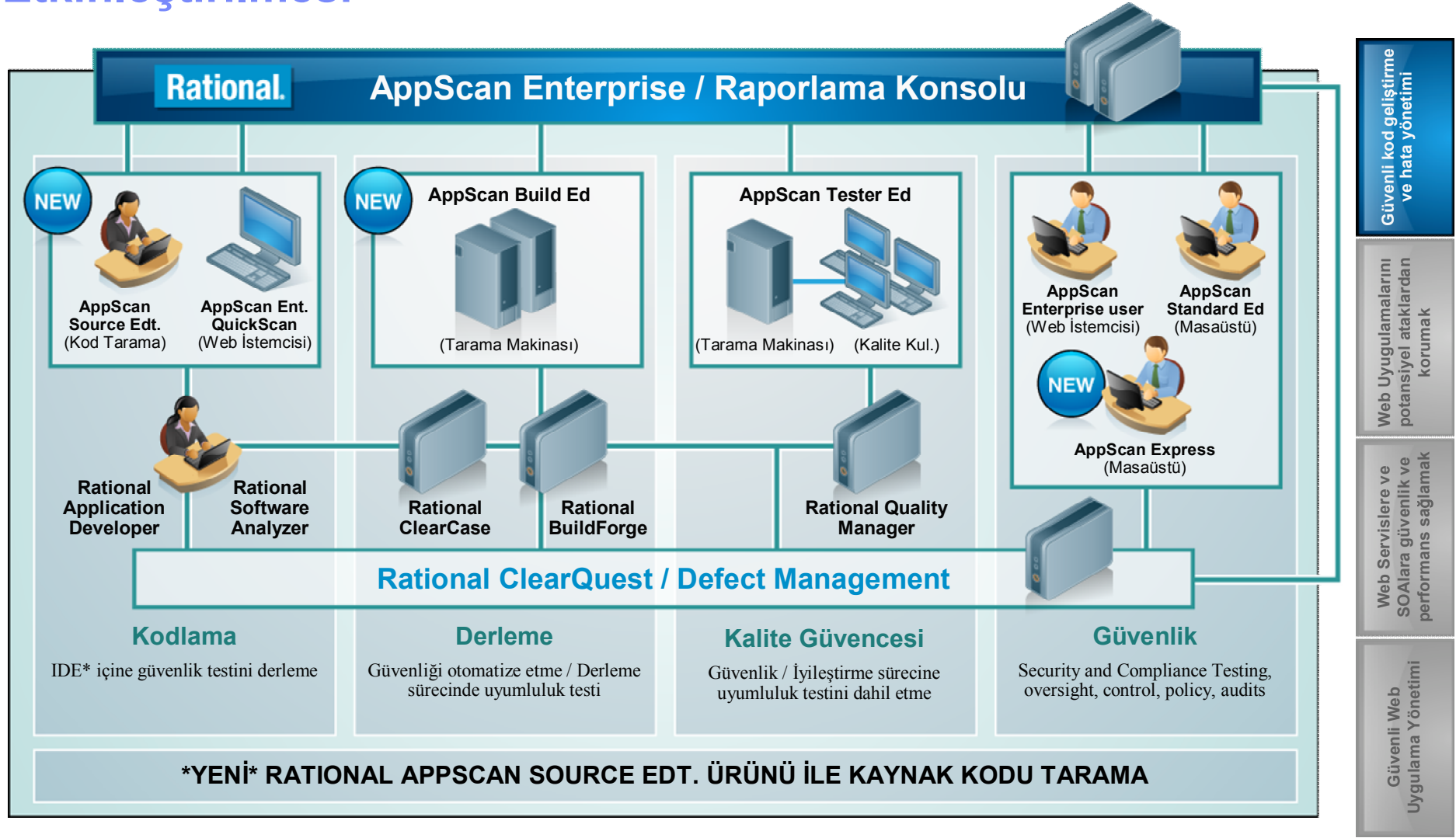
Büyük, Kompleks Web Siteleri

İyi Ayarlanmış Yapısı

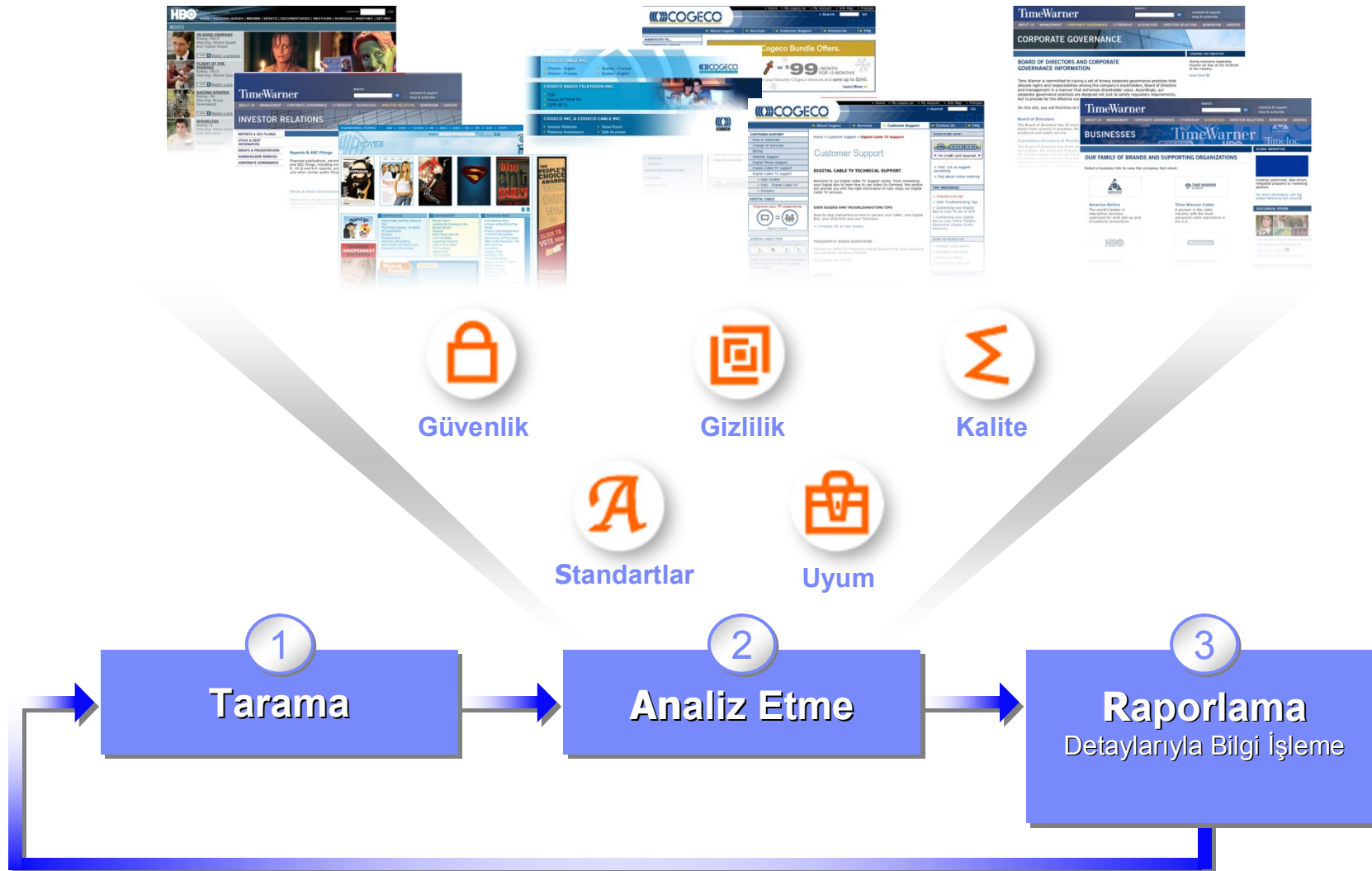
Kapsamlı Müşteri Verileri

Yüksek Kullanım Hacmi

Yazılım Geliştirme Sürecinde Güvenlik Testlerinin Etkinleştirilmesi



AppScan Teknolojisi Nasıl Çalışır ?



IBM Rational AppScan Standard Edition

The screenshot displays the IBM Rational AppScan Standard Edition interface. The main window shows the results of a scan for 'My Application'. The scan is 12/13 complete, and the results are arranged by severity in descending order. There are 72 security issues identified, including Database Error Pattern Found (9), Format String Remote Command Execution (1), Inadequate Account Lockout (1), Predictable Login Credentials (1), Session Identifier Not Updated (1), and SQL Injection (9).

