NUOVI PERCORSI PER LA PUBBLICA AMMINISTRAZIONE

Domenico Ercolani
Rational Sales Specialist

domenico_ercolani@it.ibm.com *+39 335 5788700*

Come gestire al meglio la sicurezza delle applicazioni Web

IBM ITALIA aderisce al progetto Impatto Zero® di LifeGate.
Riduce e compensa le emissioni di Co2 con la creazione di nuove foreste.

Agenda

- Concetti generali di sicurezza applicativa
- Rational AppScan

Sapevate che …

75%

Degli attacchi alla sicurezza informatica sono diretti verso il livello delle applicazioni Web…

NUOVI PERCORSI PER LA
PUBBLICA AMMINISTRAZIONE

IBM

Genova - Attacco Hacker

Mar, 08/01/2008 – 11:36

fonte: il secolo XIX 06/01/08

«L'hacker ha colpito due volte»

Graziano Cetara

UN ATTACCO senza precedenti», fa sapere il minist
progredire dei controlli, sta assumendo proporzior
dell'anno nuovo, ha mandato in tilt i computer di p
caso pilota a livello nazionale e i risultati dell'indag
governo, per adottare nuove misure di sicurezza a
italiani. Le prime indagini della postale hanno scop
natura. È stato un doppio attacco, messo a segno
riguardato solo i centocinquanta terminali di palaz
postazioni dei giudici del tribunale civile, cancelleri
altro stabile.

Non solo. Il file, da indiscrezioni, non sarebbe arriv
protetta da password o da sistemi di sicurezza par
un terminale interno al tribunale. E per farlo, sarel
riservata di servizio. Le indagini sono in corso per
restringere il cerchio e arrivare in tempi brevi alla
stanno cercando di isolare il computer dal quale il
pirata. I
configu
sortito e
distrugg
procura
contem

Il server
più grav
genoves
dei mag
inquiren
potrebb
blitz potrebbe essere il frutto di una vendetta inte
criminale di un pazzo informatico senza alcuno sco

LUNEDÌ 14 gennaio 2008

CORRIERE DELLA SERA

Home | Opinioni | Corriere TV | Salute | Casa | Viaggi | Rubriche | *Il quotidiano* | Annunci | Dizionari

MA PAGINA | E-DICOLA | CORRIERE DEL MEZZOGIORNO | ARCHIVIO | INIZIATIVE IN EDICOLA | ABBONAMENTI - ORE7

Corriere della Sera » Edicola » *Archivio Storico*

edicola

ARCHIVIO DEL CORRIERE DELLA SERA

Torna indietro | Stampa

Sezione: criminalita' - Pagina: 012/013

(13 gennaio, 2008) - Corriere della Sera

Focus Gli 007 *** L' allarme dell' Fbi Secondo gli investigatori americani i pericoli maggiori vengono dagli hacker. Tra le vittime il Pentagono e il cancelliere Angela Merke. lIn Italia Sono in azione, soprattutto nel Nordest: agenti cinesi cercano di reclutare personalità per carpire notizie su prodotti nei settori della moda e dell' arredamento

PIÙ
1 «
2 I'
3 C
4 A
5 P
re

PR

Italian Bank XSS utilized by fraudsters

Posted 1/14/08 by Robert from the sanitize your input/output department

"An extremely convincing phishing attack is using a cross-site scripting vulnerability on an Italian Bank's own website to attempt to steal customers' bank account details. Fraudsters are currently sending phishing mails which use a specially-crafted URL to inject a modified login form onto the bank's login page.

The vulnerable page is served over SSL with a bona fide SSL certificate issued to Banca Fideuram S.p.A. in Italy. Nonetheless, the fraudsters have been able to inject an IFRAME onto the login page which loads a modified login form from a web server hosted in Taiwan. "

Good real life example of XSS being used.

pedine. Una battaglia che allarma i nostri James Bond: «Siamo tornati all' epoca della guerra fredda», è l' analisi delle intelligence Nato. Dal cielo e dal mare Le ombre che vengono da Mosca amano i nuovi mezzi di infiltrazione - leggi Internet - ma non abbandonano la tradizione. I loro aerei hanno ripreso le ricognizioni ai confini dei Paesi dell' Alleanza Atlantica. Voli di disturbo per mostrare le ali e buttare un occhio - elettronico - su quello che accade. In Mediterraneo, invece, sono tornate le vecchie navi spia

«L
nu
15::
coll

la Repubblica.it | Tecnologia&Scienze

Home | Affari&Finanza | Sport | Spettacoli&Cultura | Tecnologie&Scienze | Motori | Moda | Viaggi | Roma | Milano

Salute

Tecnologie&Scienze

- Prodotti
- Sicurezza Web
- VideoGiochi
- Mondo Mac
- Software
- Come fare
- Gallerie

TECNOLOGIA & SCIENZA

Stampa Invia

Due cronisti e un hacker aggirano il sistema di sicurezza
Milioni di utenti a rischio truffa. Possibile accedere a dati e password

Nel grande buco nero di eBay "Così abbiamo violato il sito"

di MARCO MENSURATI e FABIO TONACCI

La sede centrale di eBay in California

ROMA – C'è un buco nel sistema di sicurezza di eBay. Un buco che si apre e che si chiude di continuo, come la porta automatica di un grande magazzino. E che permette a qualunque hacker minimamente capace di entrare in possesso delle informazioni personali riservate dei clienti. E di derubarli. Noi questo buco lo abbiamo individuato, lo abbiamo aperto e poi ci siamo entrati dentro (il video si può vedere sul sito di RepubblicaTv).

Dimostrando, così, quanto sia semplice rubare i dati personali e bancari degli utenti eBay che partecipavano a una determinata asta. Un'asta come tante, usata però come esca. Con l'aiuto di un hacker abbiamo sfruttato quella che tecnicamente si chiama vulnerabilità "cross-site scripting". L'operazione non è così complessa come sembra.

EBay, il più grande sito di compravendita online, dà la possibilità agli utenti che ritiene affidabili di abbellire graficamente le proprie pagine con particolari linguaggi di programmazione. Consegna loro delle chiavi per interagire con la grafica ufficiale, personalizzando l'architettura del sito. Con quelle chiavi – ottenute piuttosto facilmente – gli hacker costruiscono delle aste trappola (non c'è modo di distinguerle da quelle originali) e le dispongono ovunque, in quel suk virtuale che è eBay.

