

Watchfire, an IBM Company: an introduction to web application security

Presented by:
John Burroughs, CISSP
Sr. Security Architect
jburroughs@uk.ibm.com

IBM Rational Software Development Conference UK 2007



What keeps me **Rational**?



Agenda

- The Security Landscape
- An Overview of Security Vulnerabilities



Web Application Security Landscape

IBM Rational Software Development Conference UK 2007



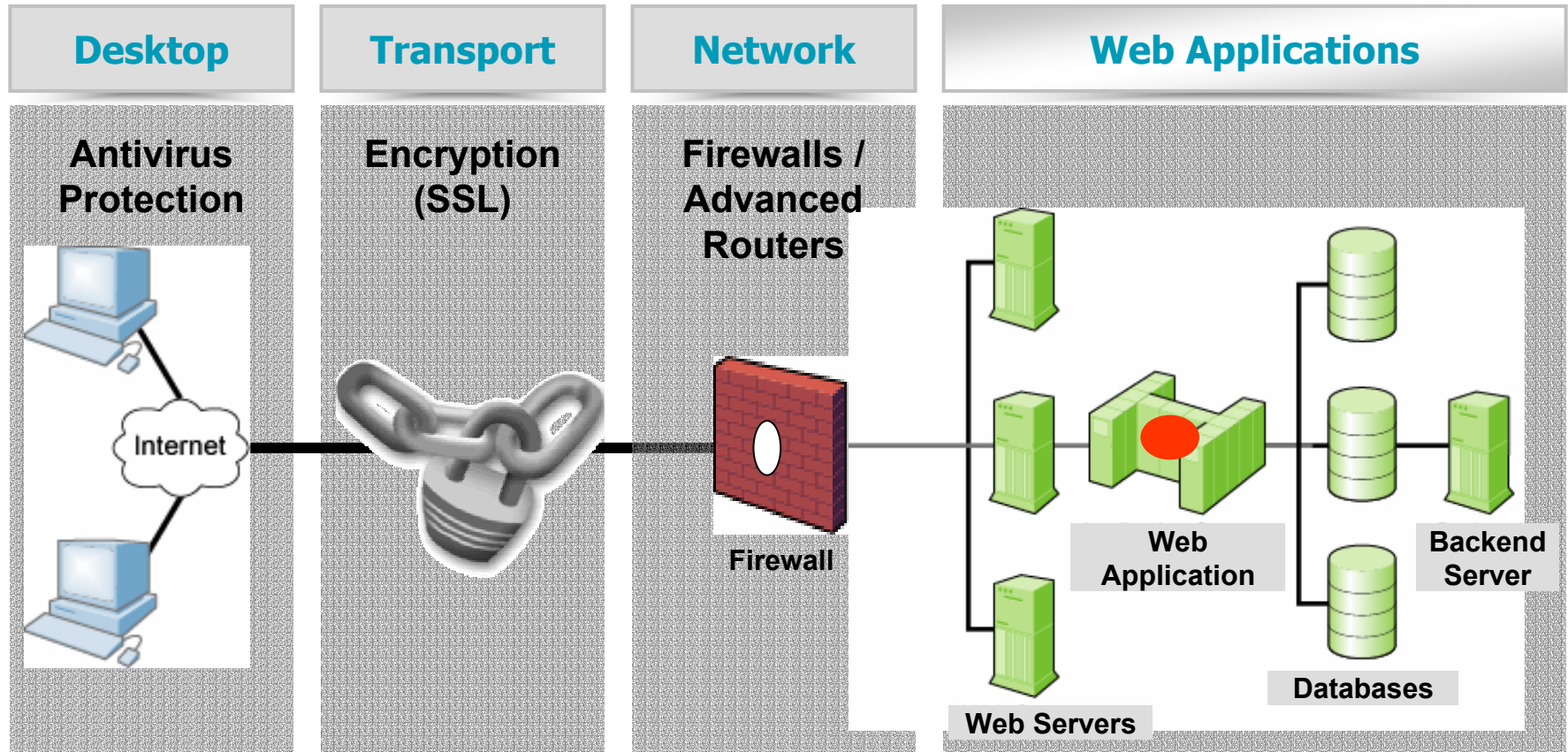
What keeps me **Rational**?



