IBM Rational AppScan

Web Uygulamaları Güvenliği & IBM Rational AppScan

Mehmet Çağrı ELİBOL
Rational Ürün Teknik Satış Uzmanı
cagrie@tr.ibm.com

Gündem

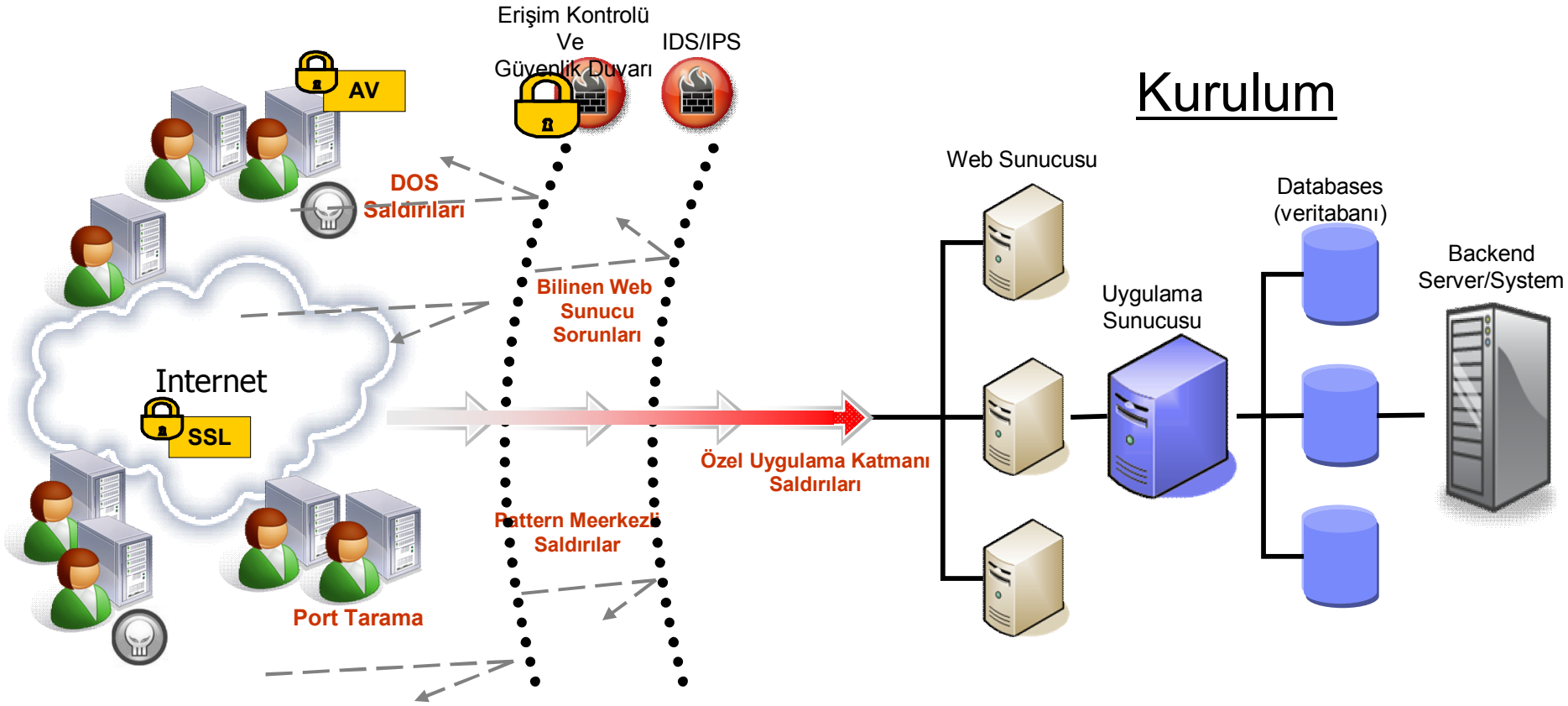
- Web Uygulamaları Güvenliği
  - Genel Bakış
  - Endüstriyel Durum
- Uygulama Güvenliği Açıkları
  - WASC, OWASP ve The OWASP Top Ten
  - 2 Yüksek Seviyeli Atağı İnceleme
- IBM Rational AppScan Ailesinin Ürünlerinin Tanıtımı
- Sorular ve Cevaplar

IBM Rational AppScan

Uygulama Güvenliği

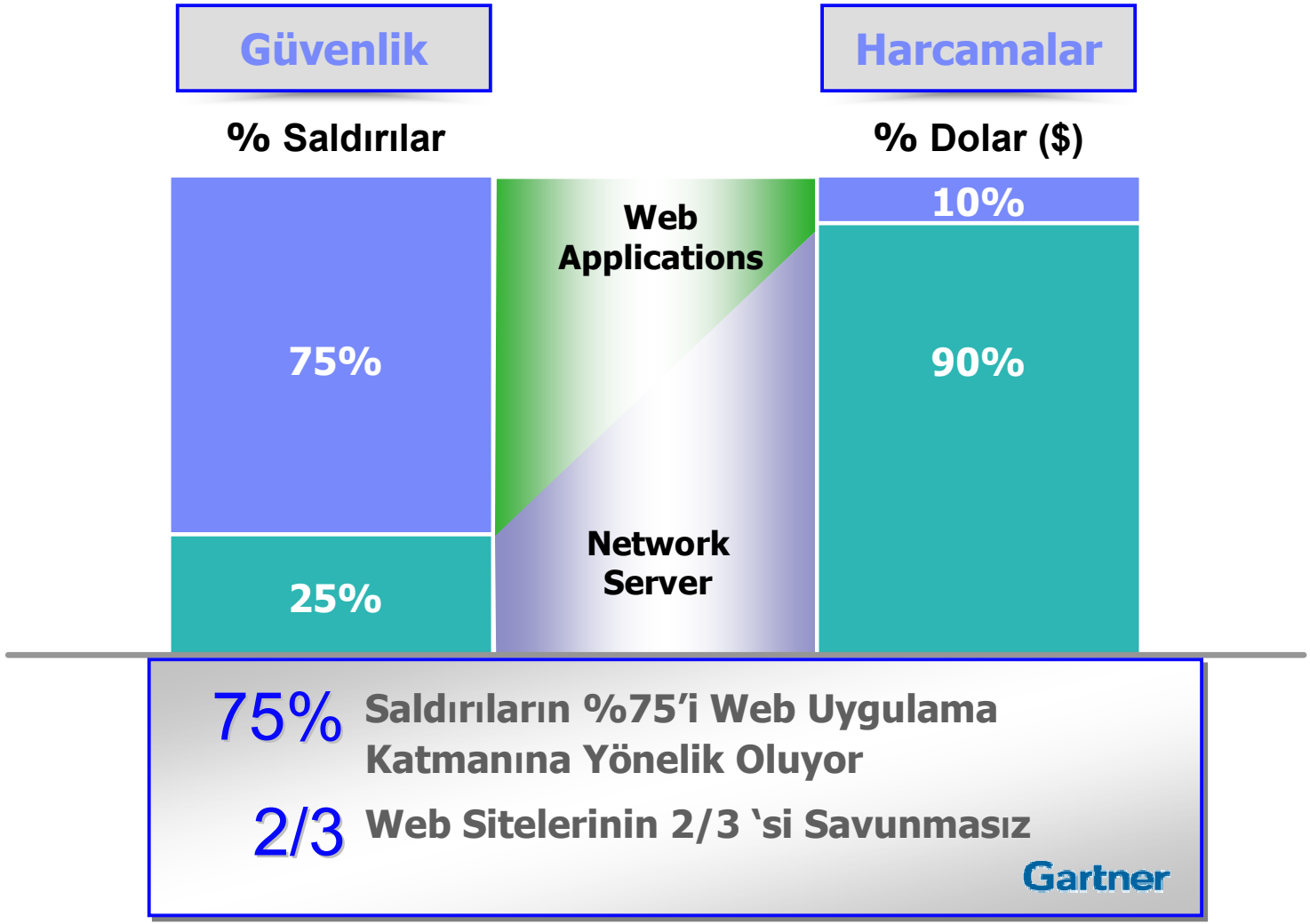
Endüstriyel Durum

Basit Güvenlik Görünümü



Saldırı Gerçekleri

Uygulama Katmanı Açıkları: Genel

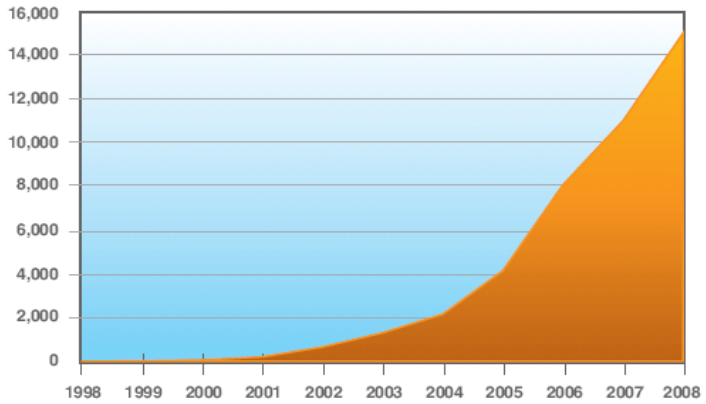


Kaynaklar: Gartner, Watchfire

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.!