TECNOLOGIA

CRONACHE | COSTUME | ECONOMIA | TECNO

MODA | MOTORI | SCIENZA | SCUOL

iminali
Veb

esse da criminali informatici per
ettendo in atto uno dei più grandi

irizza in automatico i visitatori a
a di entrare nel PC dell'utente. I
e il navigatore possa rendersene

ano normalmente su Internet
libero. Persino i siti web affidabili

affermato Craig Schmugar,
glio giusto, ma non è sufficiente.

mato le pagine web tramite un
server non protetti e il successivo
dirizzare verso un sito che si trova
rabilità in Windows, RealPlayer e

ne. Una back door permette la
iminali informatici stanno

Il mito: “Il nostro sito Web è sicuro”

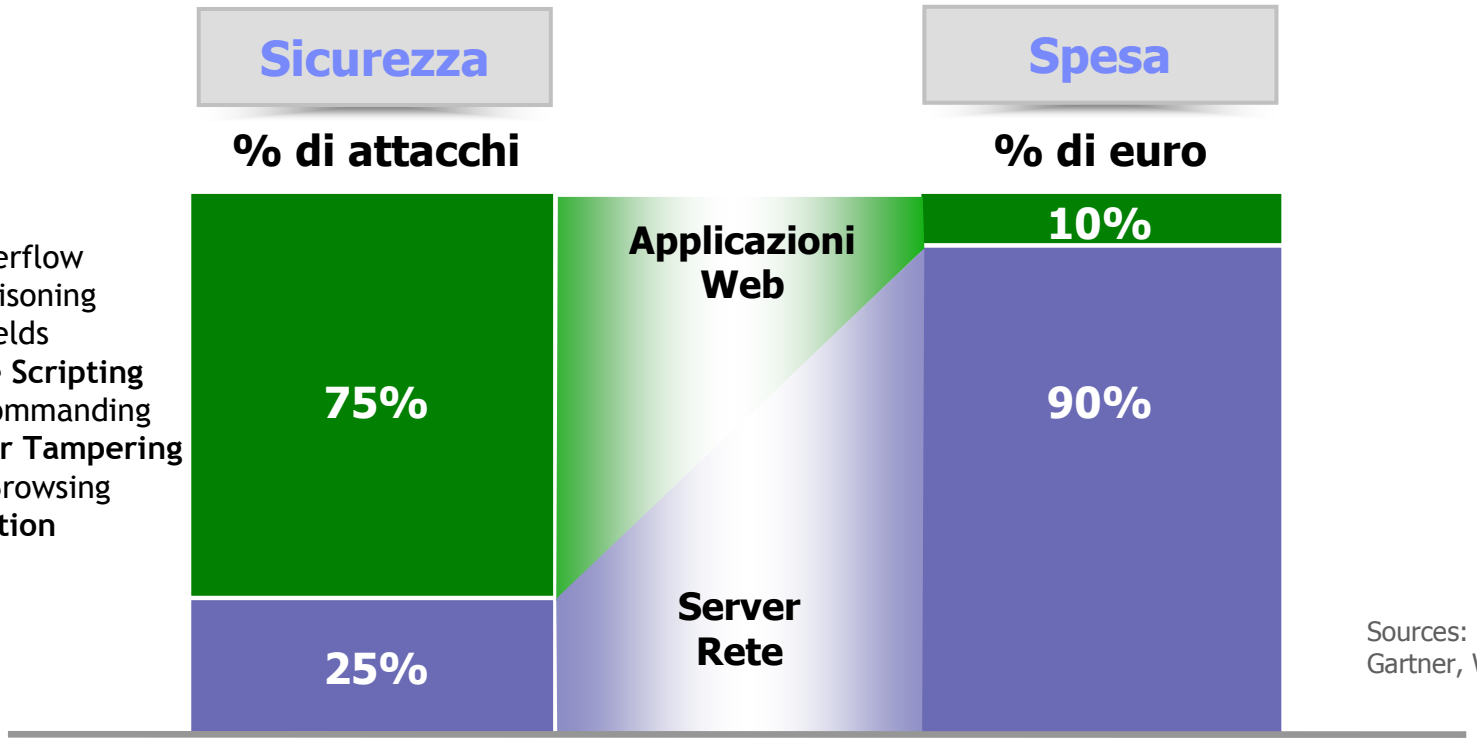
Abbiamo dei Firewalls

Abbiamo dei revisori che effettuano ogni trimestre test di intrusione

Utilizziamo strumenti di controllo della vulnerabilità della rete

La realtà: sicurezza e spesa non sono bilanciati

- Buffer Overflow
- Cookie Poisoning
- Hidden Fields
- **Cross Site Scripting**
- Stealth Commanding
- **Parameter Tampering**
- Forceful Browsing
- **SQL Injection**
- Etc…



Sources:
Gartner, Watchfire

75% degli attacchi alla sicurezza informatica sono diretti verso il livello delle applicazioni Web

2/3 di tutte le applicazioni Web sono considerate vulnerabili

Gartner

Lista OWASP “Top 10” (Open Web Application Security Project)

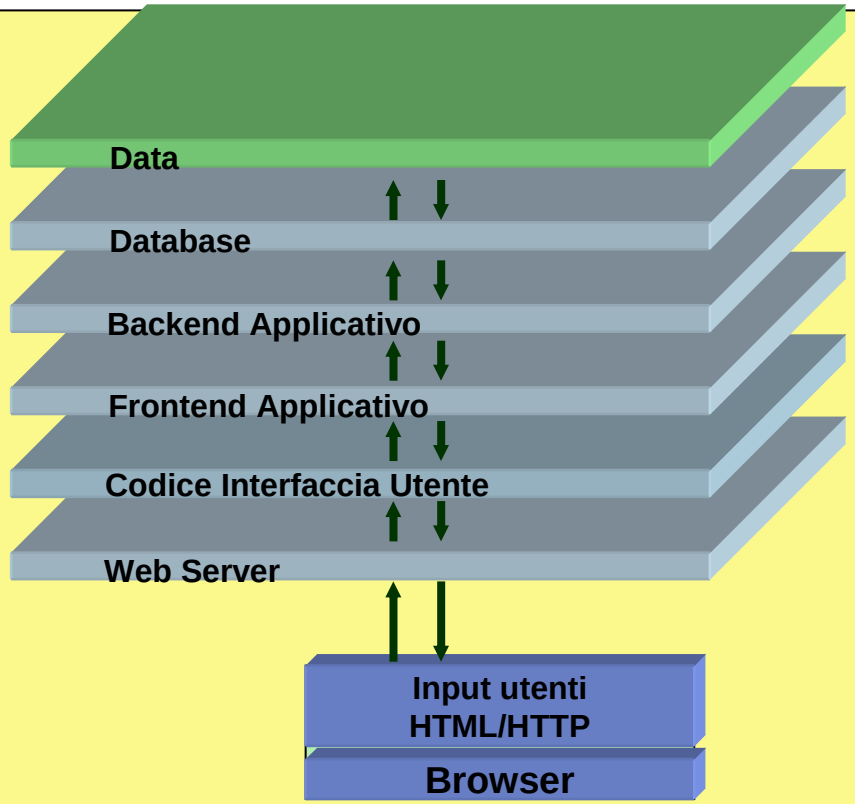
Tipologia attacco	Impatto negativo	Esempio di impatto
Cross Site Scripting	Identity Theft, Sensitive Information Leakage, …	Hackers can impersonate legitimate users, and control their accounts.
Injection Flaws	Attacker can manipulate queries to the DB / LDAP / Other system	Hackers can access backend database information, alter it or steal it.
Malicious File Execution	Execute shell commands on server, up to full control	Site modified to transfer all interactions to the hacker.
Insecure Direct Object Reference	Attacker can access sensitive files and resources	Web application returns contents of sensitive file (instead of harmless one)
Cross-Site Request Forgery	Attacker can invoke “blind” actions on web applications, impersonating as a trusted user	Blind requests to bank account transfer money to hacker
Information Leakage and Improper Error Handling	Attackers can gain detailed system information	Malicious system reconnaissance may assist in developing further attacks
Broken Authentication & Session Management	Session tokens not guarded or invalidated properly	Hacker can “force” session token on victim; session tokens can be stolen after logout
Insecure Cryptographic Storage	Weak encryption techniques may lead to broken encryption	Confidential information (SSN, Credit Cards) can be decrypted by malicious users
Insecure Communications	Sensitive info sent unencrypted over insecure channel	Unencrypted credentials “sniffed” and used by hacker to impersonate user
Failure to Restrict URL Access	Hacker can access unauthorized resources	Hacker can forcefully browse and access a page past the login page

Previsione di Gartner sulla sicurezza applicativa

"Entro il 2009, l'80% delle aziende dovranno affrontare problemi di sicurezza applicativa e, di conseguenza, dovranno provvedere identificando ruoli adeguati nei team di sviluppo e di test per garantire che la sicurezza sia introdotta e gestita anche al livello applicativo"

"Entro il 2008, la sicurezza applicativa diventerà un importante criterio di valutazione, paragonabile a quello di accessibilità al sistema"

Come è fatta un'applicazione Web?