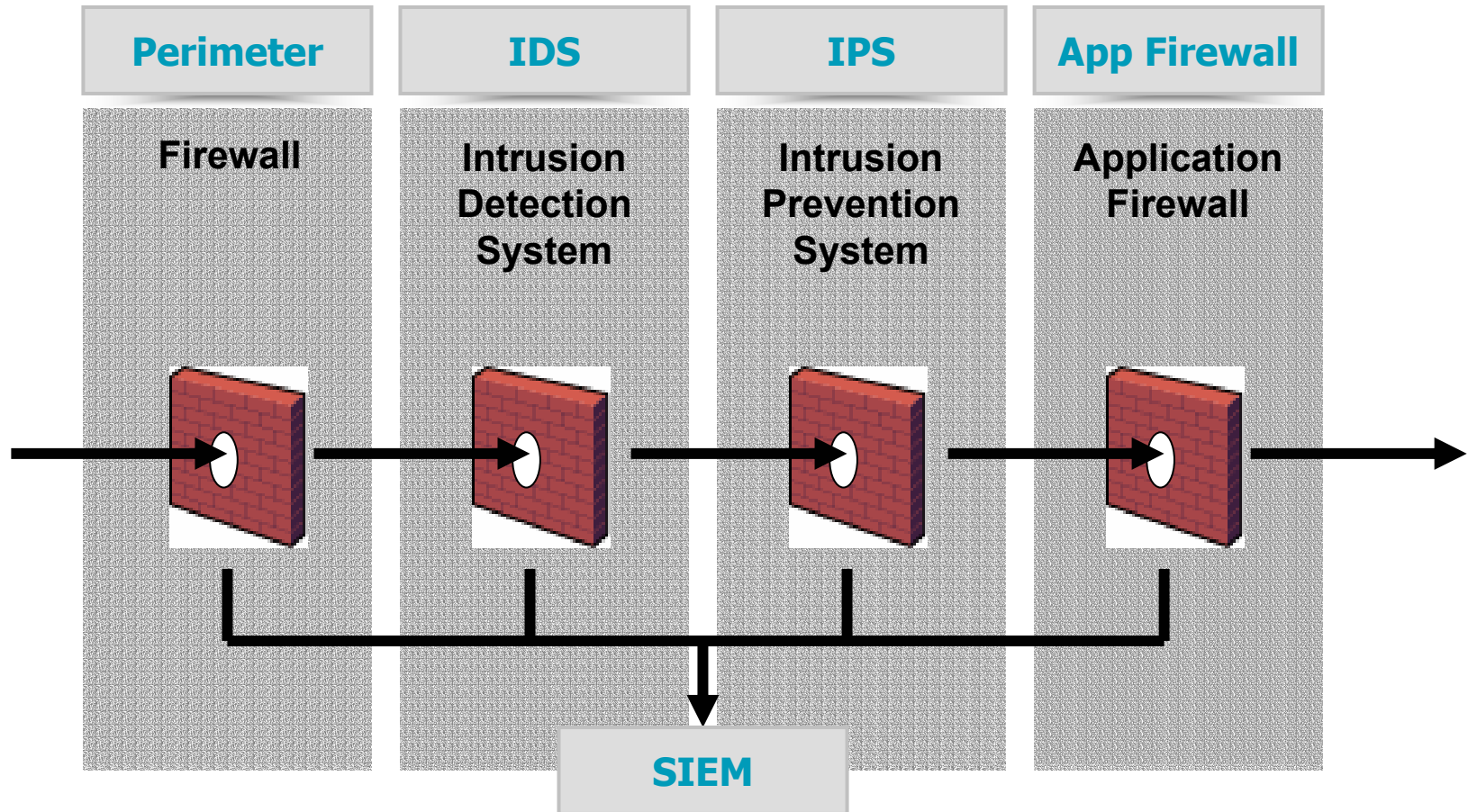
Select View/Master/Slide Master to add Session Number Here



