Rational. software

# The Hacker's New Target

## Application Software Security

## *Your Last Line of Defense*

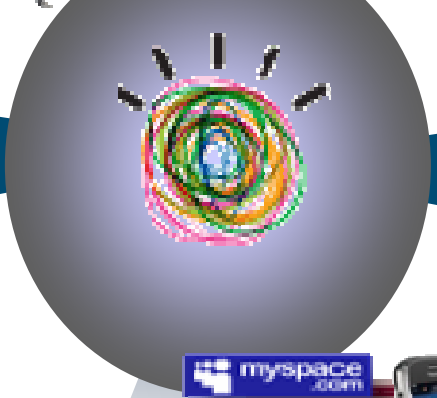
**Anthony Lim**
**MBA FCITIL CISSP CSSLP**
*Director, Security*
*Rational Software - Asia Pacific*

***IBM BAIT Discovery Series 2010***
***Kuala Lumpur 09 Mar 2010***

# Welcome to THE SMARTER PLANET

Globalization and Globally Available Resources

**Billions of mobile devices accessing the Web**



**Access to streams of information in the Real Time**



*** Web 2.0**

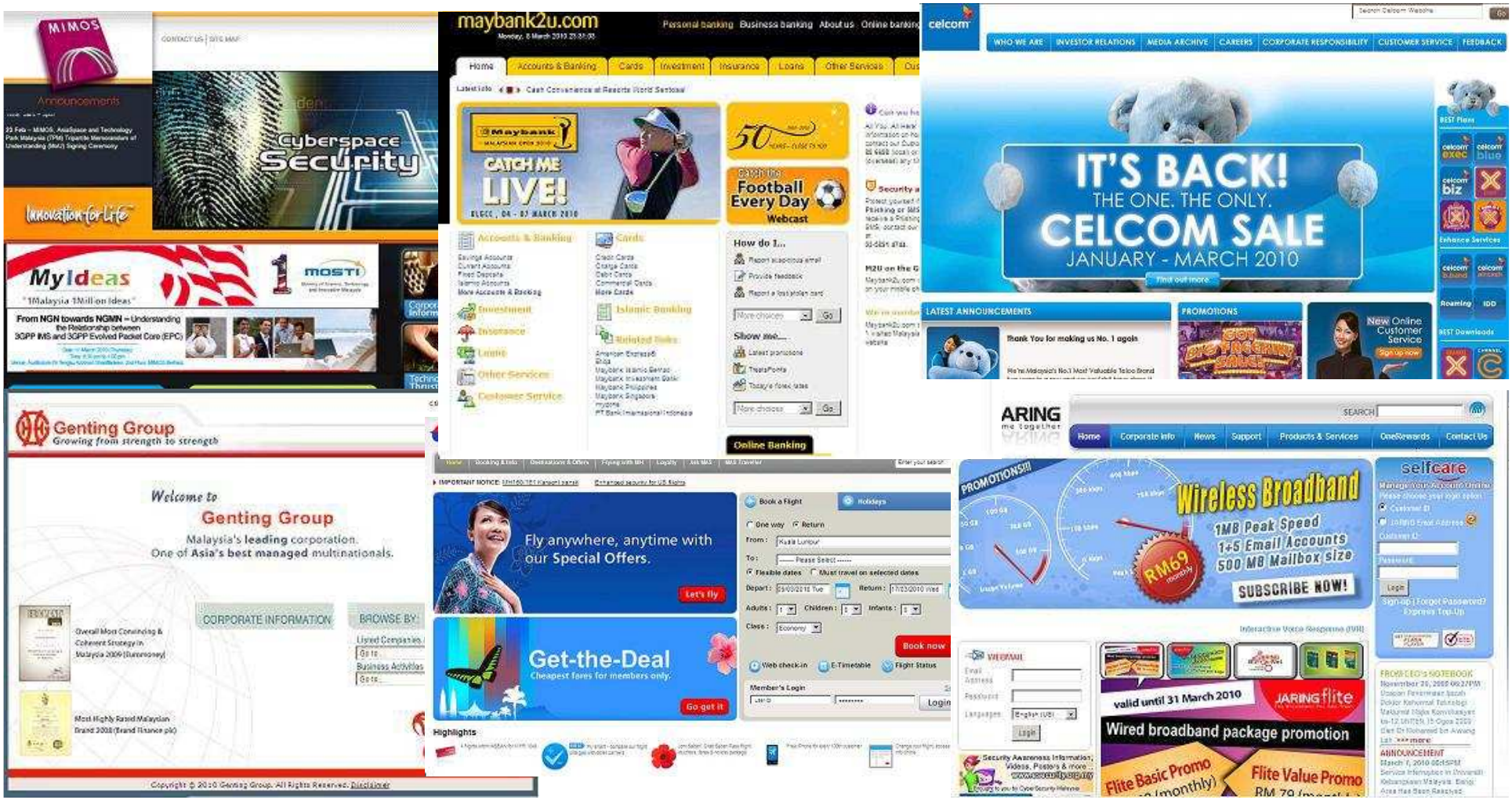
**• SOA**

**• CLOUD**

**New Possibilities..**

# Smarter Planet - Changing Security Landscape of Today

## "Webification" has changed everything



# Smarter Planet - 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


## Many Web Security Drivers

- Increase in vulnerabilities / disclosures
  - Application security has become the top threat
- Regulatory Compliance
  - Requirements such as PCI, HIPAA, GLBA, etc
- User demand
  - For rich applications is pushing development to advanced code techniques – Web 2.0 introducing more risks to threats
- Enterprise Modernization
  - Driving traditional applications to online world (SOA), increasing corporate risk
- Cost cutting in current economic climate
  - Demands increased efficiencies

# The Security Journey Continues

- **New and More …**
  - **Applications**
  - **Services**
  - **Systems**

    **-> Vulnerabilities**

    **-> Hacking methods**

    **-> Viruses, Worms, RATS, Bots …**

    **(Remote Access TROJANS = Spyware)**

    **MALWARE, “BLENDED” THREATS**

    **-> 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

# 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**

# 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

# SOMETHING IS STILL OUT THERE ...

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.**

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.


Monster is a leading online jobs service

c|net NEWS.com

http://news.cnet.com/8

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 a been rigged by hackers to serve up malicious software that attempts to exploit a critical V experts said Friday.

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

"We've just confirmed multiple reports about Asus.com, a very well known hardware mar compromised," a researcher with Kaspersky Lab wrote on the company's Viruslist.com s

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

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 ing 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

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

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

STRAITS TIMES SINGAPORE
13 SEP 09

# Hackers steal gamers' currency

MapleStory players blame company for lax security

By Tan Weizhen

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

home. STRAITS TIMES, SINGAPORE FRI FEB 27 09



# 'Errors' on Facebook a cyber trap

Viral application enables perpetrator to access personal data

By Serene Leo

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.

serl@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

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*

# Are you on Facebook? Beware of hackers

Cyber crooks targeting social networking sites

Internet enthusiasts surfing the web during the annual Campus Party in Valencia. The event, now into its 13th year, is one of the world's biggest gatherings of web fans. Experts there also spoke on the dangers of data posted on websites - names, dates of birth, addresses, job details, e-mail addresses and phone numbers - being

# WORST CREDIT CARD IDENTITY THEFT CASE
# - DONE BY SQL INJECTION : A WEB APP ATTACK!

**STRAITS TIMES SINGAPORE 19AUG09**

prime news

THE STRAITS TIMES WEDNESDAY, AUGUST 19 2009 PAGE A6

## Hacker accused of stealing 130 million credit card numbers

WASHINGTON: A former government informant known online as "soupnazi" stole information from 130 million credit and debit card accounts in what federal prosecutors are calling the largest case of identity theft yet.

Albert Gonzalez, 28, and two other men have been charged with allegedly stealing more than 130 million credit and debit card numbers in the largest hacking and identity theft case in the United States.

Gonzalez is already in jail in connection with hacking into 40 million other accounts, which at that time was believed to be the biggest case of its kind. Two unnamed Russians were also indicted in the latest charges.

Gonzalez, who lives in Florida and was indicted on Monday in New Jersey, is a one-time informant for the US Secret Service who had once helped to hunt hackers, said the authorities.

The agency later found out that he also had been working with criminals and fed them information on investigations, even warning off at least one individual, according to the authorities.

Gonzalez and the Russians, identified as "Hacker 1" and "Hacker 2", targeted large corporations by scanning the list of Fortune 500 companies and exploring corporate websites before setting out to identify vulnerabilities. The goal was to sell the stolen data to others.

The ring targeted customers of the giant 7-Eleven convenience store and the regional Hannaford Brothers supermarket chain. He also took aim at the Heartland Payment Systems, a New Jersey-based card payment processor.

The Justice Department said the new case represents the largest alleged credit and debit card data breach ever prosecuted in the US.

Gonzalez faces up to 30 years in prison if convicted on the new charges. The scheme began in October 2006 and ended last year when he was nabbed in the earlier hacking case.

Gonzalez allegedly devised a sophisticated attack to penetrate the computer networks and steal the card data.

He then sent that data to computer servers in California, Illinois, Latvia, the Netherlands and Ukraine.

"The scope is massive," Assistant US Attorney Erez Liebermann said yesterday in an interview.

Last year, the Justice Department charged Gonzalez and others with hacking into retail companies' computers with the theft of approximately 40 million credit cards.

At the time, that was believed to have been the biggest single case of hacking private computer networks to steal credit card data, puncturing the electronic defences of retailers including T.J. Maxx, Barnes & Noble, Sports Authority and OfficeMax.

Prosecutors said Gonzalez was the ringleader of the hackers in that case and caused more than US$400 million (S$580 million) in damage.

At the time of those charges, officials said the alleged thieves were not computer geniuses, just opportunists who used a technique called "wardriving".

This involved cruising through different areas with a laptop computer and looking for accessible wireless Internet signals.

Gonzalez faces a possible life sentence if convicted in the earlier case.

Restaurants are among the most common targets for hackers, experts said, because they often fail to update their antivirus software and other computer security systems.

Mr Scott Christie, a former federal prosecutor now in private practice, said the case shows that despite the best efforts by companies to protect data privacy, there remain individuals capable of sneaking in.

"Cases like this do cause companies to sit up and take notice that this is a problem and more needs to be done," he said.

ASSOCIATED PRESS, REUTERS

### *Poking holes in computer security*

ALBERT Gonzalez and his conspirators reviewed lists of Fortune 500 companies to decide which corporations to take aim at.

Then the men visited their stores to monitor which payment systems they used and their vulnerabilities, prosecutors said.

The online attacks took advantage of flaws in the SQL programming language, which is commonly used for databases.

Prosecutors said the defendants used malicious software known as malware and so-called injection strings to attack the computers and steal data.

They created and placed "sniffer" programs on corporate networks; the programs intercepted credit card transactions in real time as they moved through the computer networks.

These programs transmitted the numbers to computers that the defendants had leased in the United States, the Netherlands and Ukraine.

The hackers used instant messaging services to advise each other on how to navigate the systems, according to the indictment.

The conspirators attempted to erase all digital footprints left by their attacks.

They programmed malware to evade detection by antivirus software and erase files that might detect its presence, prosecutors said.

THE NEW YORK TIMES, BLOOMBERG

# Hackers cash in on Chinese gaming craze

**BEIJING**

THE craze in online games among Chinese netizens is fuelling an increasingly lucrative real-world market for computer **hackers**, security firms have said.

"There is a huge underground market and major revenue comes from selling game accounts or virtual items stolen

om hijacked c
r Zhang Yumu
Beijing Rising
ftware, one of
urity firms.

A report by state broadcaster CCTV said **Trojan-horse** attacks, which allow hackers remote access to a targeted computer system, make up a market expected to be worth 10 billion yuan (S$2 billion) this year.

The report cited a hacker saying he could get hundreds of thousands of yuan every month by hacking into computers and

as weapons and clothes, for sale through online sites.

The **hijacked** computer's accounts are sold for other uses, such as joining online attacks and piling up false traffic data.

Trojan-horse attacks have became a major online threat in China in recent years, accounting for over 95 per cent of all online attacks.

jan-horse attackers came from selling online game accounts and virtual items.

The number of Trojan-horse attacks in China surged 10 times last year and should be up 60 per cent this year.

Sales revenues in China's online game market grew 76 per cent last year to 18.3 billion yuan, going by official figures.

security firms, said joint efforts by online gaming and security firms have slowed the growth of Trojan-horse attacks.

CHINA DAILY/ANN

## HELPDESK 我的字典

**Hackers:** 骇客 hài kè

**Trojan-horse:** 特洛伊木马程序的

éng shī

prime.news

THE STRAITS TIMES

THE STRAITS TIMES TUESDAY, JANUARY 5 2010 PAGE A3

# WARNING: .sg websites get red-flagged

## Global security study by software firm ranks them 10th riskiest

BY TAN WEIZHEN

SINGAPORE websites are becoming increasingly risky to visit because they expose their users to virus attacks and malicious software.

