Governance and Risk Management

Your Web and Applications

The Hacker's New Target

Anthony Lim

MBA CISSP CSSLP FCITIL

Director, Security, Asia Pacific

Rational Software

Social Engineering in the Business World

July 9, 2009

Organized by:

Prolog: The Security Journey Continues

- **New, More, Bigger, Better …**
  - **SYSTEMS**
  - **APPLICATIONS**
  - **SERVICES**
    - -> *New Risks*
    - -> *New Vulnerabilities*
    - -> *New Hacking methods*
      - *Viruses, Worms, RATS, Bots …*

(Remote Access TROJANS = Spyware)

-> NEW: ***GOVERNANCE & COMPLIANCE!***

CEP Points!

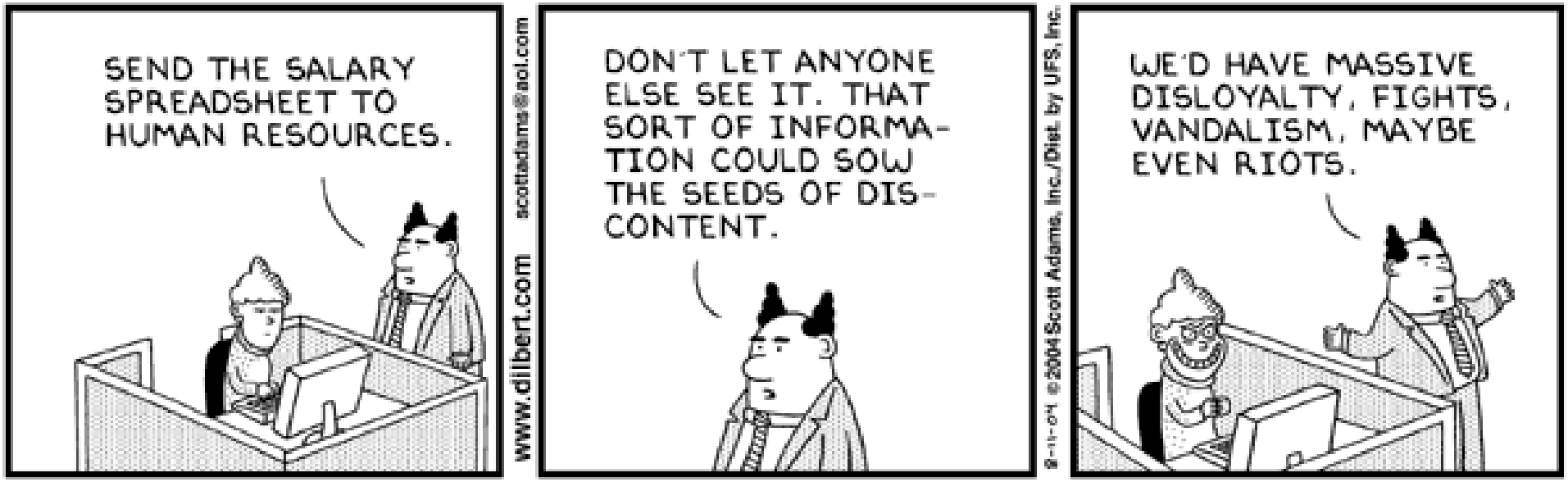
- **Data Privacy**
- **Data Leakage**

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



GOVERNANCE AND COMPLIANCE

ILLEGAL TO STEAL AND /OR MISUSE DATA INCLUDING ELECTRONIC DATA

home. The Straits Times Singapore Wednesday 05 Nov 2008

COMPUTER BREACH

Ex-warden gets three months' jail

He used prison's computer to illegally obtain information

BY SUJIN THOMAS

A FORMER officer of the Queenstown Remand Prison was jailed yesterday for accessing the facility's computer records illegally to get personal information on a former inmate for a friend.

Luke Teo Qing Wang, 26, who pleaded guilty to the charge under the Computer Misuse Act, was given a three-month jail term in a district court.

Fired from the Singapore Prison Service when he was caught, he had made a scripted mitigation plea to District Judge Liew Thiam Leng the day before.

Reading from it, he said: "I did not derive any benefit from my moment of folly. This will be my last brush with the law following my harrowing experience."

But Judge Liew told the court yesterday that, as a prisons officer, Teo should have known what his duties were, and that he had abused his position.

According to court documents, Teo befriended two inmates, Mr Tan Jek Sen and Leong Ken Lee, in the course of his work in the prison. Teo kept in touch with Mr Tan after his release in August.

When Leong failed to be eligible for the home detention scheme later that month, his father sought Mr Tan's help to get a lawyer to fight his son's case.

Mr Tan found a lawyer named Mr Toh Gim Por.

Leong's father gave Mr Tan $1,500 to pay the lawyer but when he tried to call him using a phone number that Mr Tan had provided, a man named Tommy who took the call said that Mr Tan had set him up.

When confronted, Mr Tan said he himself had been cheated by the "lawyer", who had apparently gone missing.

This was when Teo entered the picture. Since he knew Mr Toh, also known as Tommy, was a former inmate, he accessed the prison's computer system without authorisation to obtain his particulars, which he then passed to Mr Tan.

When the security breach came to light, the Corrupt Practices Investigation Bureau was called in.

suiint@sph.com.sg

Teo abused his position by giving a friend the personal particulars of an ex-inmate. ST PHOTO: WANG HUI FEN

$12k fine for accessing clients' data

A FORMER clerk who illegally accessed information on insurance policyholders was fined $12,000 on Monday.

Helen Foo Mei Hwa (right), 41, admitted to three charges of mining information on 156 policyholders from her workstation without clearance from The Asia Insurance Company, her then-employer in August 2005.

Two other similar charges were taken into consideration.

She passed on the details to an insing its rule against misusing or divulging information. She is now a freelance insurance agent.

Her lawyer, Mr Suresh Damodara, said his client, who is separated and has two children, had not benefited from the offences. He added that the last three years had been traumatic for her, with the investigation hanging over her head.

She could have been fined up to $5,000 and/or jailed for up to two years on each charge.

It Gets Worse

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

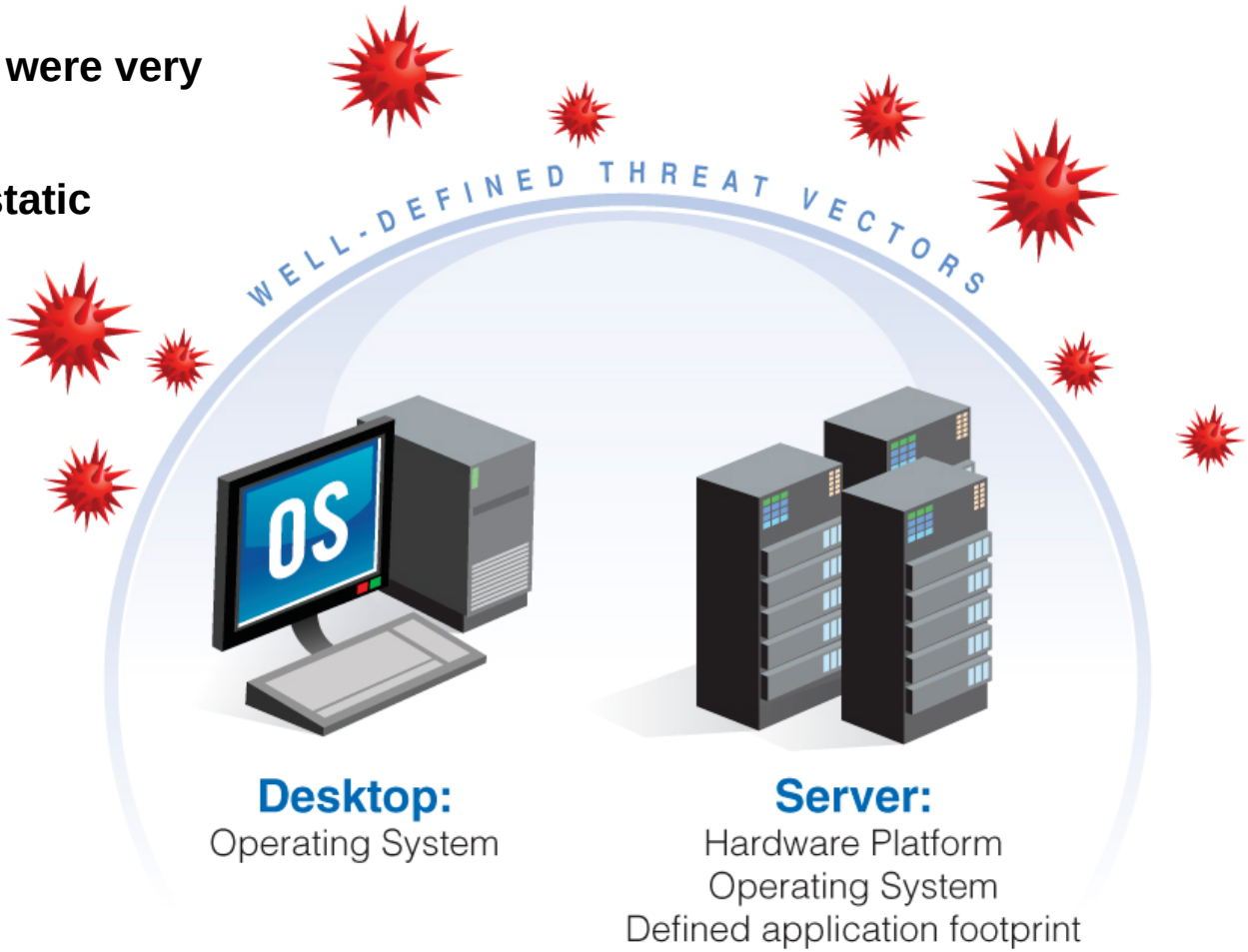
A hacker no longer needs a big machine

The Security Equation Has Changed

- **How businesses look at security has changed**
  - Security is now business driven not technology driven
  - Security is now defined through risk management and compliance disciplines instead of threat and technology disciplines
- **The threat landscape has changed**
  - Traditional operating system and native client application security risks have become somewhat passé
  - Client threats are now all about the browser environment
  - Server threats are now all about web applications

The Security Landscape of the past

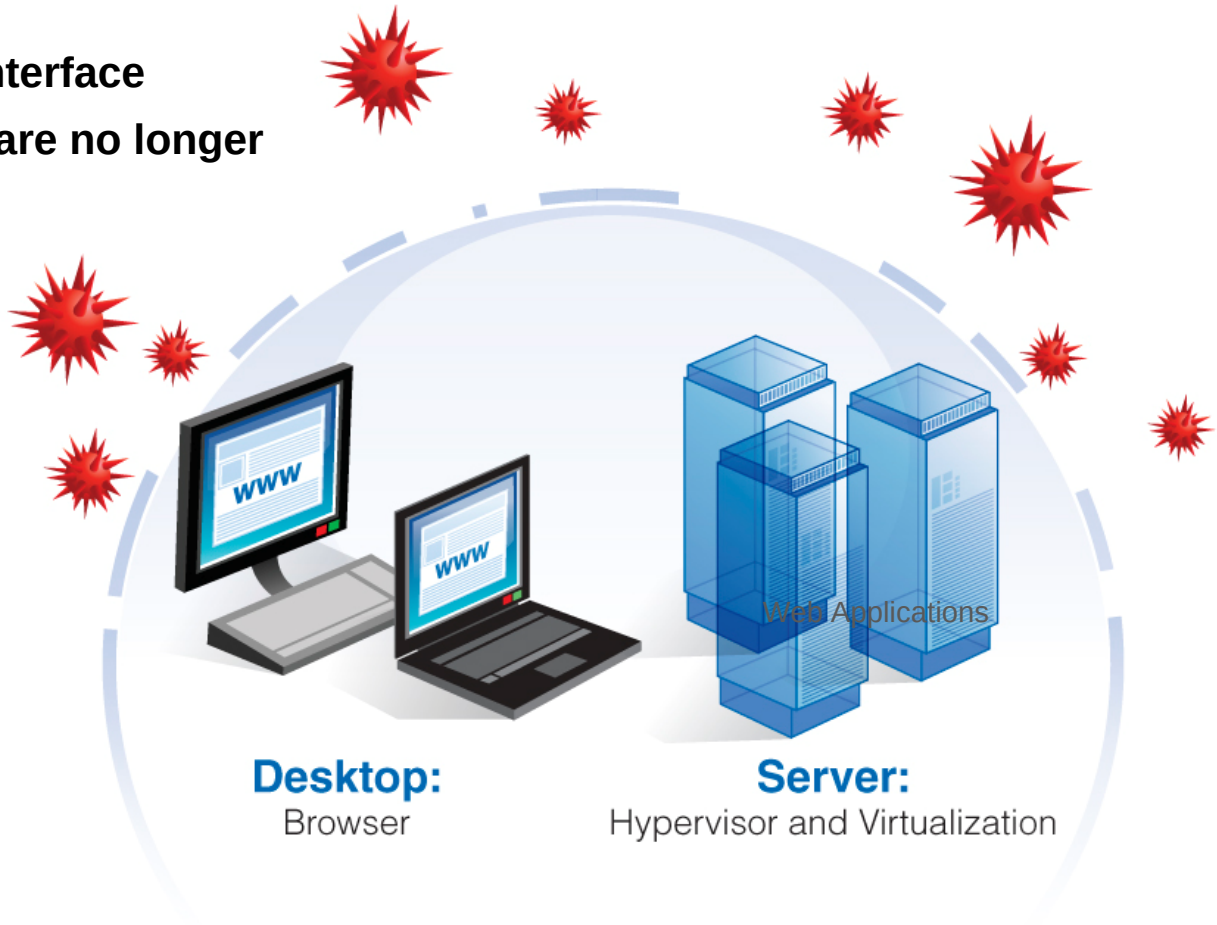
- Traditional Infrastructure was easier to protect . . .
- **Concrete entities that were easy to understand**
- **Attack surface and vectors were very well-defined**
- **Application footprint very static**
- **Perimeter defense was king**



Changing Security Landscape of Today

"Webification" has changed everything …

- **Infrastructure is more abstract and less defined**
- **Everything needs a web interface**
- **Agents and heavy clients are no longer acceptable**
- **Traditional defenses no longer apply**



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

SO WHY ARE THESE HAPPENING?