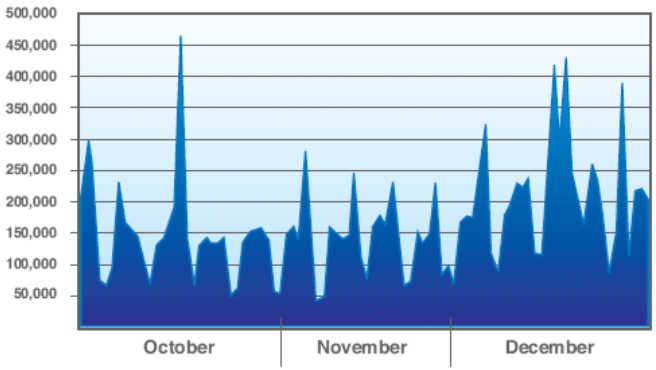
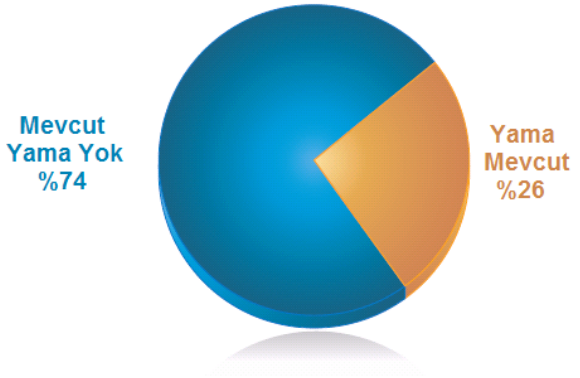


Figure 21: SQL Injection Attacks Monitored by IBM ISS Managed Security Services, Q4 2008

Source: 2008 IBM ISS X-Force Annual Report

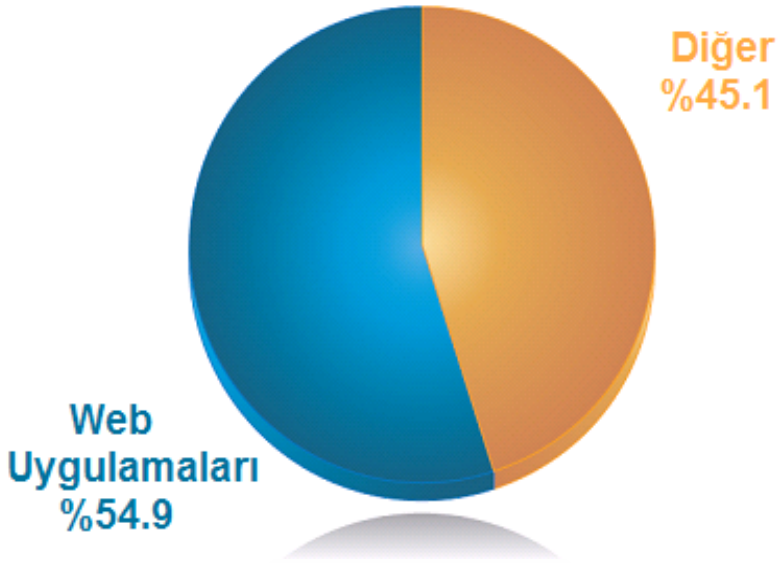
Web Uygulamaları Güvenlik Açıkları Yüzdesi (yamalarla birlikte)



- **2008 yılında IBM Mss milyonlarca SQL İnjection Saldırılarına Tanık Olmuştur**
- **Hackerların Hedefledikleri Çaldıkları Verilerle Yasal,Meşru Siteleri Zararlı Sitelere Yönlendirmektir**
- **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 Saldırılar Son 6 Ay İçinde Eşi Görülmemiş Derecede Artış Göstermiştir(30 kat)**

Web Tehditleri En Büyük Rolü Oynamakta

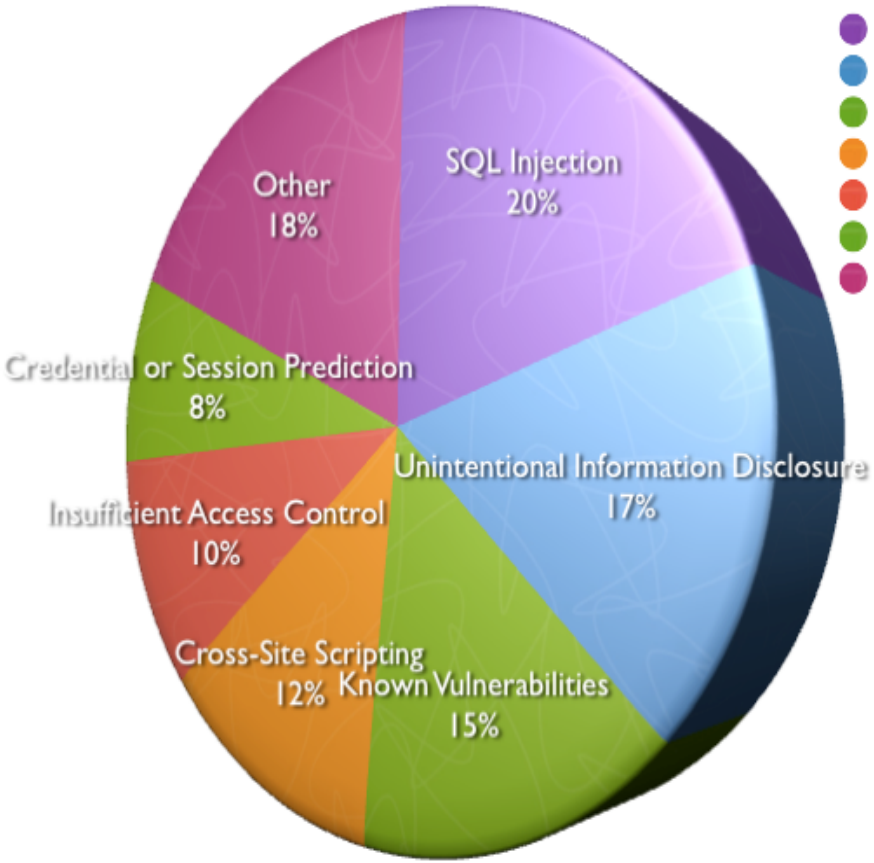
- Web Uygulama Açıkları
  - 2008 Yılı için Web Uygulamalarında %54.9 Oranında Korunmasızlık Görülmektedir



IBM Internet Security Systems X-Force® 2008 Trend & Risk Report

2007 Web Hackleme Olayları Veritabanı (WASC Projesi)

Hackerlar hangi saldırıları kullanır?



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

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

Bir Uygulama Güvenliği 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	**3ncü Parti Yazılımın Güvenliksiz Geliştirilmesi ve Deploy edilmesi**	Bize Ait Güvensiz Geliştirilen Uygulamalar
Güvenlik Açığının Olduğu Yer	3ncü 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 3ncü PartiYazılımlar Kullan	Eğitim & Tarayıcılar (Yazılım Yaşam Döngüsü Boyunca)

WASC

- Web Application Security Consortium (WASC)
  - Amaç:
    Geliştirmek, Sahip Çıkmak Ve Web Uygulamaları Güvenligi 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 Neticelere 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 ın 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 Veritabınındaki 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

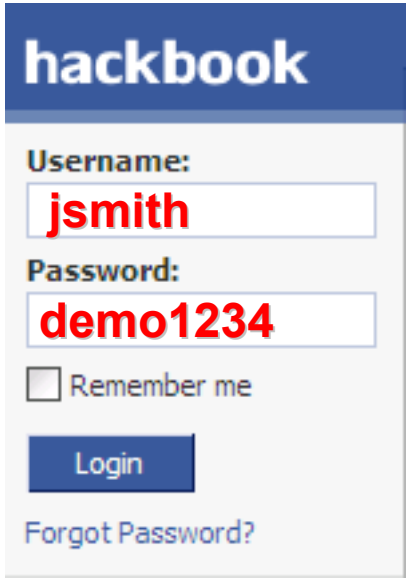
- **Nedir ?**
  - Kullanıcı Taraflı Bilgiler (veriler) Bir Komut Parçası,Sorgu Veya Data(veri) Şeklinde Yorumlayıcıya Yollanır.