A global study on the security of 104 web domains by online security software firm McAfee ranked Singapore sites as 10th worst in the world last year.

It is a significant leap up a roll of dishonour: Singapore sites were collectively ranked 67th most risky in 2008, and 63rd the year before.

The 10th-place ranking puts Singapore sites among those of Cameroon and China, with those registered in Japan and Australia being among the world's safest.

McAfee's red-flagging of Singapore as having the biggest jump in the number of risky sites in the past year could tarnish the island's image as a business hub and a nation at home with e-transactions.

Online security specialist Aloysius Cheang, president of the Special Interest Group in Security and Information Integrity, a local non-profit IT security society, said: "This could reduce trust and the probability of Singapore as a platform to build e-commerce."

Online security specialists put the trend down to a rise in computer and Internet penetration here, which entices cyber-criminals to buy up domain names ending with ".sg", all the better with which to scam Singapore netizens.

McAfee researchers who trawled through 17,630 Singapore websites found 9 per cent, or 1,607, to be "risky".

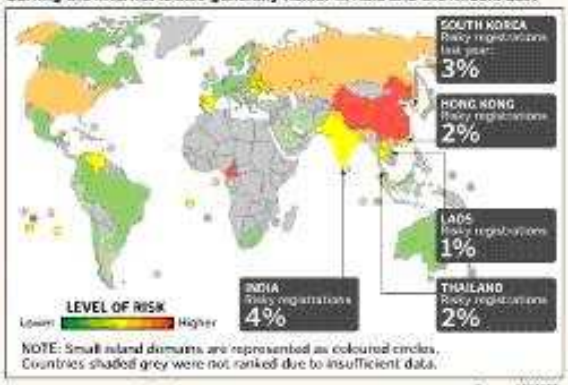
In 2008, just 0.3 per cent of these sites were malicious – that is, they could spread viruses or malware or secretly

**RISKY BUSINESS**

**More websites registered here in 2009 were spam sites or had viruses and malware, a huge jump from the previous year.**

| Rank 2009 | Country or generic domain | % of websites registered that are risky 2008 | 2009 |
|---|---|---|---|
| 1 | Cameroon | - | 70 |
| 2 | Commercial (.com) | 5.3 | 6 |
| 3 | China | 12 | 35 |
| 4 | Samoa | 4 | 35 |
| 5 | Information (.info) | 11.7 | 22.8 |
| 6 | Philippines | 8 | 26 |
| 7 | Network (.net) | 6.3 | 5.9 |
| 8 | Former Soviet Union | - | 10.3 |
| 9 | Russia | 6 | 7.6 |
| 10 | Singapore | 0.3 | 9 |

**Surfing the Internet is also generally riskier in Asia and the Middle East**




NOTE: Small inland domains are represented as coloured circles. Countries shaded grey were not ranked due to insufficient data.

Source: MCAFEE

track the keystrokes made by those who visited them, in order to mine passwords used for online transactions.

Statistics from the Singapore Network Information Centre (SGNIC), the national registry of .sg domain names, indicate that the number of domains registered here jumped from 87,650 to 111,357 between December 2007 and last month.

These sites range from music and video downloading sites to online shopping ones.

Mr Ong Geok Meng, McAfee Labs' manager of anti-malware research for Asia-Pacific and Japan, noted that a good proportion of domains rated risky were personal or commercial sites, and were either legitimate ones hacked into by scammers or set up by scammers specifically.

Mr Cheang said the high computer and Internet penetration rate here had created a large pool of potential victims for scammers. As of last October, each household here had 1.5 broadband lines, an increase on a year ago, when it was under one per household.

He noted that the situation here mirrored that of Hong Kong a few years ago. Public education drives for Internet users there have since fixed the problem: Only 2.1 per cent of Hong Kong sites were deemed risky last year, down from 10.2 per cent in 2008, said the McAfee study.

Mr Cheang pointed out that Singapore's networks being so plugged into the global network of undersea cables has a dark side: It means hackers can easily control the computers here from anywhere in the world.

Another factor lies in the ease of the registration process. Buying a Singapore domain takes only five minutes.

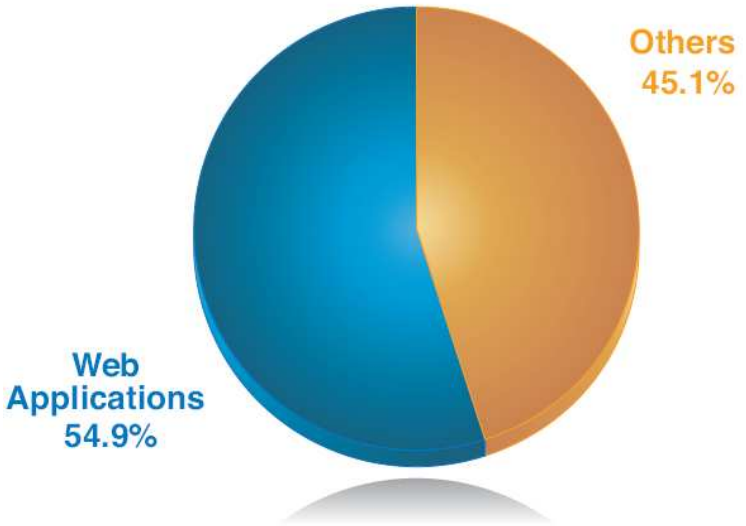
And a domain can be registered with



ration

# 2008 Web Threats Take Center Stage

- **Web application vulnerabilities**
  - Represent largest category in vuln disclosures (55% in 2008)
  - 74% of Web application vulnerabilities disclosed in 2008 have no patch to fix them



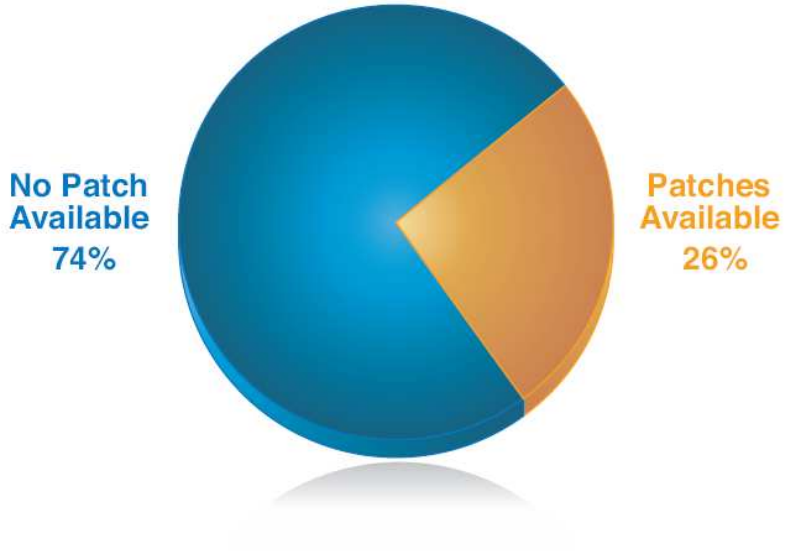
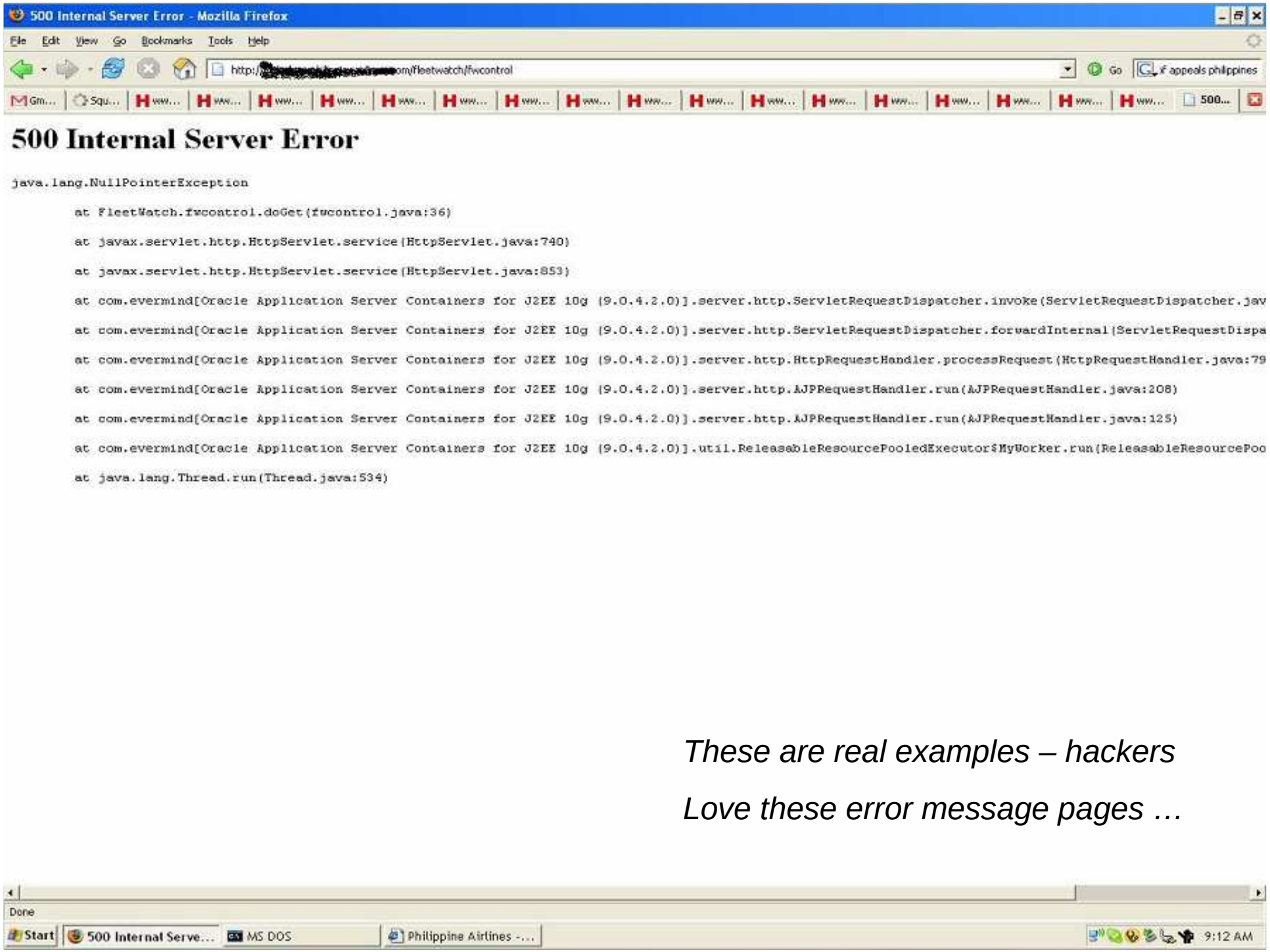
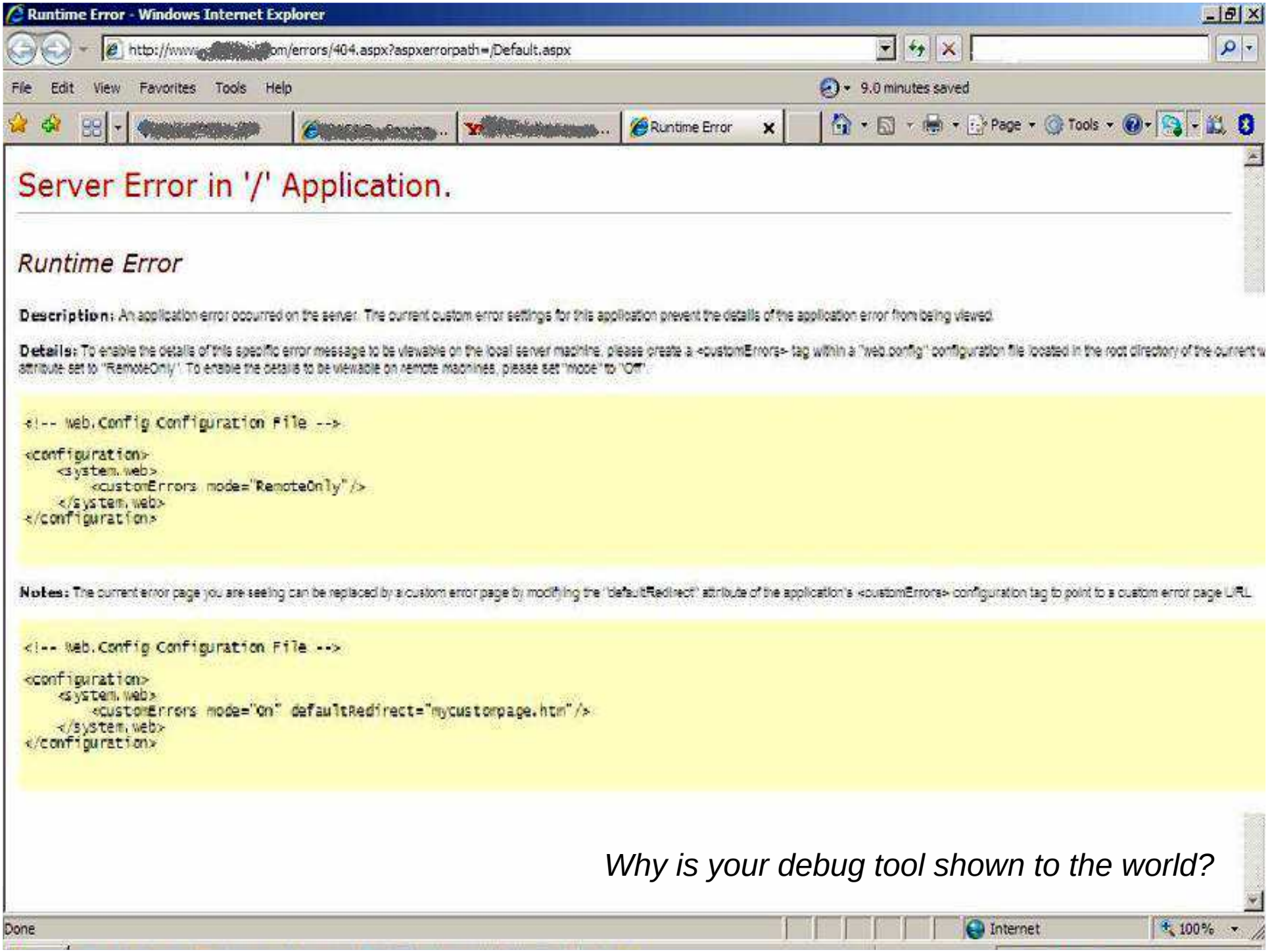