- **La logica di business abilita:**
  - Le interazioni utente con il sito Web
  - La transazionalità e l'interfacciamento con i sistemi di backend (databases, CRM, ERP, etc)
- **Sotto forma di:**
  - Pacchetti software di terze parti (e.g. web server, application server, pacchetti software, etc.)
  - Codice sviluppato in casa o da system integrator

I flussi di input e di output passano attraverso ogni livello dell'applicazione.

Una vulnerabilità in uno dei livelli può causare danni all'intera applicazione.

Le soluzioni infrastrutturali non indirizzano questa problematica

Firewalls e IPS (Intrusion Prevention System)

non bloccano eventuali attacchi al livello applicativo

La porta 80 è disponibile per essere utilizzata.

Strumenti di scansione della rete non identificano eventuali vulnerabilità applicative

Nessus, IBM ISS, Qualys, Nmap, etc.

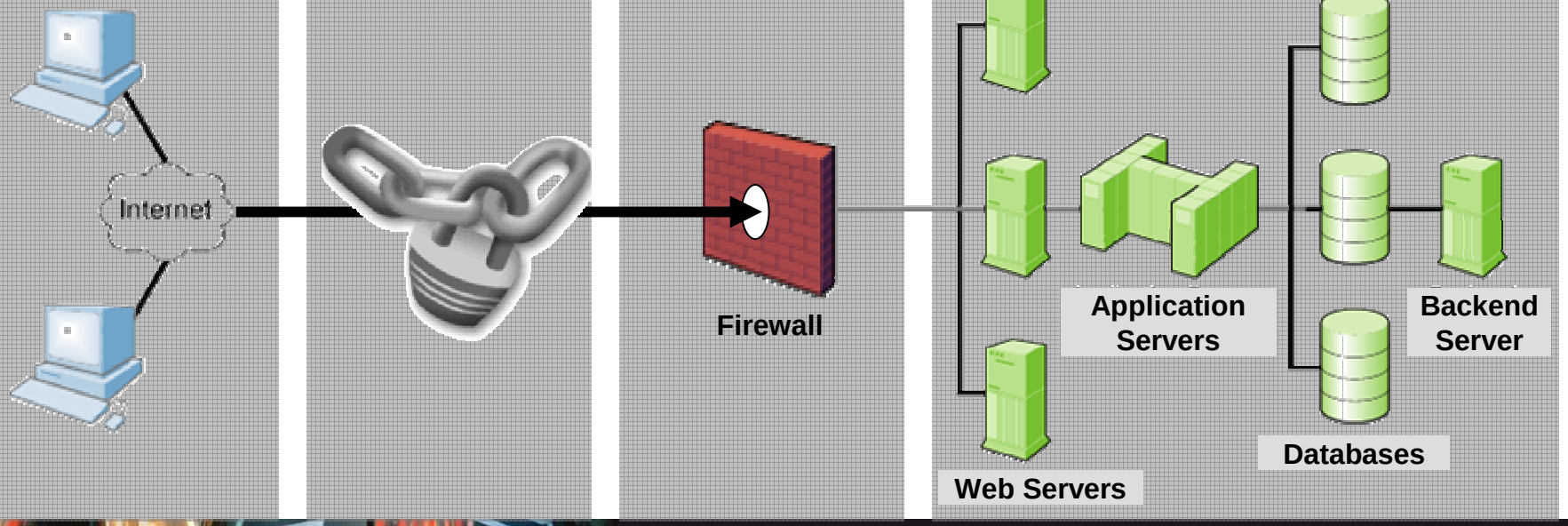
Chi sviluppa applicazioni Web non ha conoscenze adeguate di sicurezza applicativa

64% degli sviluppatori non sono confidenti di poter scrivere applicazioni sicure
(fonte Microsoft Developer Research)

Livelli di sicurezza aziendale

Rational. software

PC	Trasporto	Rete	Applicazioni Web
Protezioni Antivirus	Crittografia (SSL)	Firewalls / Routers	



Perché la sicurezza nelle applicazioni Web dovrebbe essere parte di un programma di gestione del rischio?

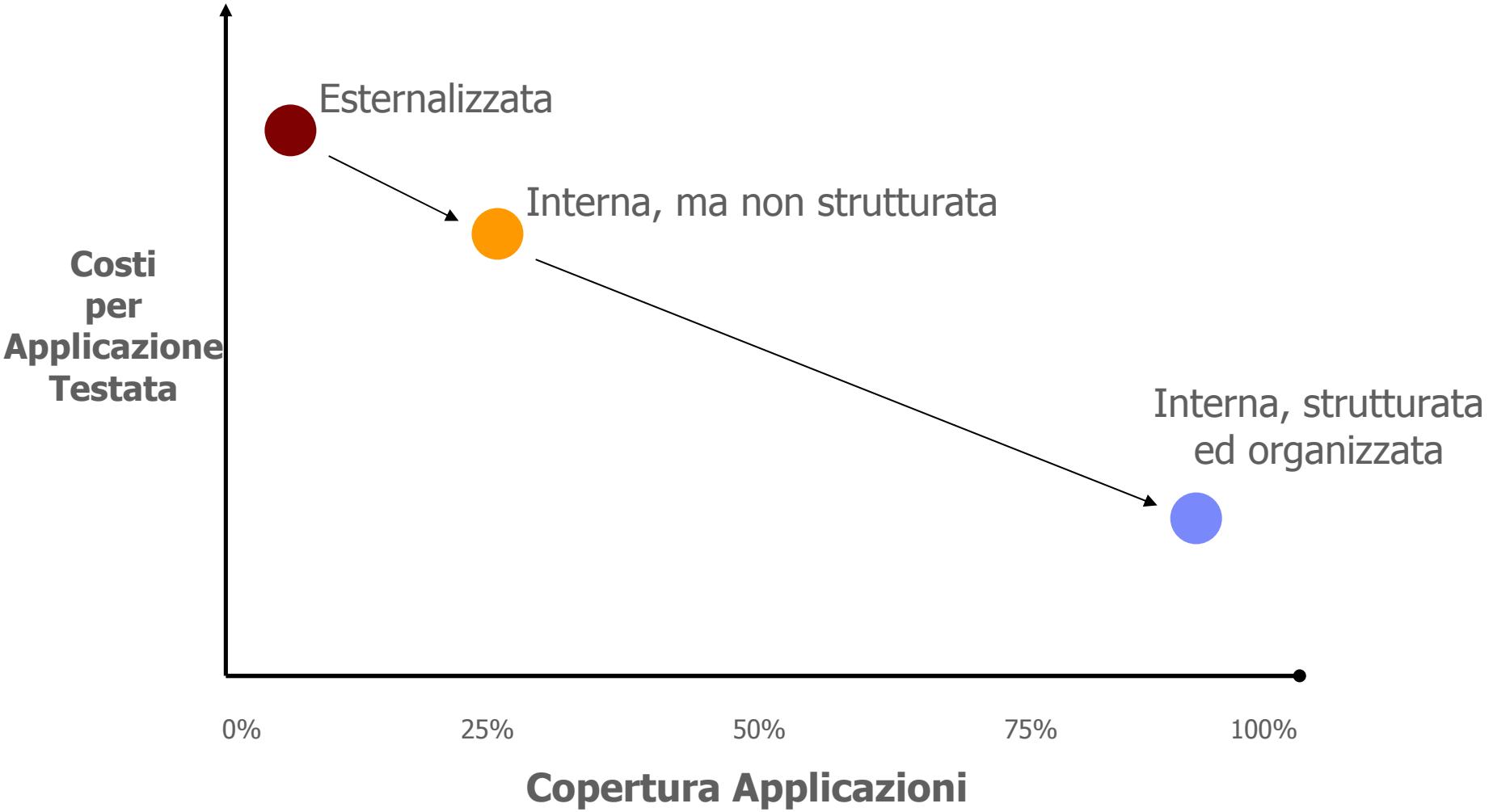
- Ridurre i costi dei *Recovery & Fixes*
- Ridurre il costo dei test di sicurezza aumentando la copertura
- Assicurare la fiducia nei clienti
- Promuovere l'adozione nell'uso dei siti Web
- Portare un vantaggio competitivo