The selected issue is 'Predictable Login Credentials' at the URL `http://local/altoro/bank/login.aspx`. The security risk is described as: 'It may be possible to escalate user privileges and gain administrative permissions over the web application'. The CVSS Metrics Scoring (8) is shown with Base, Temporal, and Environmental scores.

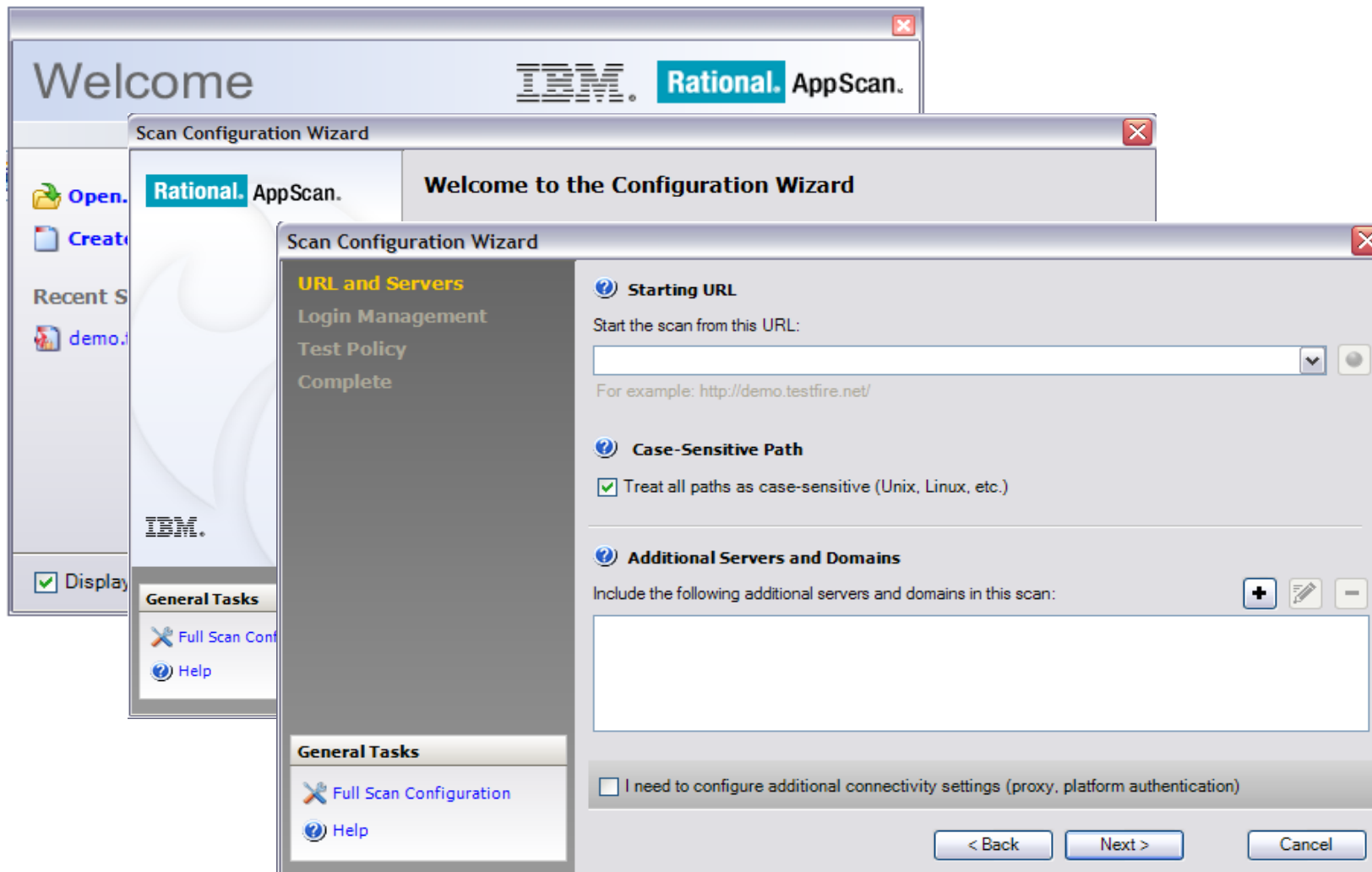
The issue information includes:

- URL: `http://local/altoro/bank/login.aspx`
- Entity: `login.aspx`
- Security Risk: It may be possible to escalate user privileges and gain administrative permissions over the web application.