BBC NEWS

Watch One-Minute World News

Front Page
Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
nce/Nature
Technology
tertainment

Last Updated: Tuesday, 21 August 2007, 10:01 GMT 11:01 UK

E-mail this to a friend Printable version

Monster attack steals user data

US job website Monster.com has suffered an online attack with the personal data of hundreds of thousands of users stolen, says a security firm.

Monster is a leading online job service

A computer program was used to access the employers' section of the website using stolen log-in credentials.

Symantec said the log-ins were used to harvest user names, e-mail addresses, home addresses and phone numbers, which were uploaded to a remote web server.

PAGE H2 STRAITS TIMES FRIDAY FEBRUARY 11, 2005

GAME OVER

Four friends spent two years amassing $15,000 worth of riches in an online game – only to lose it all to a hacker. In a new series on digital crime in Singapore, ChuaHian Hou looks at how the victims and the police teamed up to crack the first such case here

cnet NEWS.com

http://news.cnet.com/8301-107

April 6, 2007 4:39 PM PDT

Asus Web site harbors threat

Posted by Joris Evers

It is not such a Good Friday for ASUStek Computer.

The main Web site of the Taiwanese hardware maker, known for its Asus branded PCs and moth been rigged by hackers to serve up malicious software that attempts to exploit a critical Windows experts said Friday.

The attackers added an invisible frame, a so-called iframe, to the front page of the Asus.com Wel the site, a victim's browser will silently connect to another Web site that tries to install a malicious

MY PAPER TUESDAY MARCH 3, 2009

SINGAPORE TUE MAR 03 09 MYPAPER

Glitch spills UBS clients' info

Wealthy customers saw details of others' online accounts, but bank says number affected is small

KENNY CHEE

A TECHNICAL glitch at Swiss bank UBS gave its wealthy customers in Singapore and Hong Kong a shock last week when they logged on to their online accounts.

The private-banking clients found confidential details of other clients' bank statements and account information instead of their own. Clients' online accounts, though, do not indicate their names.

When contacted, a UBS spokesman confirmed the incident and said the bank was taking it very seriously.

Asked how many clients were affected, all she said was that "some limited account information concerning a small number of UBS wealth-management clients was accessible by a very limited number of other system users". She added that fewer than five accessed the information.

She told *my paper* the glitch occurred "as a result of an inadvertent technical error following an information-technology system upgrade over the weekend of Feb 21".

The bank immediately took steps to rectify the issue. UBS reviewed the circumstances leading to the incident and has implemented measures to prevent a similar occurrence in the future.

The bank also reported the incident to the banking authorities here and in Hong Kong: the Monetary Authority of Singapore (MAS) and the Hong Kong Monetary Authority (HKMA).

Asked about what MAS would be doing, its spokesman said that "we are following up with the bank", but did not elaborate.

The HKMA said it is "following up with the bank on any impact... and the remedial measures that should be taken".

Its spokesman added: "We have requested the bank to submit an investigation report to the HKMA and will examine the matter in detail once the report is available."

Mr Tan Teik Guan, chief executive of Data Security Systems Solutions, said such accidental leaks of confidential information could lead to "embarrassing situations for clients and reputation risks for banks".

"Intentional leakages are more serious as the data... (could be) used for more malicious activities," he said.

kennyc@sph.com.sg

HELPDESK 我的字典

Glitch: 小故障 xiǎo gù zhàng

Confidential: 私人的 sī rén de

Rectify: 矫正 jiǎo zhèng

STRAITS TIMES SINGAPORE
13 SEP 09

Hackers steal gamers' currency

MapleStory players blame company for lax security

BY TAN WEIZHEN

PLAYERS of the wildly popular online game MapleStory are furious with the company which hosts the game on its servers, Asiasoft.

Tens of thousands of virtual dollars were lost by gamers after Asiasoft's servers were hacked into, and players are charging that the company did not provide them with adequate protection.

Worse, they say, Asiasoft has not compensated them for their losses.

Online forums are abuzz with chatter among victims, and 20 gamers called The Straits Times to complain about being shortchanged.

The gamers, mostly professionals in their 30s, say they have spent up to $10,000 each on the game.

In MapleStory, players fight monsters and complete quests, which earn them in-game currency called "mesos".

This currency allows them to buy more powers or weapons for their characters – so they can progress to higher levels of the game – as well as more mundane items like stylish clothes.

But many who do not want to

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

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

facebook

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

STRAITS TIMES, SINGAPORE FRI FEB 27 09

home.

THE STRAITS TIMES FRIDAY, FEBRUARY 27 2009 PAGE C2

'Errors' on Facebook a cyber trap

Viral application enables perpetrator to access personal data

BY SERENE LUO

FACEBOOK users in Singapore are facing a threat from an application that may steal their personal information.

The viral application issues a prompt to users of the popular social networking site to say that other users are having problems viewing their profile.

It asks them to activate an "Error Check System" application to "correct" these errors. If they click on it, the application will send messages to their friends, to try and get them to accept the application as well.

The cyber trap has the potential to affect the 495,000 or so unique visitors from Singapore to the Facebook site monthly. Security firms and Facebook have stepped up measures to warn users that the so-called errors do not exist.

A statement from UK-based security firm Sophos, which tracks vulnerabilities on the Internet, said: "The warning messages were, in fact, a viral attempt by a third party to recruit more users and – potentially – steal personal information for financial gain."

Installing the application allows the person behind it access to one's profile, including e-mail address, phone number, occupation details and even names of family members derived from photographs posted. Banks commonly ask for such information when a customer is opening an account or applying for a credit card, for instance.

Worse still, users who use the Google search engine to try and find out more about the application may be hit by a double viral dose.

Sophos' senior technology consultant Graham Cluley found that the top search result was a website directing users to another site. The site starts a fake anti-virus scan that downloads a virus into the computer instead.

FAST-SPREADING

"When I first checked the application, two of my friends had been affected. Within an hour, it had grown to 10 to 12 people."

Blogger Josh Lim

Mr Cluley said: "Is it possible that the original Facebook application was actually a red herring, and the real dangerous payload came from people Googling for information?"

Mr Josh Lim, 25, who runs his own blog, spotted the unusual messages over the weekend, and quickly sent an alert to friends and posted a warning on his blog.

"When I first checked the application, two of my friends had been affected. Within an hour, it had grown to 10 to 12 people," he said.

His blog has received thousands of hits every day since then, from people looking for more information about the bug.

Another 10,000 worried users have formed or joined groups over the past few days to discuss the cyber trap.

A Facebook spokesman in the United States said the company has disabled "several versions" of the application, and was working "aggressively" to make sure they stayed off its website.

Facebook had also informed Google about the dangerous website listed in its search results, and it could no longer be found among the top 50 hits following checks by The Straits Times on Wednesday afternoon.

serene@sph.com.sg

How to remove it

What you will see

- Facebook notifications will tell users that their friend "has faced some errors when checking your profile".
- If they click on the link to "View The Errors Message", a prompt will ask them to "activate" the application to correct the errors. This move allows their information to be accessed.

How to remove the application

- Click on "Edit" in the Applications pane.
- Click on the "x" beside the "Error Check System" application.
- A window will pop up asking the user to confirm the removal.

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 hos: 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 lookalikes 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 percent 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 Darric 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

home. Straits Times, Singapore, Monday 13 Apr 09

THE STRAITS TIMES MONDAY, APRIL 13 2009 PAGE B2

School website tests show up security lapses

Personal data of staff and students are leaked easily, says online group

By Khushwant Singh

FOR a week, members of an online community known as the Singapore Security Meetup Group (SSMG) went onto the websites of various schools and came away with plenty of personal information, such as addresses and identity card and telephone numbers of staff and students.

SSMG members did not have to try very hard either.

No hacking, spyware or any virus was needed. All they did was use search engines such as Google – and the information fell into their laps. Just like that.

In one case, the user name and password of a system administrator also popped up. With these, a hacker could use the server at the secondary school to send spam messages or even host an Internet pornographic website.

SSMG member and chief technology officer of an IT firm, Mr Wong Onn Chee, showed The Straits Times documents containing personal information on the websites of a university, a junior college, a polytechnic, five secondary schools and a primary school which they found.

Such data leaks are not new.

In January, Internet security firm Trend Micro said it has identified at least 40 Singapore websites – which it termed "reputable" – that were guilty of security lapses. It declined to name the sites, which were mainly online shopping portals and community sites.

More ominously, said Trend Micro, the 40 sites – which have since cleaned up their act – likely form just a small proportion of those with questionable security practices.

SSMG's findings confirm this view.

The issue of data privacy had been raised in Parliament in January by Ms Lee Bee Wah, an MP for Ang Mo Kio GRC.

In his written reply, then-Minister for Information, Communications and the Arts Lee Boon Yang said an inter-ministry committee was already reviewing the issue. "As data protection is a complex issue, with extensive impact on all stakeholders, this review will take some time."

Meanwhile, lapses are continuing, warned SSMG member Franky Tjiue.

Among the lapses that the group, which has 150 online members, discovered: A teacher at Presbyterian High School posted the names, together with the IC numbers, of 34 former students involved in an orientation programme at the start of the school year.

Although meant for the school staff, the information became accessible to all as the teacher had not assigned the correct viewing rights, said principal Lim Yan Hock.

Teachers have also been reminded that it is against school policy to include IC numbers in online documents, he added.

One document on the website of the National University of Singapore (NUS) had the personal particulars of a research fellow, including his address in China.

An NUS spokesman said its users were advised not to divulge personal information in data stored for public access and they need to take personal responsibility for any disclosure.

Republic Polytechnic spokesman Khog Eu Meng blamed its leak of names, IC numbers and e-mail addresses of 300 students on "human error", and said steps have been taken to prevent any recurrence.

Mr Tjiue, an IT security consultant, warned that such information could be used in kidnapping scams. "Thanks to leaky websites, criminals could have details to convince family members that it's a real kidnapping when actually, it's just a con job."

Simply removing these documents from websites might not mean they are no longer available. These could have been archived by search engines and the affected parties would have to request that the documents be removed.

Mr Tjiue said: "Documents with personal information should be posted only on websites with the necessary safeguards, such as restricted access.

"Where data leakage is concerned, prevention is truly better than cure."

khkshp@sph.com.sg

Why leaks occur

THERE are four main reasons why data leaks out, says Mr Wong Onn Chee.

These are:

1. Web servers that are infected with malware, or malicious software, that siphons off information from the server.

2. Vulnerabilities in Web applications, such as poorly written applications, that have few or no safeguards to prevent information from being accessed by unauthorised persons.

3. Misconfigured Web servers which reveal more information than necessary.

4. Sensitive information stored on Web servers without access control.

Data leakage arising from infected Web servers and vulnerable applications could prove costly to prevent, said IT specialists. Their estimates were from $30,000 upwards.

Rectifying misconfigured Web servers and implementing access controls could be done by the system administrator.

May 7, 2009 CNet Tech News

Report: Hackers broke into FAA air traffic control systems

Memorandum

U.S. Department of Transportation
Office of the Secretary of Transportation
Office of Inspector General

Subject: ACTION: Report on Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems
Report Number: FI-2009-049

Date: May 4, 2009

From: Rebecca C. Leng
Assistant Inspector General for Financial and Information Technology Audits

Reply to Attn. of: JA-20

To: Acting Federal Aviation Administrator

This report presents the results of our audit of Web applications security and intrusion detection in air traffic control (ATC) systems. This audit was requested by the Ranking Minority members of the House Committee on Transportation and Infrastructure and its Aviation Subcommittee.

Security

May 8, 2009 1:53 PM PDT

UC Berkeley computers hacked, 160,000 at risk

by Michelle Meyers

20 comments

This post was updated at 2:16 p.m. PDT with comment from an outside database security software vendor.

Hackers broke into the University of California at Berkeley's health services center computer and potentially stole the personal information of more than 160,000 students, alumni, and others, the university announced Friday.

At particular risk of identity theft are some 97,000 individuals whose Social Security numbers were accessed in the breach, but it's still unclear whether hackers were able to match up those SSNs with individual names, Shelton Waggener, UCB's chief technology officer, said in a press conference Friday afternoon.

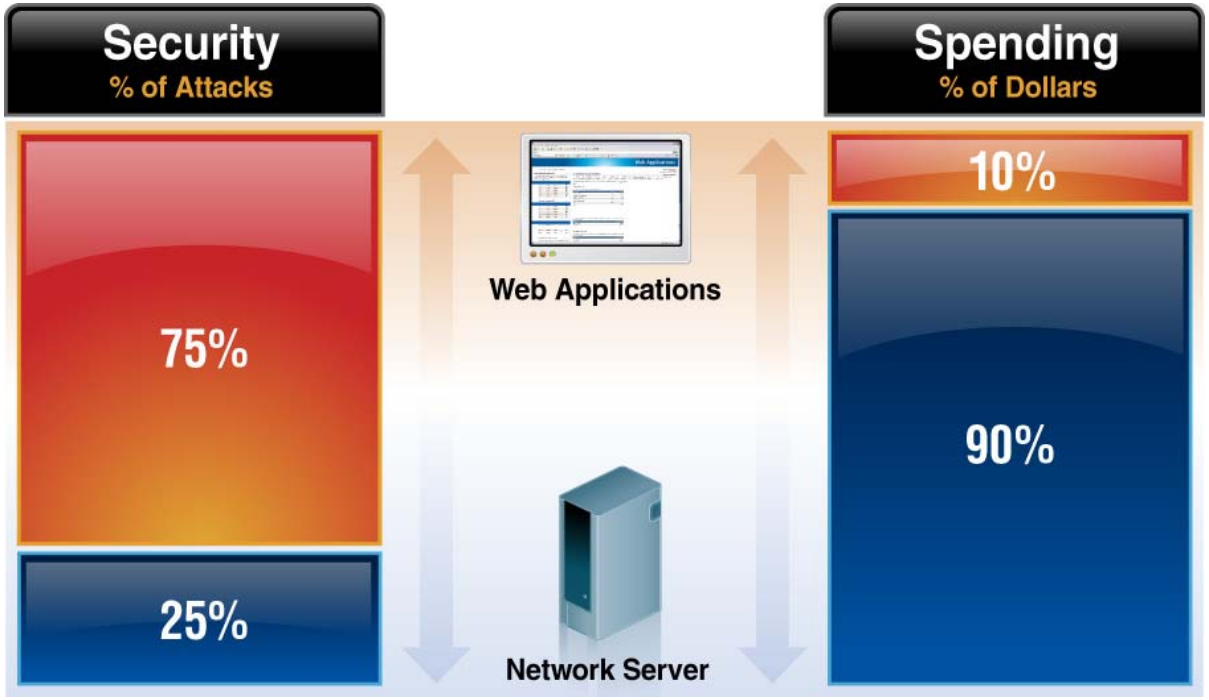
The attackers accessed a public Web site and then bypassed additional secured databases stored on the same server. In addition to SSNs, the databases contained health insurance information and non-treatment medical information, such as immunization records and names of doctors patients had seen. No medical records (i.e. patient diagnoses, treatments, and therapies) were taken, as they are stored in a separate system, emphasized Steve Lustig, associate vice chancellor for health and human services.

(Credit: University of California at Berkeley)

"Their ID has not been stolen," he added. "Some data has been stolen."

The server breach began on October 9, 2008, and continued through April 9, when a campus computer administrator doing routine maintenance discovered messages left by the attackers. Logs indicate that the hacks originated from overseas, "primarily in the Asian

Reality: Security and Spending Are Unbalanced



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

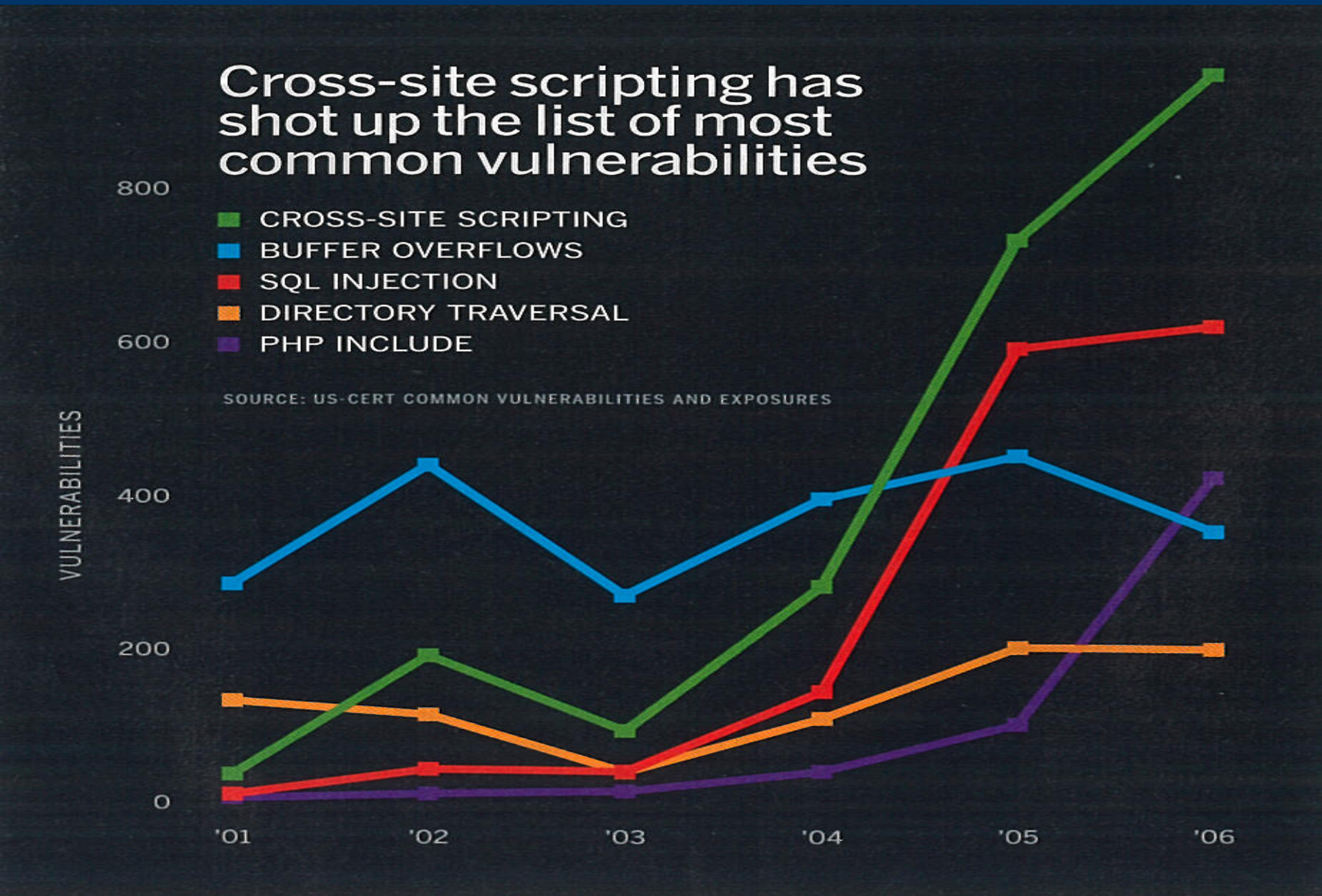
2/3 of All Web Applications are Vulnerable

***Gartner*

WHY DO HACKERS TODAY TARGET APPLICATIONS?

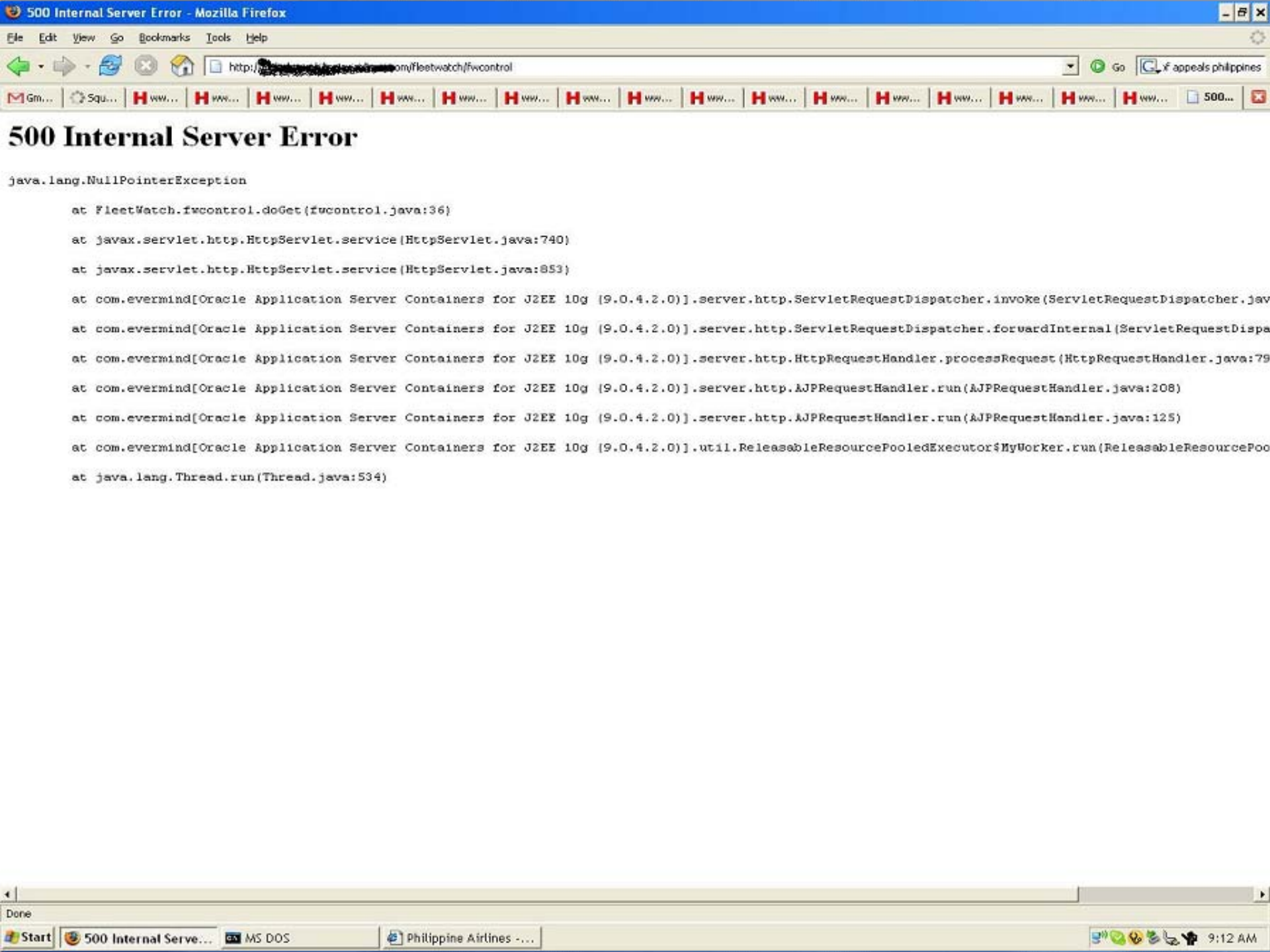
- **Because they know you have firewalls**
  - So its not very convenient to attack the network anymore
  - But they still want to attack ‘cos they still want to steal data …
- **Because firewalls do not protect against app attacks!**
  - So the hackers are having a field day!
  - Very few people are actively aware of application security issues
- **Because web sites have a large footprint**
  - No need to worry anymore about cumbersome IP addresses
- **Because they can!**
  - **It is difficult or impossible to write a comprehensively robust application**
    - Developers are yet to have secure coding as second nature
    - Developers think differently from hackers
    - Cheap, Fast, Good – choose two, you can’t have it all
    - It is also a nightmare to manually QA the application
    - “White-box” static code analyzers don’t test for inter-app relationships
    - Many companies today still do not have a software security QA policy or resource

Top Hack Attacks Today Target Web Applications



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


500 Internal Server Error - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://[redacted]/Fleetwatch/fwcontrol
Go
500 Internal Server Error
java.lang.NullPointerException
at FleetWatch.fwcontrol.doGet(fwcontrol.java:36)
at javax.servlet.http.HttpServlet.service(HttpServlet.java:740)
at javax.servlet.http.HttpServlet.service(HttpServlet.java:853)
at com.evermind[Oracle Application Server Containers for J2EE 10g (9.0.4.2.0)].server.http.ServletRequestDispatcher.invoke(ServletRequestDispatcher.jav
at com.evermind[Oracle Application Server Containers for J2EE 10g (9.0.4.2.0)].server.http.ServletRequestDispatcher.forwardInternal(ServletRequestDispa
at com.evermind[Oracle Application Server Containers for J2EE 10g (9.0.4.2.0)].server.http.HttpRequestHandler.processRequest(HttpRequestHandler.java:79
at com.evermind[Oracle Application Server Containers for J2EE 10g (9.0.4.2.0)].server.http.AJPRequestHandler.run(AJPRequestHandler.java:208)
at com.evermind[Oracle Application Server Containers for J2EE 10g (9.0.4.2.0)].server.http.AJPRequestHandler.run(AJPRequestHandler.java:125)
at com.evermind[Oracle Application Server Containers for J2EE 10g (9.0.4.2.0)].util.ReleasableResourcePooledExecutor$MyWorker.run(ReleasableResourcePoo
at java.lang.Thread.run(Thread.java:534)
Done
Start
500 Internal Serve...
MS DOS
Philippine Airlines -...
9:12 AM

Runtime Error - Windows Internet Explorer

http://www.[redacted].com/errors/404.aspx?aspxerrorpath=/Default.aspx

File Edit View Favorites Tools Help

9.0 minutes saved

Runtime Error

Page Tools

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 w
attribute set to "RemoteOnly". 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>
```

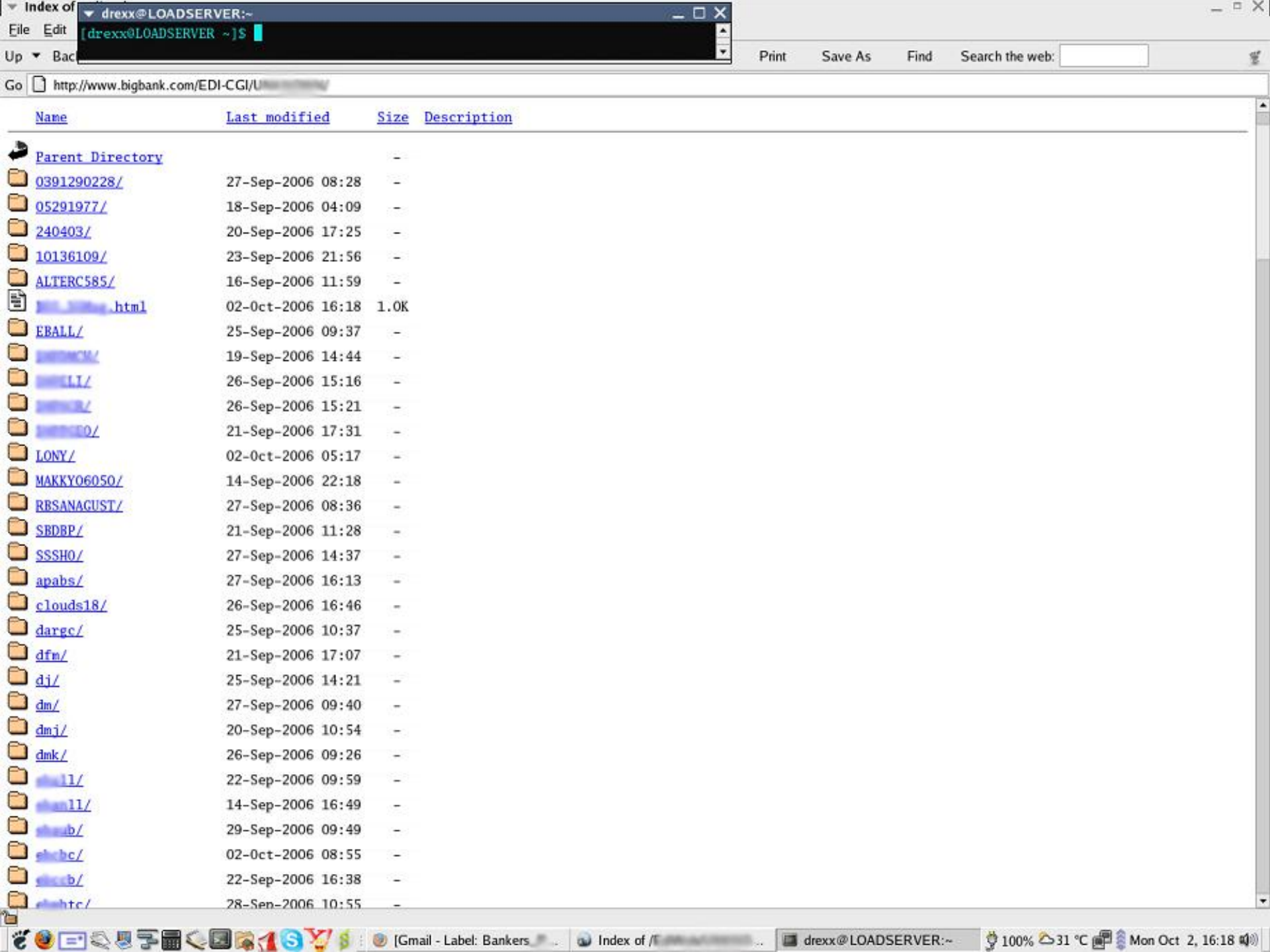
Notes: The current error page you are seeing can be replaced by a custom error page by modifying the "defaultRedirect" attribute of the application's <customErrors> configuration tag to point to a custom error page URL.

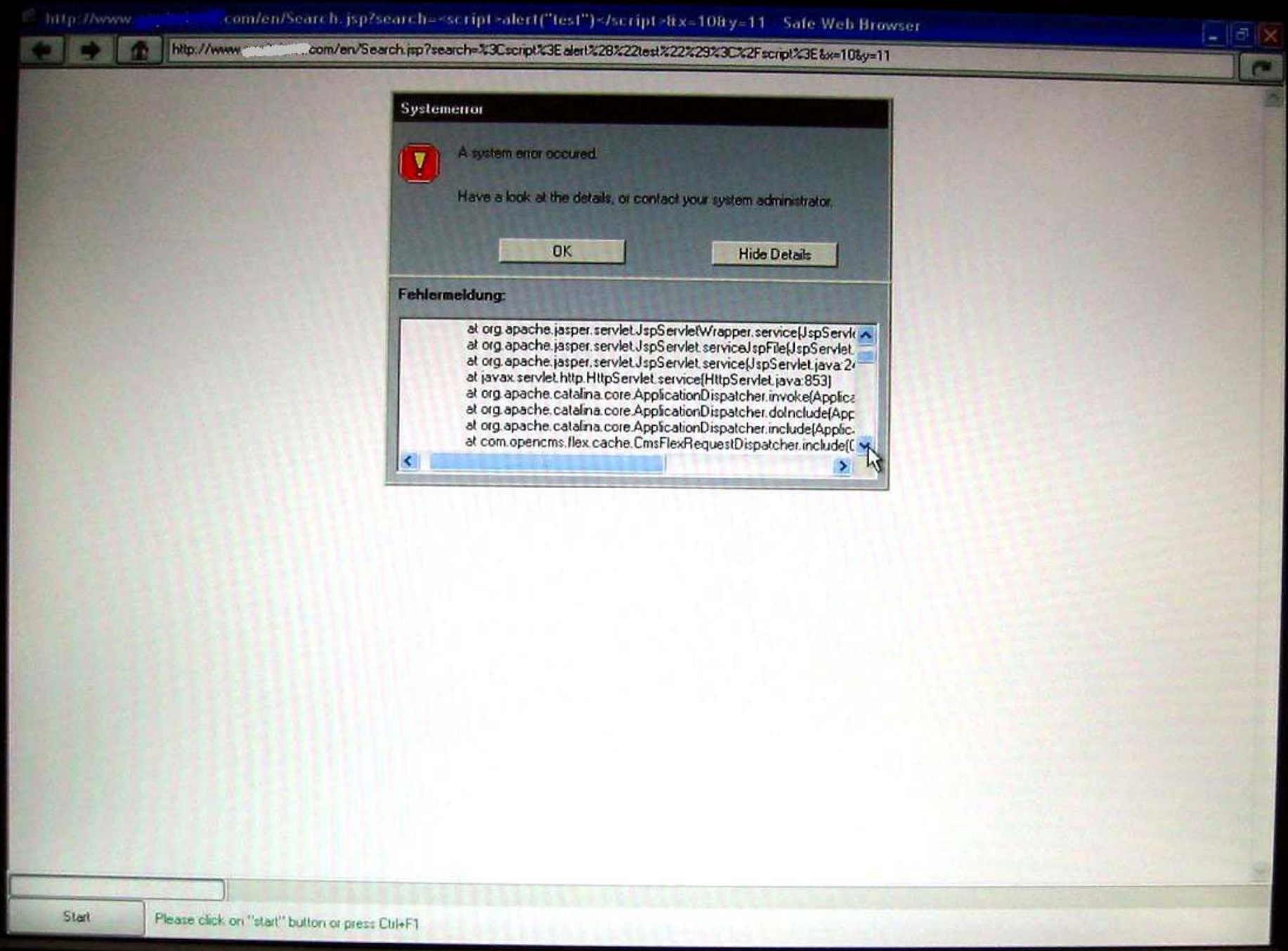
```
<!-- Web.Config Configuration File -->

<configuration>
    <system.web>
        <customErrors mode="On" defaultRedirect="mycustompage.htm"/>
    </system.web>
</configuration>
```

Done

Internet

100%


drexx@LOADSERVER:~
[drexx@LOADSERVER ~]$
File Edit
Up Bac
Print Save As Find Search the web:
Go http://www.bigbank.com/EDI-CGI/
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 -
.html 02-Oct-2006 16:18 1.0K
EBALL/ 25-Sep-2006 09:37 -
19-Sep-2006 14:44 -
26-Sep-2006 15:16 -
26-Sep-2006 15:21 -
21-Sep-2006 17:31 -
LONY/ 02-Oct-2006 05:17 -
MAKKYO605O/ 14-Sep-2006 22:18 -
RBSANAGUST/ 27-Sep-2006 08:36 -
SBDBP/ 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 -
22-Sep-2006 09:59 -
14-Sep-2006 16:49 -
29-Sep-2006 09:49 -
02-Oct-2006 08:55 -
22-Sep-2006 16:38 -
28-Sep-2006 10:55 -
[Gmail - Label: Bankers
Index of /
drexx@LOADSERVER:~
100% 31 °C Mon Oct 2, 16:18


Safe Web Browser
com/en/Search.jsp?search=%3Cscript%3Ealert%28%22test%22%29%3C%2Fscript%3E&x=10&y=11
Systemerror
A system error occured.
Have a look at the details, or contact your system administrator.
OK
Hide Details
Fehlermeldung:
at org.apache.jasper.servlet.JspServletWrapper.service(JspServl
at org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.
at org.apache.jasper.servlet.JspServlet.service(JspServlet.java:2
at javax.servlet.http.HttpServlet.service(HttpServlet.java:853)
at org.apache.catalina.core.ApplicationDispatcher.invoke(Applica
at org.apache.catalina.core.ApplicationDispatcher.doInclude(App
at org.apache.catalina.core.ApplicationDispatcher.include(Applic
at com.opencms.flex.cache.CmsFlexRequestDispatcher.include(
Start
Please click on "start" button or press Ctrl+F1

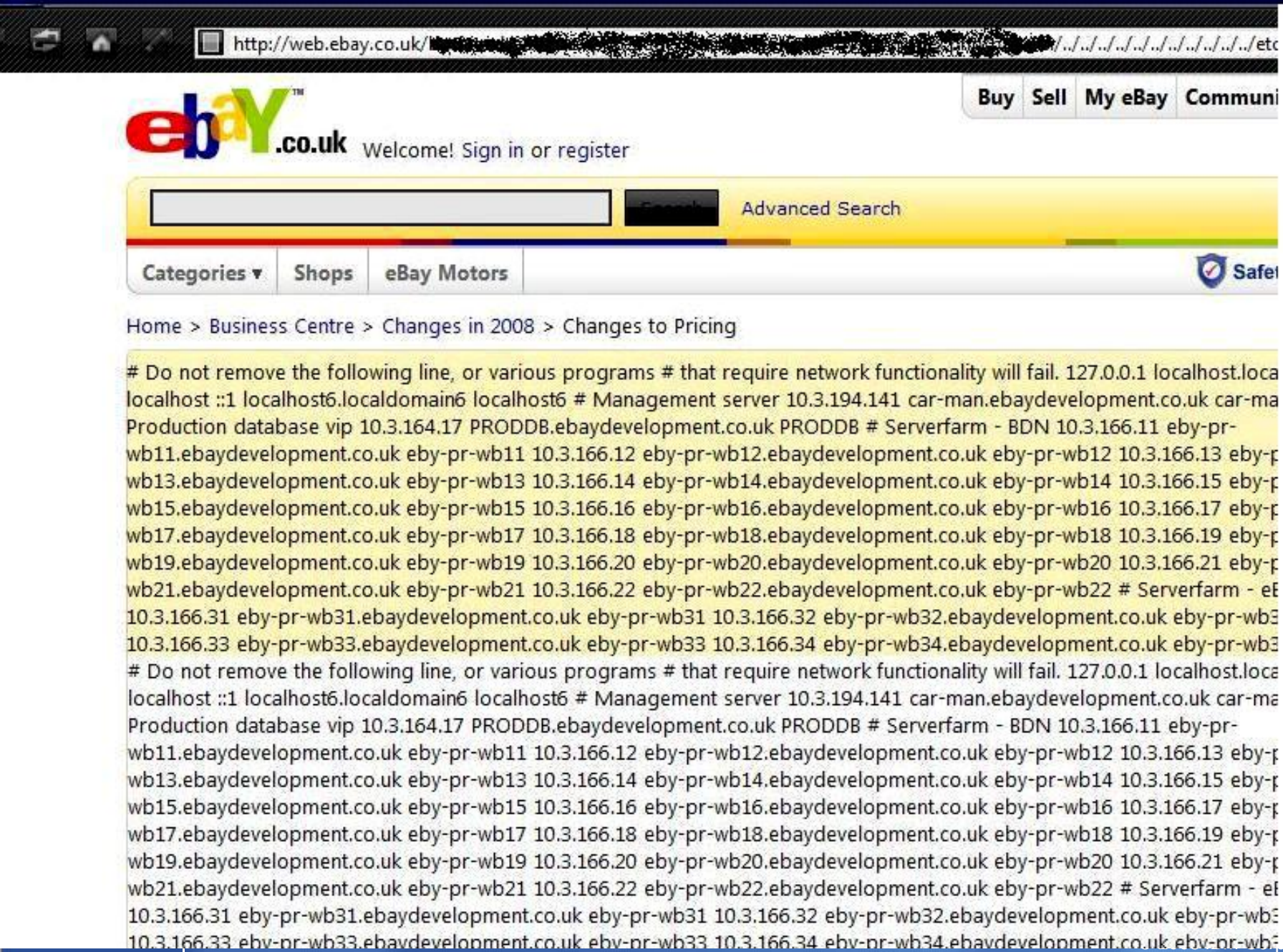
OWASP Asia Pacific Conference

25-27 FEB 2009, GOLD COAST, AUSTRALIA

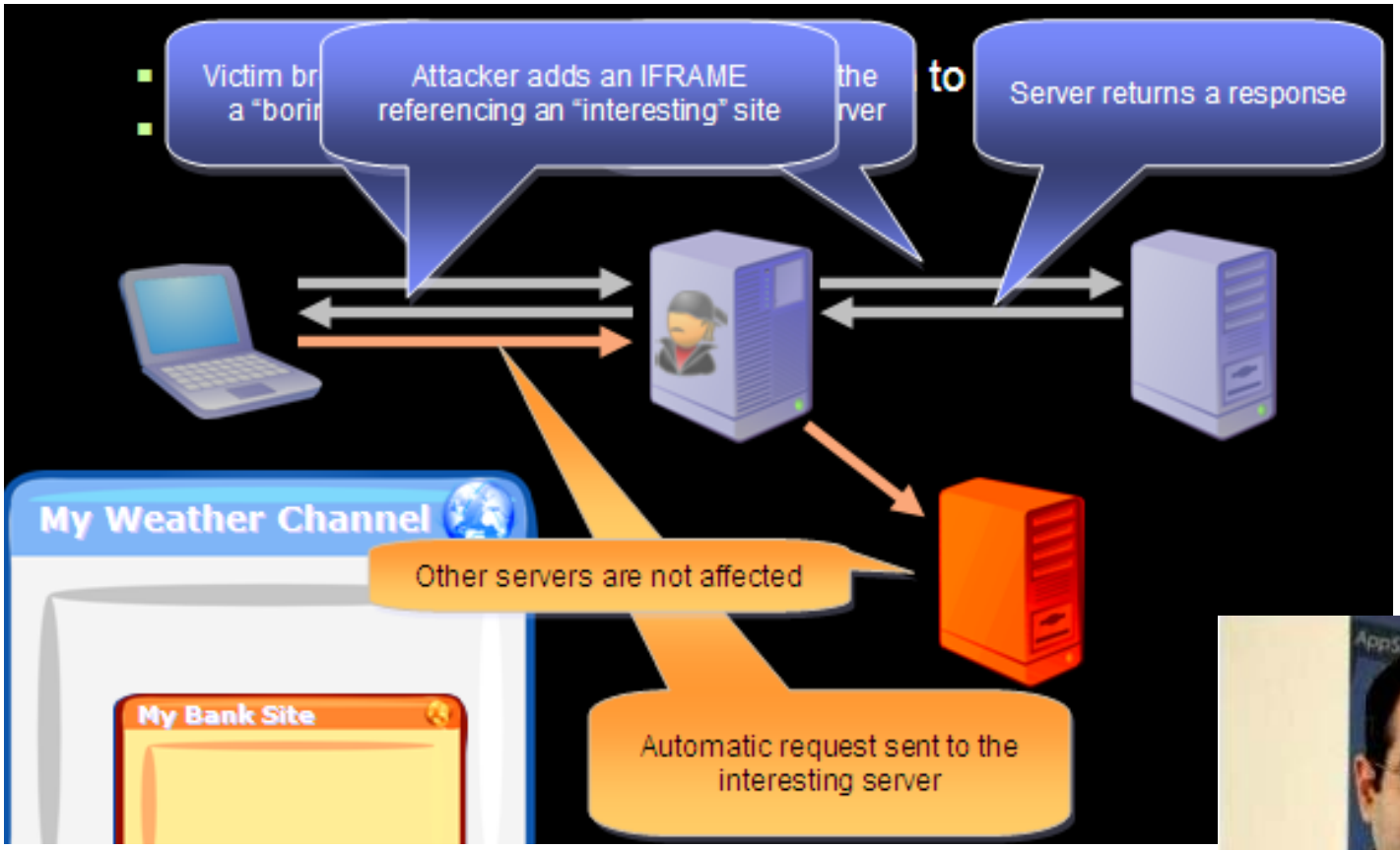
Room 5 & 6

09:00 - 10:45	Conference open & Keynote session: Web-Based Man-in-the-Middle Attacks (IBM Rational) *Adi Sharabani*
11:15 - 12:15	Examining and Bypassing the IE8 XSS Filter *Alex Kou*
13:30 - 14:00	OWASP Panel

Attackers use directory traversal attacks to read arbitrary files on web servers, such as SSL private keys and password files.



Now there's Web "Man-in-the Middle" Attacks



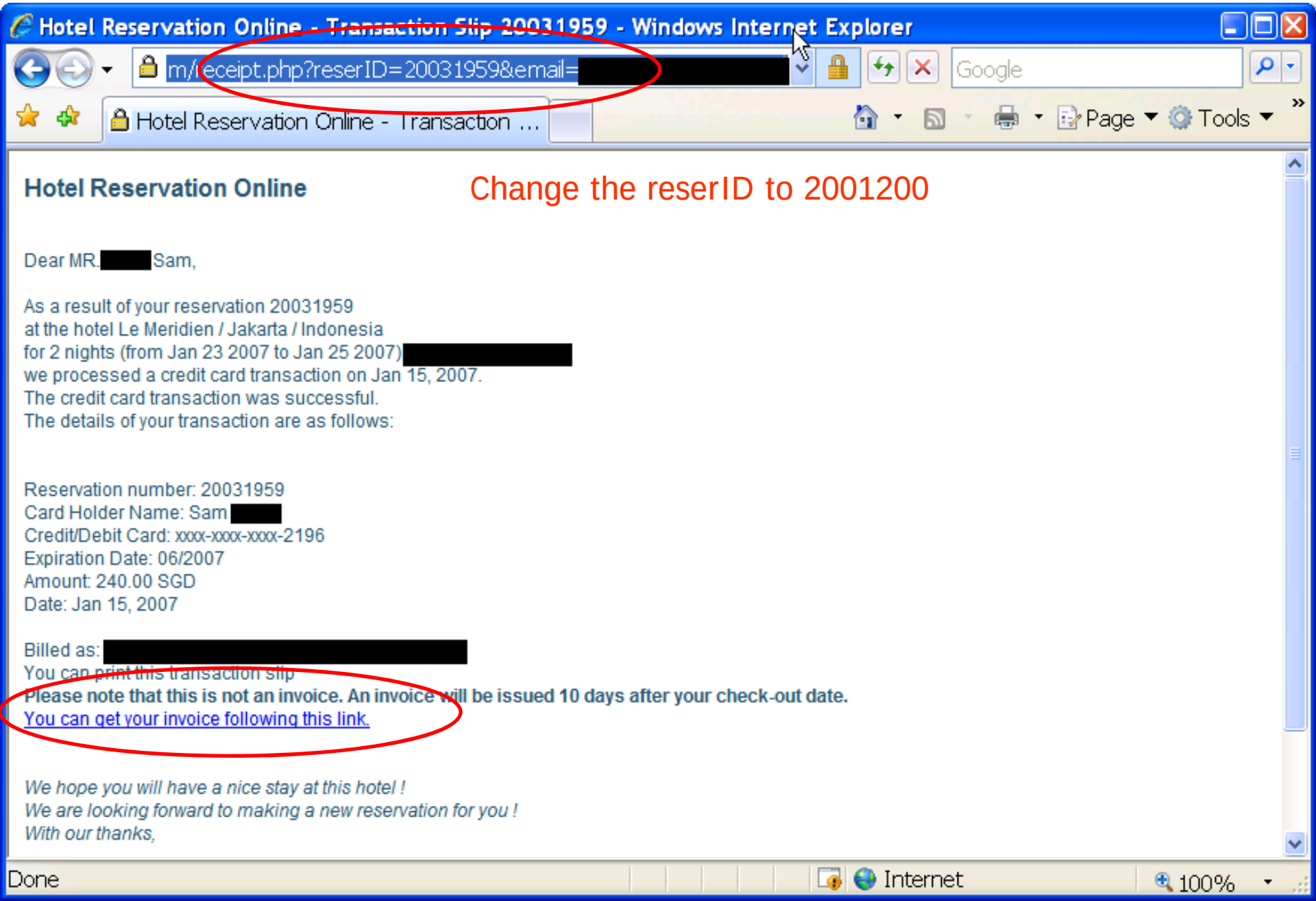
"The well-known 'man in the middle' scenario is a form of passive attack," explained Adi Sharabani, manager of security research for the Rational AppScan team in Israel. "The hacker sits and waits until the victim visits a sensitive web site and then steals information such as cookies from his browser." Sensitive sites include those where you input personal details, such as Gmail, Hotmail, eBay, Amazon, banking sites, and so forth.

First presented at OWASP AP Conference Mar 09 Brisbane

Malware on Web Applications

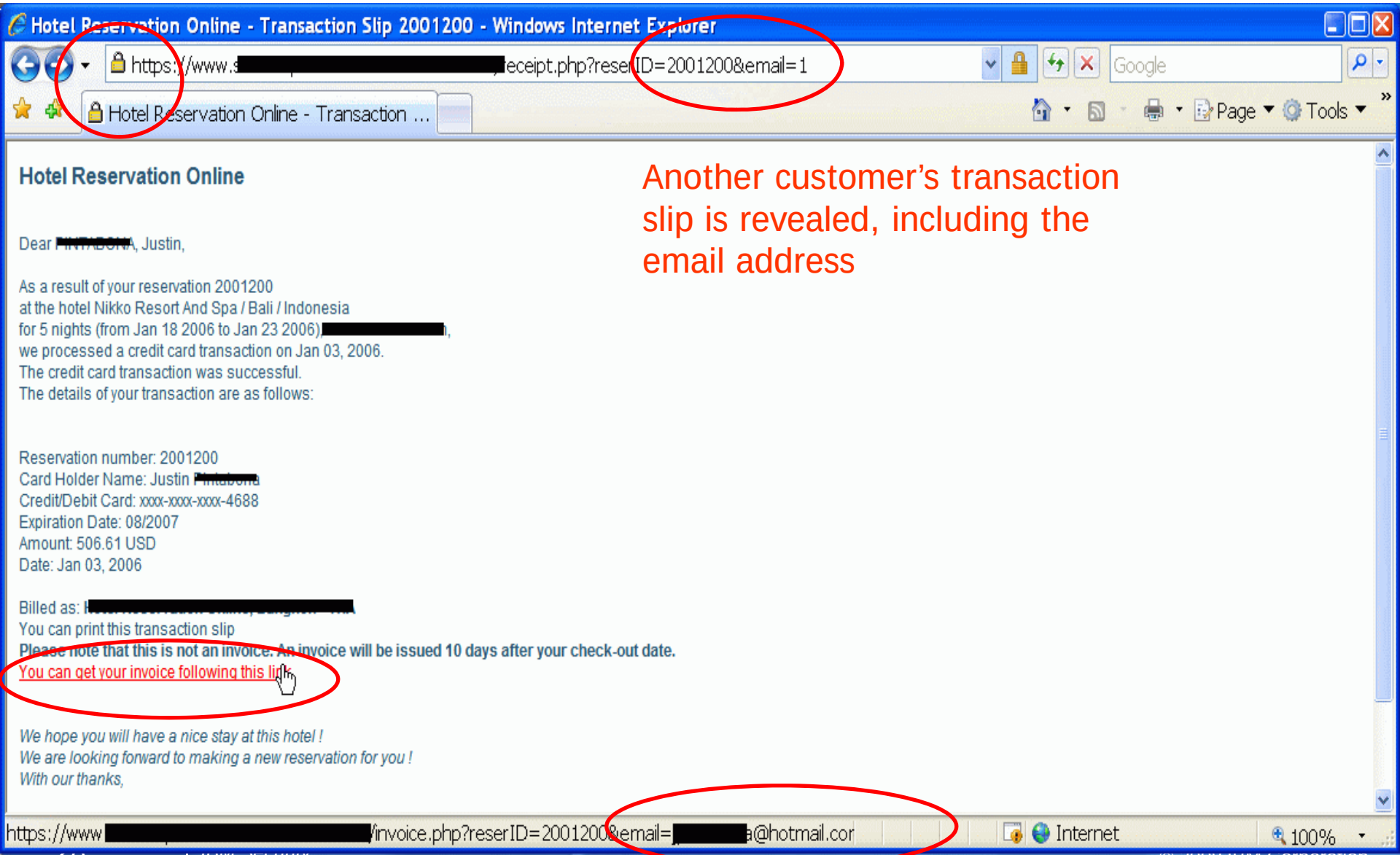
- **Malware can be delivered in many ways:**
  - E-mail, IM, network vulnerabilities…
- **Today, Malware is primarily delivered via Web Applications:**
  - Aims to infect those browsing the site
  - Installed via Client-Side (e.g. Browser) Vulnerabilities & Social Engineering
- **Malicious content can be downloaded:**
  - From the web application itself
  - Through frames & images leading to other websites
  - Through links leading to malicious destinations
- **Legitimate Sites Hijacked to distribute Malware!**
  - **McAfee, Asus, US Govt Staff Travel Site, Wordpress.org, SuperBowl, …**

Real Example: Online Travel Reservation Portal



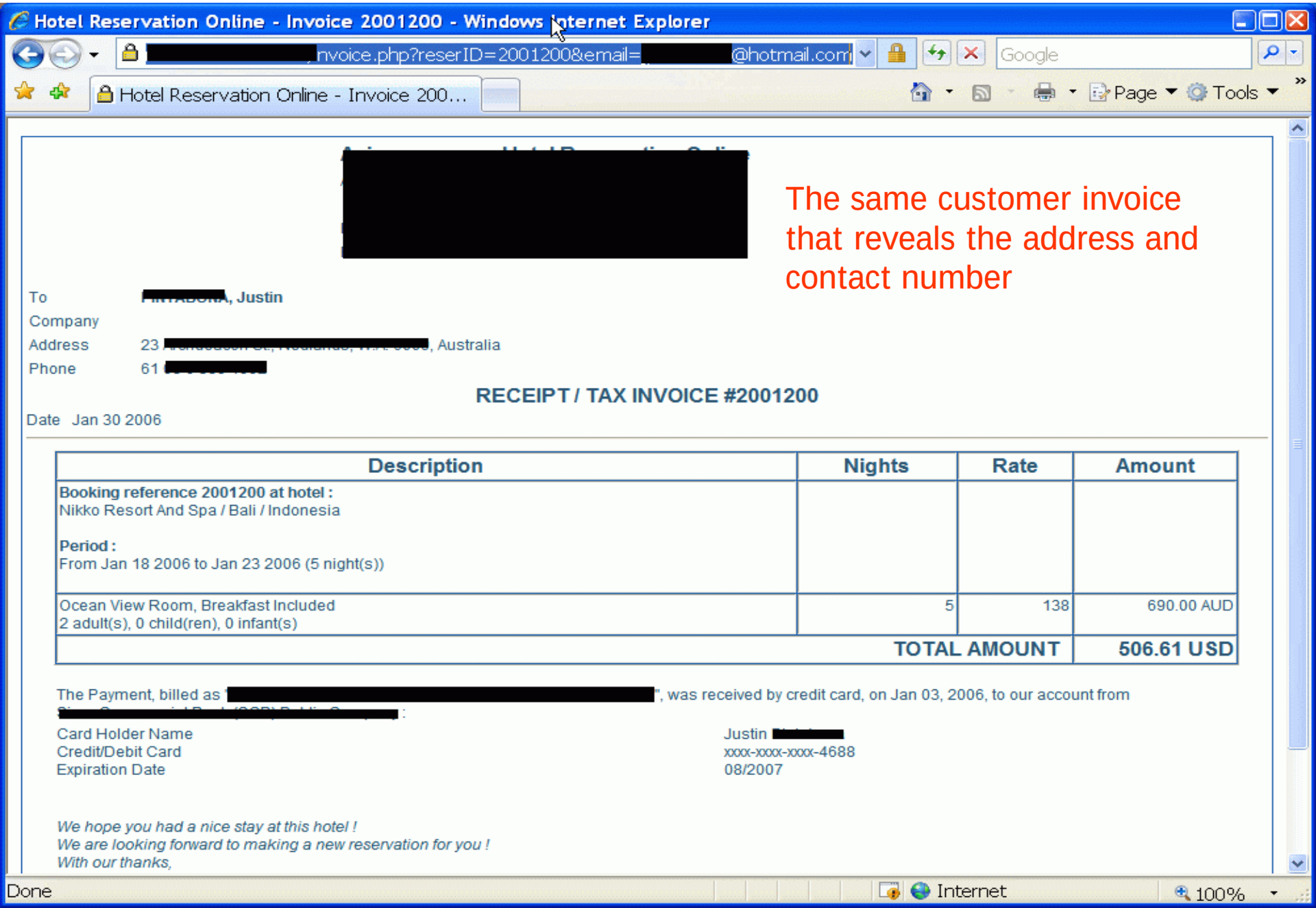
Real Example : Parameter Tampering

Reading another user's transaction – insufficient authorization



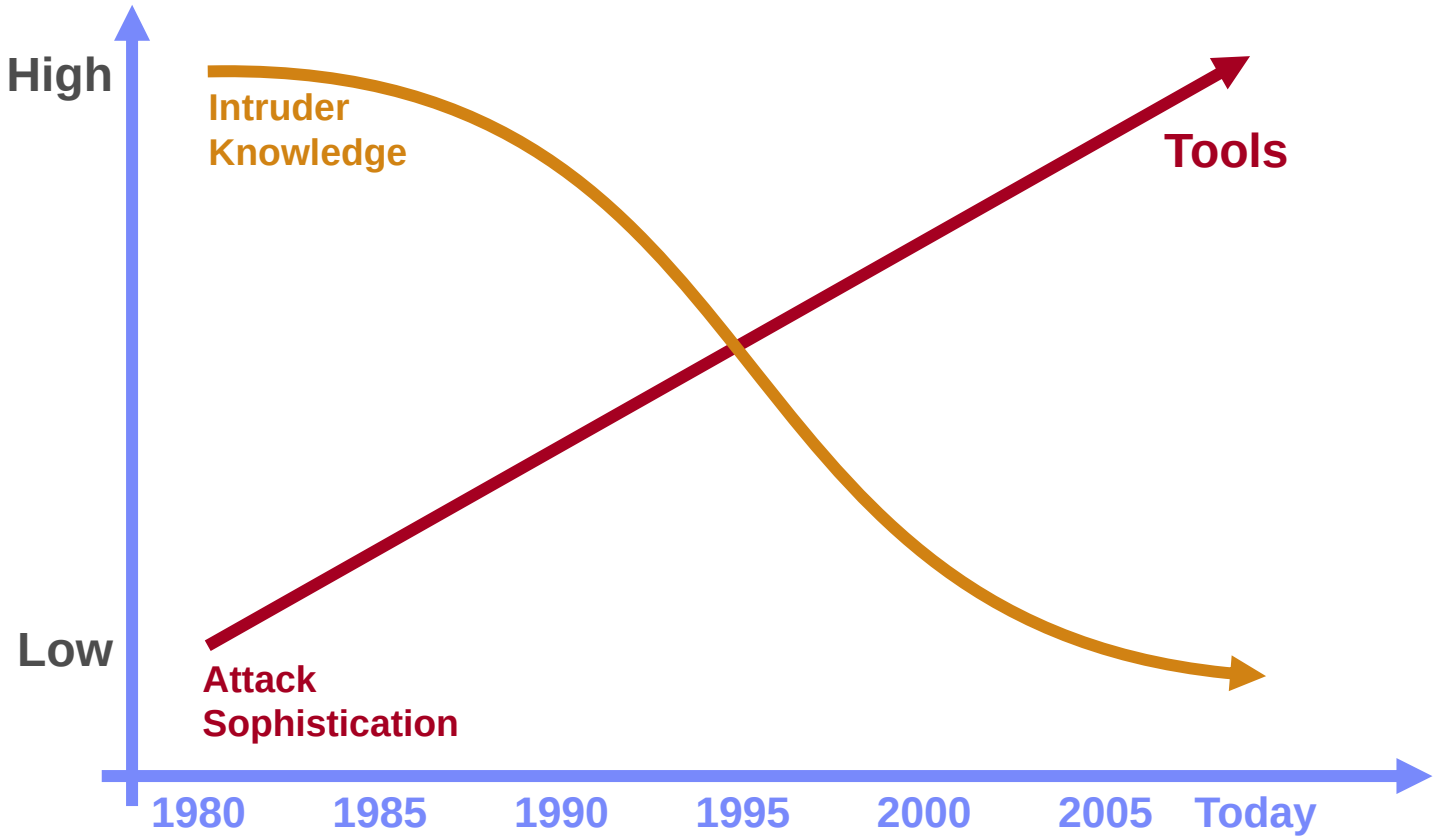
Another customer's transaction slip is revealed, including the email address

Parameter Tampering Reading another user's invoice

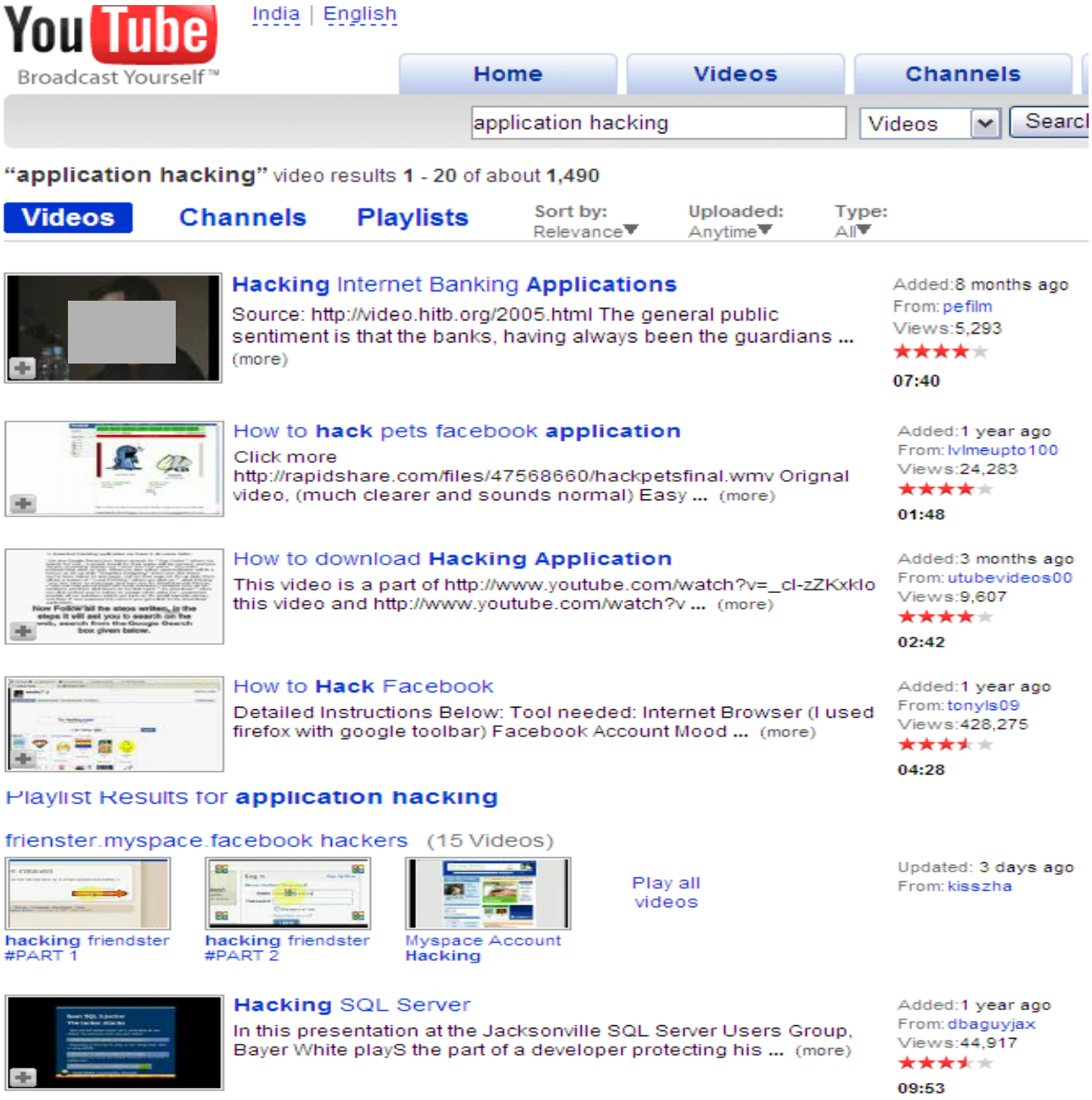


The same customer invoice that reveals the address and contact number

Attacks Sophistication vs. Intruder Knowledge



DON'T TRY THIS AT HOME!



NEW GOOGLE CHROME WEB BROWSER

SoShiok.com

http://www.soshiok.com/articles/10958

GOOGLE Singapore | GMAIL | PACNET | W3 IBM AL Home | Veritas SGP

Updated 11:29 Feb 07, 2009

Clipboard | Blogs

HOME | NEWS BITES | HOT RESTAURANTS | FOODIE FEATURES | CHEERS | COFFEE SHOP TALK | COOK

Chicken rice fans flock here for the Swee Kee

Fri Oct 10 2008
Adele Ong
The New Paper

Yeo Keng Nam chicken rice draws the crowds, from teenagers and housewives to busine... love the old-world taste that is well preserved here.

Back
Forward
Reload
Save as...
Print...
View page source
View page info
Inspect element

"INSPECT ELEMENT"

Tuck into comfort food at Yeo Keng Nam

MORE STORIES

- Now's the time to take stoc
- The very best of Spanish w
- Royal China at Raffles

COFFEE SHOP TAL

- Talk (140 replies)
- Gourmet and Fine Dining (
- Coffeeshops, Food Centre
  Courts (45 replies)
- Cafes, Bistros / Other Eate

SoShiok.com

http://www.soshiok.com/articles/10958

Updated 11:29 Feb 07, 2009

Clipboard Blogs SIGN U

HOME • NEWS BITES • HOT RESTAURANTS • FOODIE FEATURES • CHEERS • COFFEE SHOP TALK • COOK THIS

Chicken rice fans flock here for t

Fri Oct 10 2008
Adele Ong
The New Paper

Yeo Keng Nam chicken rice draws the crowds, from teenagers the old-world taste that is well preserved here.

Tuck into comfort food at Yeo K

chrome-resource://inspector/inspector.html - Google Chrome

chrome-resource://inspector/inspector.html

Elements Resources "INSPECT ELEMENT" Search

```
▶ <script>
  <script src="/javascripts/facebox.js?1220825148" type="text/javascript">
▶ <div id="secondary-content" class="clearfix bar-wrapper">
▶ <div id="footer" class="clearfix pngwrapper">
</div>
<!-- here -->
▶ <div style="display: none;">
<!-- BEGIN: M1ACV Release 2.1.1 -->
<!-- (c)2002-2008, MediaOne Network Inc. All Rights Reserved. -->
<div id="M1DIV" name="M1DIV">
<img id="M1IMG" name="M1IMG" width="0" height="0" border="0" src="http://acvs.mediaonenetwork.net/client/pixel.gif">
<script language="javascript" type="text/javascript" src="http://acvs.mediaonenetwork.net/client/acv211.js">
<script language="JavaScript" type="text/javascript" src="http://acvs.mediaonenetwork.net/mrsc/acvgo.mrsc?DTM=1233977575471&TZ=480&m1SECID=000000517-008&DOC=http%3A//www.soshiok.com/articles/10958&REF=">
<script language="JavaScript" type="text/javascript" src="http://acvs.mediaonenetwork.net/script/acvlog.js">
<noscript>
<!-- END: M1ACV -->
</body>
</html>
```

Styles

Computed Style Show inh

```
border-bottom-width: 0px;
border-left-width: 0px;
border-right-width: 0px;
border-top-width: 0px;
display: block;
font-family: Arial;
font-size: 12px;
font-style: normal;
font-weight: normal;
height: 153px;
left: 0px;
margin-bottom: 0px;
margin-left: 0px;
margin-right: 0px;
margin-top: 0px;
padding-bottom: 0px;
padding-left: 0px;
padding-right: 0px;
padding-top: 0px;
position: absolute;
top: 0px;
vertical-align: baseline;
width: 520px;
```

#top-banner #soshiok www.soshiok.com

```
height: 153px;
left: 0px;
```

html body div#main-wrapper div#top-banner a div#soshiok

GOOGLE CHROME - "VIEW PAGE SOURCE"

SoShiok.com

http://www.soshiok.com/articles/10958

Chicken rice fans flock here for the Swee Kee taste

Fri Oct 10 2008
Adele Ong
The New Paper

Back
Forward
Reload
Save as...
Print...
View page source
View page info
Inspect element

Tuck into comfort food at Yeo Keng Nam

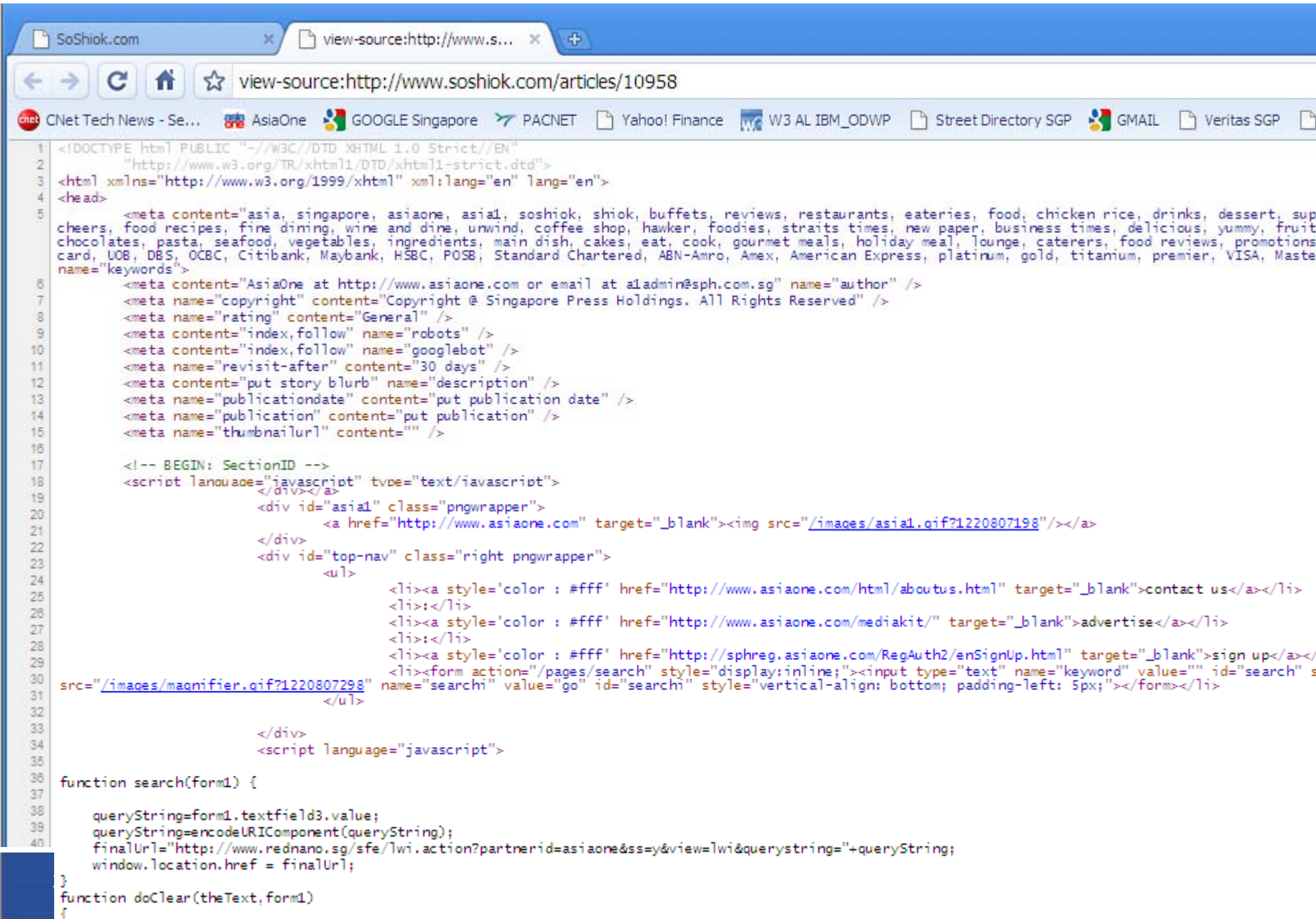
By Adele Ong

MORE STO
Now's the tim
The very bes
Royal China a

Overcoming the
STORM
with Conf
Is your compa
affected by the
current
economic
crisis?

COFFEE S
Talk (291 repl
Gourmet and
Coffeeshops
Courts (57 re
Cafes, Bistro

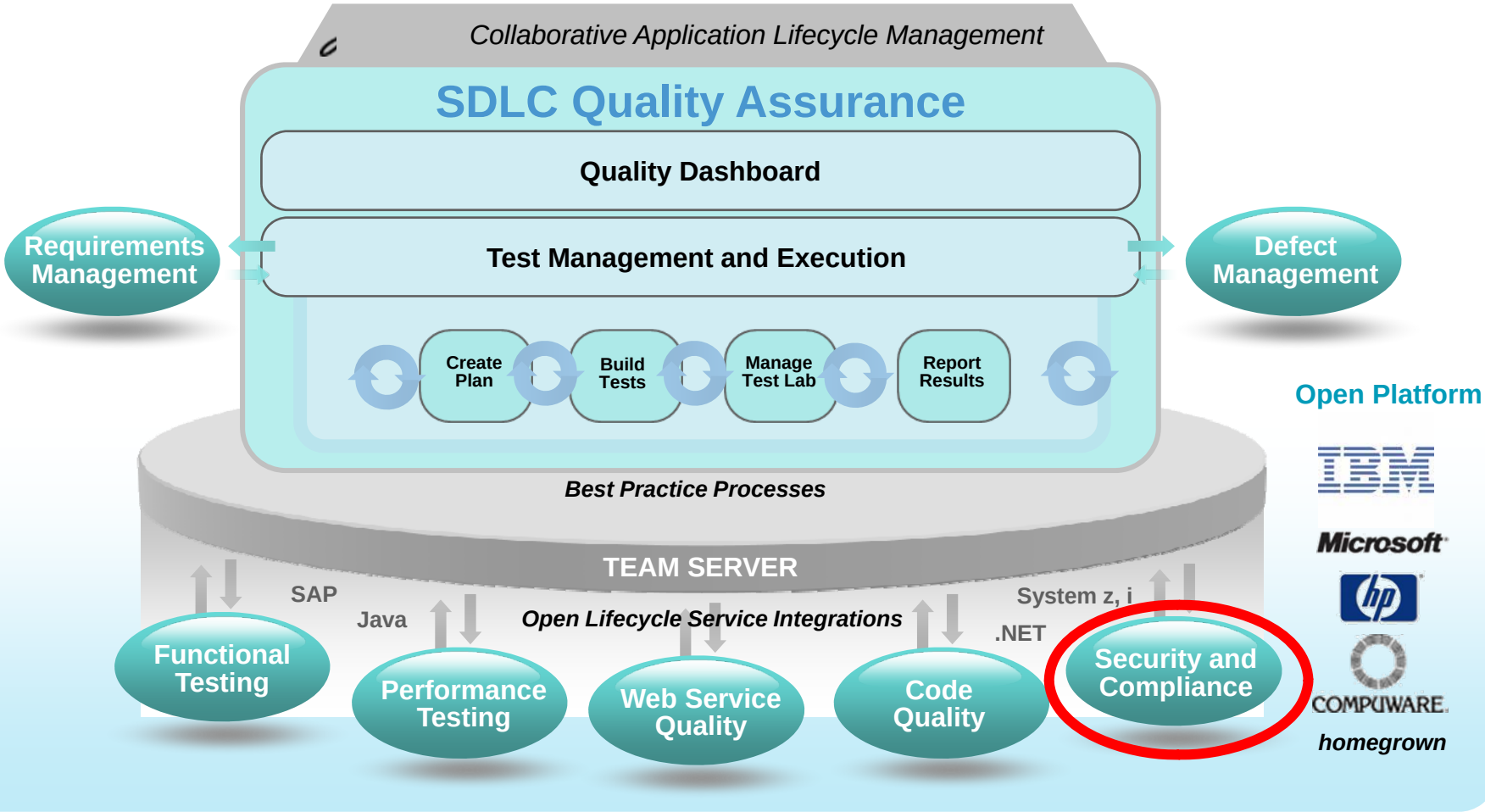
GOOGLE CHROME – ''VIEW PAGE SOURCE



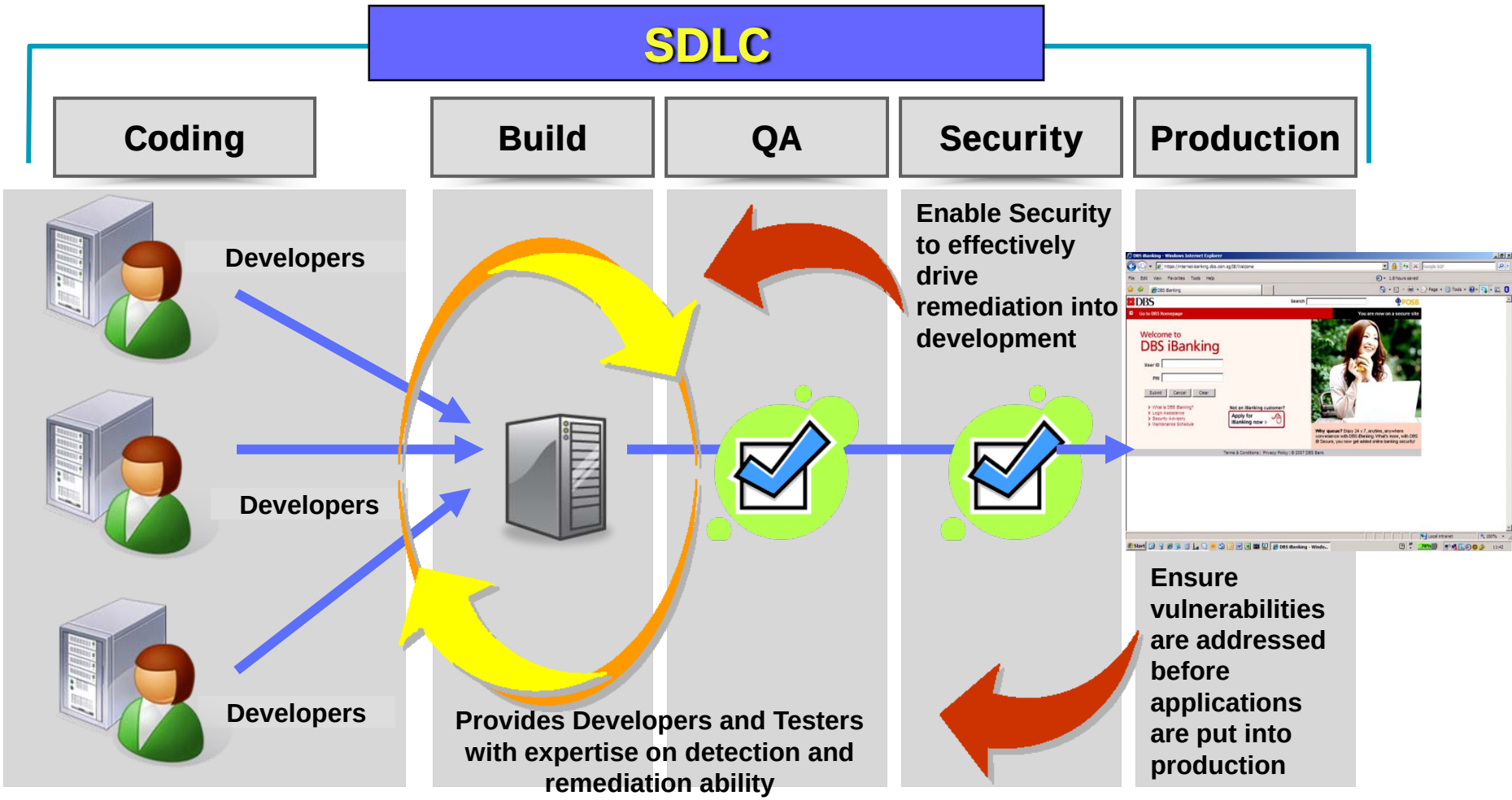
WHY DO APPLICATION SECURITY PROBLEMS EXIST?

- **IT security solutions and professionals are normally from the network /infrastructure /sysadmin side**
  - They usually have little or no experience in application development
  - And developers typically don't know or don't care about security or networking
- **Most companies today still do not have an application security QA policy or resource**
  - IT security staff are focused on other things and are swarmed
    - App Sec is their job but they don't understand it and don't want to deal with it
    - Developers think its not their job or problem to have security in coding
    - People who outsource expect the 3rd party to security-QA for them
- **It is cultural currently to not associate security with coding**
  - "Buffer Overflow" has been around for 25 years!
  - "Input Validation" is still often overlooked.

SECURITY TESTING IS PART OF SDLC QUALITY TESTING

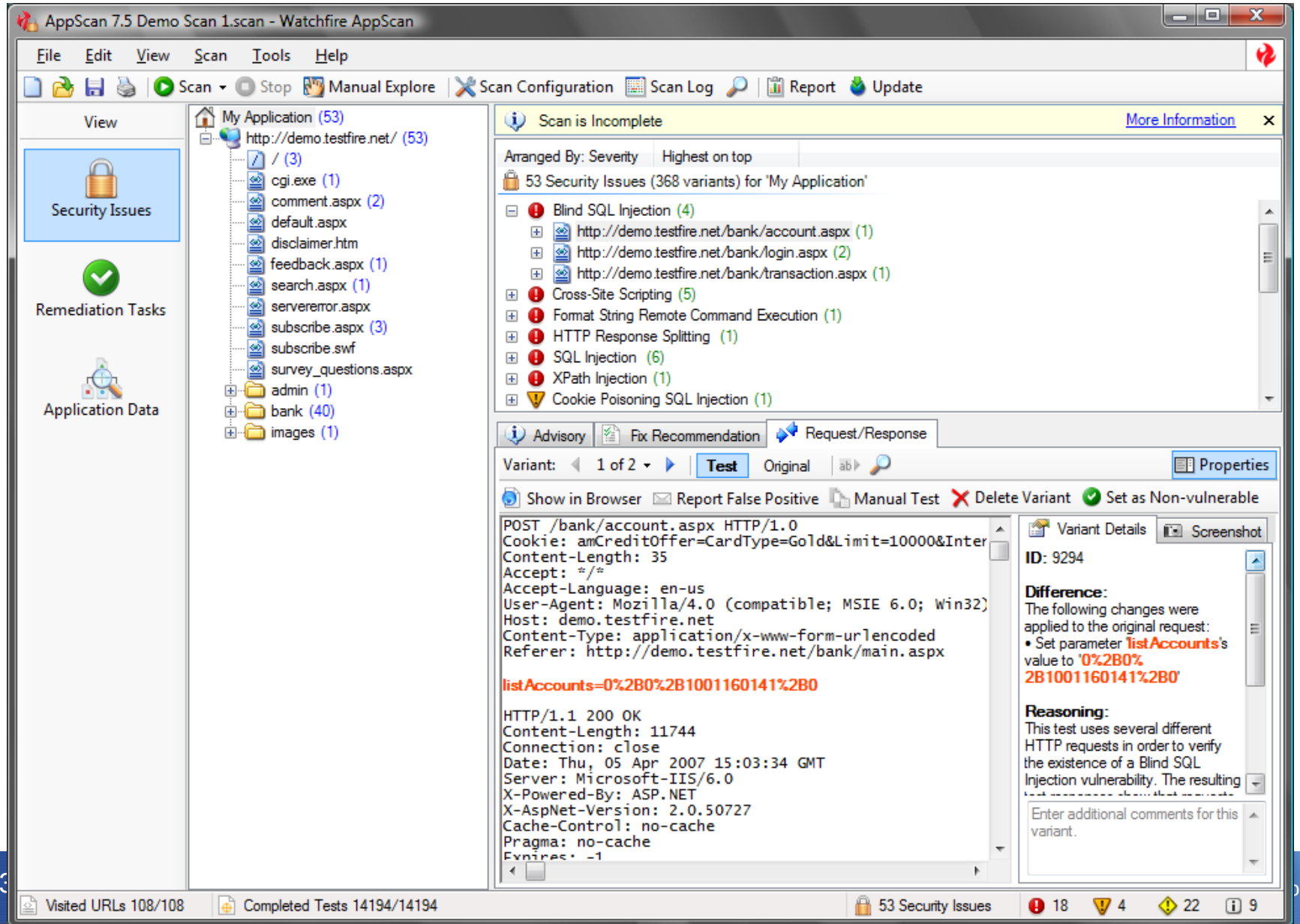


Building security & compliance into the SDLC – further back



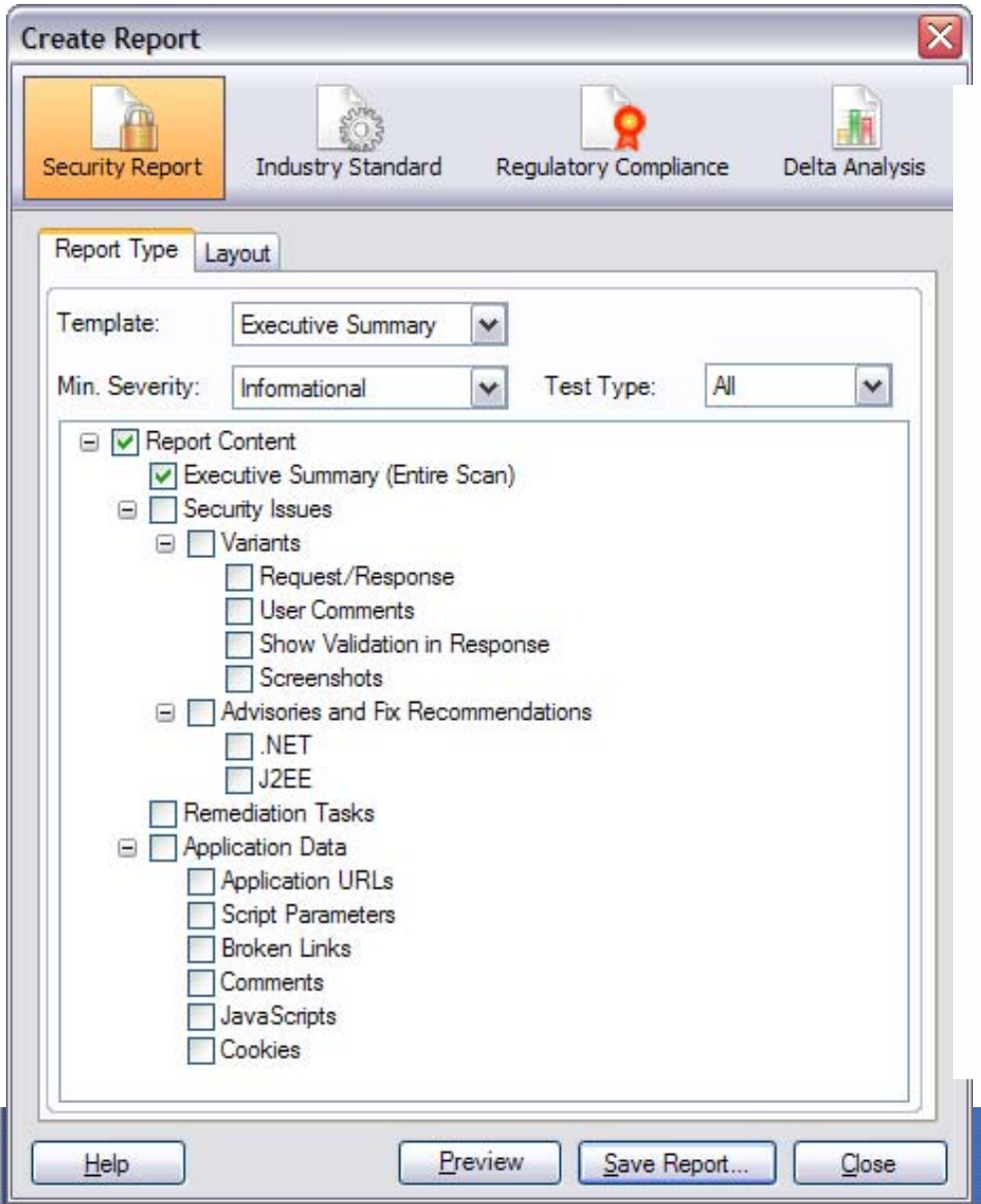
You need a professional solution to

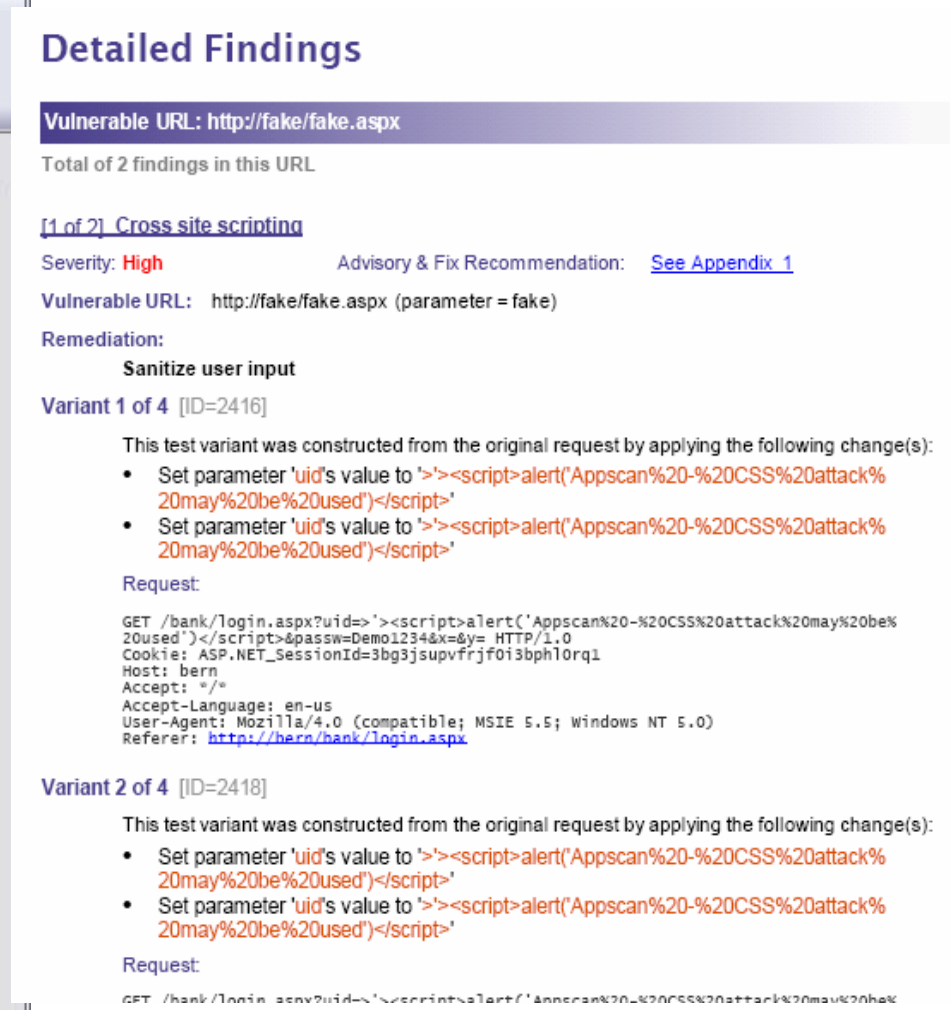
Identify Vulnerabilities



With Rich Report Options

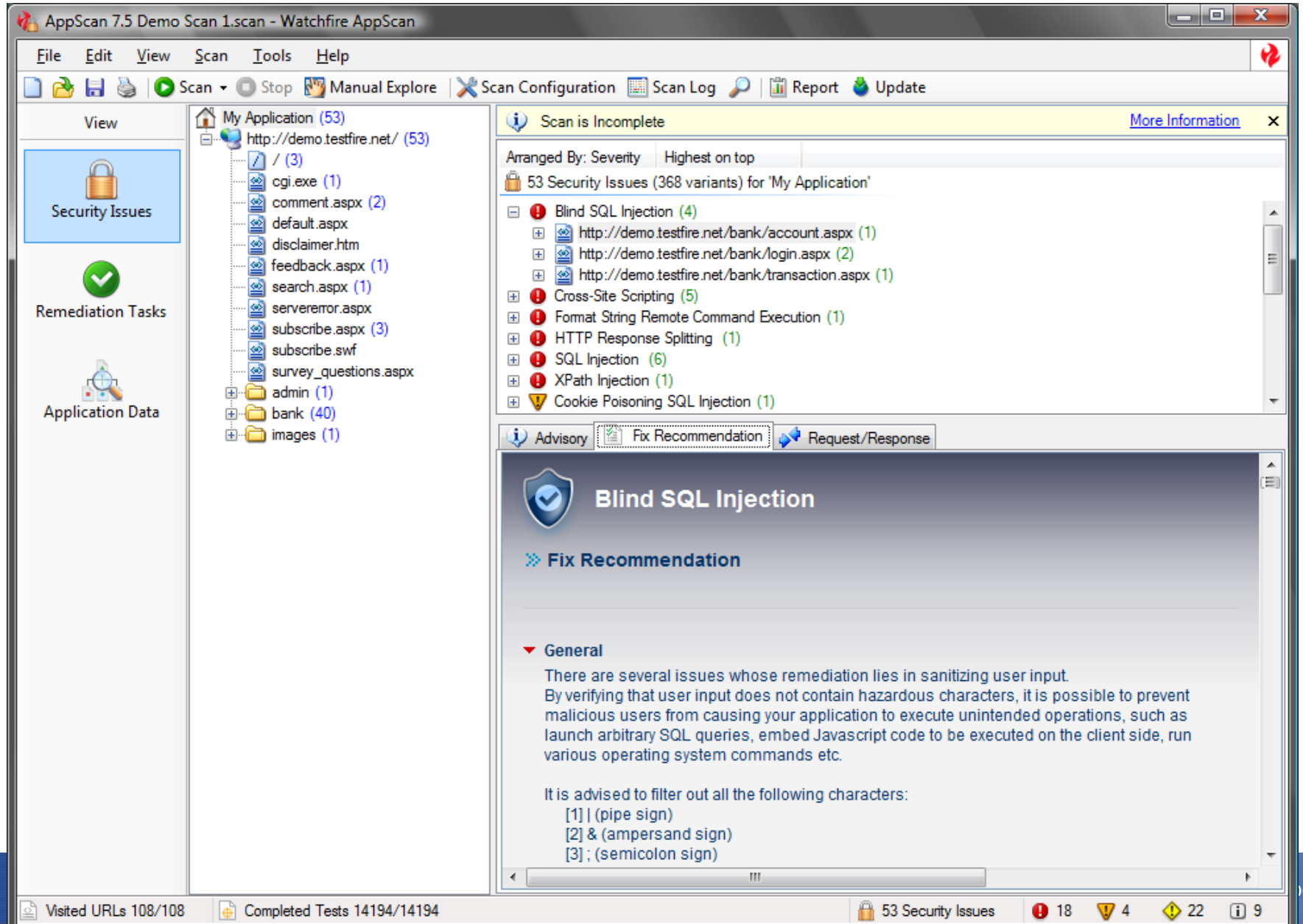
44 Regulatory Compliance Standards, for Executive, Security, Developers.





And Most Important :

Actionable Fix Recommendations



THE NEED FOR SECURITY IN SOFTWARE DEVELOPMENT HAS COME OF AGE …

1. Secure Software Concepts
2. Secure Software Requirements
3. Secure Software Design
4. Secure Software Coding and Implementation
5. Secure Software Testing
6. Software Acceptance
7. Software Deployment, Operations, Maintenance and Disposal

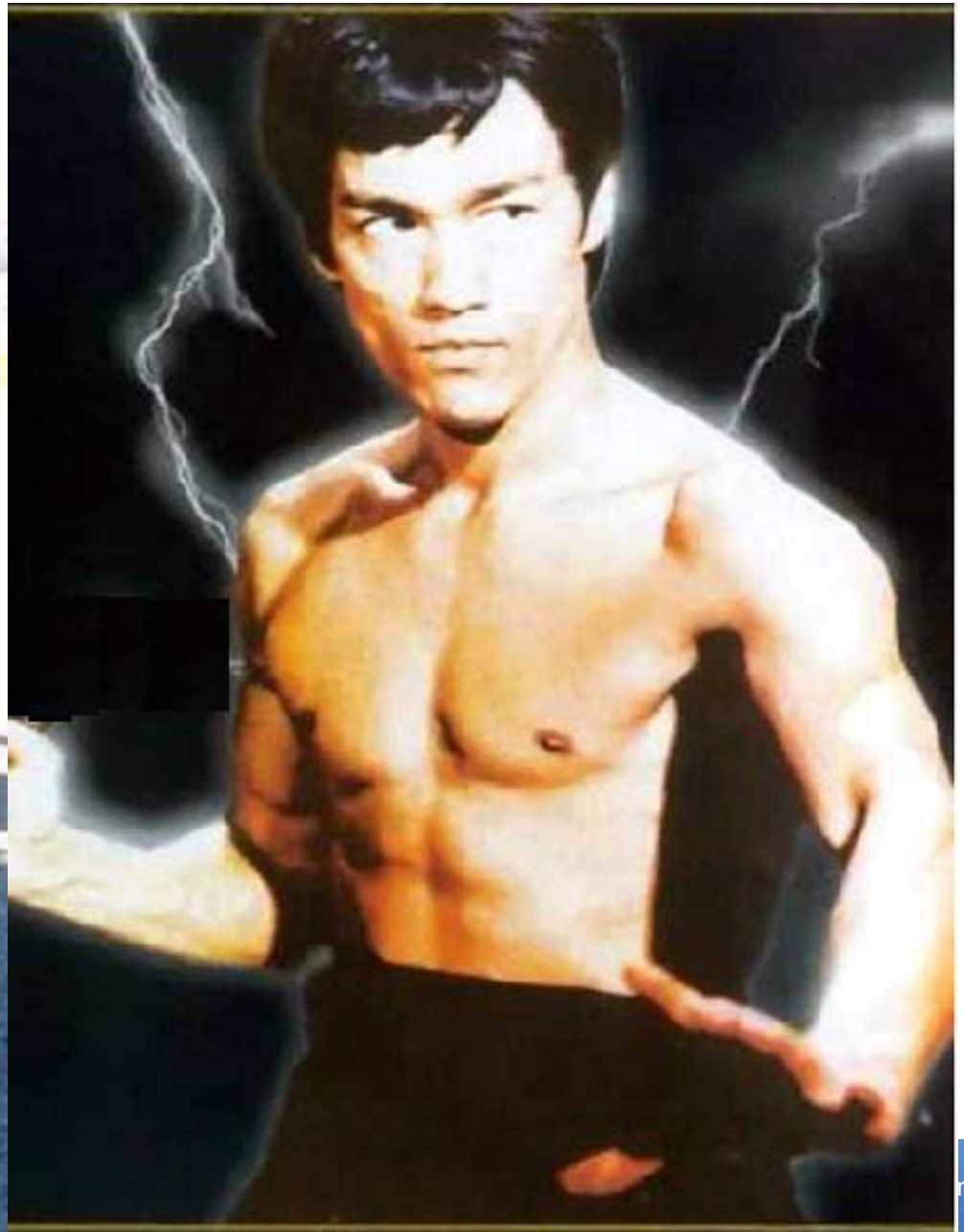
Conclusion: Application QA for Security

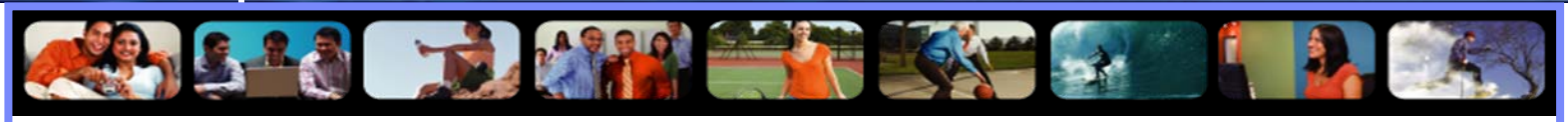
- **The Application Must Defend Itself**
  - You cannot depend on firewall or infrastructure security to do so
- Bridging the GAP between Software development and Information Security
- QA Testing for Security must now be integrated and strategic
- **We need to move security QA testing back to earlier 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

Lower Compliance & Security Costs by:

- Ensuring Security Quality in the Application up front
- Not having to do a lot of rework after production

SDLC QA - YOUR LAST LINE OF DEFENSE





WEB APPLICATION SECURITY

YOUR LAST LINE OF DEFENSE

Thank You

Anthony LIM

MBA CISSP CSSLP FCITIL

innovation that matters