Quanto costa correggere i problemi?

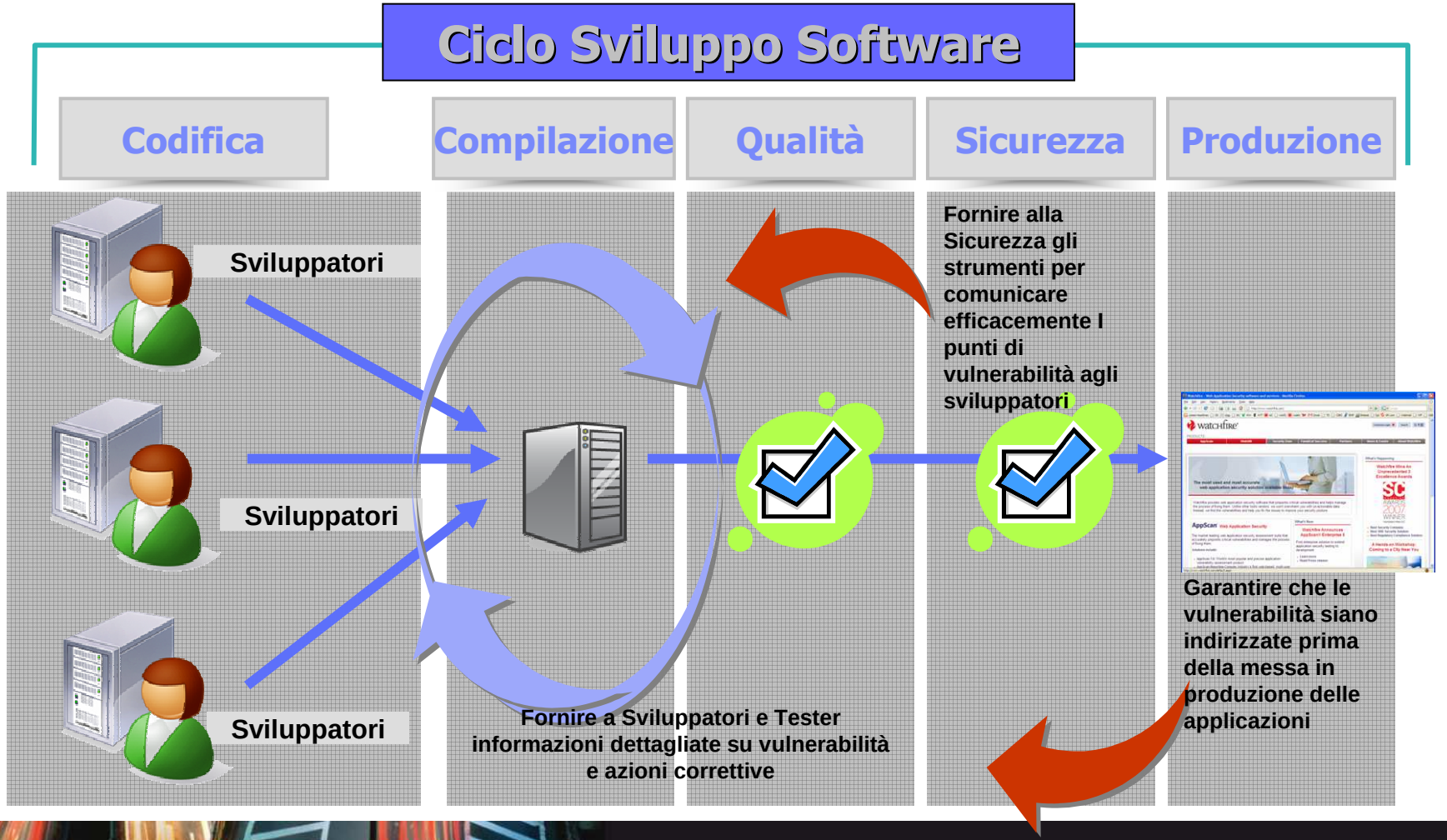
	Scoperti in fase di Disegno	Scoperti in fase di Codifica	Scoperti in Integrazione	Scoperti in Collaudo - PreProduzione	Scoperti in Produzione
Errori Architetturali	1x	5x	10x	15x	30x
Errori di Codifica		1x	10x	20x	30x
Errori di Integrazione			1x	10x	20x

* Rapporto dettagliato su costi ed impatti: http://www.nist.gov/director/prog-ofc/report02-3.pdf