High Level Web Application Architecture



Network Defenses for Web Applications



The need for Web Application Security

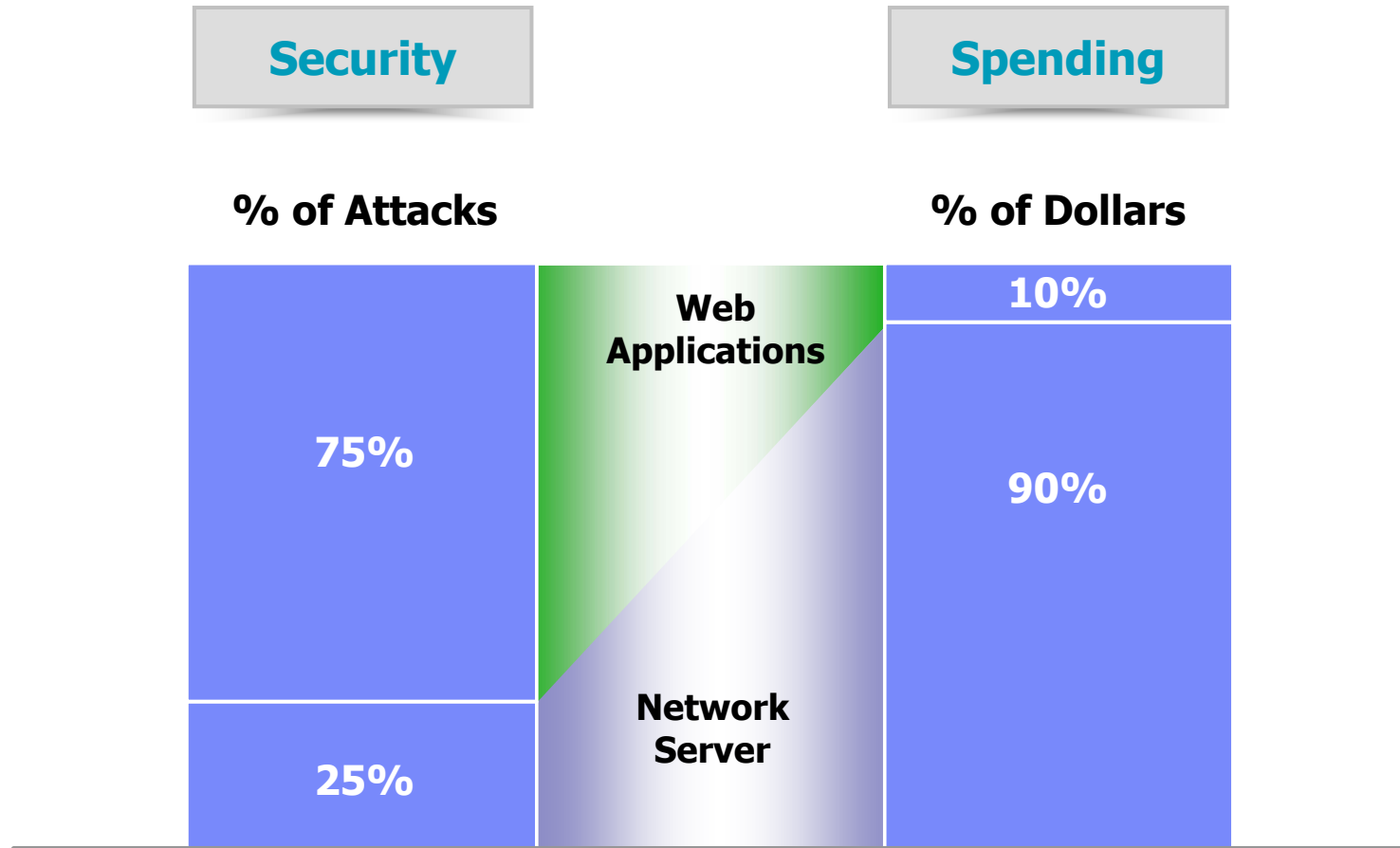
IBM Rational Software Development Conference UK 2007



▶ What keeps me **Rational**?