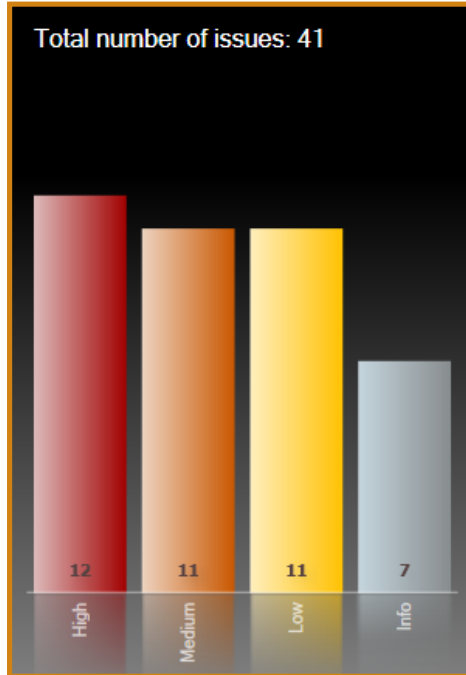
A yellow warning box states: 'The test response is the result of a login attempt with predictable credentials (such as admin:admin). Verify that it contains a "successful login" message similar to that in the original response.'

The interface also shows a 'Dashboard' with an 'Issue Severity Gauge' and a bar chart showing the total number of issues: 24 (High), 27 (Medium), 10 (Low), and 11 (Info). The status bar at the bottom indicates 72 Security Issues, 36 High, 25 Medium, 0 Low, and 11 Info.

Tarama Sihirbazı..



Kolay Sorun Algılama-Sorunlar ve Öncelikleri



Aranged 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)**

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
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 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

Problemi Belirleme(tanımlama)



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**
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 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.

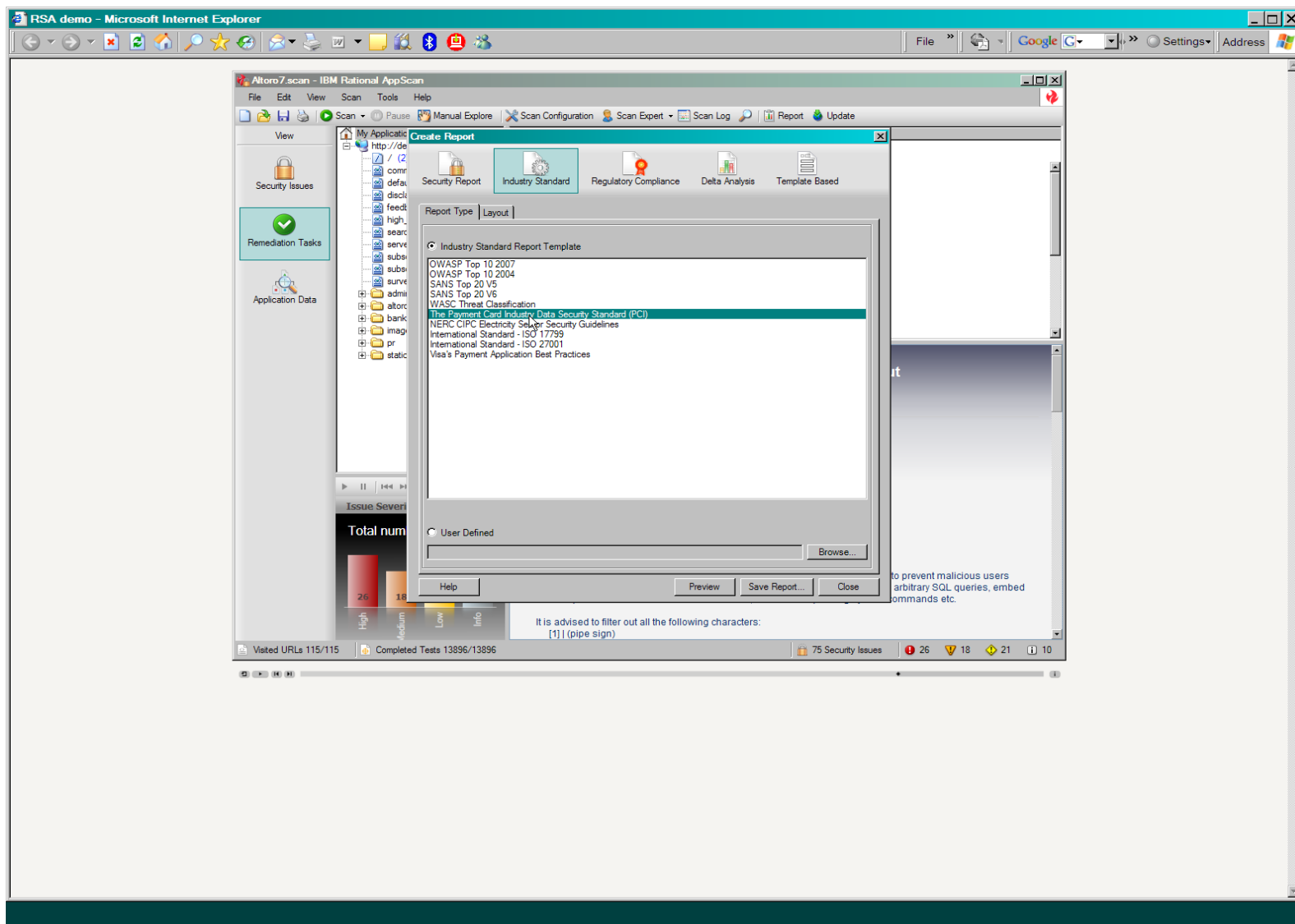
The attack proceeds as follows: The attacker lures the legitimate user to click on a link that was produced by the attacker. When the user clicks on the link, this generates a request to the web-site containing a parameter value with malicious JavaScript code. If the web-site embeds this parameter value 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](#)