Riduzione costi, aumento copertura

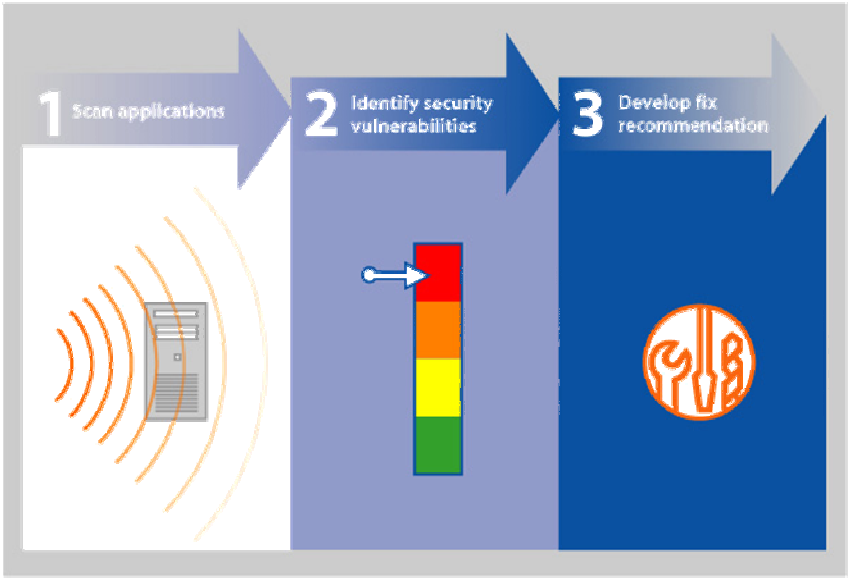


Gestire la sicurezza durante l'intero ciclo di sviluppo



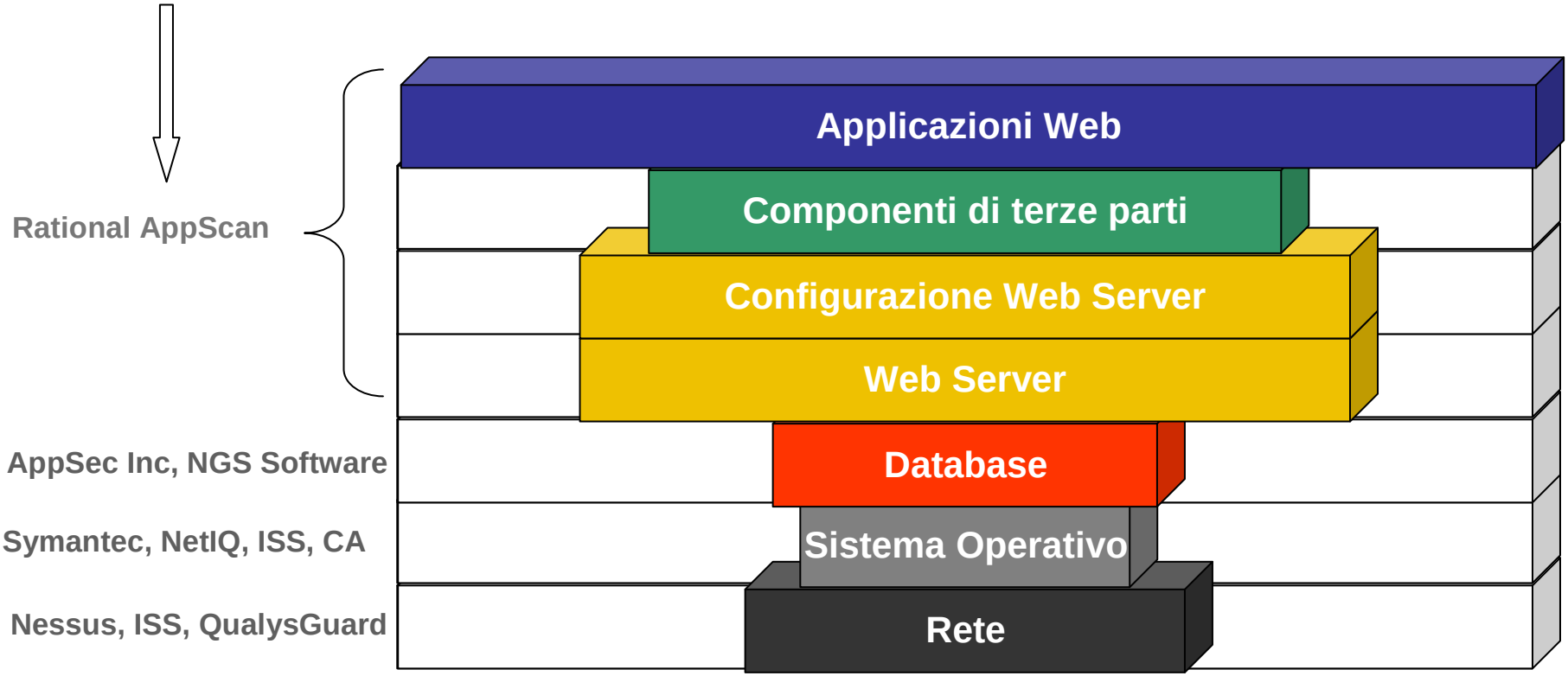
Soluzione: IBM Rational AppScan

- AppScan è la soluzione leader di mercato per l'identificazione delle vulnerabilità della sicurezza applicativa e del relativo processo di risoluzione
- Fornisce report descrittivi ed operativi con azioni e raccomandazioni concrete
- AppScan offre una soluzione per tutte le tipologie di test di sicurezza applicativa - esternalizzato, a livello utente o aziendale
- AppScan automatizza le attività di test della sicurezza applicativa durante l'intero ciclo di sviluppo
  - Dagli sviluppatori per costruire applicazioni sicure
  - Dai responsabili della qualità per garantire che le applicazioni siano sicure prima di essere rilasciate
  - Dai certificatori per monitorare continuamente lo stato della sicurezza



Qual’è il focus principale di IBM Rational AppScan?

Strumenti di scansione delle vulnerabilità e aree impattate



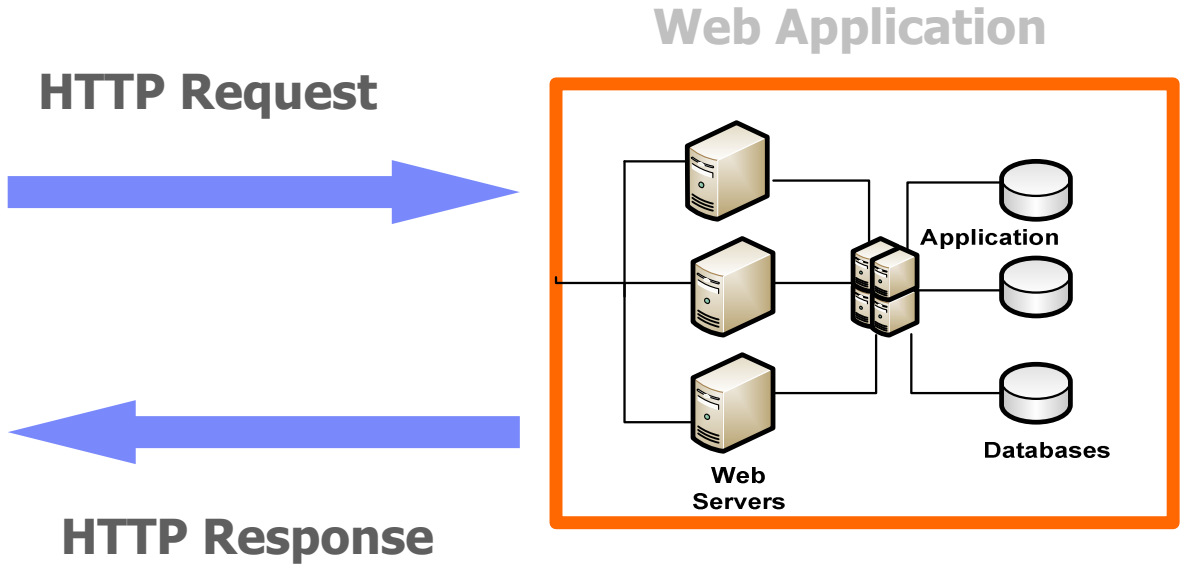
Come lavora IBM Rational AppScan?