The Challenge for Organizations



Why Application Security is a High Priority

- **Web applications are the #1 focus of hackers:**
 - ▶ 75% of today's attacks occur at Application layer (Gartner)
 - ▶ XSS and SQL Injection are rated #1 and #2 vulnerabilities (Mitre)
- **Most sites are vulnerable:**
 - ▶ 90% of sites are vulnerable to application attacks (Watchfire research)
 - ▶ 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,



Top Attacks Overview

IBM Rational Software Development Conference UK 2007



What keeps me **Rational**?



Select View/Master/Slide Master to add Session Number Here





Security

The Myth: “Our Site Is Safe”

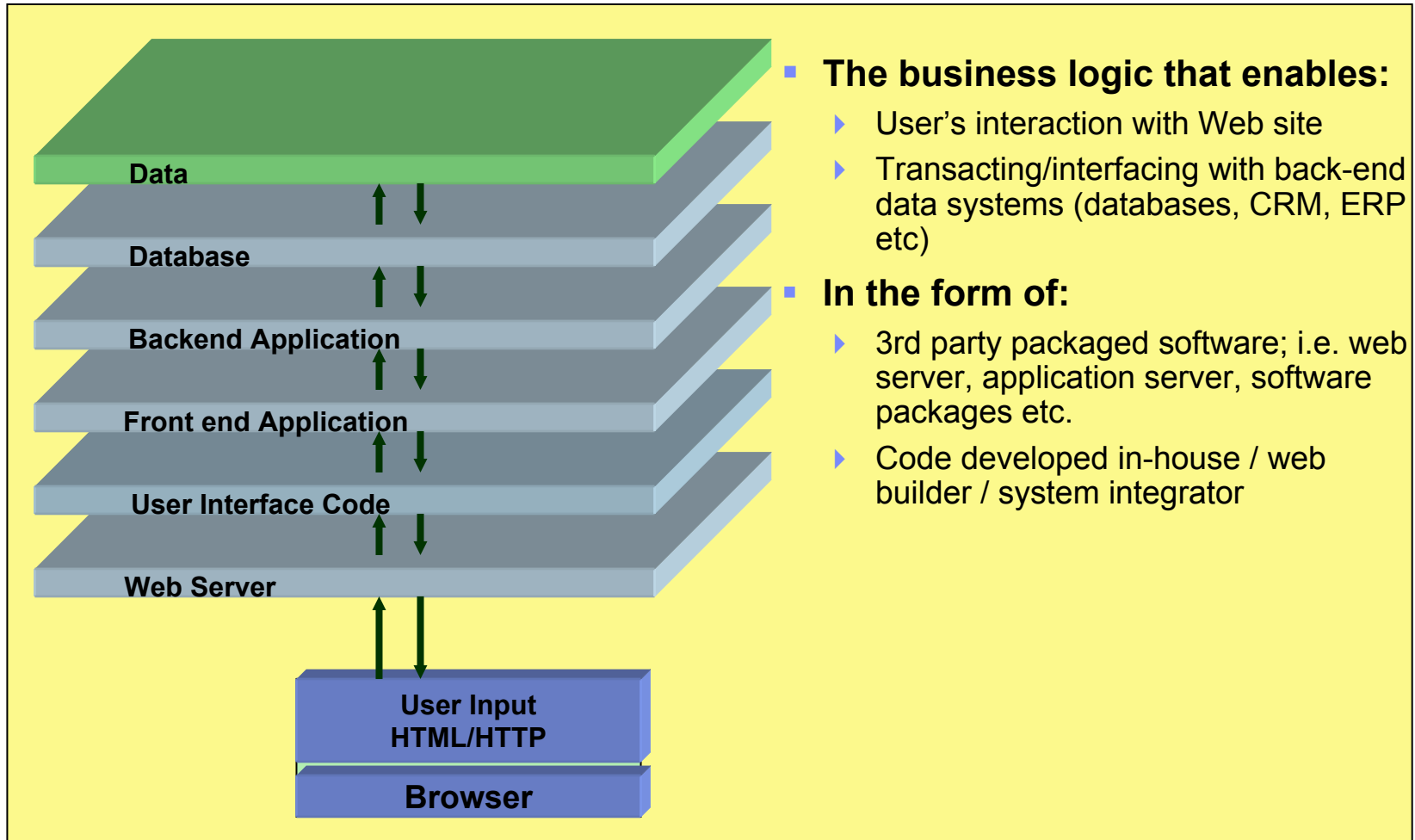
**We Have Firewalls
in Place**

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

**We Use Network
Vulnerability Scanners**



What is a Web Application?