- **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 + "'";
```

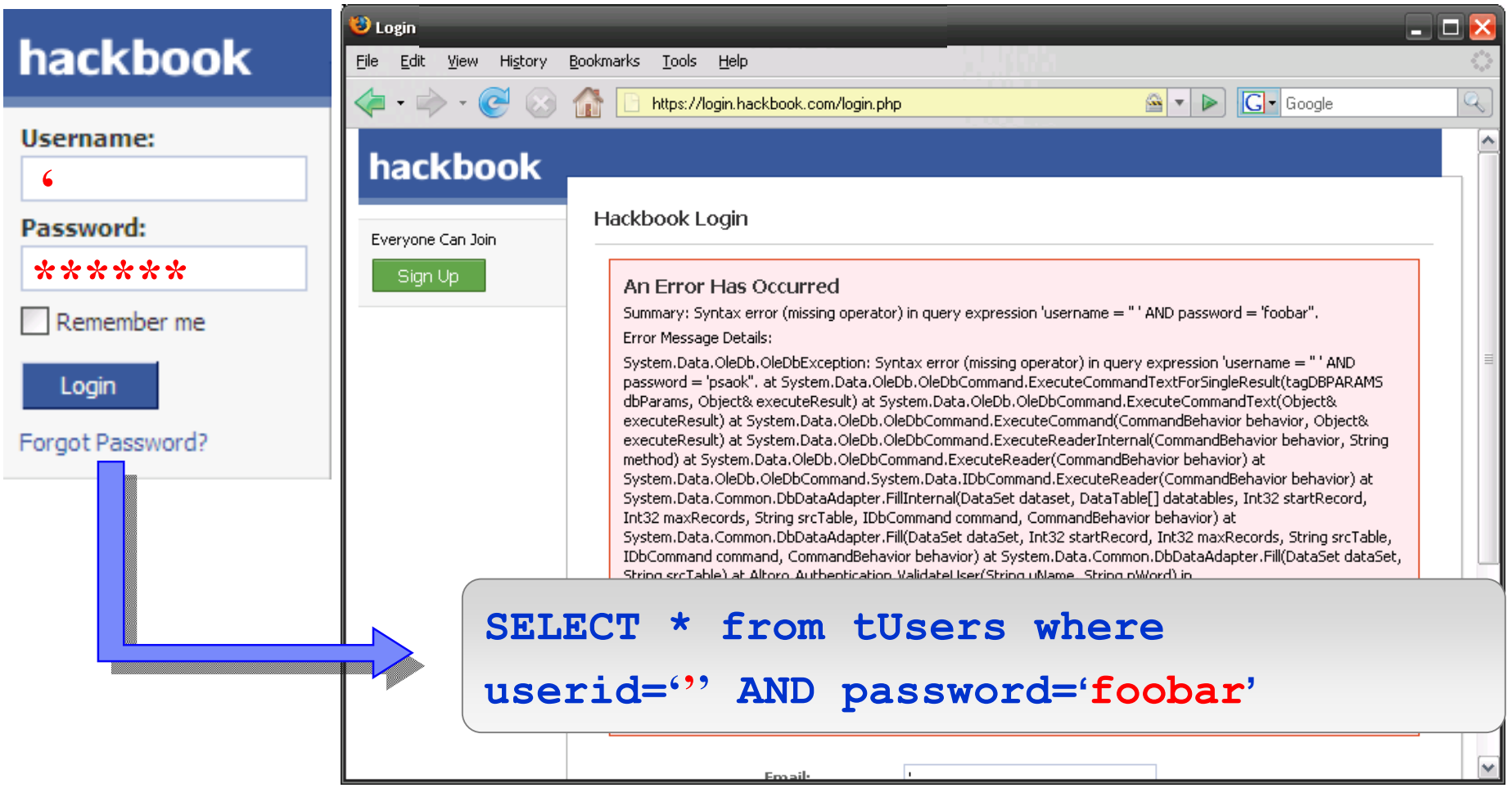


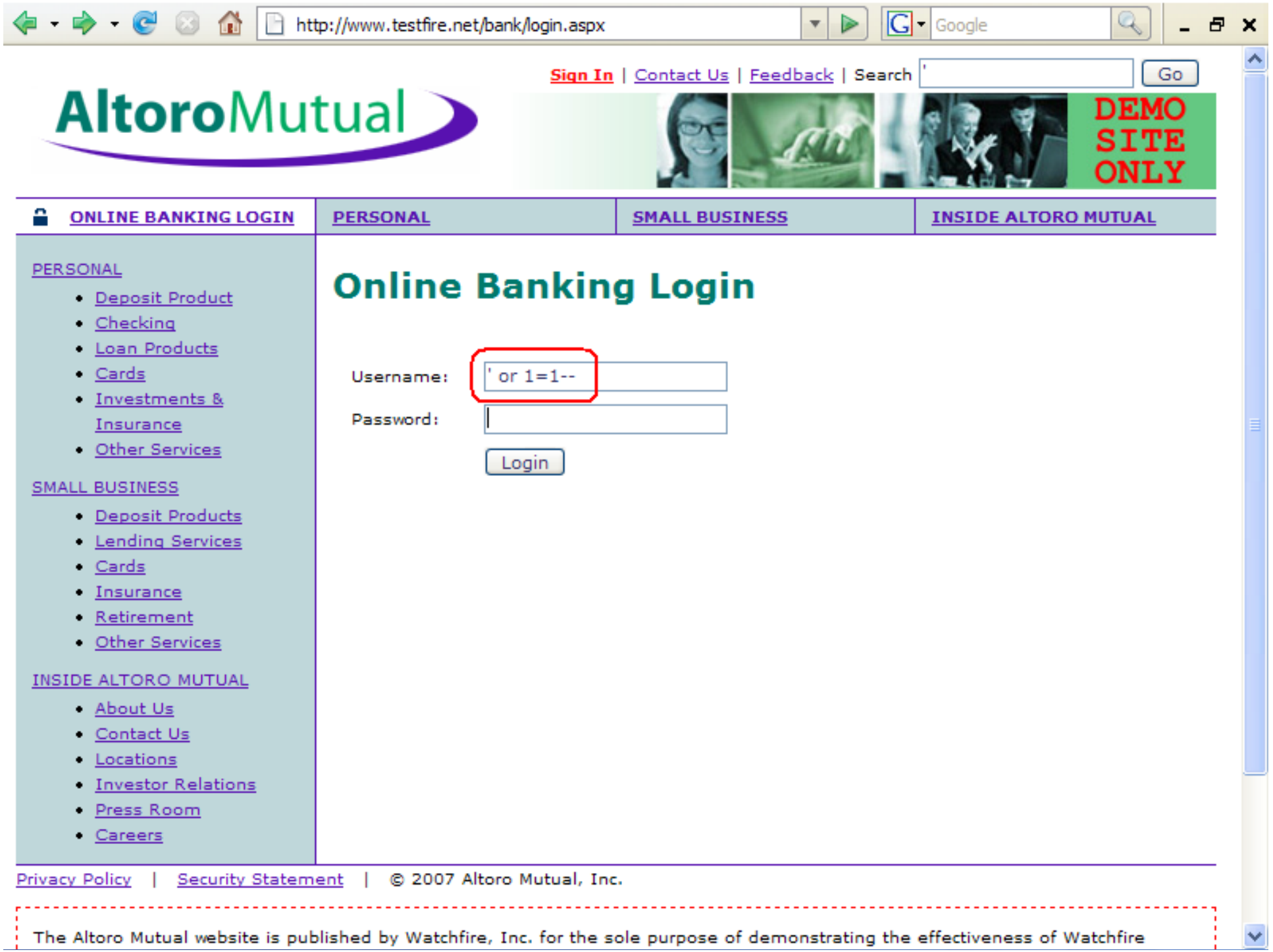
UserID	Username	Password	Name
1824	jsmith	demo1234	John Smith

- Hacker Girdileri(Verileri) Orjinal Veriyi Değiştirir, Bir Örnekle:
  - `iUserID = ' or 1=1 --`

UserID	Username	Password	Name
1	admin	$#kaoeFor56	Administrator

SQL Injection Algılama (Black Box)




http://www.testfire.net/bank/login.aspx
Google
Sign In | Contact Us | Feedback | Search
'
Go
AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