Ha un approccio di tipo “black-box”

Naviga sull’applicazione e costruisce il “site model”

Determina i tipi di attacchi basandosi sulle “Test policy” selezionate

Esegue i test mandando verso l’applicazione richieste HTTP modificate ed esaminando le risposte HTTP utilizzando regole di validazione



Configurazioni tipiche di IBM Rational AppScan

Utilizzo completo a livello aziendale
Rational AppScan Enterprise

Capacità di eseguire i controlli sulle vulnerabilità da parte di tutti i ruoli impattati e relativa condivisione dei dati

Accesso report a livello aziendale
Rational AppScan Reporting Console

Accesso alle informazioni relative alle vulnerabilità identificate da parte di tutti i ruoli impattati

Audit/certificatori interni
Rational AppScan

Verifica regolare delle vulnerabilità applicative da parte di organismi interni di controllo

Test esternalizzati

Utilizzo di consulenti esterni per test effettuati su un numero ristretto di applicazioni critiche

IBM Rational AppScan Enterprise

IBM Rational Software Quality Management

BUSINESS

SVILUPPO

SOLUZIONI DI GESTIONE DELLA QUALITA'

Test e Gestione Cambiamenti

Requisiti	Test	Cambiamenti	Difetti
Rational RequisitePro	Rational ClearQuest	Rational ClearQuest	Rational ClearQuest

Automazione Test

Test Sviluppo
Rational PurifyPlus
Rational Test RealTime

Test Funzionale
Rational Functional Tester Plus

Automatici	Manuali
Rational Functional Tester	Rational Manual Tester
Rational Robot	

Test Sicurezza e Conformità
AppScan
Policy Tester

Test Prestazionale
Rational Performance Tester

Metriche Qualità

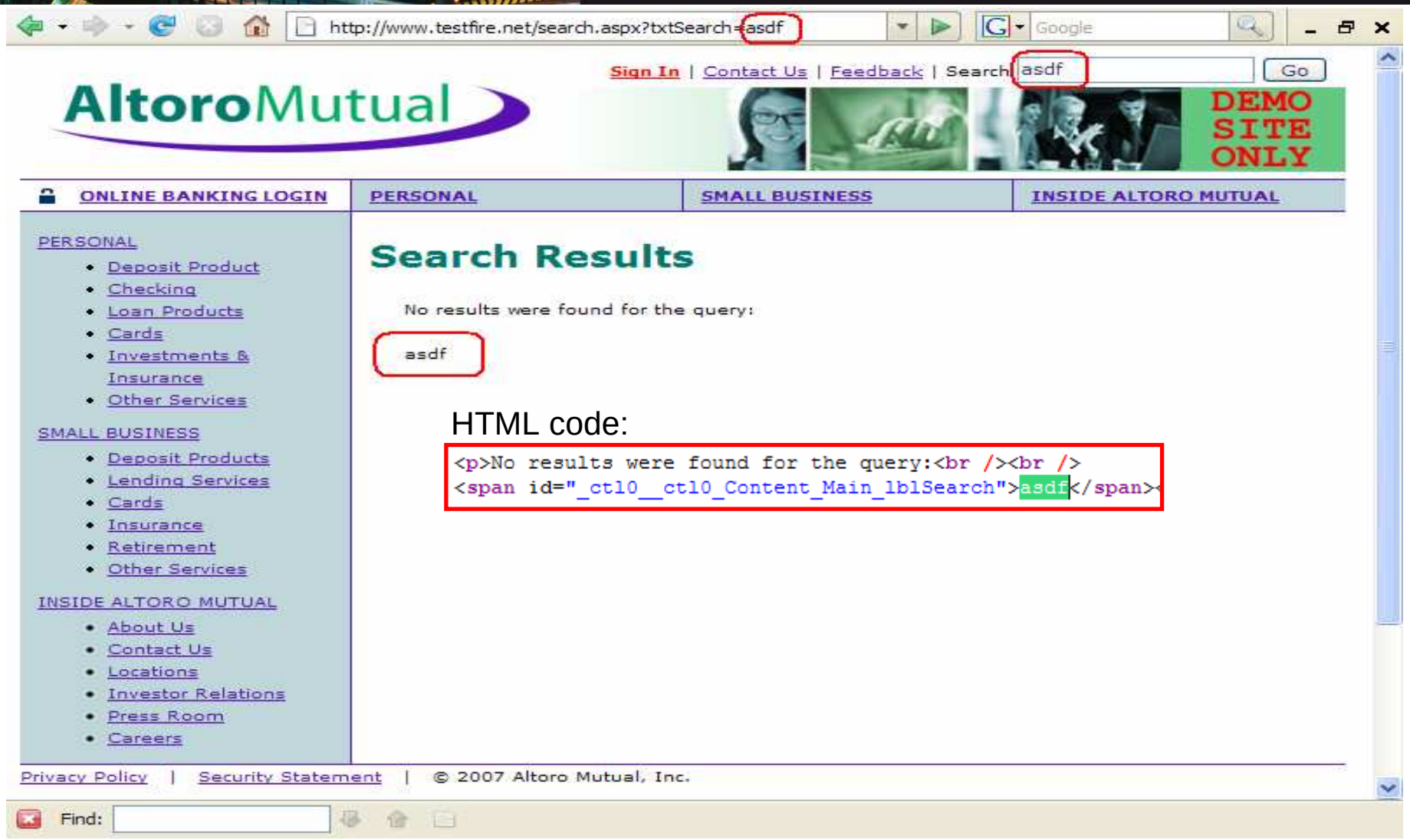
Controllo Progetti **Dettaglio Risultati Test** **Report Qualità**

ESERCIZIO

BACK UP

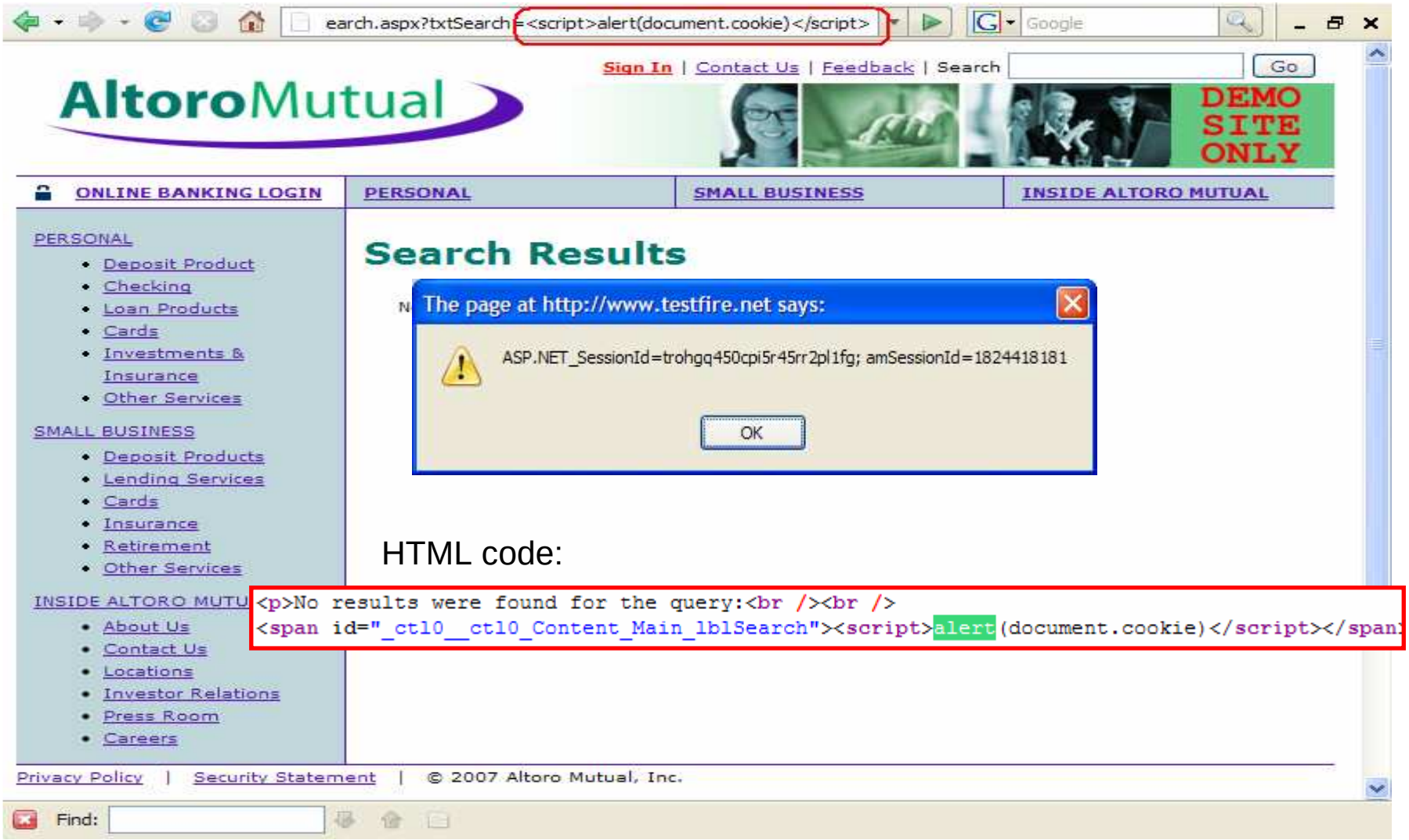
Example 1. Cross-Site Scripting (XSS)