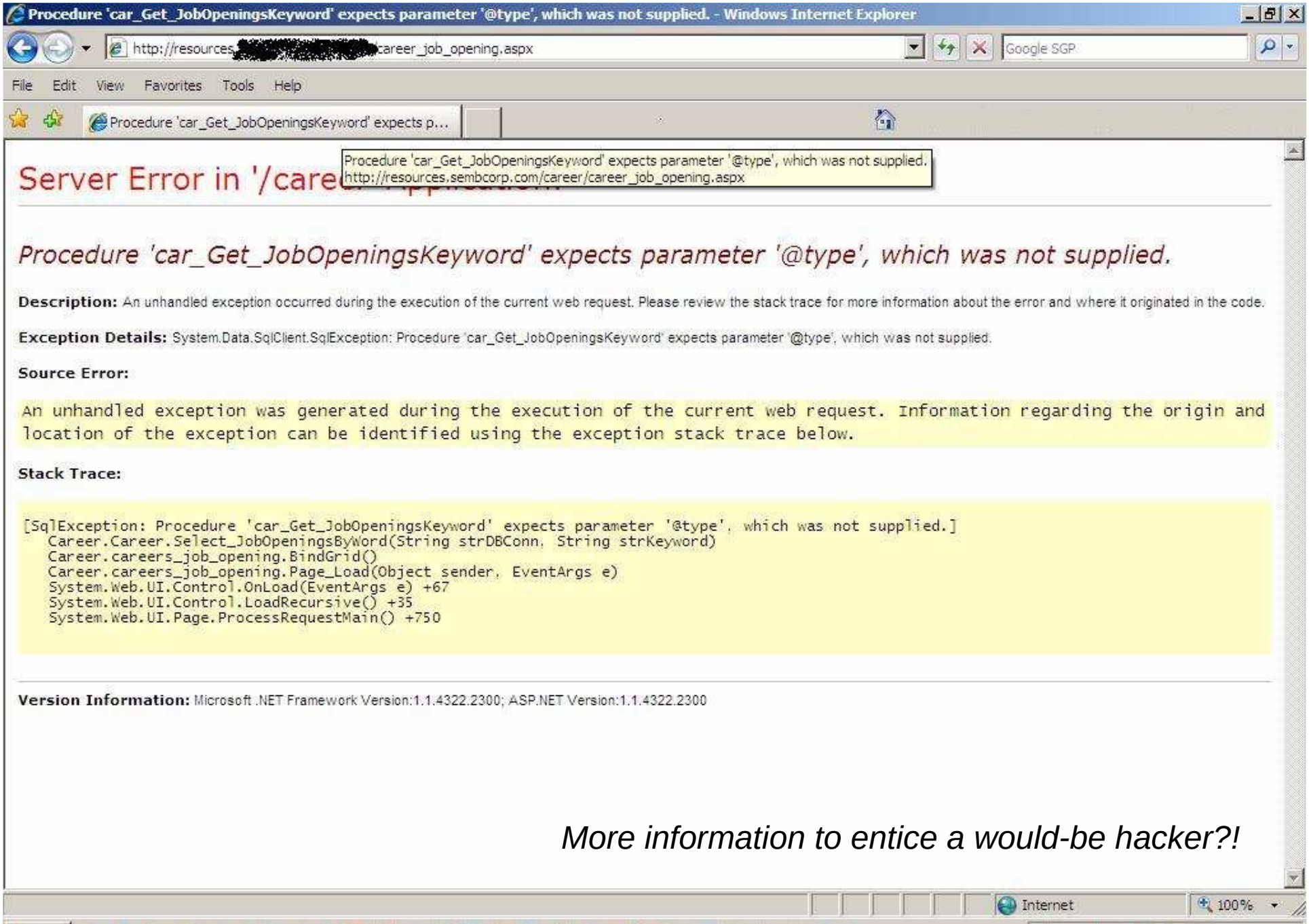

*Figure 22: Percent of 2008 Web Application Vulnerabilities with No Vendor-Supplied Patch Available at the End of 2008*



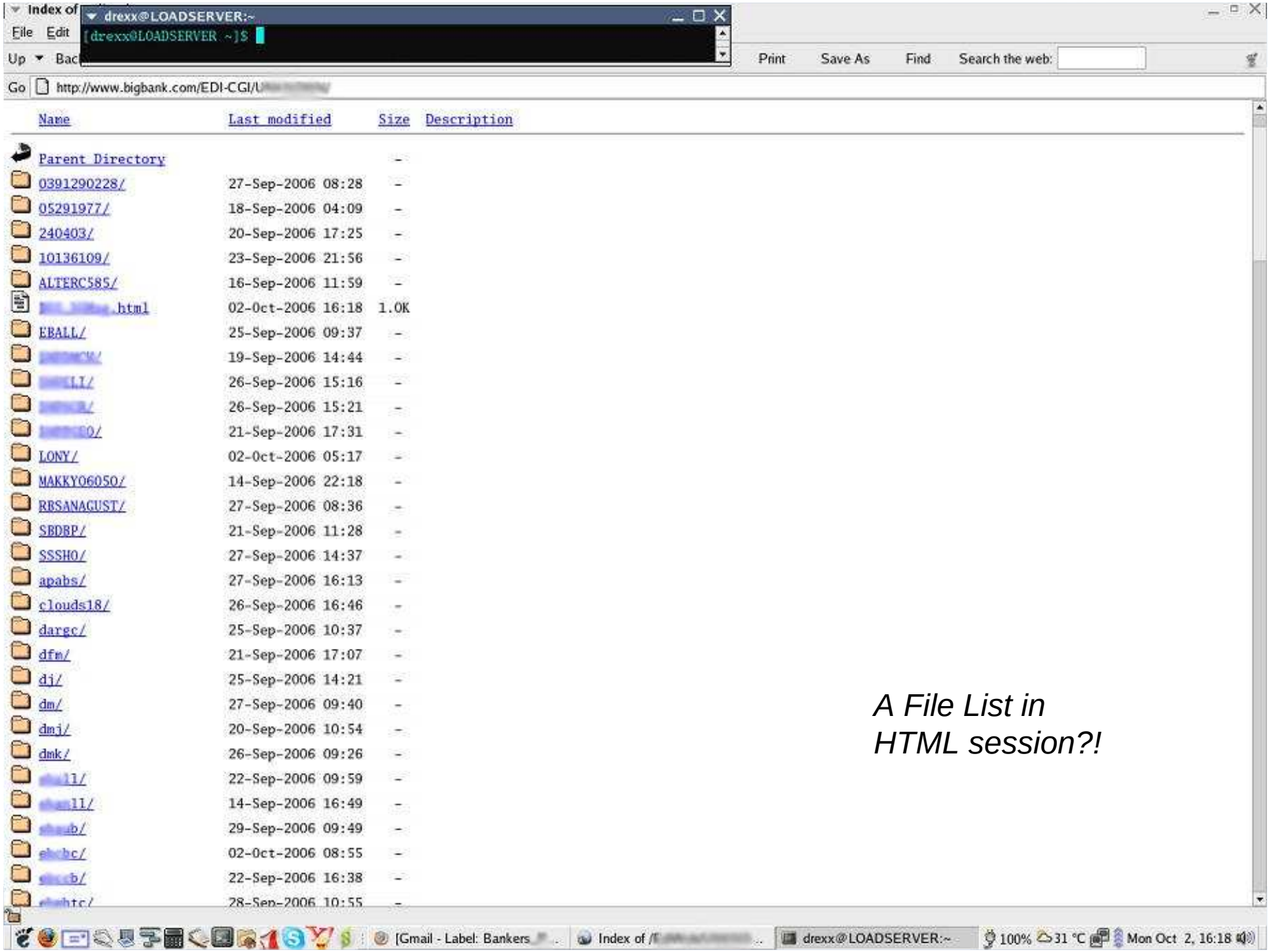

*These are real examples – hackers*

*Love these error message pages …*

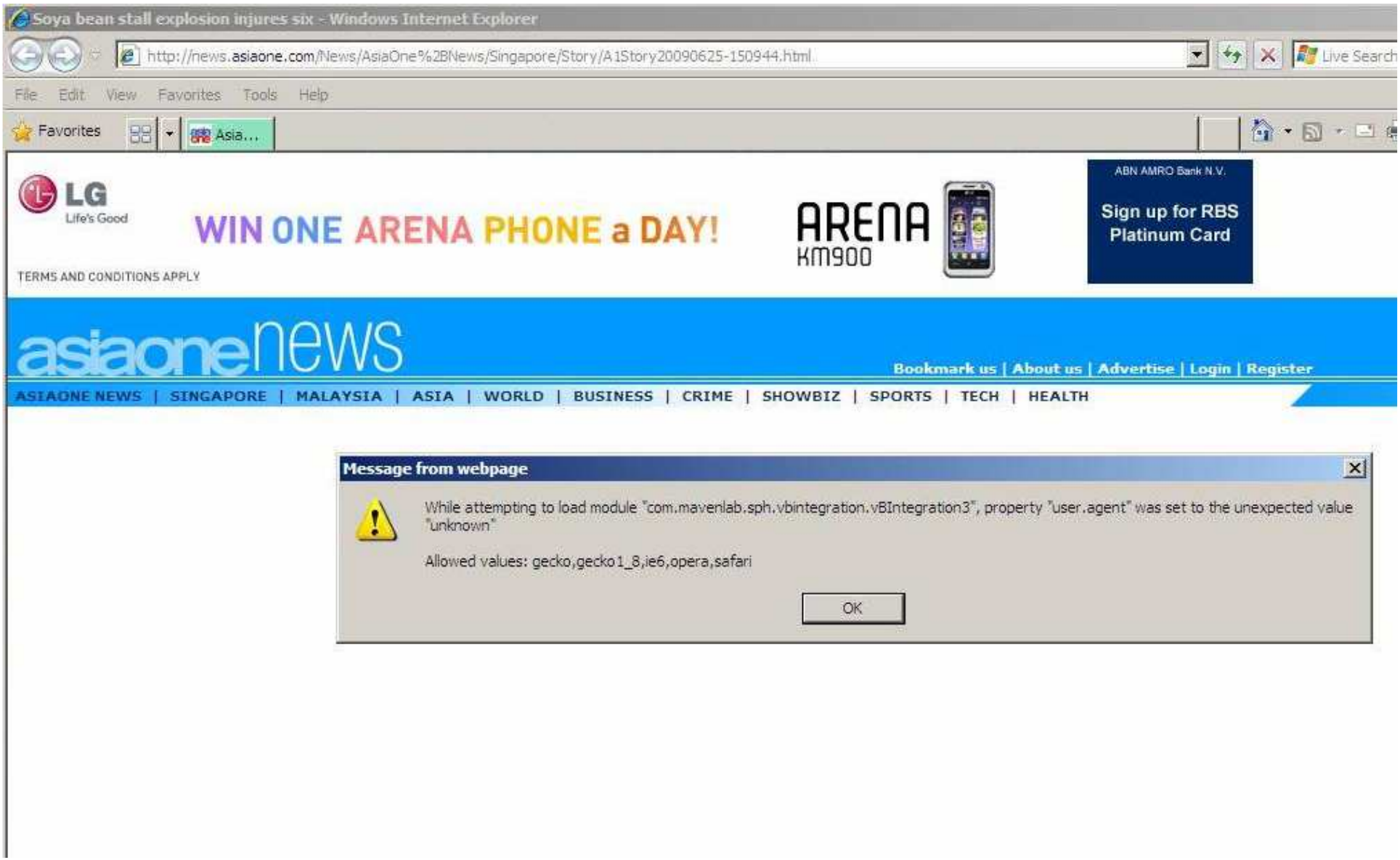

Runtime Error - Windows Internet Explorer
http://www.[redacted].com/errors/404.aspx?aspxerrorpath=/Default.aspx
File Edit View Favorites Tools Help
9.0 minutes saved
Runtime Error
Page Tools
Server Error in '/' Application.
Runtime Error
Description: An application error occurred on the server. The current 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 web application. This <customErrors> tag should then have its "mode" 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>
Why is your debug tool shown to the world?
Done
Internet
100%