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:
' or 1=1--
Password:
Login
Privacy Policy | Security Statement | © 2007 Altoro Mutual, Inc.
The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire

AltoroMutual

Hello, John Smith

Welcome to Altoro Mutual Online.

View Account Details: 1001160140 Checking GO

Congratulations!

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

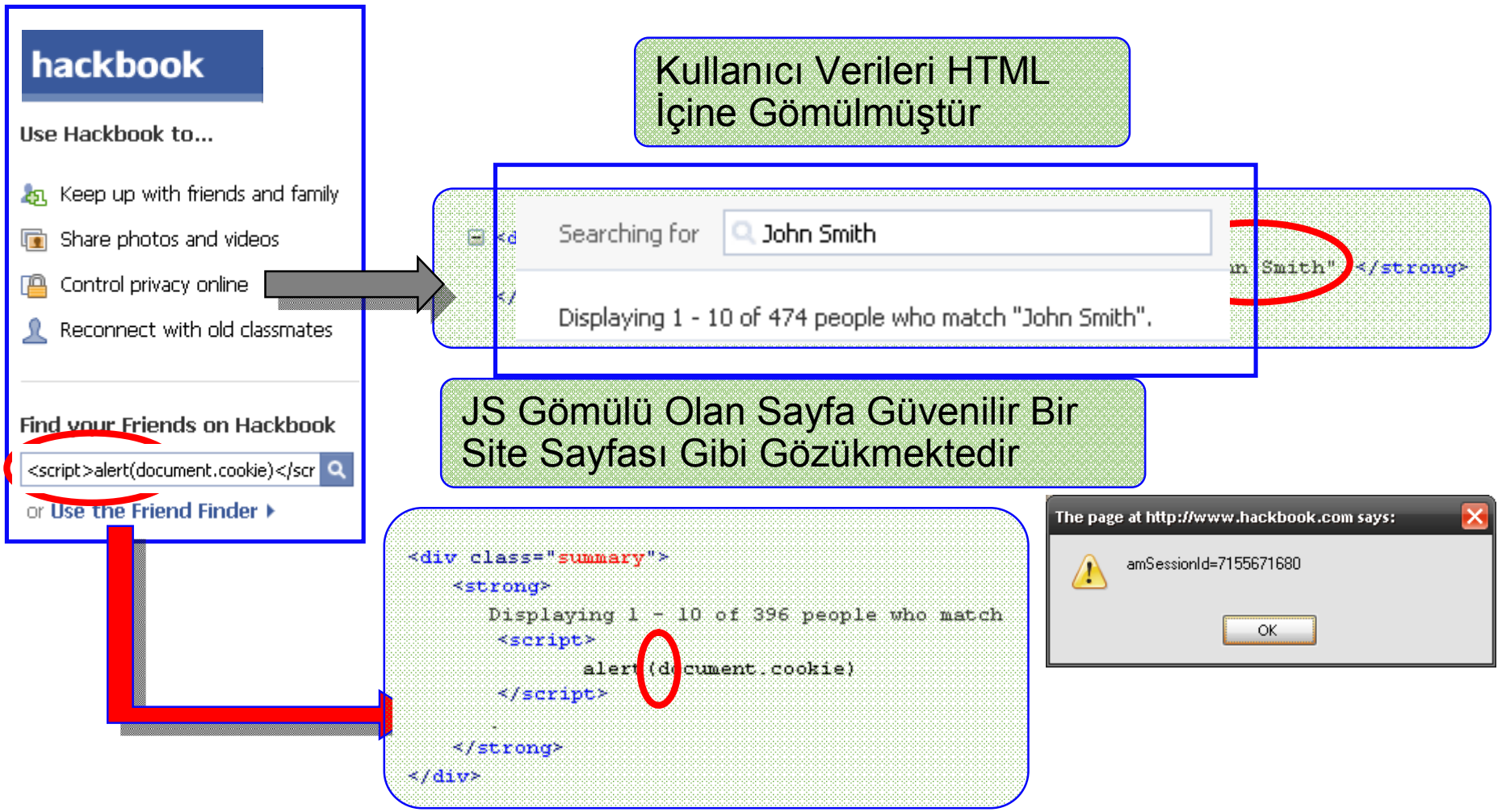
Click Here to apply.

1. Cross Site Scripting (XSS)

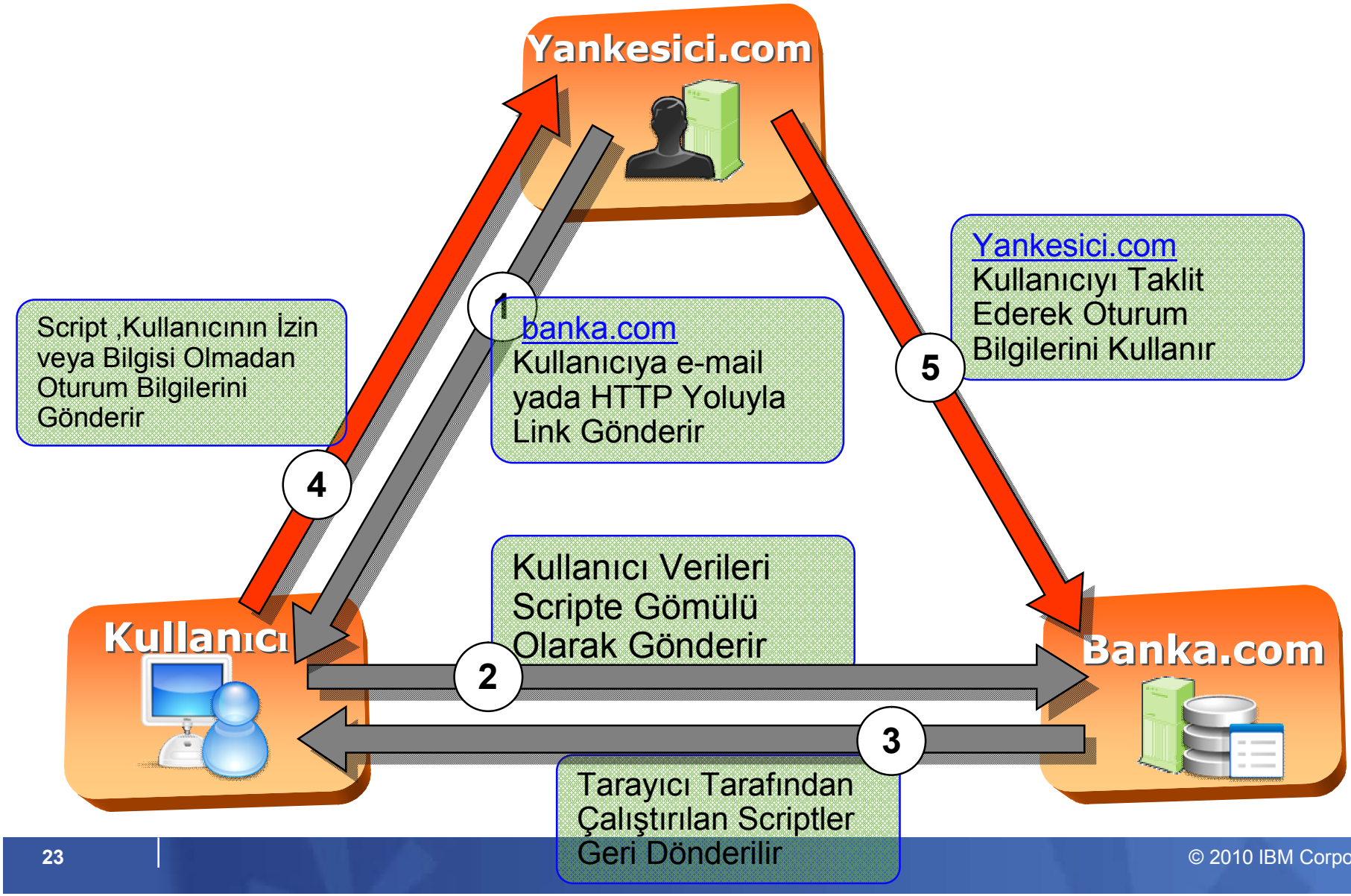
- **Nedir ?**
  - Geri Dönen HTML İçinde Zararlı Program Yankılanır, Ve Güvenilir Modda Çalışır