Input and Output flow through each layer of the application



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 3 rd party SW | Insecure application development In-house |
| Location within Application | 3 rd 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 3 rd party software | Early detection saves \$\$\$ |



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



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





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

asdf

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:

asdf

HTML code:

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




[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:

The page at http://www.testfire.net says:



ASP.NET_SessionId=trohgg450cpi5r45rr2pl1fg; amSessionId=1824418181

OK

HTML code:

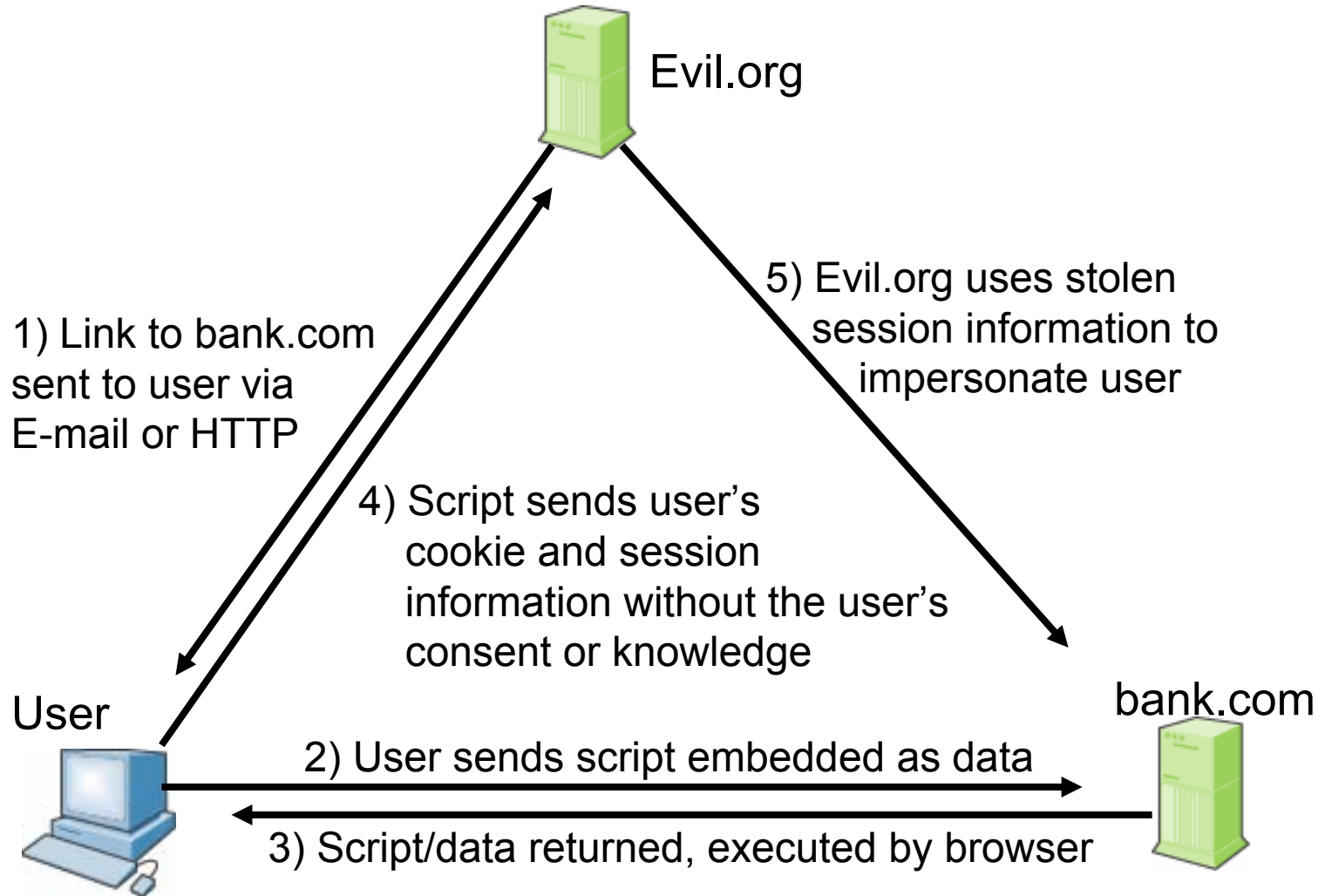
```
<p>No results were found for the query:<br /><br />
<span id="_ctl0__ctl0_Content_Main_lblSearch"><script>alert(document.cookie)</script></span>
```