**Gömülü Web Tabanlı
(Video) Eğitim**

Rational AppScan: Raporlama Evresi



IBM Rational AppScan Developer & Build Editions

J2EE - AltoroScan - 9/22/08 4:56 PM - Eclipse SDK

File Edit Navigate Search Project Run Window Help

AltoroScan.sscn *AltoroScan - 9/22/08 4:56 PM x

Security Report

Scan Progress: Complete

Correlated Dynamic Analysis Issues

7 security issues with 7 variants found

- Cross-Site Scripting (7)
 - http://localhost:8080/altoromutual/account.jsp (2)
 - http://localhost:8080/altoromutual/search.jsp (1)
 - query
 - http://localhost:8080/altoromutual/sendFeedback (1)

Related Static Analysis Issues

1 security issues with 1 variants found

- Cross-Site Scripting (1)
 - dynamic/searchform.jsp (1)
 - dynamic/searchform.jsp on Line 17 (1)

Details

Advisory | Fix Recommendation | Static Analysis

Output method: JspWriterImpl.print(...)

dynamic/searchform.jsp (Line 17) <%= query %>

dynamic/searchform.jsp (Line 5) String query = request.getParameter("query");

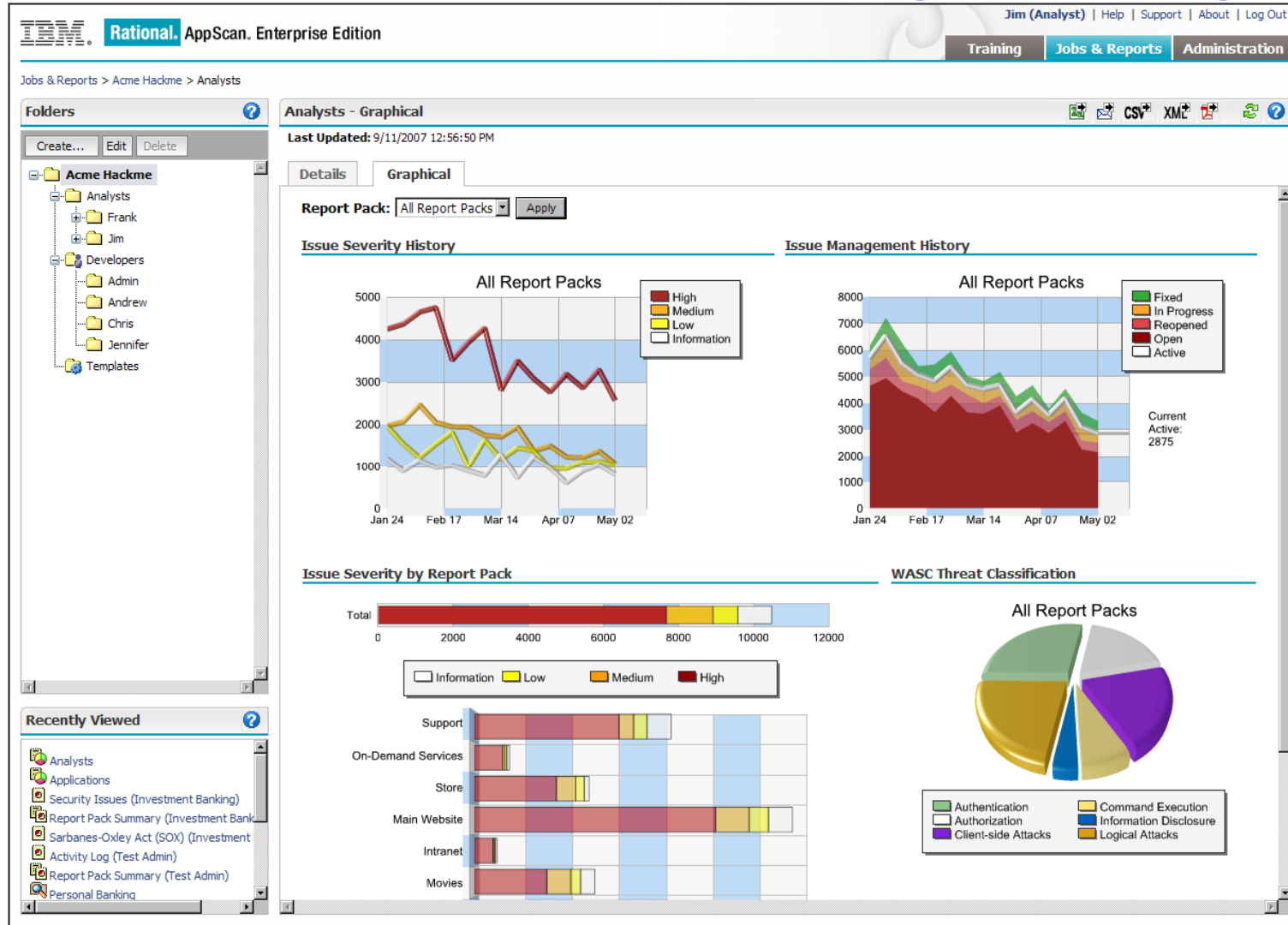
```

2 <%@page import="com.ibm.rational.appscan.altoromutual.util.ServletUtil"%>
3
4 <%
5 String query = request.getParameter("query");
6 String[] results = null;
7 if (query != null && query.trim().length()>0)
8     results = ServletUtil.searchSite(query, request.getSession().getServletContext().getRealPath("/static/"));

```

Input method: ServletRequest.getParameter(...)