- **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 ?



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
- **Arkaplan (Tarihçe) :**
  - Merkezi Boston da Olmak Üzere 190 Çalışanıyla 1996'da Kuruldu
  - İlk Uygulama Güvenlik Test Ürünü Oluşturuldu

Uygulama Güvenliğinde 1 Numaralı Pazar Payına Sahip
– Gartner & IDC

SC MAGAZINE AWARDS 2007 WINNER

En İyi Güvenlik Şirketi

Şuan da 800'den Fazla Şirket Watchfire'le Çalışmaktadır

9 of the Top 10 Largest U.S. Retail Banks

Bank of America – Higher Standards
citi
JPMorgan
WELLS FARGO
WACHOVIA
Washington Mutual
usbank
SunTrust

8 of the Top 10 Technology Brands

IBM
Microsoft
intel
NOKIA
Cisco Systems
SONY
DELL

7 of the Top 10 Pharma / Clinical Companies

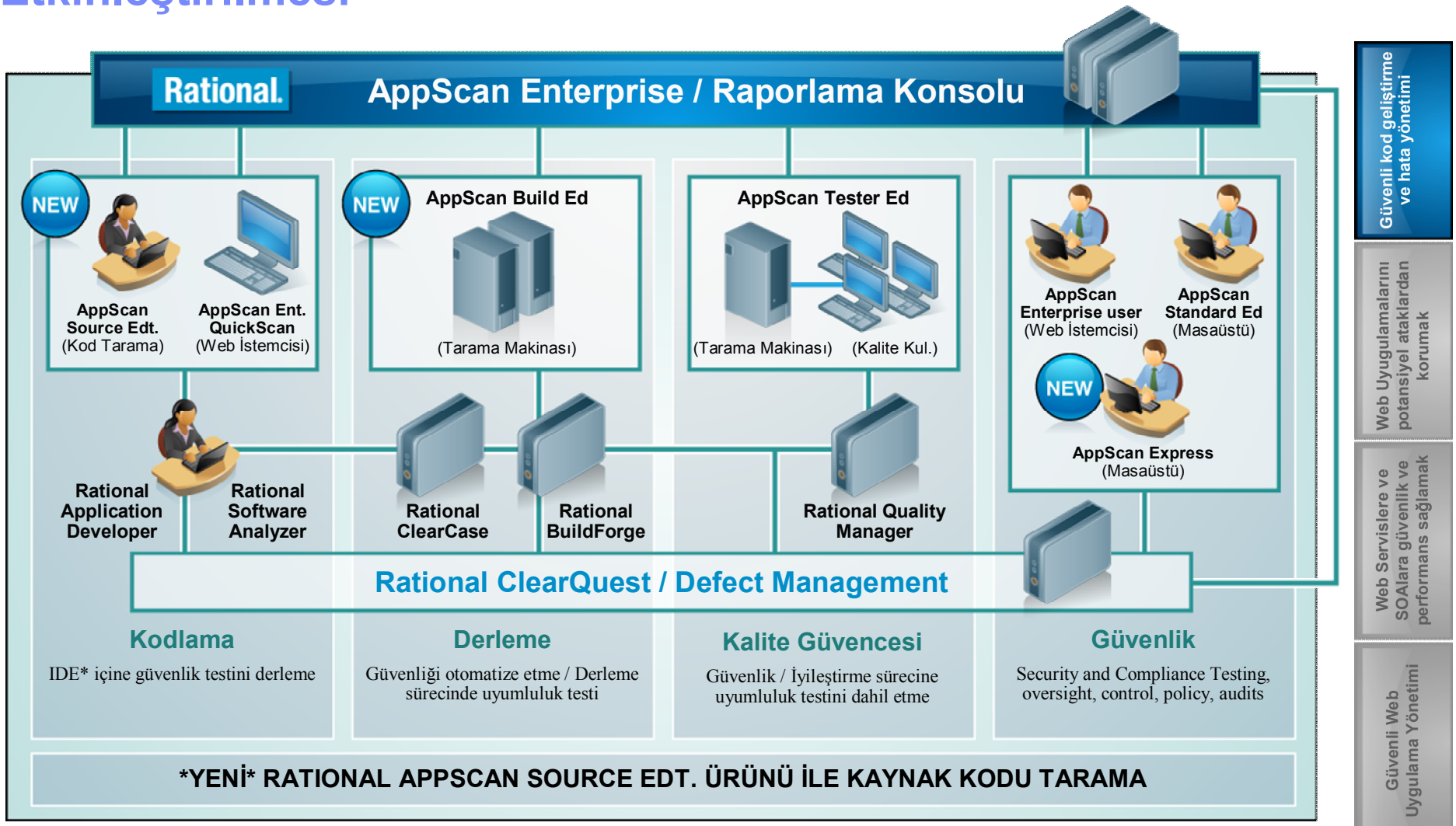
Wyeth
NOVARTIS
AstraZeneca
Abbott Laboratories
Aventis
Roche
Genentech – IN BUSINESS FOR LIFE

Multiple Large Government Agencies

Veteran's Affairs
Army
Navy
Air Force
Marines
Social Security Administration – USA
United States Postal Service

- Büyük, Komplex Web Siteleri
- Kapsamlı Müşteri Verileri
- İyi Ayarlanmış Yapısı
- Yüksek Kullanım Hacmi

Yazılım Geliştirme Sürecinde Güvenlik Testlerinin Etkinleştirilmesi