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)



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





[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](#)

Online Banking Login

Username:

Password:

Login



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)



[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](#)

Online Banking Login

Username:

Password:

Login



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

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

Hello, John Smith

Welcome to Altoro Mutual Online.

View Account Details:

1001160140 Checking

Congratulations!

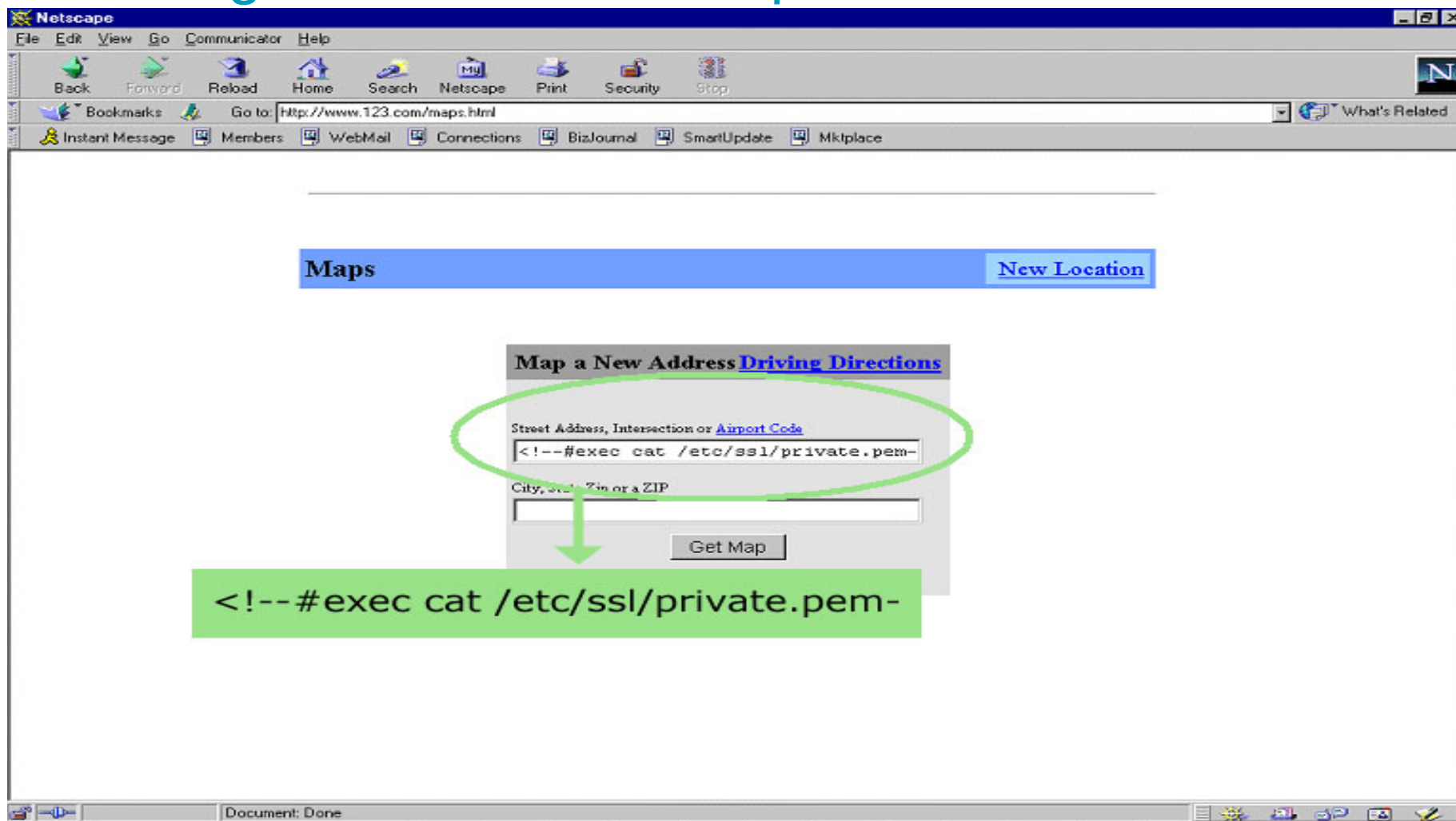
You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