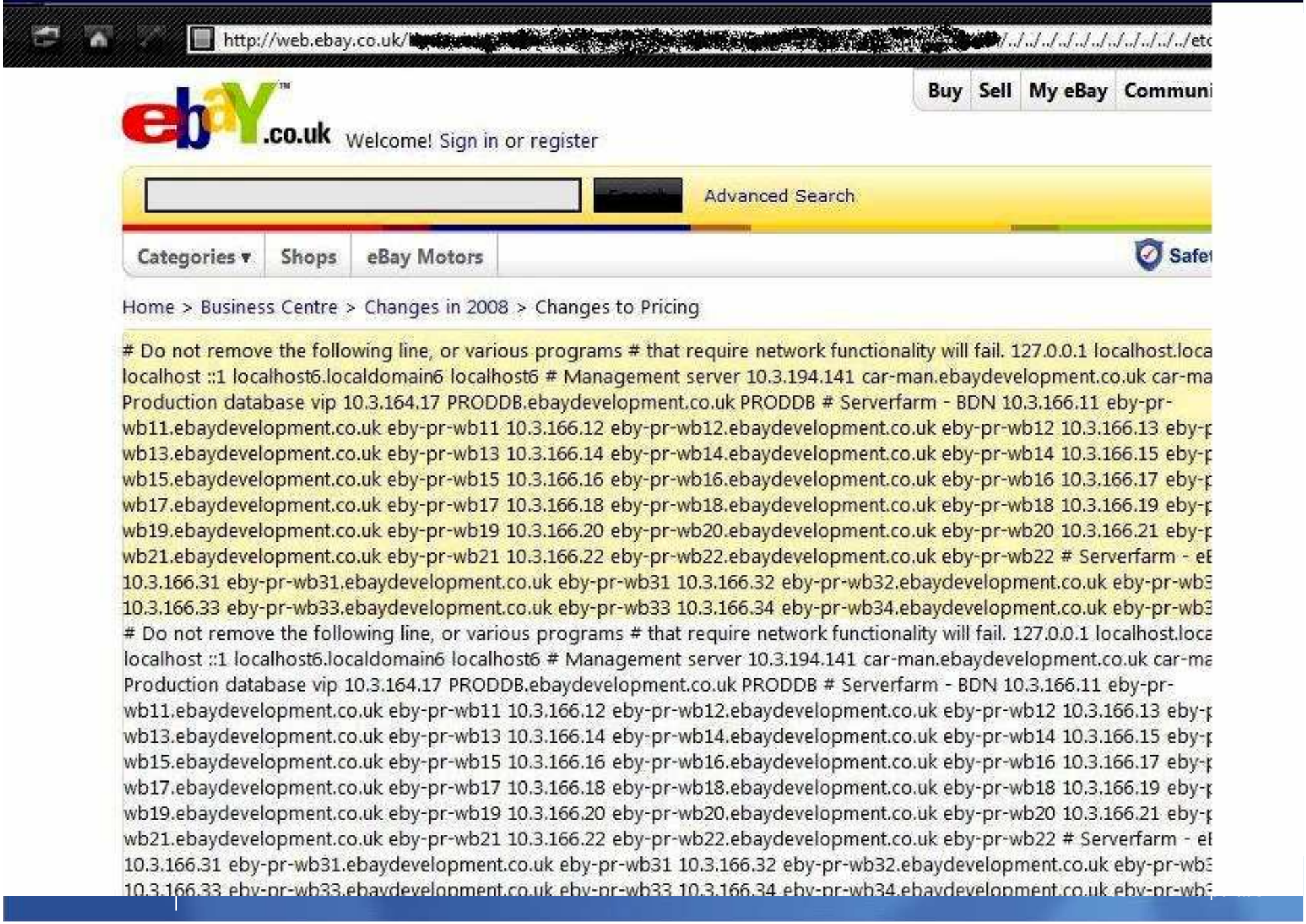

*More information to entice a would-be hacker?!*




*A File List in HTML session?!*

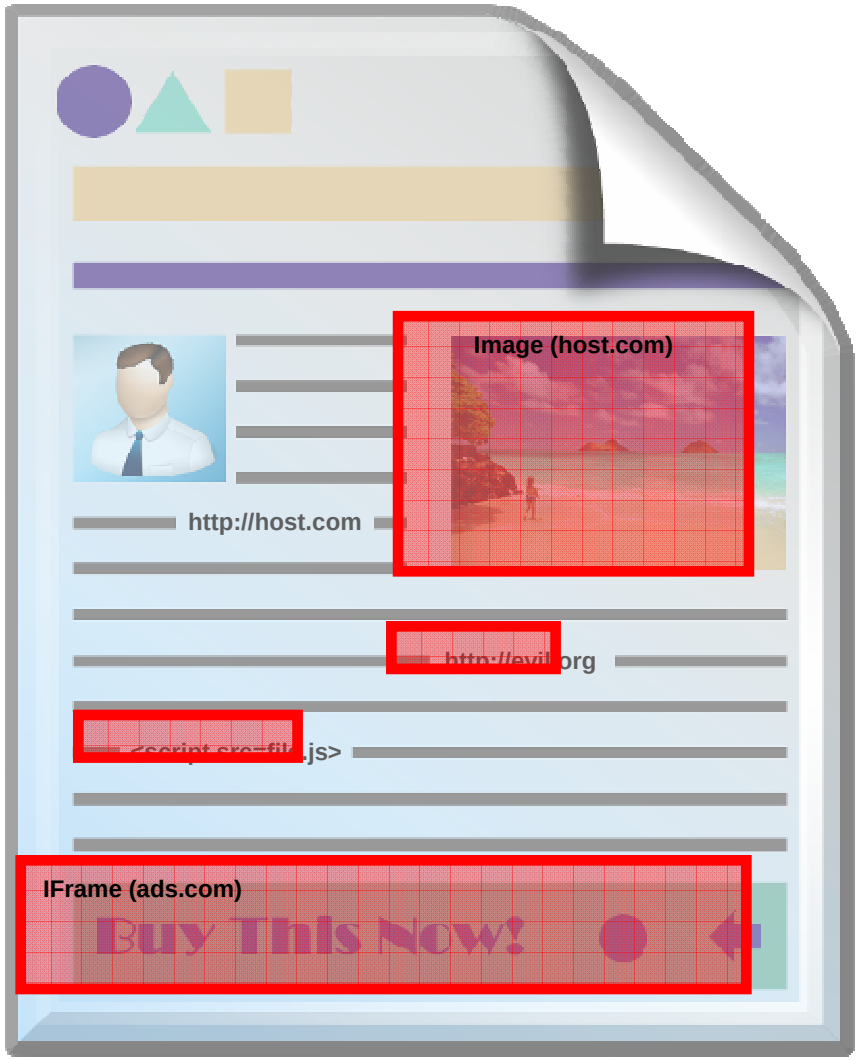


Attackers use directory traversal attacks to read arbitrary files on web servers, such as SSL private keys and password files.