AppScan Teknolojisi Nasıl Çalışır ?

Güvenlik

Gizlilik

Kalite

Standartlar

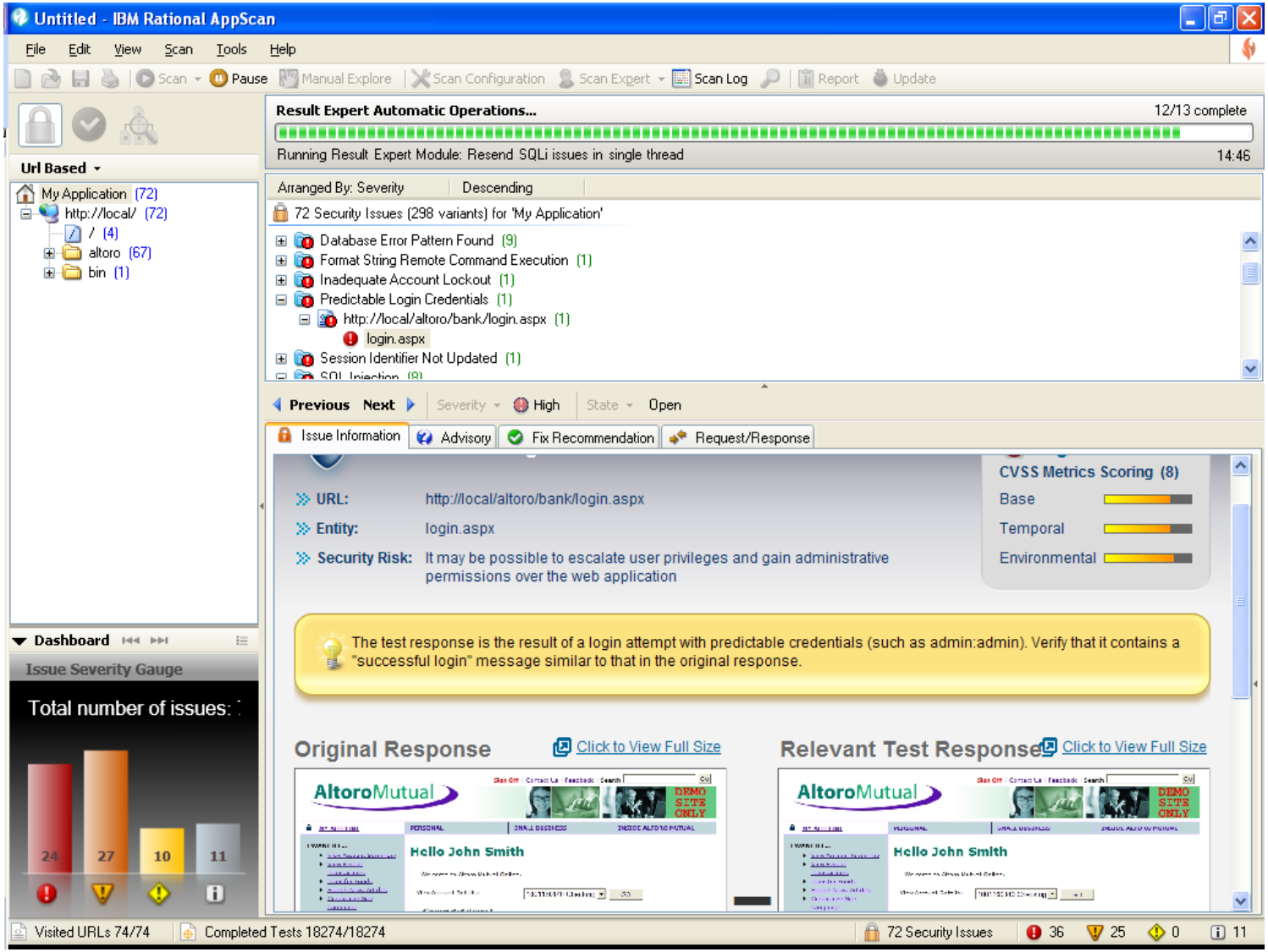
Uyum

1 **Tarama**

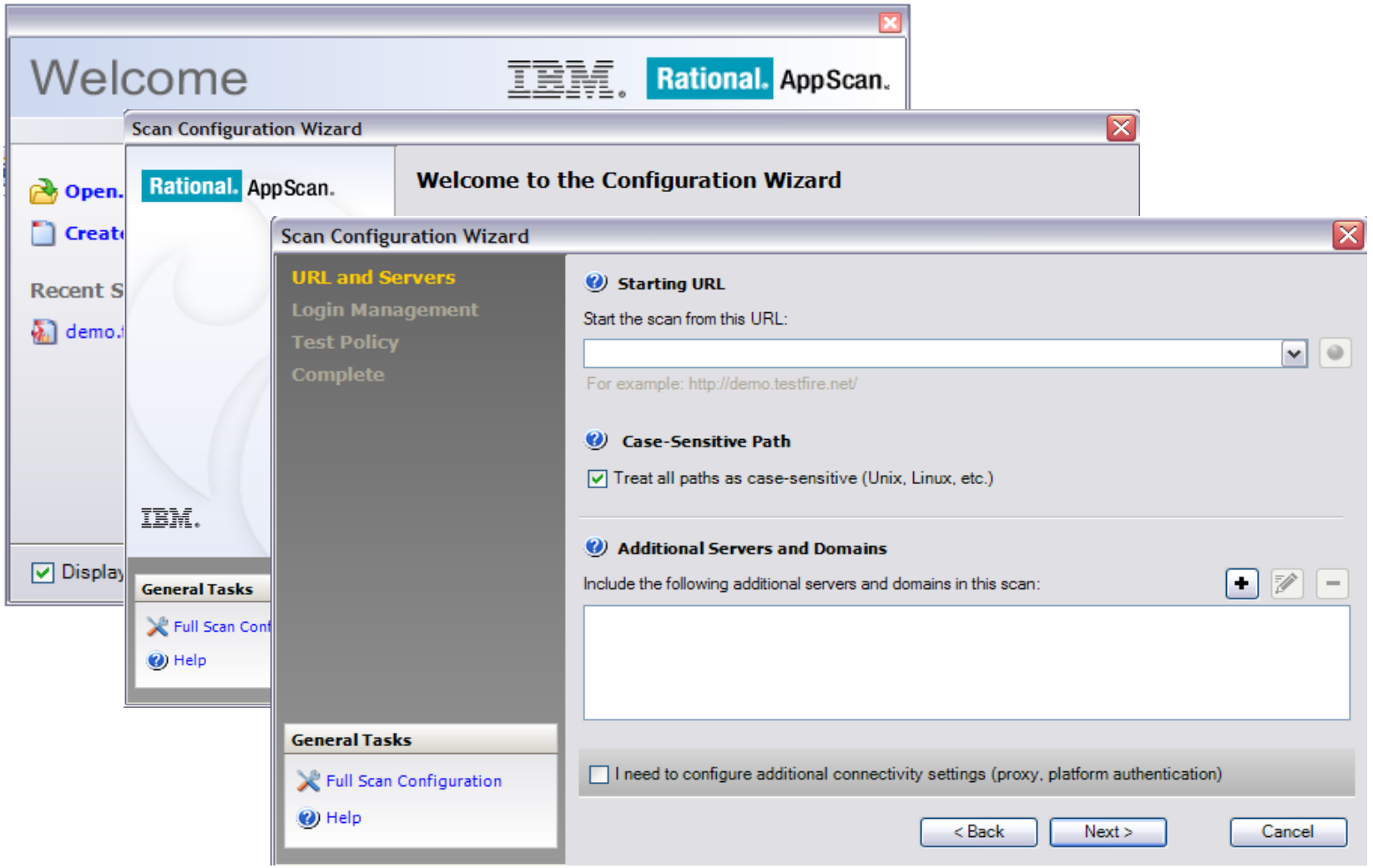
2 **Analiz Etme**

3 **Raporlama**
Detaylarıyla Bilgi İşleme

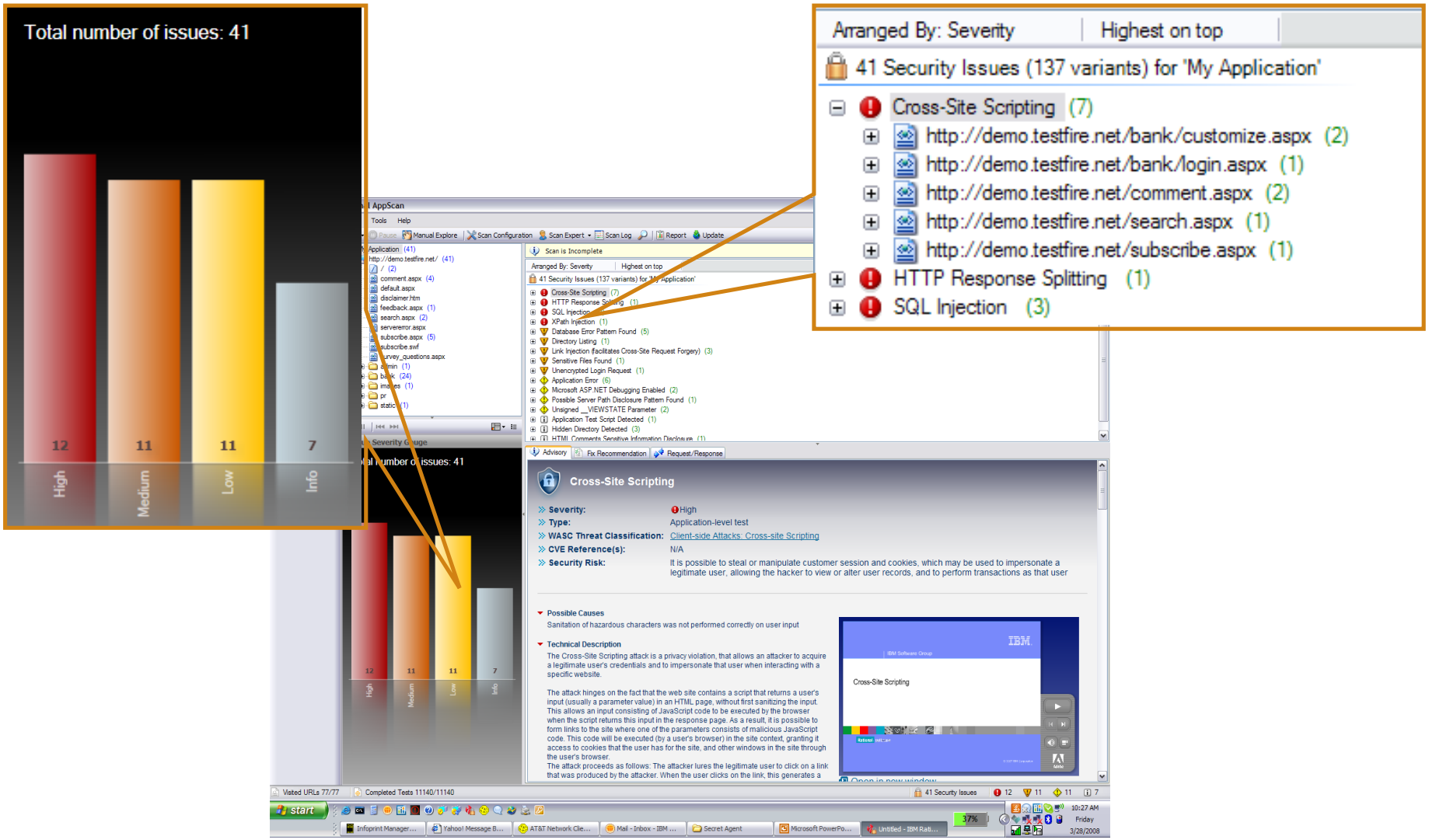
IBM Rational AppScan Standard Edition



Tarama Sihirbazı..



Kolay Sorun Algılama-Sorunlar ve Öncelikleri



Problemi Belirleme(tanımlama)

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

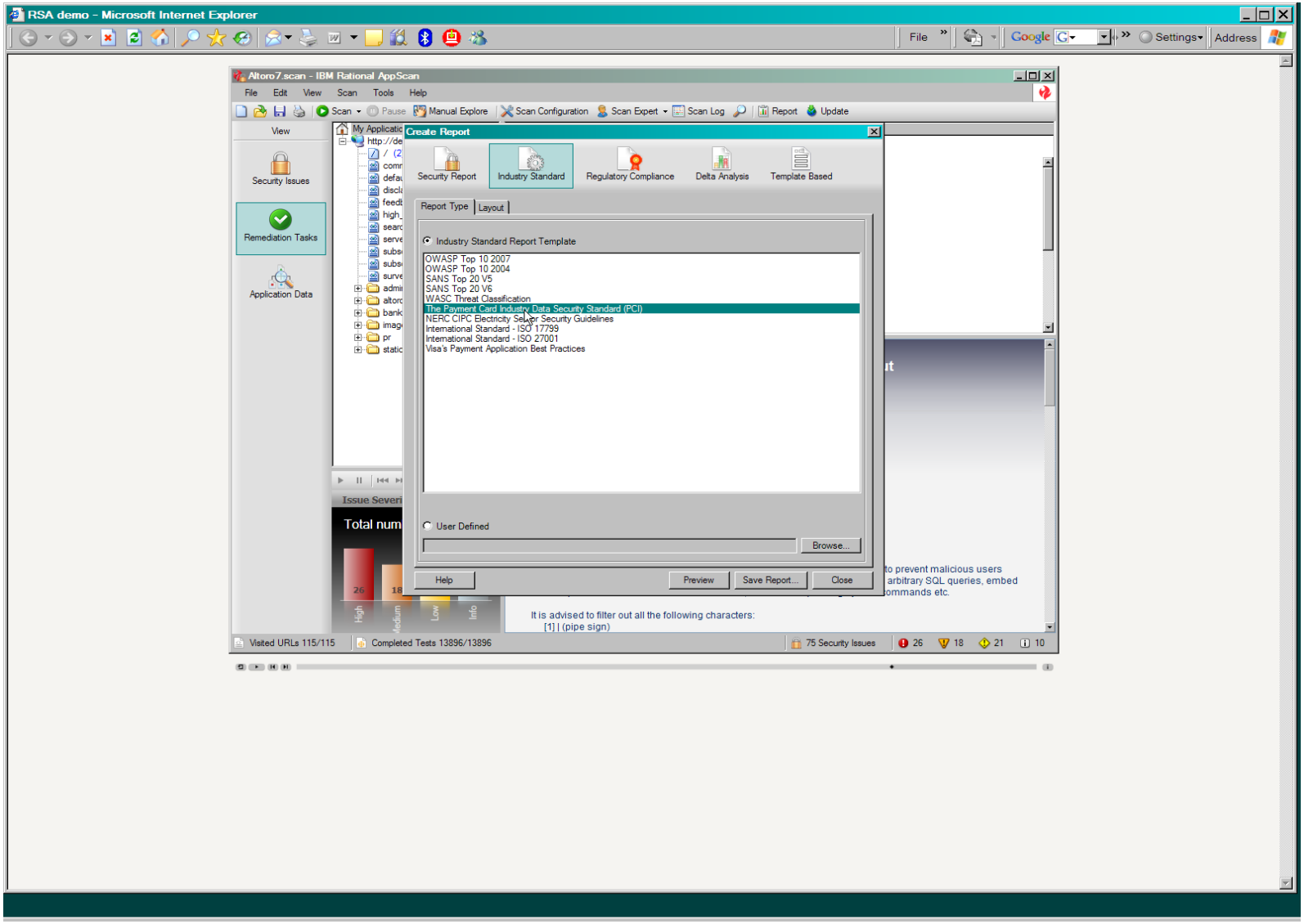