- What is it?
  - Malicious script echoed back into HTML returned from a trusted site, and runs under trusted context
- What are the implications?
  - Session Tokens stolen (browser security circumvented)
  - Complete page content compromised
  - Future pages in browser compromised



HTML code:

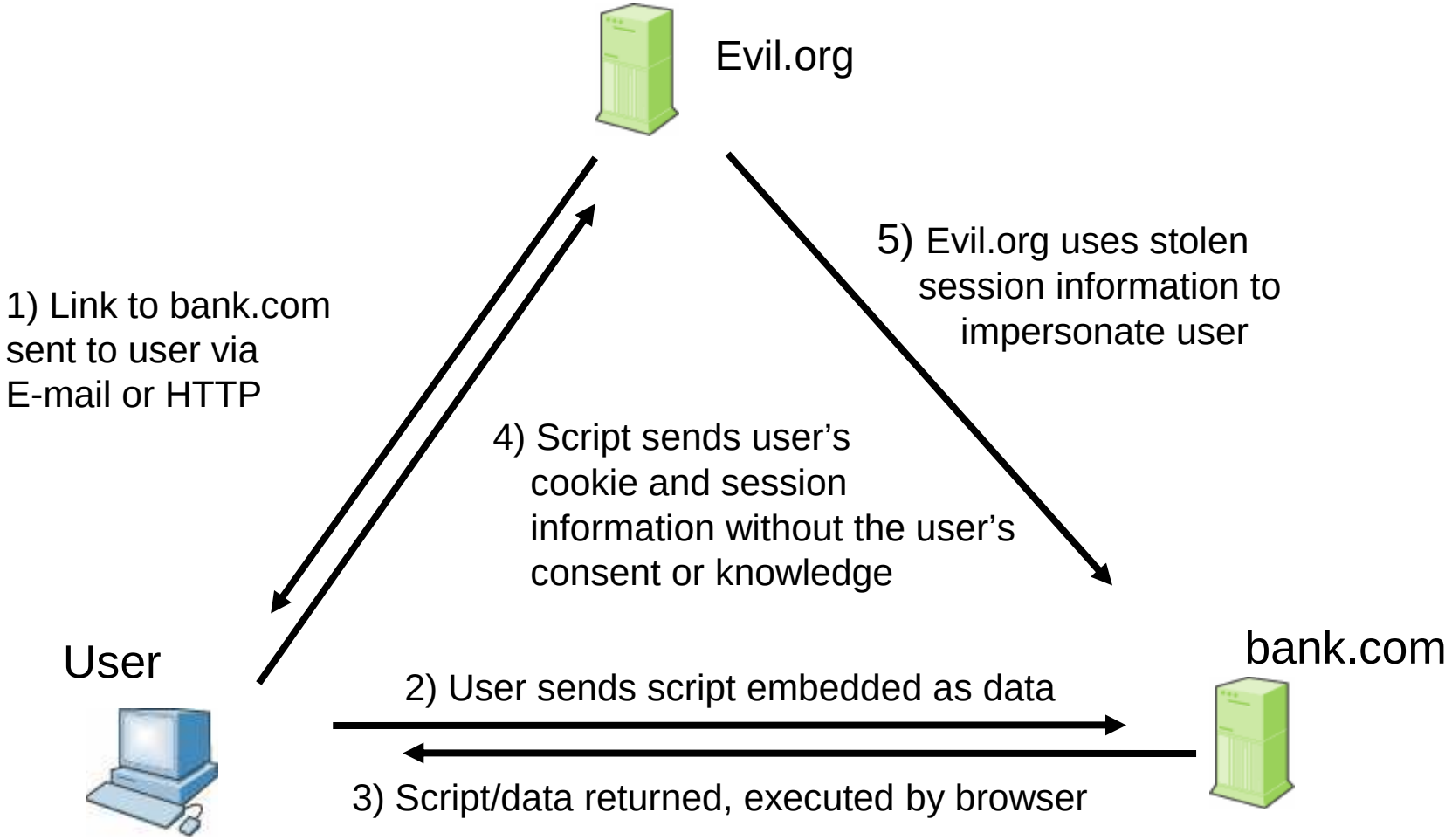
```
<p>No results were found for the query:<br /><br />
<span id="_ctl0__ctl0_Content_Main_lblSearch">asdf</span>
```



XSS – Details

- Common in Search, Error Pages and returned forms.
  - But can be found on any type of page
- Any input may be echoed back
  - Path, Query, Post-data, Cookie, Header, etc.
- Browser technology used to aid attack
  - XMLHttpRequest (AJAX), Flash, IFrame…
- Has many variations
  - XSS in attribute, DOM Based XSS, etc.

Cross Site Scripting – The Exploit Process



Exploiting XSS

- If I can get you to run my JavaScript, I can…
  - Steal your cookies for the domain you're browsing
  - Track every action you do in that browser from now on
  - Redirect you to a Phishing site
  - Completely modify the content of any page you see on this domain
  - Exploit browser vulnerabilities to take over machine
  - …

XSS is the Top Security Risk today (most exploited)