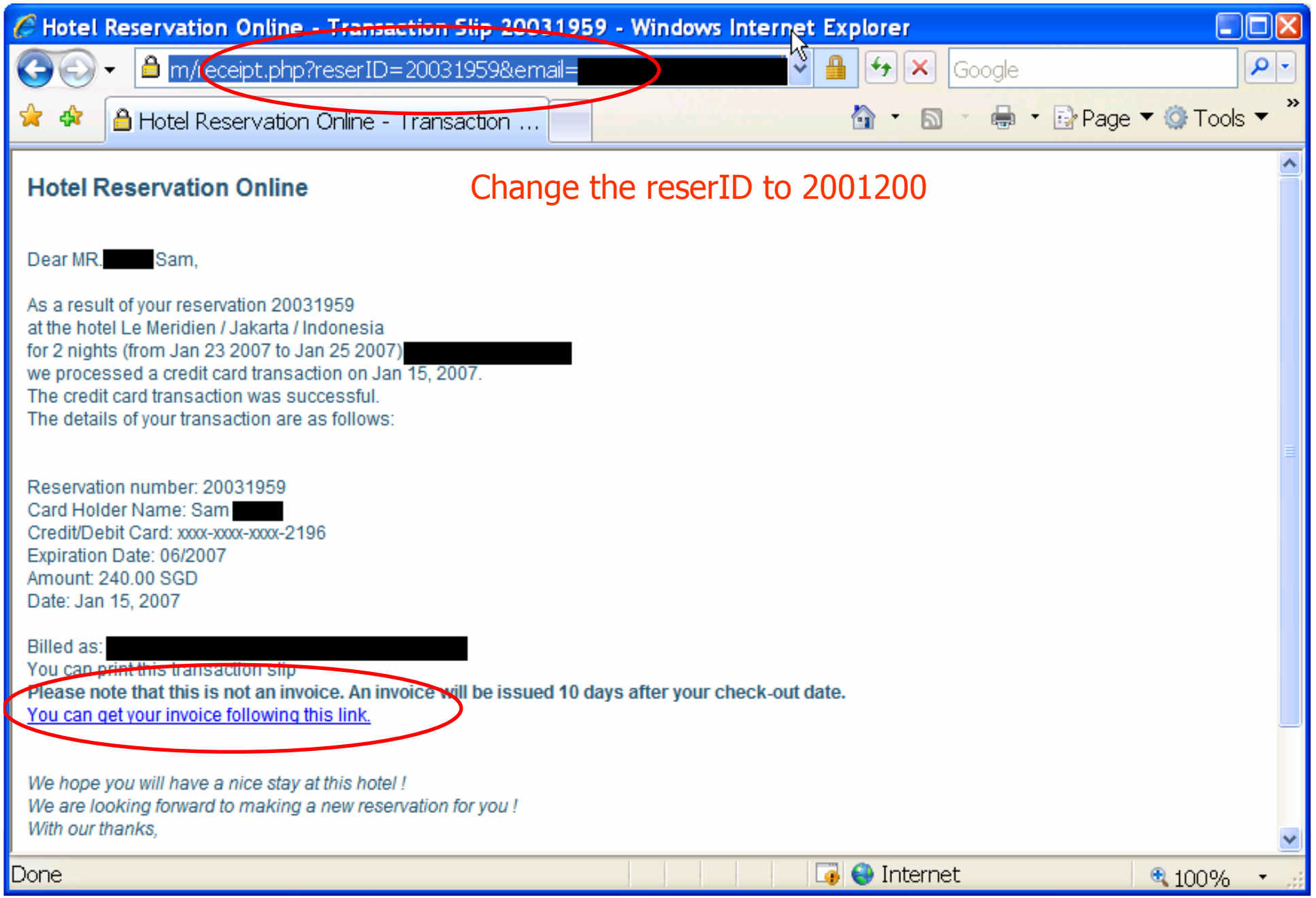


# Malware on Web Applications

- **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, …**

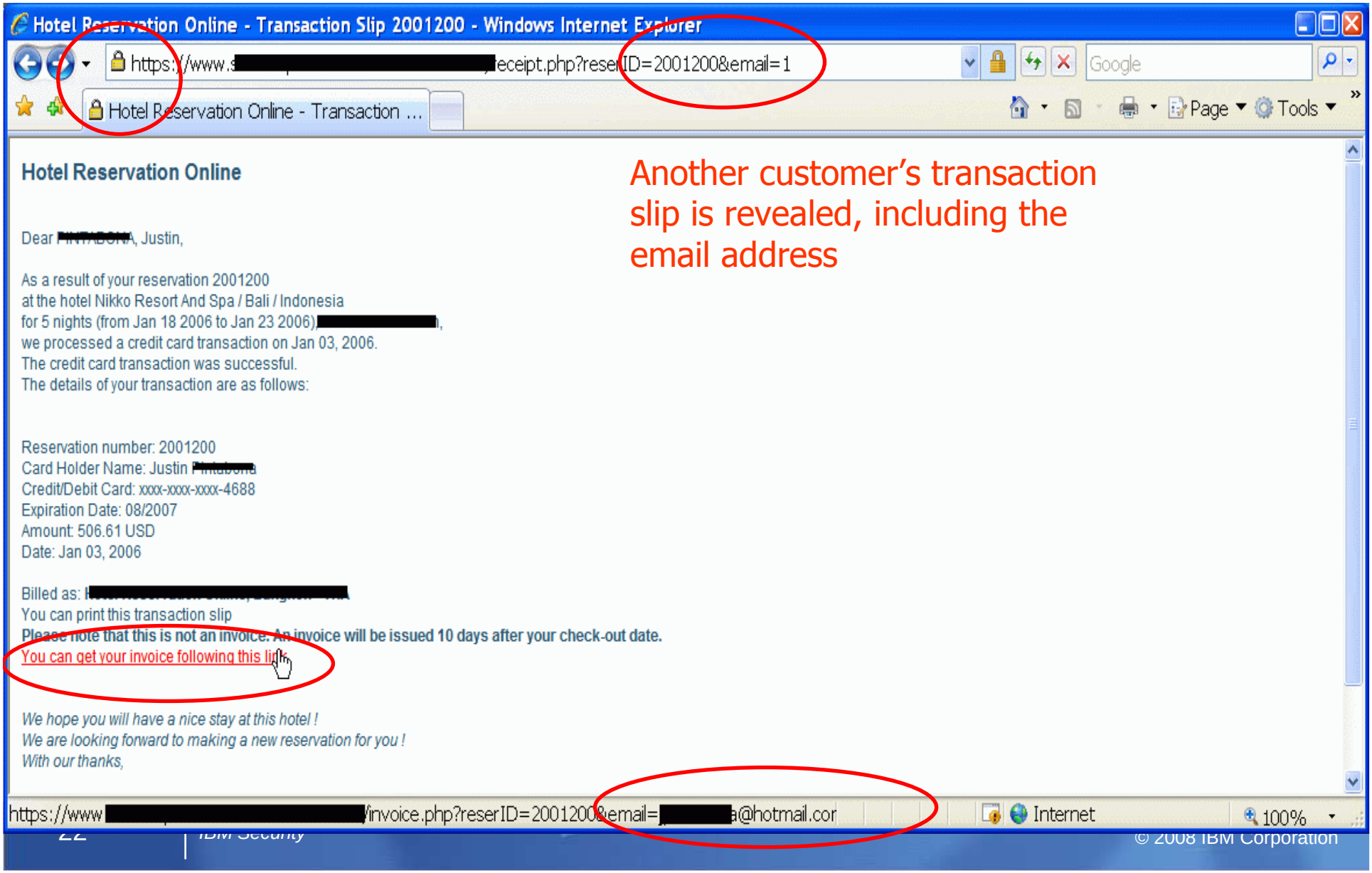


# Real Example: Online Travel Reservation Portal

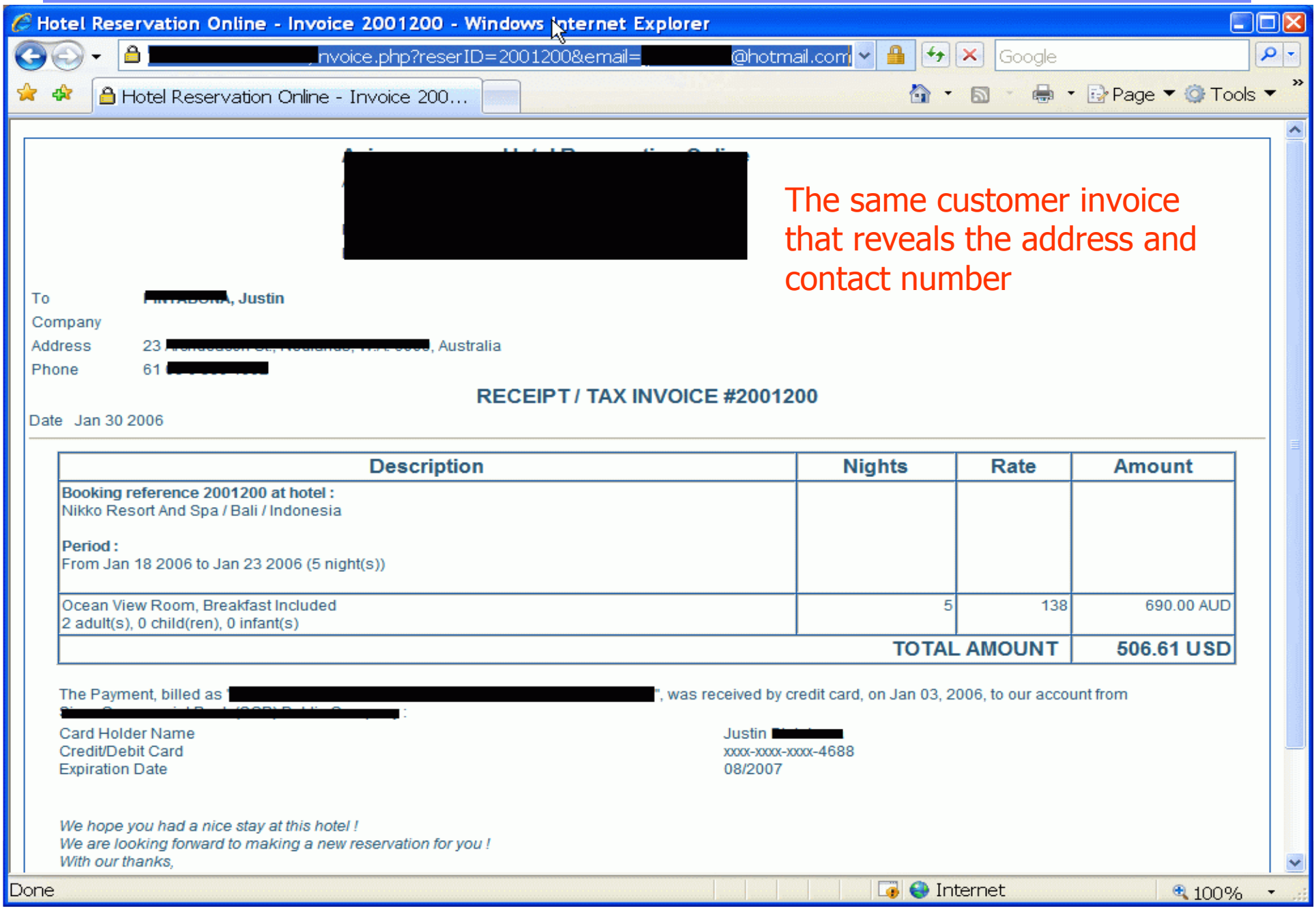


# Real Example : Parameter Tampering

## Reading another user's transaction – insufficient authorization

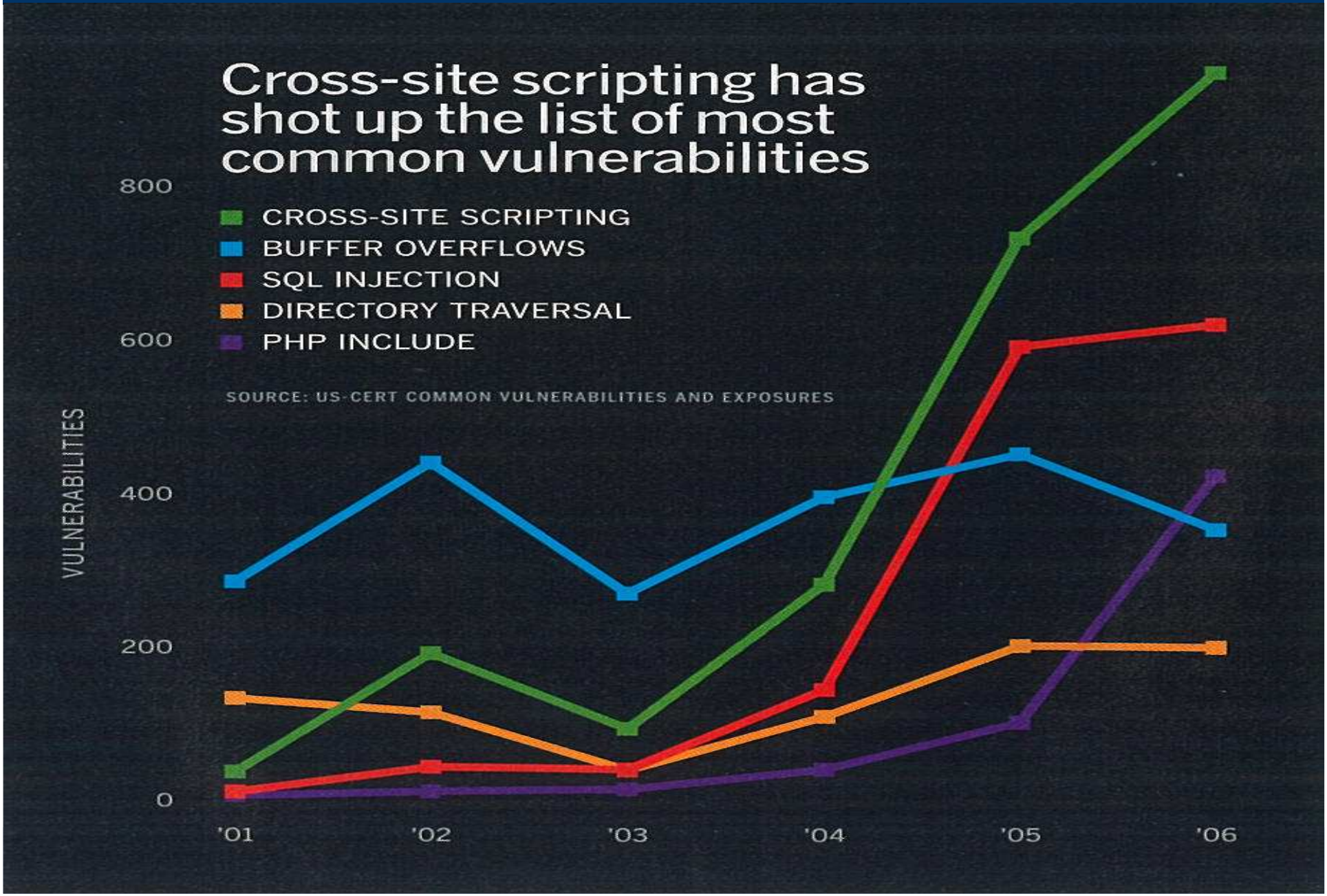


# Parameter Tampering Reading another user's invoice




The same customer invoice that reveals the address and contact number

# Top Hack Attacks Today Target Web Applications



# Top 10 OWASP Critical Web Application Security Issues '09

1 Unvalidated Input
2 Broken Access Control
3 Broken Authentication and Session Management
4 Cross Site Scripting Flaws
5 Buffer Overflows

6 Injection Flaws
7 Improper Error Handling
8 Insecure Storage
9 *Denial of Service*
10 Insecure Configuration Management

# 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 a nightmare to manually QA the application**
    - **Many companies today still do not have a software security QA policy or resource**