The Cross-Site Scripting attack is a privacy violation, that allows an attacker to acquire a legitimate user's credentials and to impersonate that user when interacting with a specific website.

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.

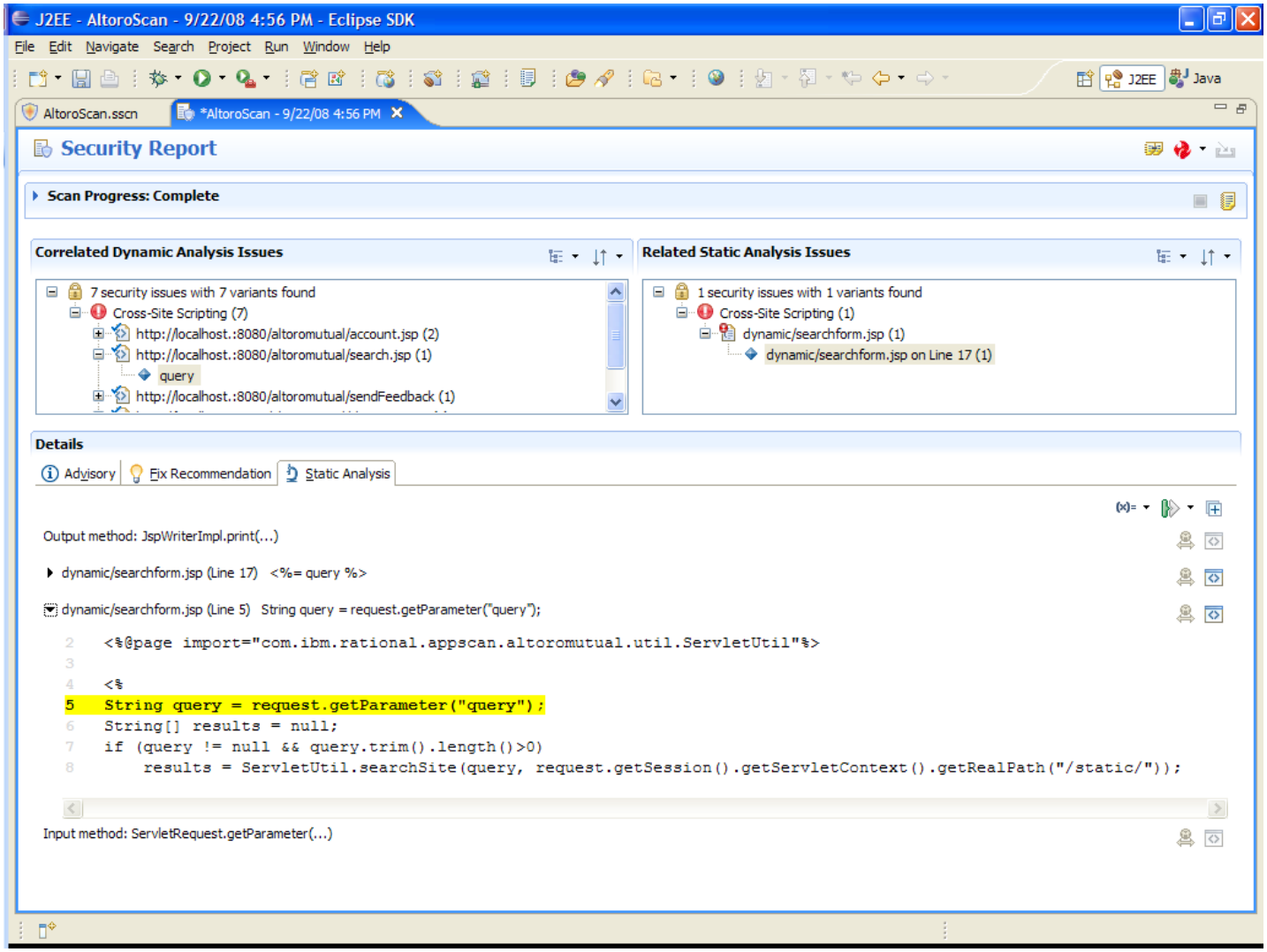
Open in new window

Gömülü Web Tabanlı (Videolu) Eğitim

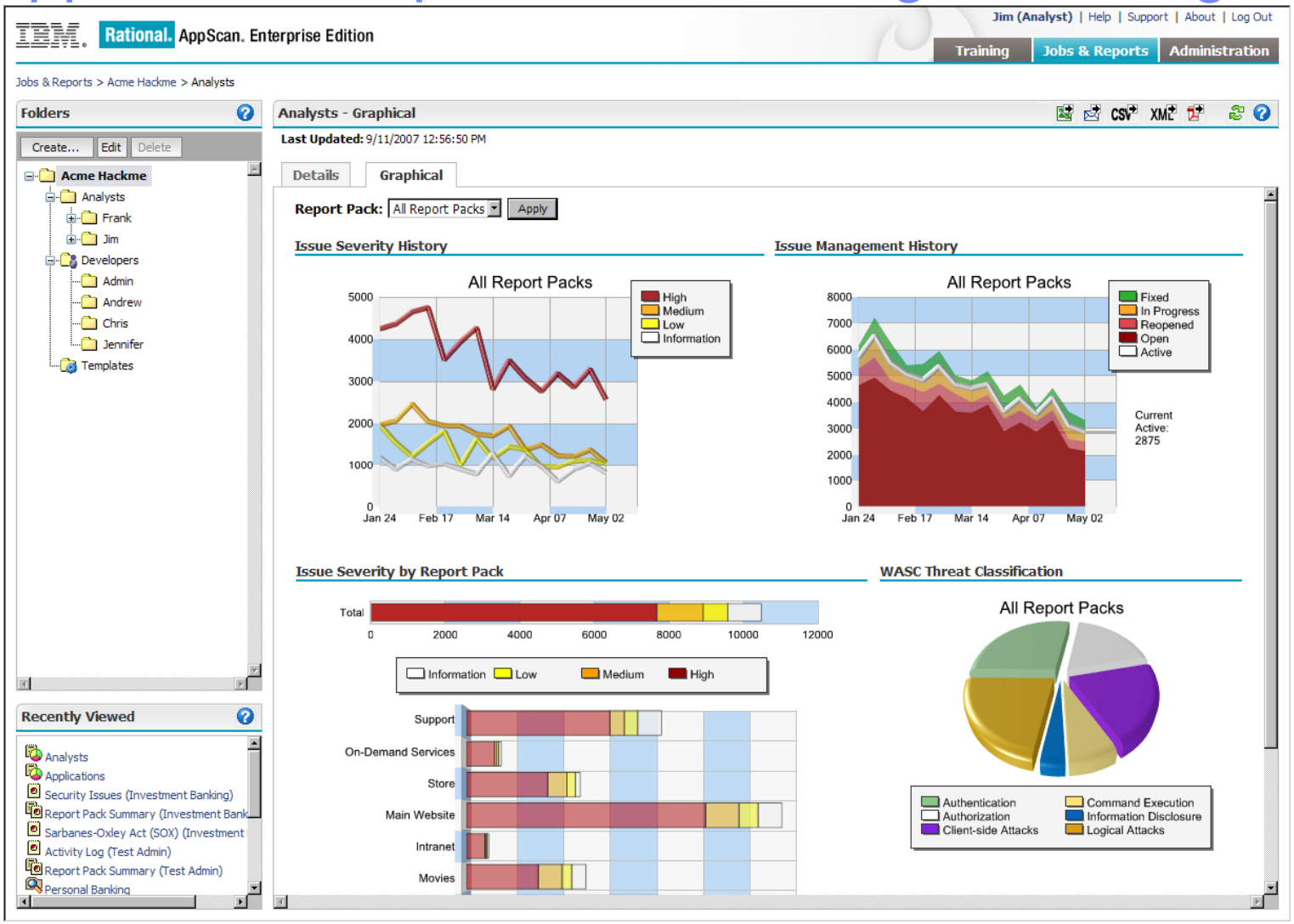
Rational AppScan: Raporlama Evresi



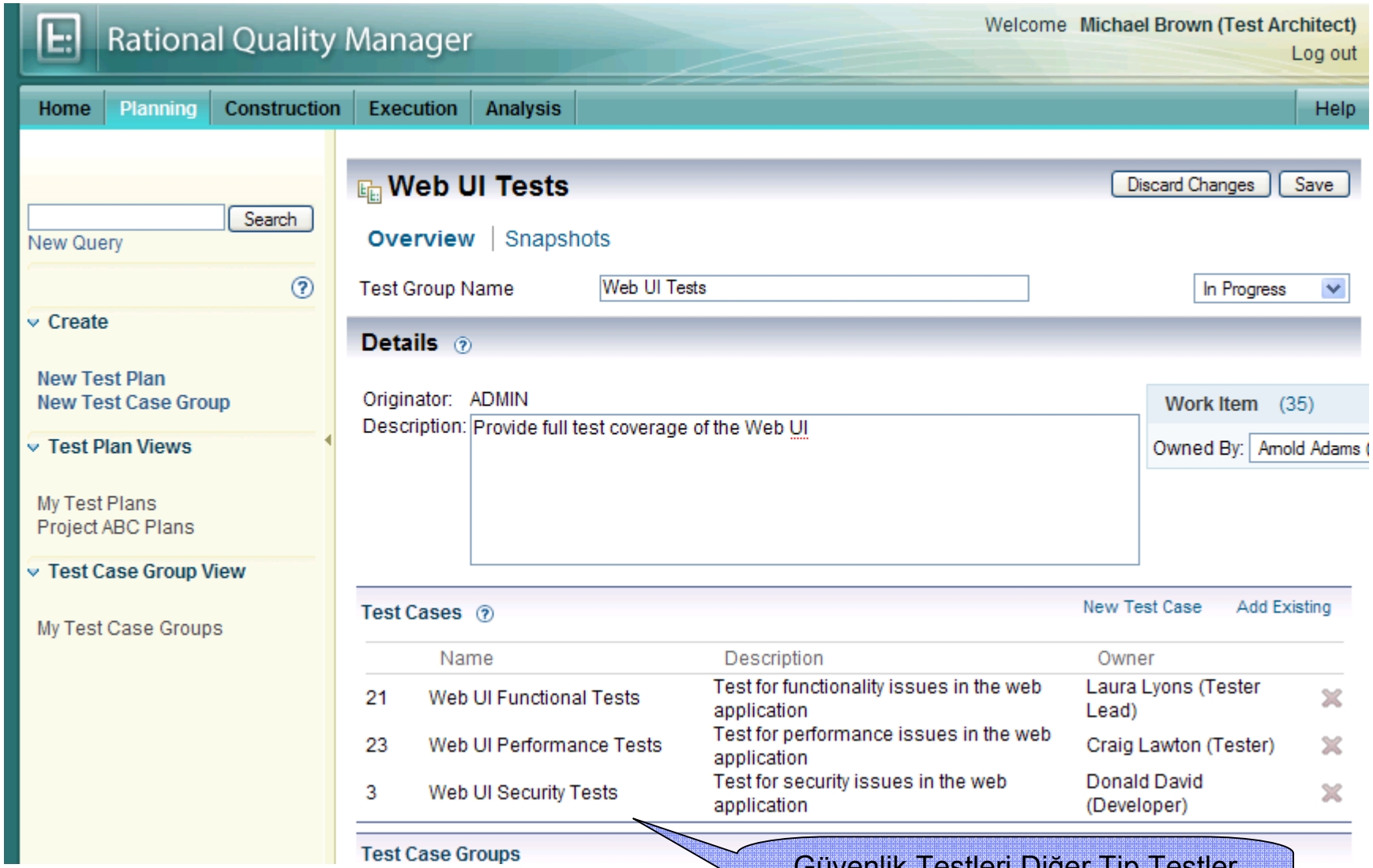
IBM Rational AppScan Developer & Build Editions



AppScan Enterprise – Metrik Değer Gösterge Panosu



RQM İçin AppScan Tester Edition



Go to IBM