Click [Here](#) to apply.

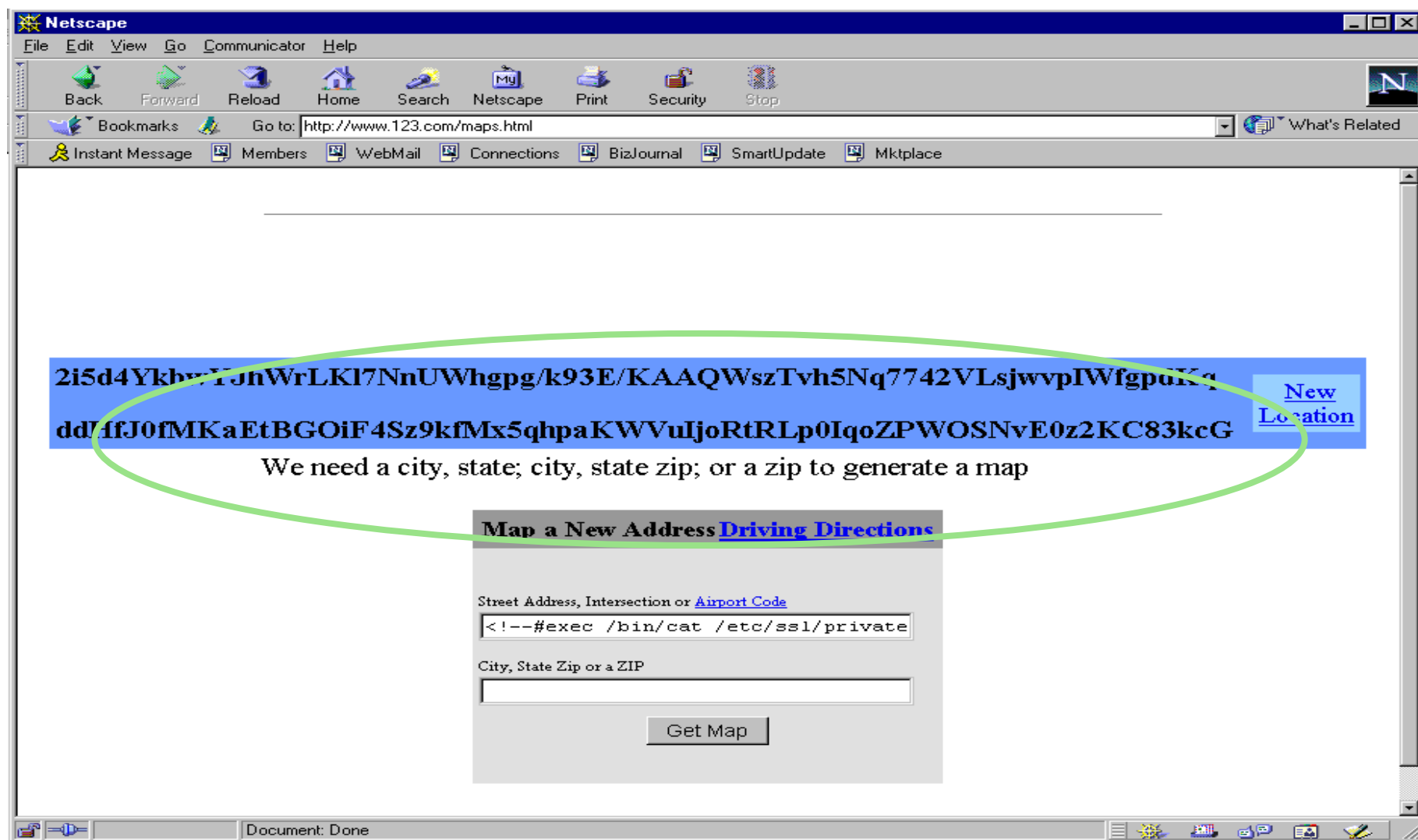
The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites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

Injection Flaws (SSI Injection Example)

Creating commands from input



The return is the private SSL key of the server



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



**ONLINE
BANKING 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](#)

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/feedback.aspx |
| Cookie | ASP.NET_SessionId=adp4vz550 |

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

OK

Cancel

Submit

Clear Form

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/feedba |
| 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



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

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





**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](#)

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



[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



[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](#)

```
[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
```

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





[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:

Login

`<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"`



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 User/Pass Error

|  <u>ONLINE BANKING LOGIN</u> | <u>PERSONAL</u> | <u>SMALL BUSINESS</u> | <u>INSIDE ALTORO MUTUA</u> |
|--|--|-----------------------|----------------------------|
| <u>PERSONAL</u> <ul style="list-style-type: none">• Deposit Product• Checking• Loan Products• Cards• Investments & Insurance• Other Services <u>SMALL BUSINESS</u> <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> | | |

|  <u>ONLINE BANKING LOGIN</u> | <u>PERSONAL</u> | <u>SMALL BUSINESS</u> | <u>INSIDE ALTORO MUTUA</u> |
|--|--|-----------------------|----------------------------|
| <u>PERSONAL</u> <ul style="list-style-type: none">• Deposit Product• Checking• Loan Products• Cards• Investments & Insurance• Other Services <u>SMALL BUSINESS</u> <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> | | |

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

PERSONAL

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

SMALL BUSINESS

Online Banking Login

Username:

Password:

MY ACCOUNT PERSONAL SMALL BUSINESS

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:

</admin/admin.aspx>






Simple user logs in, forcefully browses to admin page

| ONLINE BANKING LOGIN | PERSONAL | SMALL BUSINESS |
|---|--|--------------------------------|
| PERSONAL <ul style="list-style-type: none">Deposit ProductCheckingLoan ProductsCardsInvestments & InsuranceOther Services SMALL BUSINESS | <h2>Online Banking Login</h2> <p>Username: <input type="text" value="jsmith"/></p> <p>Password: <input type="password" value="*****"/></p> <p><input type="button" value="Login"/></p> | |

← → ↻ × 🏠 🔍 Google

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

AltoroMutual

   **DEMO SITE ONLY**

| MY ACCOUNT | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL |
|---|---|--------------------------------|--------------------------------------|
| I WANT TO ... <ul style="list-style-type: none">View Application ValuesEdit Users | <h2>Edit User Information</h2> <p>Add an account to an existing user.</p> <p>Users: <input type="text" value="100116014 jsmith"/> Account Types: <input type="text" value="Savings"/> <input type="button" value="Add Account"/></p> <p>Change user's password</p> | | |



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



Q & A

Questions?



Resources

- Download AppScan 7.0 - <http://www.watchfire.com>
- Latest whitepapers visit:
<http://www.watchfire.com/news/whitepapers.aspx>
- Visit Watchfire at one of our upcoming shows
<http://www.watchfire.com/news/events.aspx>
- Register for upcoming web seminars visit
<http://www.watchfire.com/news/seminars.aspx>
- Contact us at sales@watchfire.com



Thanks for joining me today!

IBM Rational Software Development Conference UK 2007



 What keeps me **Rational**?



Select View/Master/Slide Master to add Session Number Here