# Software Application Development Pressures

**Today I'm being asked to:**

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

***Cheap***
***Fast***
***Good***
***- Choose 2***

# 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

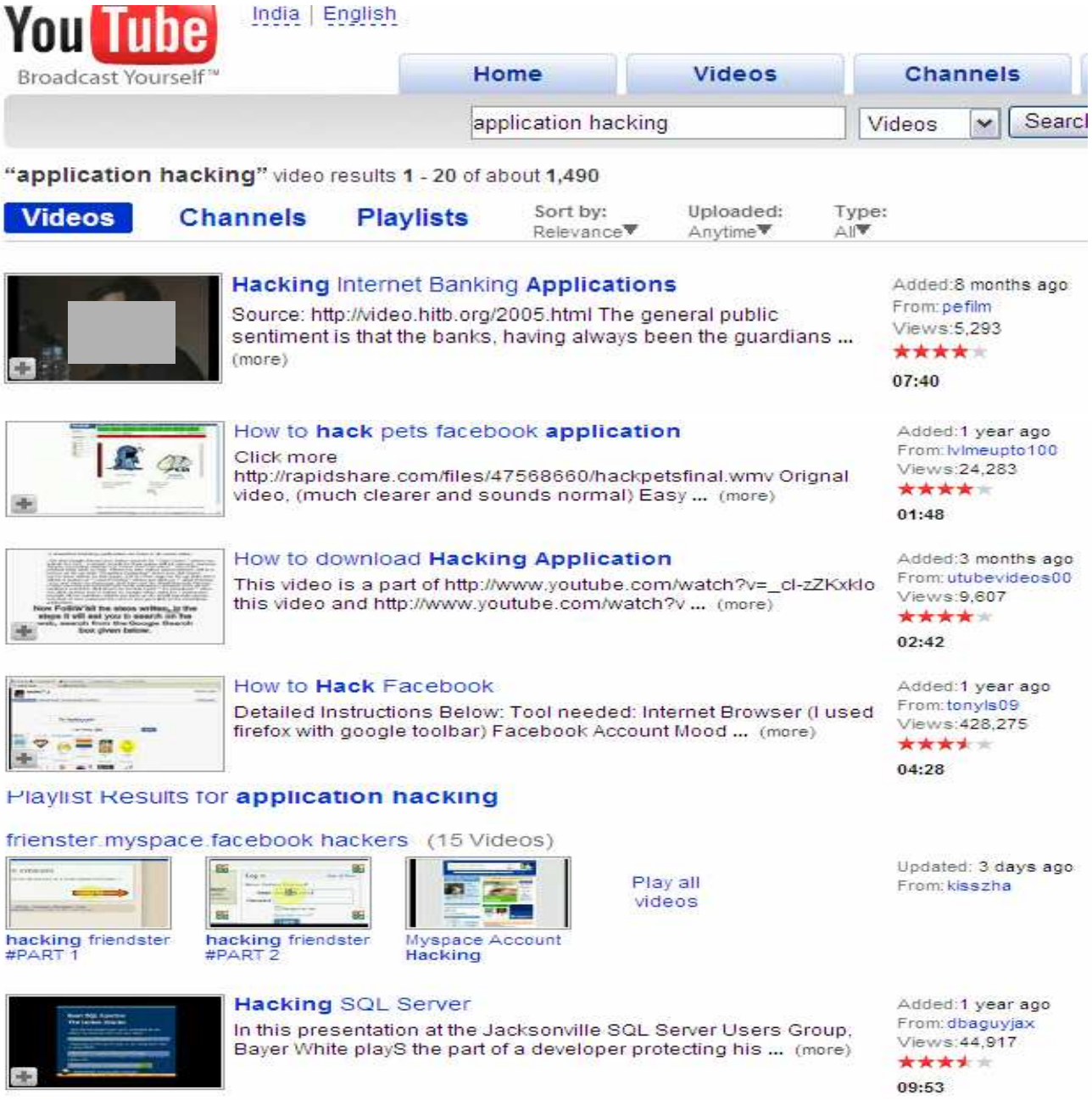
- **Most companies today still do not have an application security QA policy or resource**
  - IT security staff are focused on other things and are swarmed
    - App Sec is their job but they don't understand it and don't want to deal with it
    - Developers think its not their job or problem to have 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.

***Back then coding was done by engineers …***

***Then came Y2K …***

# DON'T TRY THIS AT HOME!



# The Application Security Challenge

## What?

1. **Need to** mitigate the risk **of a Security breach**
2. **Need to** find **and** remediate **these vulnerabilities**
3. **Must utilize a** cost effective **way of doing this that makes sense**

## Who?

- **Software security represents the** intersection between security & development **– solution needs to be a joint collaboration**
- **Starts with Security Auditor (can also be outsourced)**
- **Larger organizations require the scaling of security testing into the development organization**

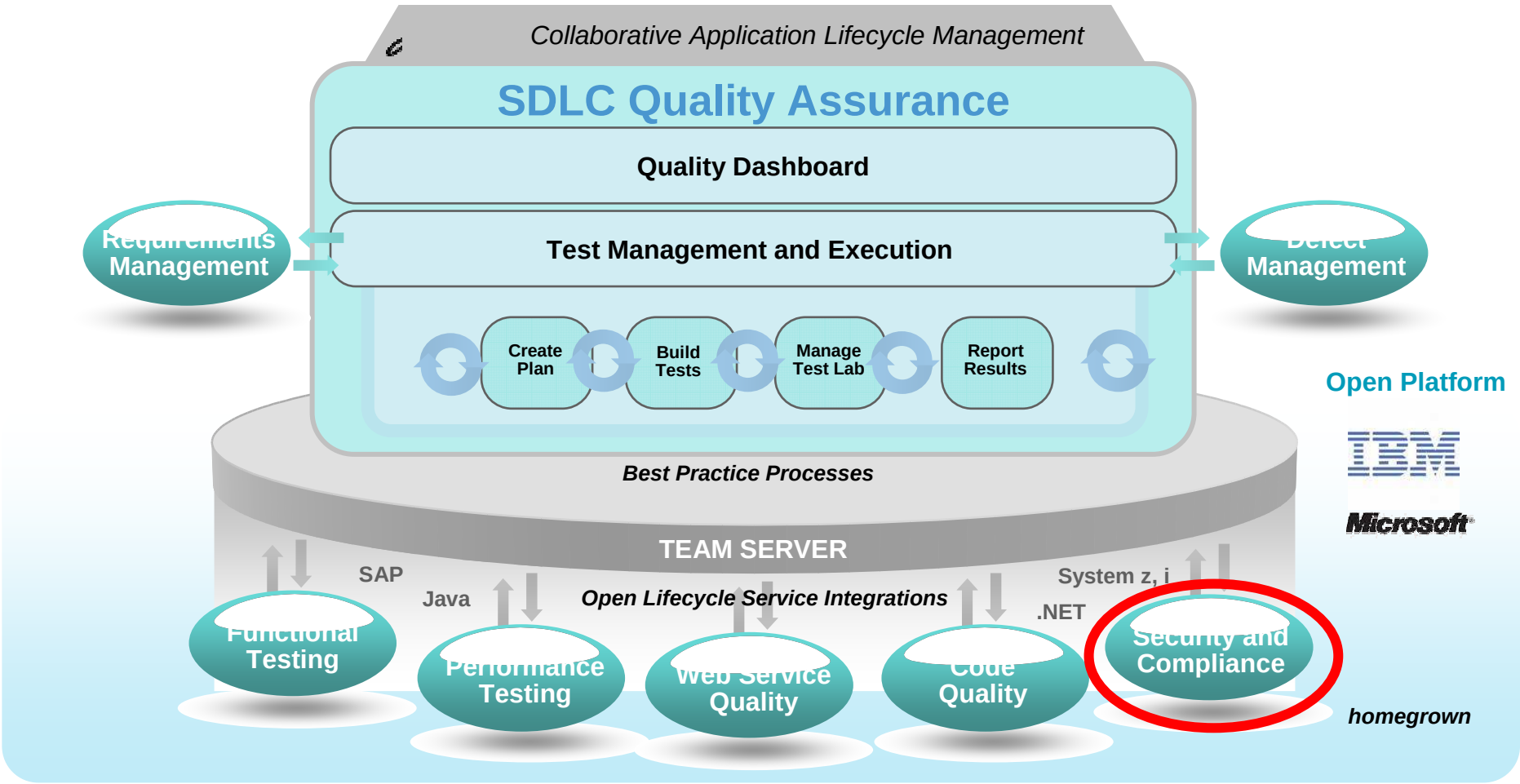
# Web Application Securirty - Solution Strategy

- **Reduce Cost and Time to Market**
  - Find the issues earlier in the Software Development Life Cycle
  - Automate the process
  - Use less security-savvy employees by leveraging tools
- **Mitigate Risk and increase quality**
  - Increase coverage
  - Involve more people in the process: Developers / QA
- **Increase Visibility Of The Security Issue**
  - Distribute reports to different levels
  - Dashboards
- **Increase Productivity**
  - Build the knowledge among the team
  - Prevent making the same mistakes

# Web Application Security Testing – Black & White Boxes

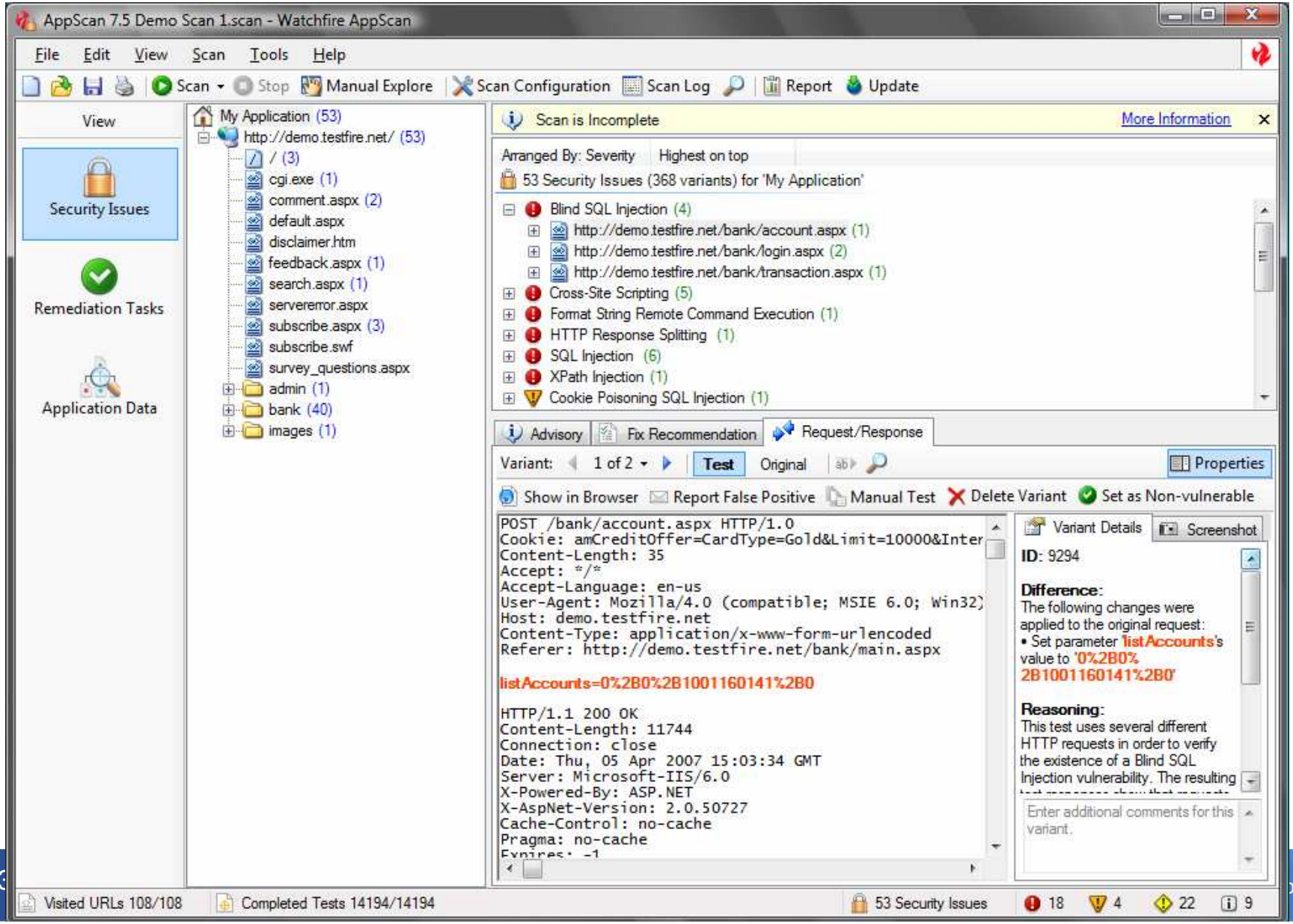
| BLACK BOX | WHITE BOX |
| --- | --- |
| - Application Scanning (tests for app behavior) | - Source Code Scanning (tests for code integrity) |
| - Dynamic Analysis | - Static Analysis |
| - Used by security folks & auditors, don't need source code | - Used by Development folks, who are not into security |
| - Tests for relationship between application and environment | |

# SECURITY TESTING IS PART OF SDLC QUALITY TESTING



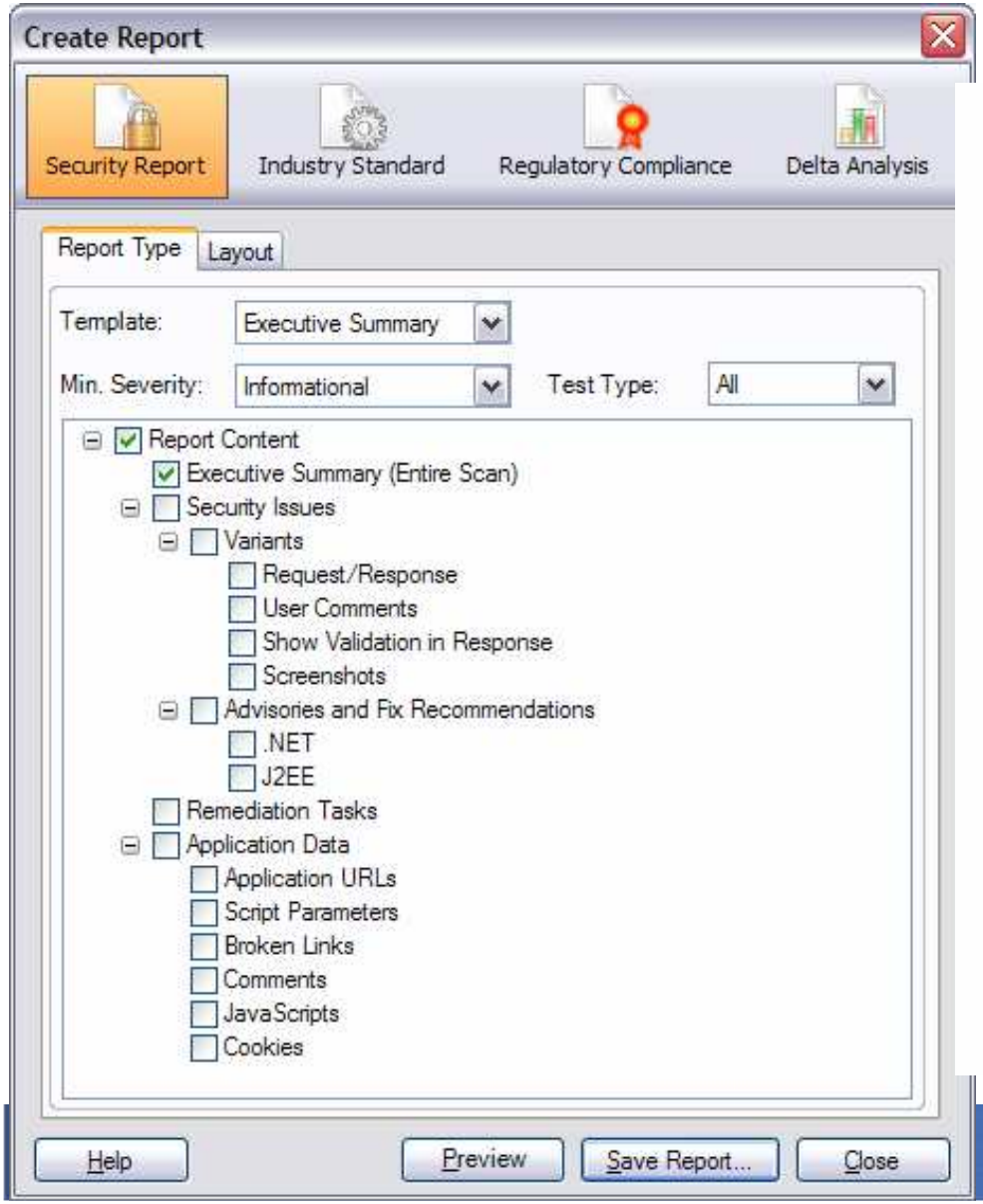
*You need a professional solution to*

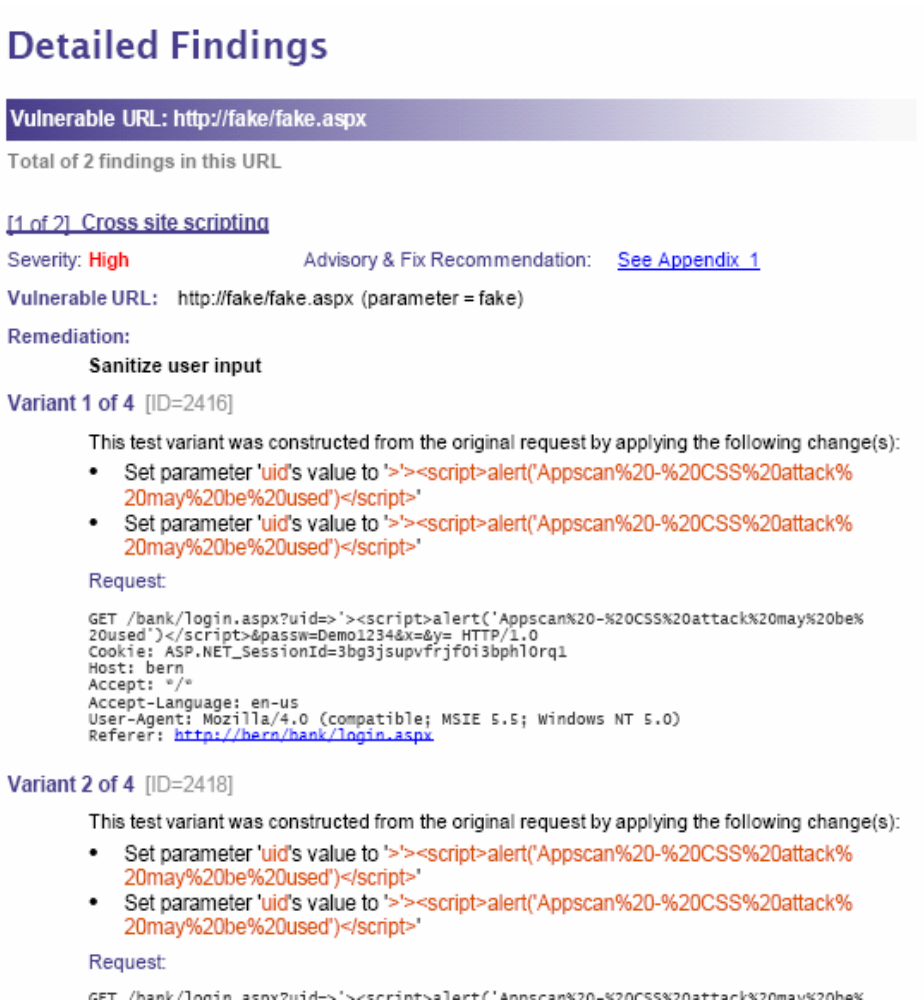
# Identify Vulnerabilities



# *With* Rich Report Options

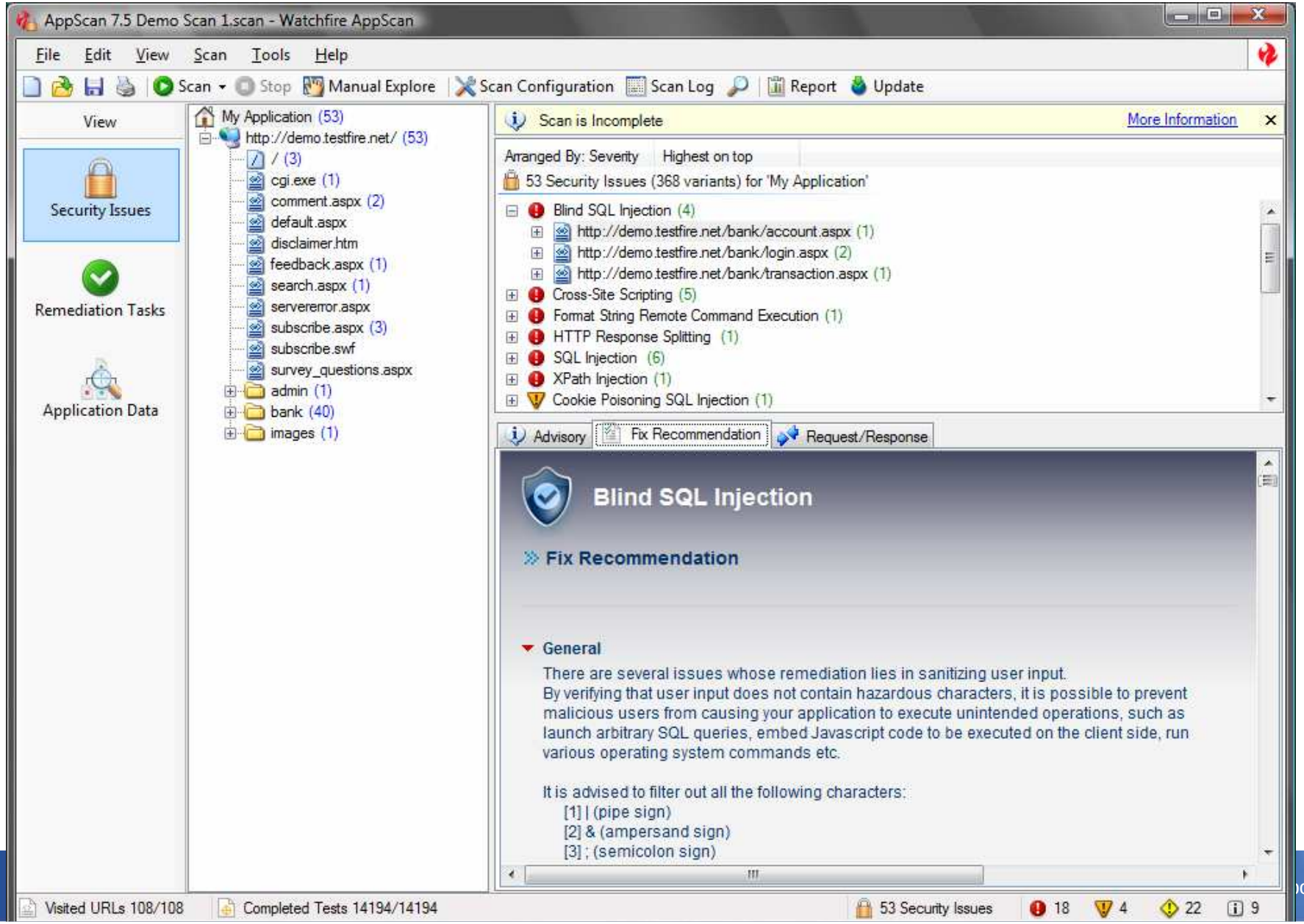
## *44 Regulatory Compliance Standards, for Executive, Security, Developers.*