AppScan Enterprise – Metrik Değer Gösterge Panosu



RQM İçin AppScan Tester Edition

The screenshot shows the IBM Rational Quality Manager interface. The top navigation bar includes 'Home', 'Planning', 'Construction', 'Execution', 'Analysis', and 'Help'. The main content area is titled 'Web UI Tests' and includes a 'Discard Changes' and 'Save' button. Below this, there are tabs for 'Overview' and 'Snapshots'. The 'Overview' tab is active, showing the 'Test Group Name' as 'Web UI Tests' and the status as 'In Progress'. The 'Details' section shows the 'Originator' as 'ADMIN' and the 'Description' as 'Provide full test coverage of the Web UI'. A 'Work Item (35)' is also shown, owned by 'Arnold Adams'. At the bottom, there is a table of 'Test Cases' with columns for 'Name', 'Description', and 'Owner'.

	Name	Description	Owner	
21	Web UI Functional Tests	Test for functionality issues in the web application	Laura Lyons (Tester Lead)	✘
23	Web UI Performance Tests	Test for performance issues in the web application	Craig Lawton (Tester)	✘
3	Web UI Security Tests	Test for security issues in the web application	Donald David (Developer)	✘

Güvenlik Testleri Diğer Tip Testler Gibi Yönetilir

Tesekkürler

[→ Go to IBM](#)

© Copyright IBM Corporation 2007. 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, the on-demand business logo, Rational, the Rational 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.