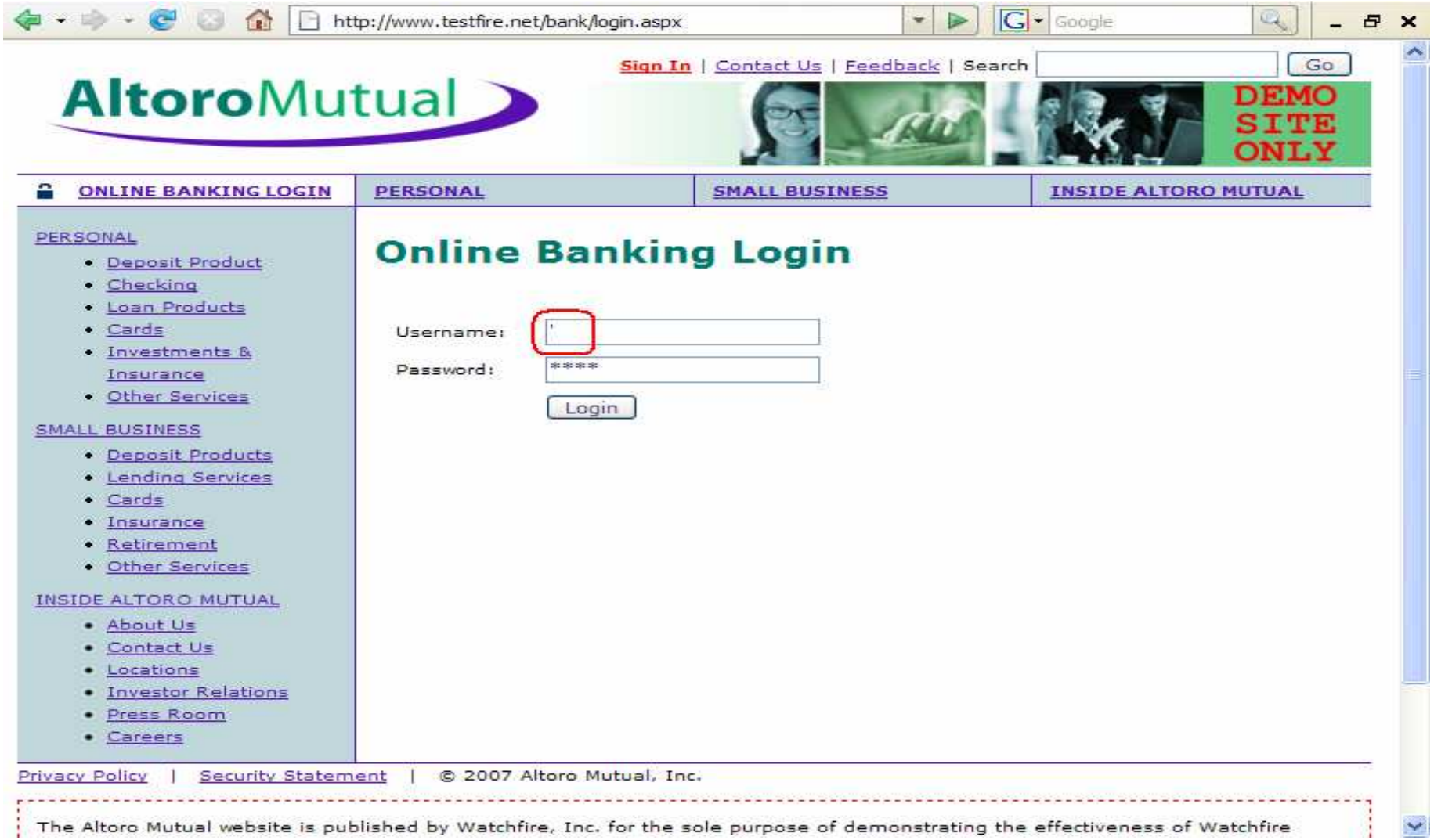
Example 2 - Injection Flaws

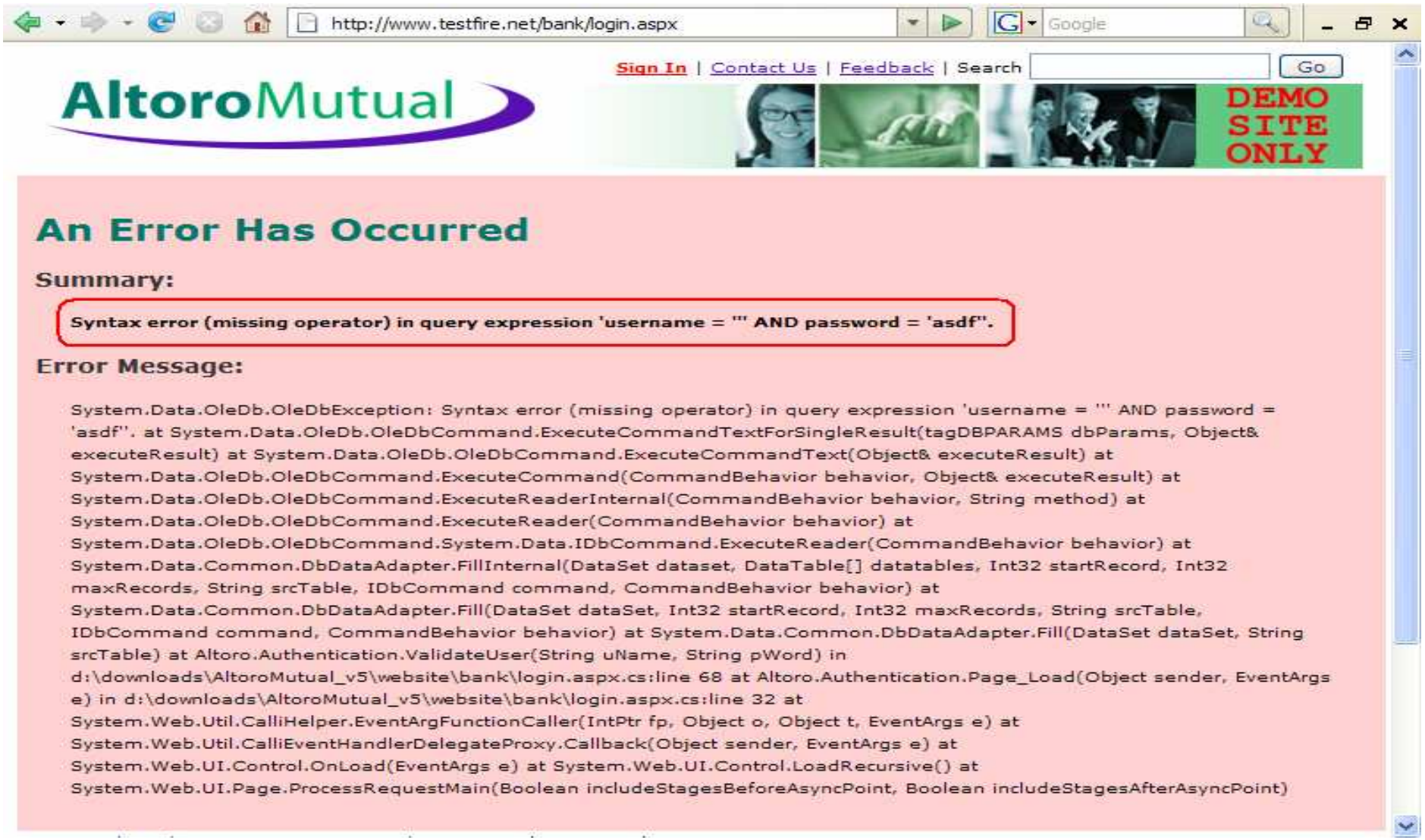
- What is it?
  - User-supplied data is sent to an interpreter as part of a command, query or data.

- What are the implications?
  - SQL Injection – Access/modify data in DB
  - SSI Injection – Execute commands on server and access sensitive data
  - LDAP Injection – Bypass authentication
  - …

SQL Injection

- User input inserted into SQL Command:
  - Get product details by id:
    Select * from products where id='$REQUEST["id"]';
  - Hack: send param id with value ' or '1'='1
  - Resulting executed SQL:
    Select * from products where id='' or '1'='1'
  - All products returned





http://www.testfire.net/bank/login.aspx

Google

Sign In | Contact Us | Feedback | Search ' Go

AltoroMutual

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

http://www.testfire.net/bank/main.aspx

Google

Sign Off | Contact Us | Feedback | Search Go

AltoroMutual

DEMO SITE ONLY

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: 1001160140 Checking GO

Congratulations!

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

Click Here to apply.

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 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.

Copyright © 2007, Watchfire Corporation, All rights reserved.

Find: