

IBM Rational Software Development Conference 2008

WHERE TEAMS ARE **R-HEROES**



APPLICATION SECURITY

* YOUR LAST LINE OF DEFENSE! *

Anthony Lim

MBA CISSP FCITIL

Director Asia Pacific, Security

Rational Software

IBM, Singapore

What is Your Most Important/Strategic IT Infrastructure Requirements in 2006-07?



Top Priorities	2006 Rank	2007 Rank
Building a secure IT environment - <i>Security threats, business continuity, access control</i>	1	2
Reducing total cost of IT over time - <i>Resource utilization, growing infrastructure requirements, more cost effective technologies/services</i>	2	1
Faster deployment of applications - <i>expedite applications availability or functionality enhancements to corporate users</i>	3	3
Outsourcing part of IT	4	4
Building a Utility/On-demand/ Adaptive/Dynamic IT environment	5	5

In terms of Top business goals:

#1 reducing cost structure

#2 expanding business in existing or new geographies

#3 Improving customer service

The Security Journey Continues

- **New and More ...**

- Applications

- Services

- Systems

- > Vulnerabilities

- > Hacking methods

- > Viruses, Worms, RATS, Bots ...

(Remote Access TROJANS = Spyware)

- > **GOVERNANCE &
COMPLIANCE!**



**NEW AREAS
OF IT SECURITY
WEAKNESS
ARISE ALL THE
TIME**



It Gets Worse

- WAP, GPRS, EDGE, 3G
- 802.1x
- Broadband



A hacker no longer needs a big machine

Sheer Volume of Applications Keeps You From Getting Ahead of the Problems

1**Security Team Has Become a Bottleneck****2****Lack of Control and Visibility****3****Catching Problems Late in the Cycle****4****Not Monitoring Deployed Applications****5****Difficulty Managing 3rd Party Vendors**

Have to do more with less, still; Risk is high, accountability is prevalent



Software Application Development Pressures

4 most common laments of the development executive

I'm being asked to:

- **Deliver product faster (a lot faster!)**
- **Increase product innovation**
- **Improve quality**
- **Reduce cost**



APPLICATIONS – THE HACKER’S NEW TARGET

- **Next-generation hack attacks?**
- **“guided” “cyber-biological” attack?**
- **IT Security: People don’t really know what they want to do so they just put up physical defenses**

- **WHAT DOES A HACKER WANT?**
- **WHY DOES A HACKER ATTACK?**
 - ▶ **Short of denial of service, hack attacks are aimed at the software / application / database, not the network /infrastructure**



BEST EXAMPLE OF APPLICATIONS VIS-À-VIS SECURITY ISSUE: WEB APPLICATIONS WEB SERVICES

**AND A LOT OF APPLICATIONS TODAY USE A WEB –
BASED GRAPHICAL INTERFACE FOR USER ACCESS**



WE ARE HIGHLY DEPENDENT ON WEB SERVICES TODAY

- **WORK / BUSINESS**
 - ▶ INTERNET, INTRANET, EXTRANET
 - ERP, SCM, CRM, SAP, B2BM, B2C, COMPANY INTERNAL INFO SERVICES
- **PLAY / SOCIAL NETWORKING / RECREATION**
 - ▶ YouTube, Facebook, Second Life, Friendster, iTunes, MySpace, BLOGS! ...
- **EDUCATION / RESEARCH**
- **TRANSACTIONS / ONLINE SERVICES**
 - ▶ INTERNET BANKING, MEMBERSHIP PORTAL, TRAVEL BOOKING, TRADING
 - B2C, C2C, Amazon, EBay E*Trade ...
- **COMMUNICATION**
- **WEB 2.0, SOA**
- **ONLINE STORAGE SERVICES**
-



The Alarming Reality

LexisNexis Data Breach
- Washington Post
Feb 17, 2008

IndiaTimes.com Malware
- InformationWeek
Feb 17, 2008

Mac blogs defaced by XSS
• The Register, Feb 17, 2008

Chinese hacker steals 18M identities
- HackBase.com, Feb 10, 2008

Hacker breaks into Ecuador's presidential website
- The Indian, Feb 11, 2008

Two Indonesian government web sites defaced
- CNET Asia, Mar 29, 2008

Hacker steals Davidson Cos client data
- Falls Tribune, Feb 4 2008

U.S. Embassy Web Site In Manila, Defaced
- AllHeadlineNews, Mar 27, 2008

Hacking Stage 6
- Wikipedia, Feb 9 2007

Greek Ministry websites attacked
- eKathimerini, Jan 31, 2008

Drive-by Pharming in the Wild
- Symantec, Jan 21 2008

RIAA wiped off the Net
- TheRegister, Jan 20 2008

Italian Bank hit by XSS fraudsters
- Netcraft, Jan 8 2008



with an events section called "We are hiring!".

DUO CHARGED WITH MAID ABUSE

MAZLINDA Mohamed, 32, and Zahara Zainal Abidin, 57, were charged in court yesterday with six counts in total for abusing their Indonesian maid. Both are unemployed. The case was adjourned to April 24.

FREE FOR PREGNANT LOW-INCOME MUMS

A PRIVATE card blood bank, CoidLife, announced yesterday a programme to offer low-income expectant mothers with free banking service if their family has a history of diseases which can be treated using stem cells. To qualify, the monthly household income of the expectant mother must not be more than S2,000.

my paper 我报

ENGLISH EDITORIAL

Consulting Editor: FELIX SOH
felix@sph.com.sg

Editor: YEOW KAI CHAI
kacha@sph.com.sg

Deputy Editor: SARAH NG
ngsw@sph.com.sg

Money Editor: NG SUI HONG
ngsui@sph.com.sg

News Editor: ESTHER AU YONG
estheray@sph.com.sg

Foreign Editor: LEE SEOK HWA
seokhwa@sph.com.sg

Entertainment/
Lifestyle Editor: LEE SZE YONG
szeyong@sph.com.sg

Sports Editor: CHA HANWEONG
hankong@sph.com.sg

Art Director: PETER WILLIAMS
peterwill@sph.com.sg

Chief Sub-editor: GEORGE PERERA
george@sph.com.sg

Design Editor: LIM KOK WAH
kokwah@sph.com.sg

HOTLINE: 6319-8888

email: myo@sph.com.sg

ON THE WEB: mypaper.sg

TO ADVERTISE: 800-822-6382

TO GET A COPY: CRM@sph.com.sg
or call our circulation department at
6388 3638 from Mon-Fri (9am-5pm)

SINGAPORE PRESS HOLDINGS

There, it advertises for and hopes to recruit young frontline service staff.

Miss Eileen Ang, 30, the hotel's human resource manager, said: "Facebook is also a good way to keep in touch with old employees and inform them of our new career opportunities."

Though Royal Plaza still recruits through usual avenues such as recruitment agencies and online job portals, Miss Ang said that using Facebook is an "out of the box" way to appeal to younger recruits, who may be attracted to a hip and refreshing image of the hotel.

The Straits Times Razor TV, an interactive web TV service, is another employer which has been using Facebook to advertise various job openings - for multimedia journalists, videographers and presenters.

Since last December, editor Eugene Leow has posted the openings on Facebook's marketplace, where users can view and post classified advertisements.

So far, he has been getting around a dozen responses to the postings each week.

facebook

Some say Facebook appeals to a younger target group in tune with Internet culture

Said Mr Leow: "We use Facebook because its users are our ideal target group. We are looking for people who are in tune with Internet culture and are totally comfortable with the online realm."

One successful Facebook recruit is Rosalind Loy, 26, a multimedia journalist with Razor TV. She checked out its job postings on Facebook after hearing about them from a friend last December.

She sent in her resume via e-mail and successfully went through the usual application process. This included face-to-face interviews and a writing test.

Said Miss Loy: "I think it's an innovative method of recruiting. The use of Facebook lightened the tone of the entire application process."

"It was less intimidating."

Some recruitment agencies have taken the Facebook phenomenon one step further.

iHipo, an online global recruitment agency, built their own Facebook application - which gives users a feed of the most recent jobs, mainly entry-level executive jobs and internships with local and international firms.

Said Singapore-based co-founder Amout Wagenaar, 26: "Since we built our iHipo

in any fashion. "Professional networks are far better for targeting quality candidates."

On why other recruitment agencies are reluctant to use Facebook for recruitment, Mr Wagenaar explained: "Recruitment over Facebook is still in a very young phase."

"Some recruitment agencies are reluctant to use it because they aren't familiar with online concepts."

"Facebook is still regarded as a social website, but its use may slowly shift to a more professional one, which includes recruitment."

datwnt@sph.com.sg

HELPDESK 我的字典

- Videographer:** 电视录像员
diàn shì lù xiàng yuán
- Resume:** 简历 jiǎn lì
- Innovative:** 创新的
chuàng xīn de

Social networking sites targeted by hackers

ANDREA SOH

JUST keep to legitimate websites and you will be safe from security threats? Think again, warns a US-headquartered computer security company.

While it used to be that Netizens could fall prey to security breaches by unknowingly visiting malicious sites or accidentally clicking on malicious e-mail attachments, these days they can be affected just by visiting regular, everyday websites.

More of such websites, like those of banks, social networking and government websites, are being targeted by hackers.

In the Internet Security Threat Report released yesterday, Symantec noted that there

were 87,963 phishing hosts - computers which host phishing websites - in the second half of 2007, an increase of 167 per cent compared to the first half.

Phishing, or the theft of personal information such as bank and credit card accounts details, is done through creating look-alikes of these legitimate sites, e-mail and instant messaging.

Mr Stephen Trilling, Symantec Security Technology and Response vice president said: "Avoiding the dark alleys of the Internet was sufficient advice in years past. Today's criminal is focused on compromising legitimate websites to launch attacks on end-users, which underscores the importance of maintaining a strong security posture no matter where you go and what you do on the Internet."

The report provides a six-month update from of Internet threat activity in the Asia Pacific region from July to December last year. It includes an analysis of disclosed vulnerabilities, malicious code reports and security risks.

Also, stolen information obtained through phishing and keystroke logging, has become so plentiful that the price of stolen data has hit a new low, my paper reported on Wednesday.

A full identity, including a person's name, address, date of birth, a functioning credit card number and US Social Security number, can be purchased in the underground economy for as little as US\$1 (S\$1.40), Symantec said. Previously, it costs between US\$10 and US\$150.

Spam has also continued to be a menace, peaking at all-time highs of 88 per cent of all e-mails last month. It rose from an average of 78.5 per cent in January to 81 per cent in March this year.

Social networking sites such as Bahu, a private social networking site for international students to stay in touch with friends, have also been the target of spammers. Said Symantec Singapore general manager Darnic Hor: "Social networking sites are especially attractive because not only do the profiles on such sites contain a significant amount of personal information, users usually allow a trusted site to execute code on their computers."

sandrea@sph.com.sg



The Myth: “Our Site Is Safe”

We Have Firewalls and IPS in Place

Port 80 & 443 are open for the right reasons

We Audit It Once a Quarter with Pen Testers

Applications are constantly changing

We Use Network Vulnerability Scanners

Neglect the security of the software on the network/web server

We Use SSL Encryption

Only protects data between site and user not the web application itself



Server Error in '/' Application.

Runtime Error

Description: An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed.

Details: To enable the details of this specific error message to be viewable on the local server machine, please create a <customErrors> tag within a "web.config" configuration file located in the root directory of the current web site. To enable the details to be viewable on remote machines, please set "mode" to "Off".

```
<!-- Web.Config Configuration File -->  
  
<configuration>  
  <system.web>  
    <customErrors mode="RemoteOnly" />  
  </system.web>  
</configuration>
```

Notes: The current error page you are seeing can be replaced by a custom error page by modifying the "defaultRedirect" attribute of the application's <customErrors> configuration tag to point to a custom error page URL.

```
<!-- Web.Config Configuration File -->  
  
<configuration>  
  <system.web>  
    <customErrors mode="On" defaultRedirect="mycustompage.htm" />  
  </system.web>  
</configuration>
```



An Error Has Occurred

Summary:

Unclosed quotation mark after the character string ''.

Error Message:

```
System.Data.OleDb.OleDbException: Unclosed quotation mark after the character string ''. Incorrect syntax near 'a'. at
System.Data.OleDb.OleDbDataReader.ProcessResults(OleDbHResult hr) at System.Data.OleDb.OleDbDataReader.NextResult() 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 c:\Altoro_Demo\website\bank\login.aspx.cs:line 68 at Altoro.Authentication.Page_Load(Object
sender, EventArgs e) in c:\Altoro_Demo\website\bank\login.aspx.cs:line 33 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)
```

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.

```
Index of / drex@LOADSERVER:~  
File Edit  
drex@LOADSERVER ~]$
```

Go


Name	Last modified	Size	Description
Parent Directory		-	
0391290228/	27-Sep-2006 08:28	-	
05291977/	18-Sep-2006 04:09	-	
240403/	20-Sep-2006 17:25	-	
10136109/	23-Sep-2006 21:56	-	
ALTERC585/	16-Sep-2006 11:59	-	
www.bigbank.html	02-Oct-2006 16:18	1.0K	
EBALL/	25-Sep-2006 09:37	-	
EMERSON/	19-Sep-2006 14:44	-	
EMELLI/	26-Sep-2006 15:16	-	
EMERSON/	26-Sep-2006 15:21	-	
EMERSON/	21-Sep-2006 17:31	-	
LONY/	02-Oct-2006 05:17	-	
MAKYO6050/	14-Sep-2006 22:18	-	
RBSANAGUST/	27-Sep-2006 08:36	-	
SBD8P/	21-Sep-2006 11:28	-	
SSSHO/	27-Sep-2006 14:37	-	
apabs/	27-Sep-2006 16:13	-	
clouds18/	26-Sep-2006 16:46	-	
dargc/	25-Sep-2006 10:37	-	
dfm/	21-Sep-2006 17:07	-	
dj/	25-Sep-2006 14:21	-	
dm/	27-Sep-2006 09:40	-	
dmj/	20-Sep-2006 10:54	-	
dmk/	26-Sep-2006 09:26	-	
dmll/	22-Sep-2006 09:59	-	
dmll/	14-Sep-2006 16:49	-	
dmab/	29-Sep-2006 09:49	-	
dmcb/	02-Oct-2006 08:55	-	
dmcb/	22-Sep-2006 16:38	-	
dmhtc/	28-Sep-2006 10:55	-	

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

Systemerror

 A system error occurred.

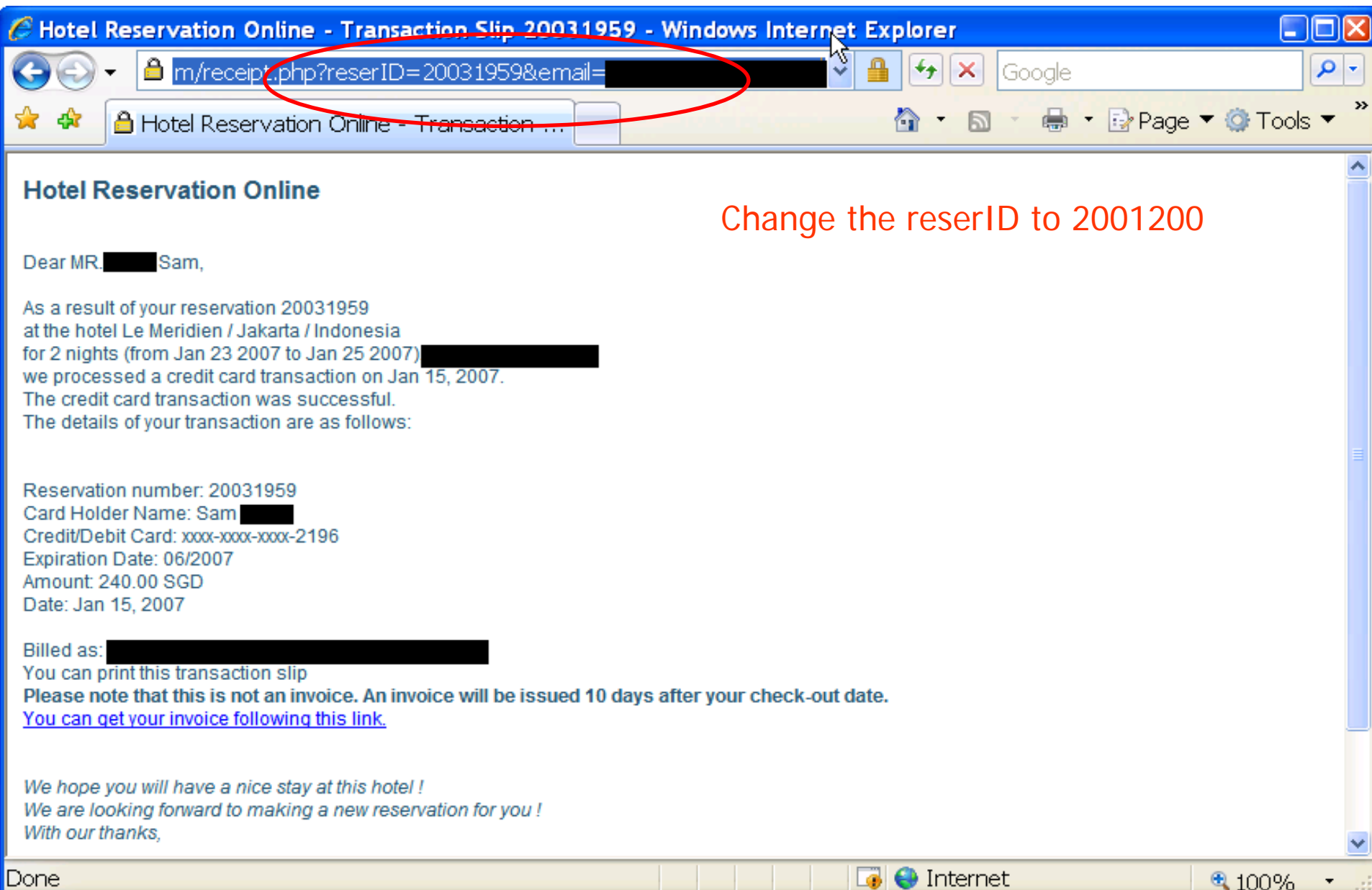
Have a look at the details, or contact your system administrator.

OK Hide Details

Fehlermeldung:

```
at org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:670)
at org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:247)
at org.apache.jasper.servlet.JspServlet.service(JspServlet.java:214)
at javax.servlet.http.HttpServlet.service(HttpServlet.java:853)
at org.apache.catalina.core.ApplicationDispatcher.invoke(ApplicationDispatcher.java:471)
at org.apache.catalina.core.ApplicationDispatcher.doInclude(ApplicationDispatcher.java:374)
at org.apache.catalina.core.ApplicationDispatcher.include(ApplicationDispatcher.java:348)
at com.opencms.flex.cache.CmsFlexRequestDispatcher.include(CmsFlexRequestDispatcher.java:100)
```


Real Example: Online Travel Reservation Portal



Hotel Reservation Online - Transaction Slip 20031959 - Windows Internet Explorer

m/receipt.php?reserID=20031959&email= [REDACTED]

Hotel Reservation Online

Dear MR. [REDACTED] Sam,

As a result of your reservation 20031959 at the hotel Le Meridien / Jakarta / Indonesia for 2 nights (from Jan 23 2007 to Jan 25 2007) [REDACTED] we processed a credit card transaction on Jan 15, 2007. The credit card transaction was successful. The details of your transaction are as follows:

Reservation number: 20031959
Card Holder Name: Sam [REDACTED]
Credit/Debit Card: xxxx-xxxx-xxxx-2196
Expiration Date: 06/2007
Amount: 240.00 SGD
Date: Jan 15, 2007

Billed as: [REDACTED]

You can print this transaction slip
Please note that this is not an invoice. An invoice will be issued 10 days after your check-out date.
[You can get your invoice following this link.](#)

*We hope you will have a nice stay at this hotel !
We are looking forward to making a new reservation for you !
With our thanks,*

Change the reserID to 2001200

Done Internet 100%

Real Example : Parameter Tampering

Reading another user's transaction – insufficient authorization

Hotel Reservation Online - Transaction Slip 2001200 - Windows Internet Explorer

https://www.██████████.com/receipt.php?reserID=2001200&email=1

Hotel Reservation Online - Transaction ...

Hotel Reservation Online

Dear ██████████, Justin,

As a result of your reservation 2001200 at the hotel Nikko Resort And Spa / Bali / Indonesia for 5 nights (from Jan 18 2006 to Jan 23 2006) ██████████, we processed a credit card transaction on Jan 03, 2006. The credit card transaction was successful. The details of your transaction are as follows:

Reservation number: 2001200
Card Holder Name: Justin Pintaona
Credit/Debit Card: xxxx-xxxx-xxxx-4688
Expiration Date: 08/2007
Amount: 506.61 USD
Date: Jan 03, 2006

Billed as: ██████████

You can print this transaction slip

Please note that this is not an invoice. An invoice will be issued 10 days after your check-out date.

[You can get your invoice following this link](#)

*We hope you will have a nice stay at this hotel !
We are looking forward to making a new reservation for you !
With our thanks,*

https://www.██████████.com/invoice.php?reserID=2001200&email=██████████@hotmail.com

Internet 100%

Another customer's transaction slip is revealed, including the email address

Parameter Tampering - Reading another user's invoice



Hotel Reservation Online - Invoice 2001200 - Windows Internet Explorer

invoice.php?reserID=2001200&email=[REDACTED]@hotmail.com

Hotel Reservation Online - Invoice 2001200

[REDACTED]

To [REDACTED], Justin
Company [REDACTED]
Address 23 [REDACTED], Australia
Phone 61 [REDACTED]

RECEIPT / TAX INVOICE #2001200

Date Jan 30 2006

Description	Nights	Rate	Amount
Booking reference 2001200 at hotel : Nikko Resort And Spa / Bali / Indonesia			
Period : From Jan 18 2006 to Jan 23 2006 (5 night(s))			
Ocean View Room, Breakfast Included 2 adult(s), 0 child(ren), 0 infant(s)	5	138	690.00 AUD
TOTAL AMOUNT			506.61 USD

The Payment, billed as [REDACTED], was received by credit card, on Jan 03, 2006, to our account from [REDACTED]:

Card Holder Name Justin [REDACTED]
Credit/Debit Card xxxx-xxxx-xxxx-4688
Expiration Date 08/2007

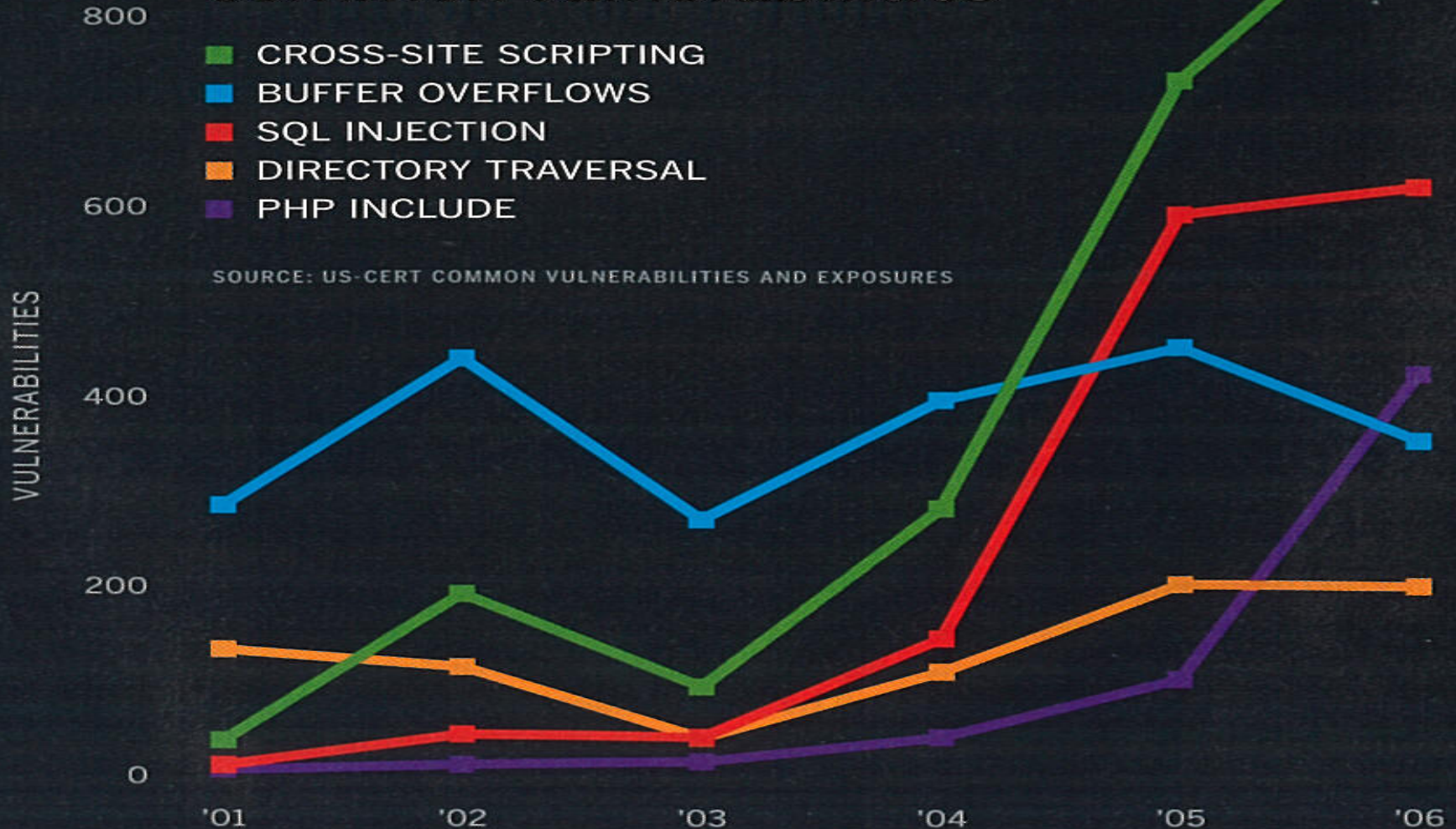
*We hope you had a nice stay at this hotel !
We are looking forward to making a new reservation for you !
With our thanks,*

Done Internet 100%

The same customer invoice that reveals the address and contact number

Top Hack Attacks Today Target Web Services

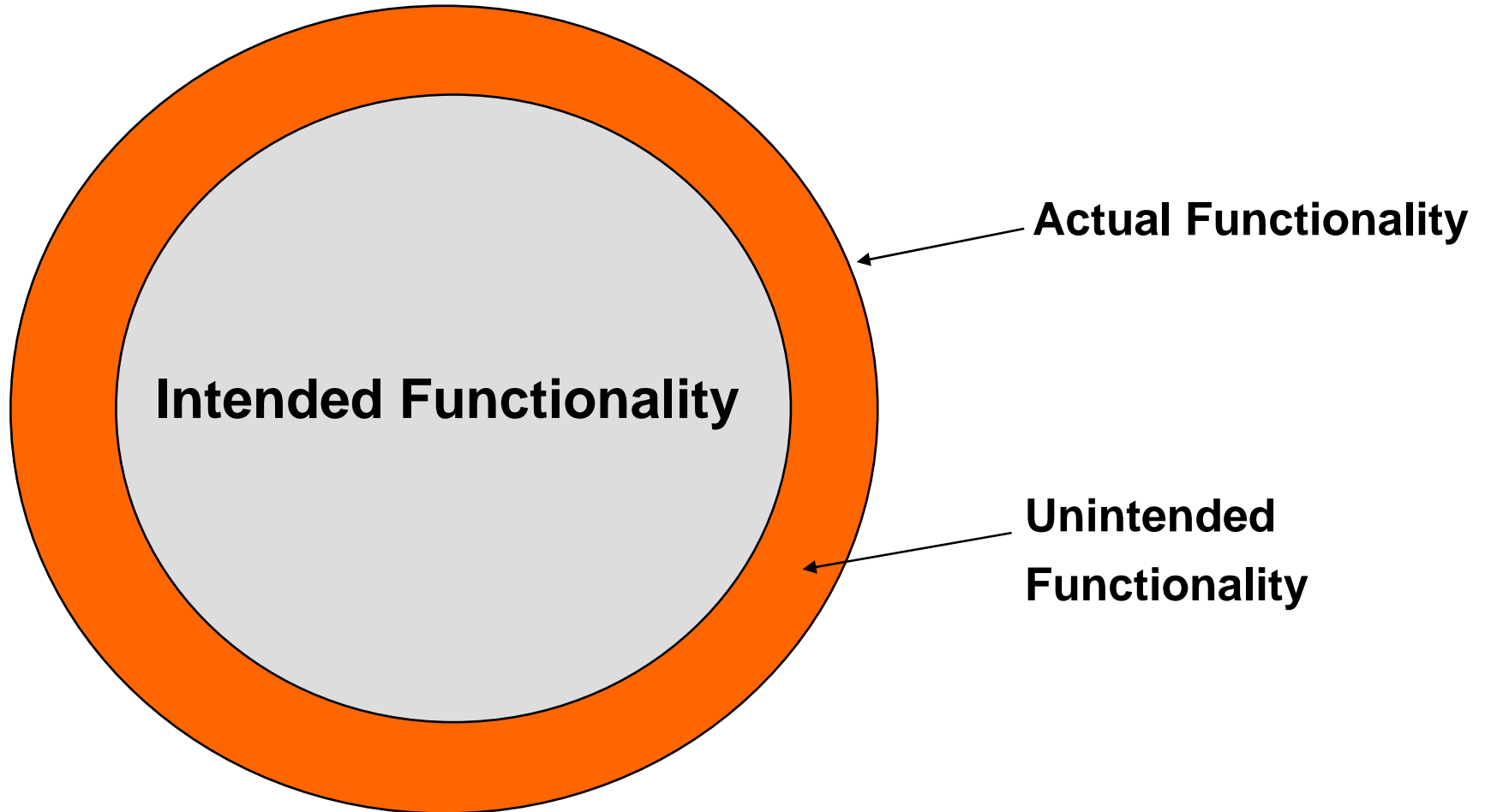
Cross-site scripting has shot up the list of most common vulnerabilities



Web Application Hacks are a Business Issue

Application Threat	Negative Impact	Potential Business Impact
Buffer overflow	Denial of Service (DoS)	Site Unavailable; Customers Gone
Cookie poisoning	Session Hijacking	Larceny, theft
Hidden fields	Site Alteration	Illegal transactions
Debug options	Admin Access	Unauthorized access, privacy liability, site compromised
Cross Site scripting	Identity Theft	Larceny, theft, customer mistrust
Stealth Commanding	Access O/S and Application	Access to non-public personal information, fraud, etc.
Parameter Tampering	Fraud, Data Theft	Alter distributions and transfer accounts
Forceful Browsing/ SQL Injection	Unauthorized Site/Data Access	Read/write access to customer databases

Hackers Attack Apps by Exploiting Unintended Functionalities



Why Do Application Security Problems Exist



Existing Solutions Don't Address App Security

- **IT Security Solutions are usually for network and infrastructure**
 - ▶ Firewalls and IPS's don't block application attacks
 - ▶ Port 80, 8080 and 443 are open
 - ▶ Network scanners won't find application vulnerabilities.
 - Nessus, ISS, Qualys, Nmap, etc.
- **IT Security professionals are typically from the network /infrastructure area, and usually have little experience in software application development**
- **Developers are usually not trained in or mandated to security.**
 - ▶ 64% of developers are not confident in their ability to write secure applications – Microsoft Developer Research
 - ▶ Developers do not care about security, they think its someone else's job
 - (even though they are the root cause)
- **Security teams are focused on other issues (network, desktops, etc) and overwhelmed**
 - *They don't want to have to deal with another new issue that they don't understand*
- **No defined policy, accountability or process to deal with the issue (*not many people understand application attacks today*)**



Why would anyone want to attack a web site?

DBS iBanking - Windows Internet Explorer

https://internet-banking.dbs.com.sg/IB/Welcome

1.8 hours saved

DBS iBanking

Search

POSB

Go to DBS Homepage

You are now on a secure site

Welcome to DBS iBanking

User ID

PIN

Submit Cancel Clear

- > What is DBS iBanking?
- > Login Assistance
- > Security Advisory
- > Maintenance Schedule

Not an iBanking customer?

Apply for iBanking now >

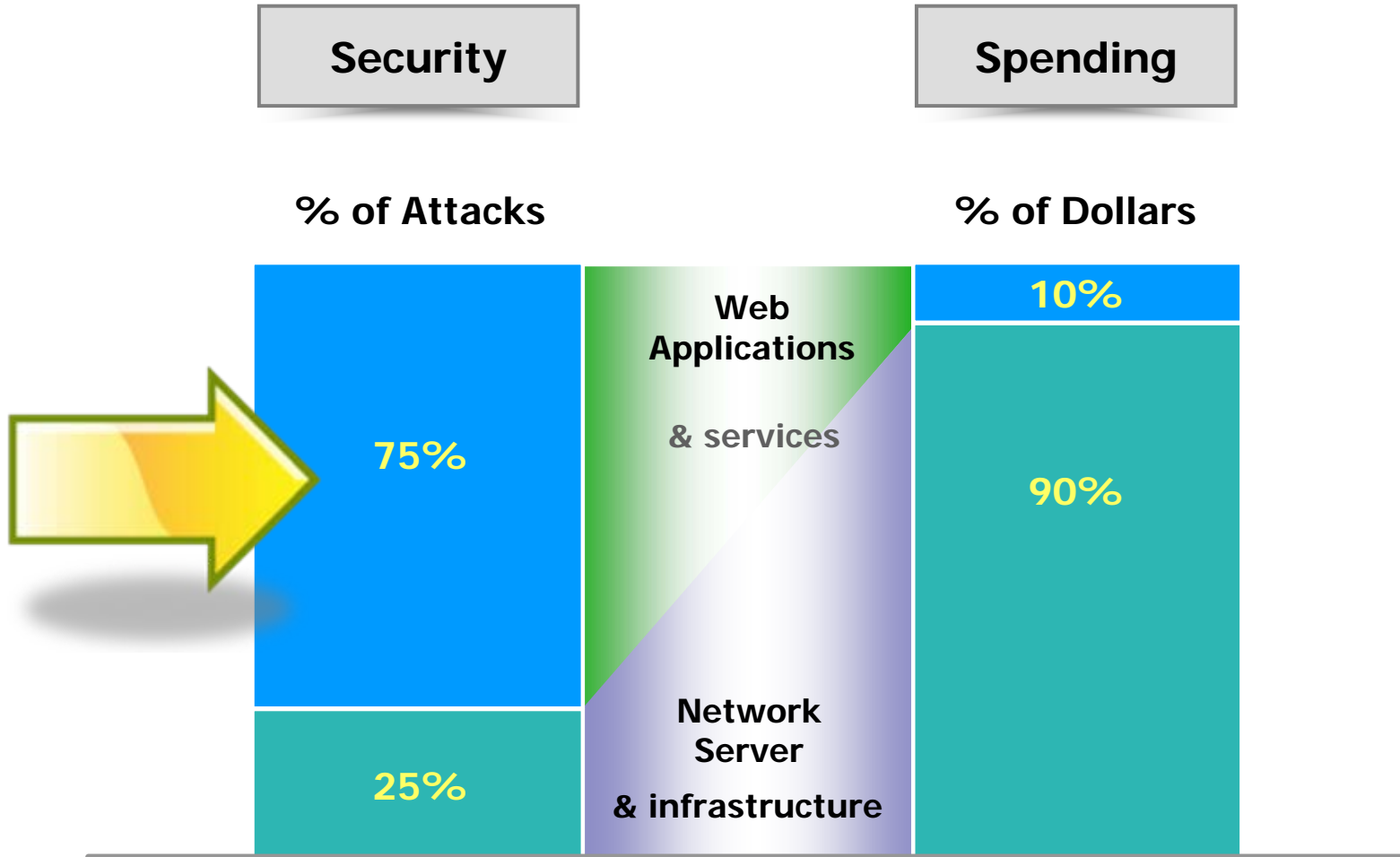
Why queue? Enjoy 24 x 7, anytime, anywhere convenience with DBS iBanking. What's more, with DBS iSecure, you now get added online banking security!

Terms & Conditions | Privacy Policy | © 2007 DBS Bank

Local intranet 100%

78% 11:42

The Fact: Attacks targetted at a new area



In an organization, IT Security people and developers are poles apart



Regulation & Compliance SARBANES-OXLEY, HIPAA, BASEL II ...

- It is part of doing business
- Business Continuity
- An environment of TRUST
 - ▶ For doing business
 - ▶ Ensure Orderliness in Internet world
 - ▶ Promote Economic growth
- More than just Confidentiality, Integrity and Availability
- Privacy

3rd Party Customer Data

People never learn –there will be another Edison Chen case – that’s why I still have a job today

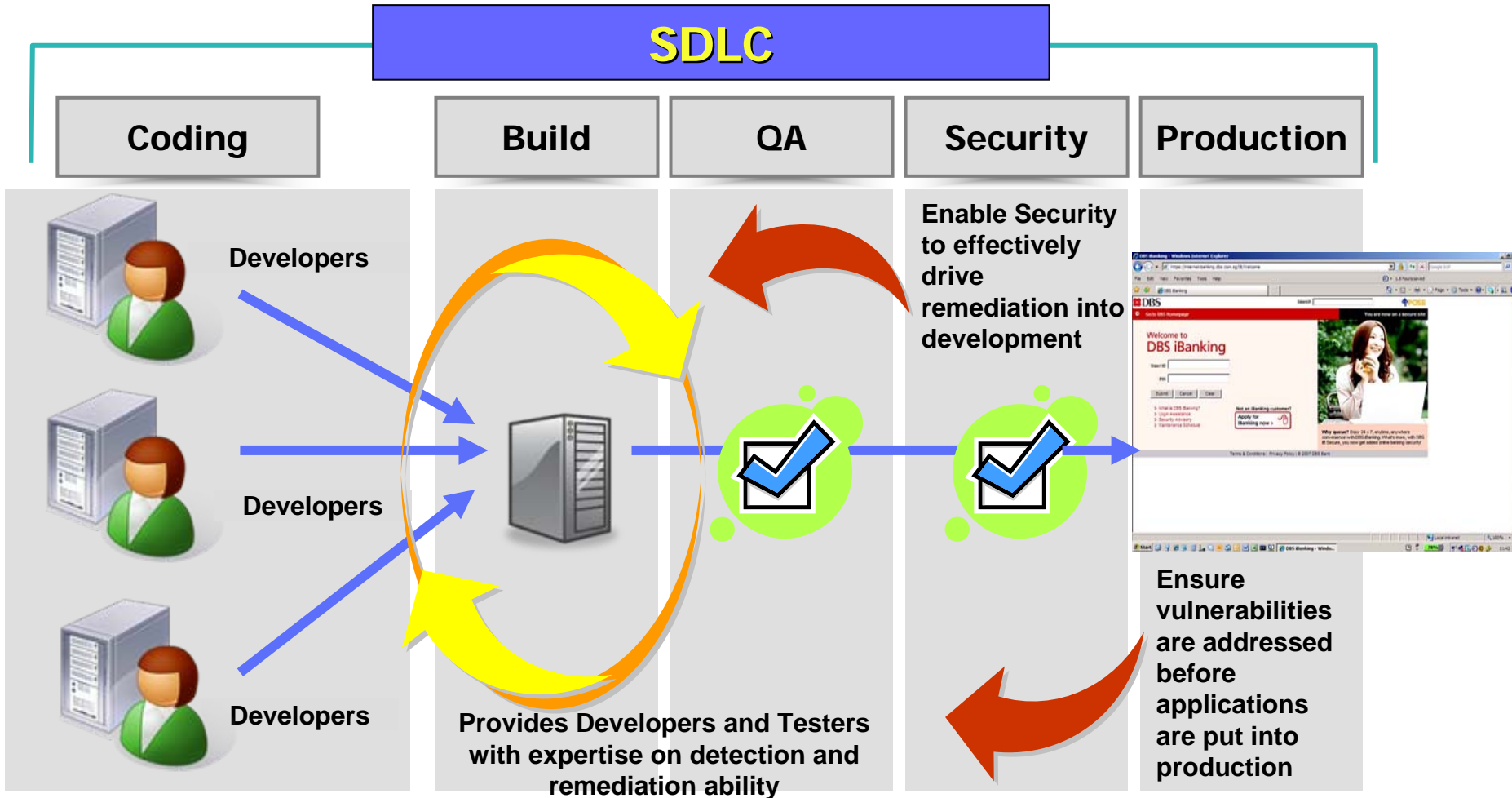


ISSUES WITH APPLICATION SECURITY & COMPLIANCE TODAY

- Penetration Test services usually do not include security-testing the software applications, yet
- Penetration Test services are usually only as good as the tester
- Highly-qualified /experiences technical consultants tend to be opinionated
- Many companies, due to cost, ignorance or apathy, will do only the minimum for security compliance audit
 - ▶ *Don't be like the Singapore Mercedes Benz owner 😊*
- Free tools?!
 - ▶ *Don't bet your company's IT security or audit on these alone!*
 - *Free tools are good for your own personal use and testing but be sure of origin!*
- *Why do I still have a job (in IT Security) today?*



Building security & compliance into the SDLC



Conclusion: Application QA for Security

■ **The Application Must Defend Itself**

- ▶ You cannot depend on firewall or infrastructure security to do so

■ **Bridging the GAP between Software development and Information Security**

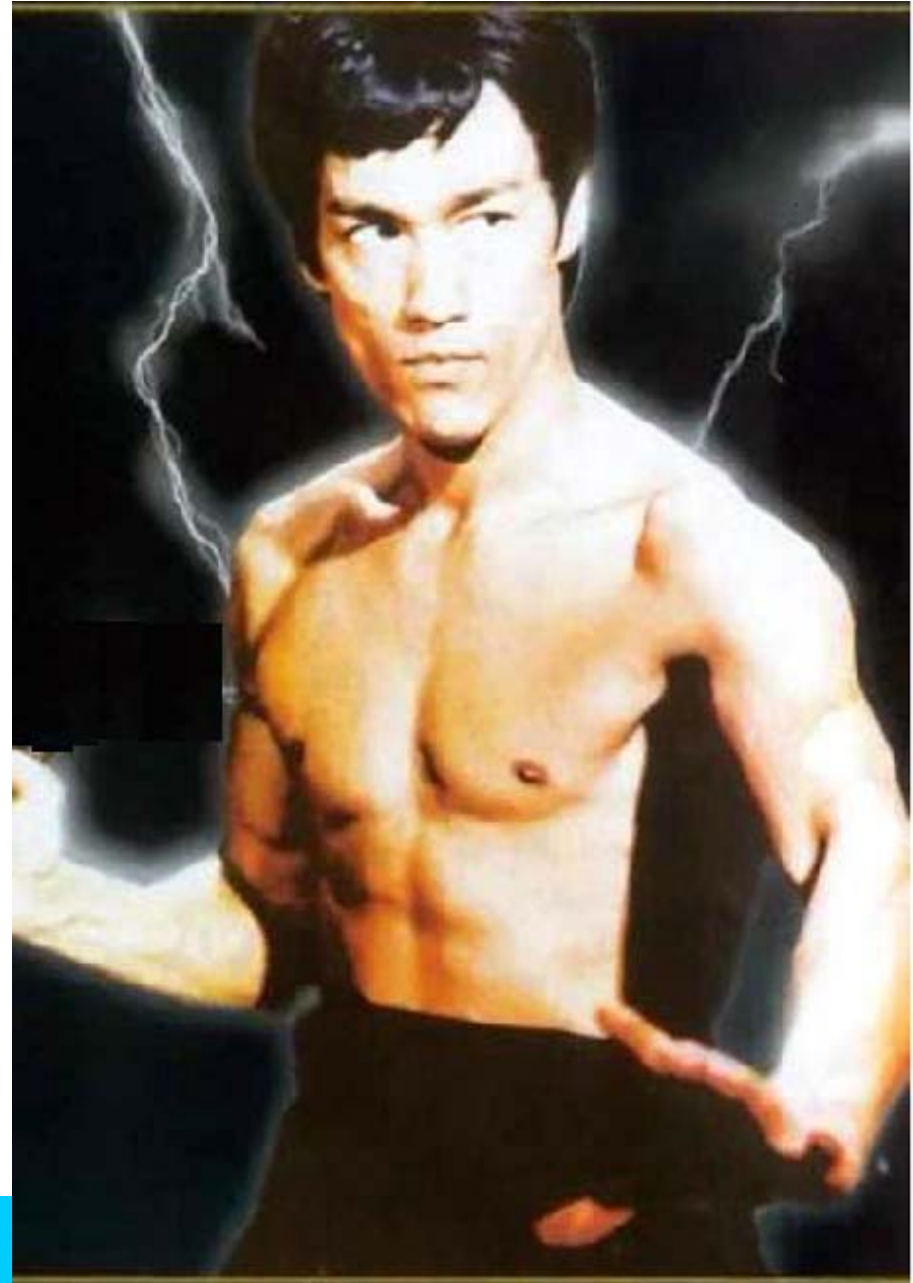
■ **QA Testing for Security must now be integrated and strategic**

■ **We need to move security QA testing back to earlier in the SDLC**

- ▶ at production or pre-production stage is late and expensive to fix
- ▶ Developers need to learn to write code defensively and securely



SDLC QA - YOUR LAST LINE OF DEFENSE



IBM Rational Software Development Conference 2008



WHE



APPLICATION SECURITY ***YOUR LAST LINE OF DEFENSE***

Anthony Lim
Director, Asia Pacific, Security, Rational Software

Thank You