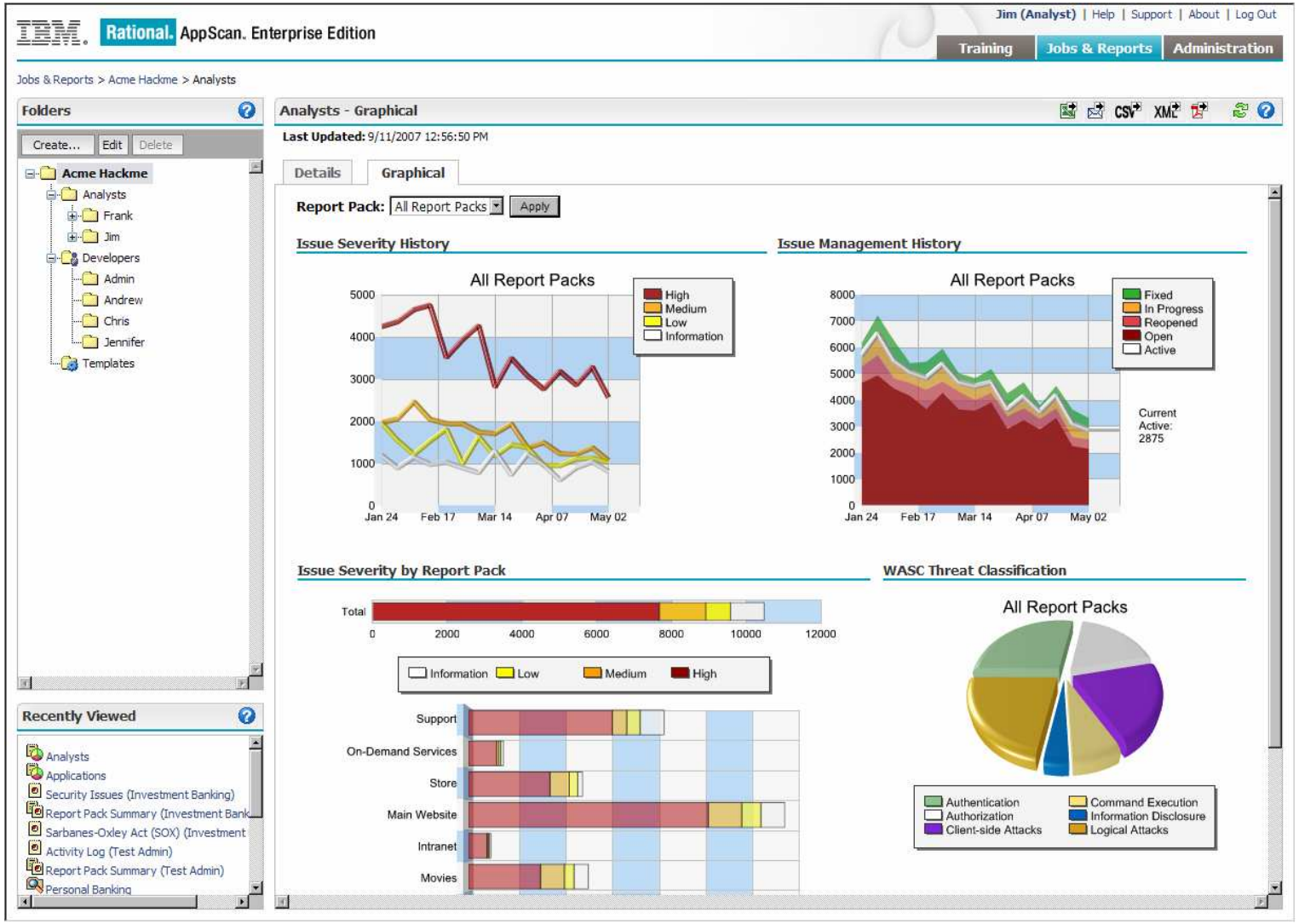



*And Most Important :*

# Actionable Fix Recommendations



# AppScan Enterprise – Dashboards and Metrics



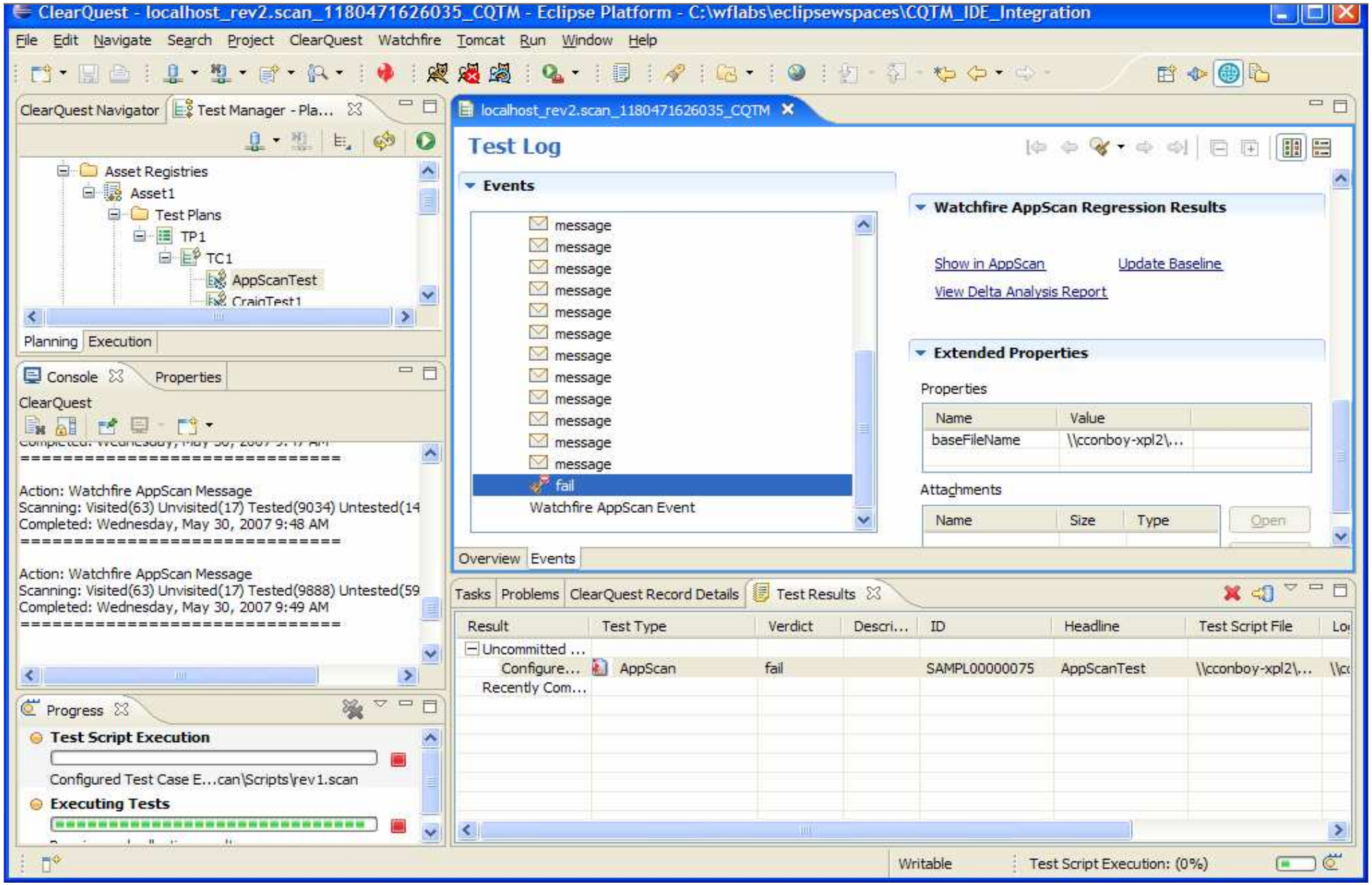

***Policies***

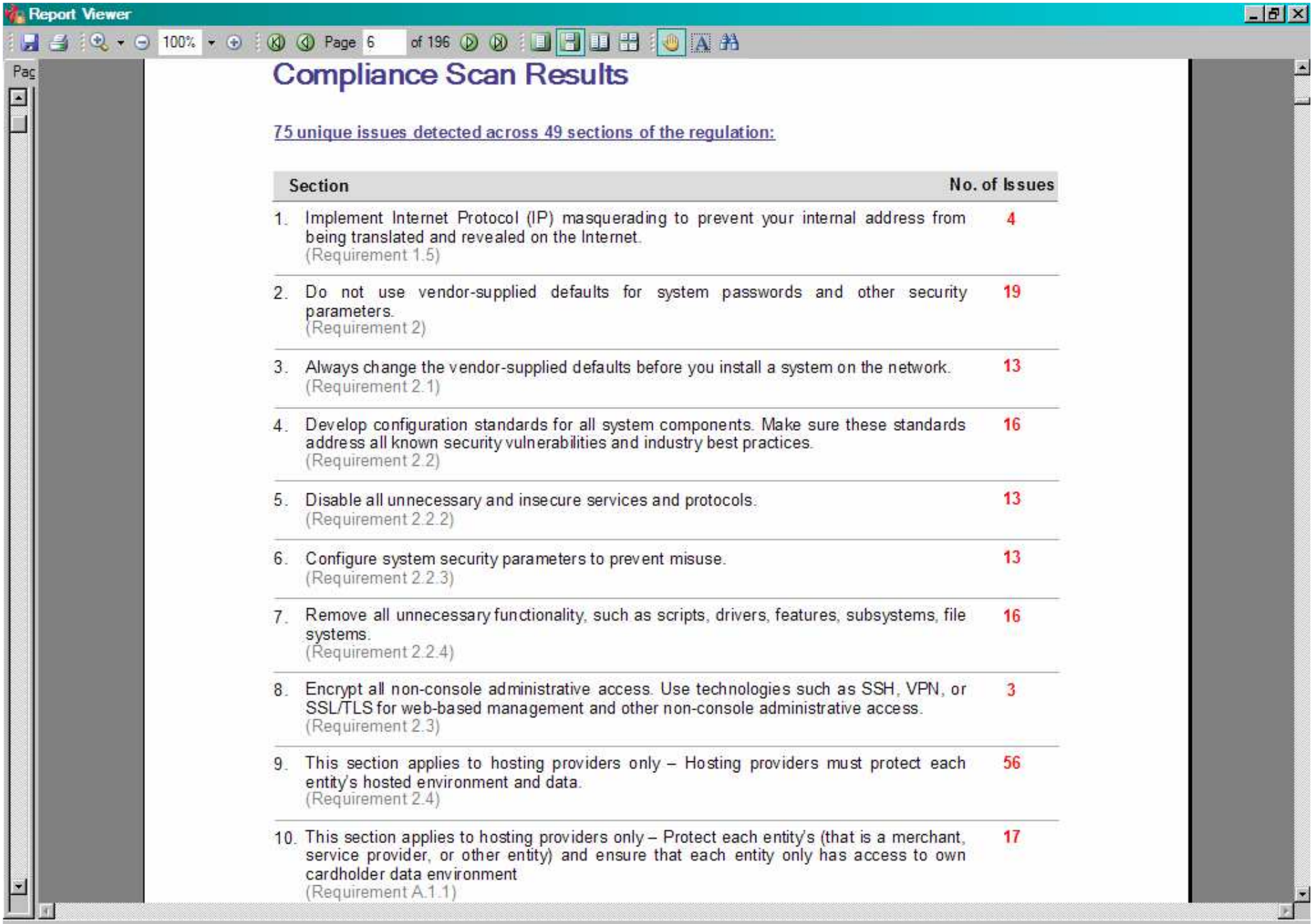
***Controls***

***Compliance***

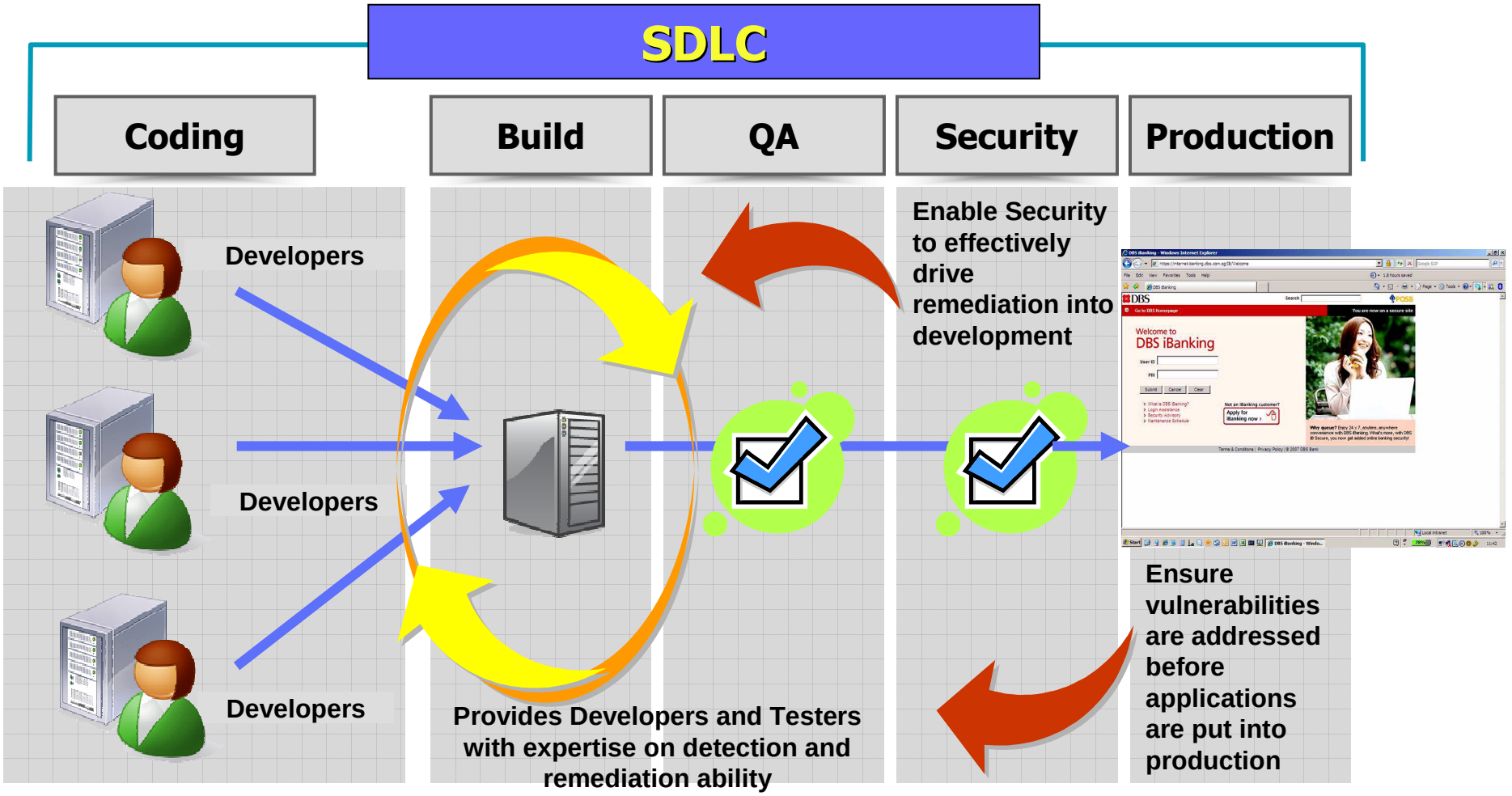
- www.owasp.org
- www.isc2.org
- www.ibm.com/security
- **Wikipedia –> “application security”**

# AppScan - CQTM & RQM Integration *Protect Your Investment*




Report Viewer
100%
Page 6 of 196
Compliance Scan Results
75 unique issues detected across 49 sections of the regulation:
Section
No. of Issues
1. Implement Internet Protocol (IP) masquerading to prevent your internal address from being translated and revealed on the Internet. (Requirement 1.5) 4
2. Do not use vendor-supplied defaults for system passwords and other security parameters. (Requirement 2) 19
3. Always change the vendor-supplied defaults before you install a system on the network. (Requirement 2.1) 13
4. Develop configuration standards for all system components. Make sure these standards address all known security vulnerabilities and industry best practices. (Requirement 2.2) 16
5. Disable all unnecessary and insecure services and protocols. (Requirement 2.2.2) 13
6. Configure system security parameters to prevent misuse. (Requirement 2.2.3) 13
7. Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems. (Requirement 2.2.4) 16
8. Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access. (Requirement 2.3) 3
9. This section applies to hosting providers only – Hosting providers must protect each entity's hosted environment and data. (Requirement 2.4) 56
10. This section applies to hosting providers only – Protect each entity's (that is a merchant, service provider, or other entity) and ensure that each entity only has access to own cardholder data environment (Requirement A.1.1) 17

# Building security & compliance into the SDLC – further back

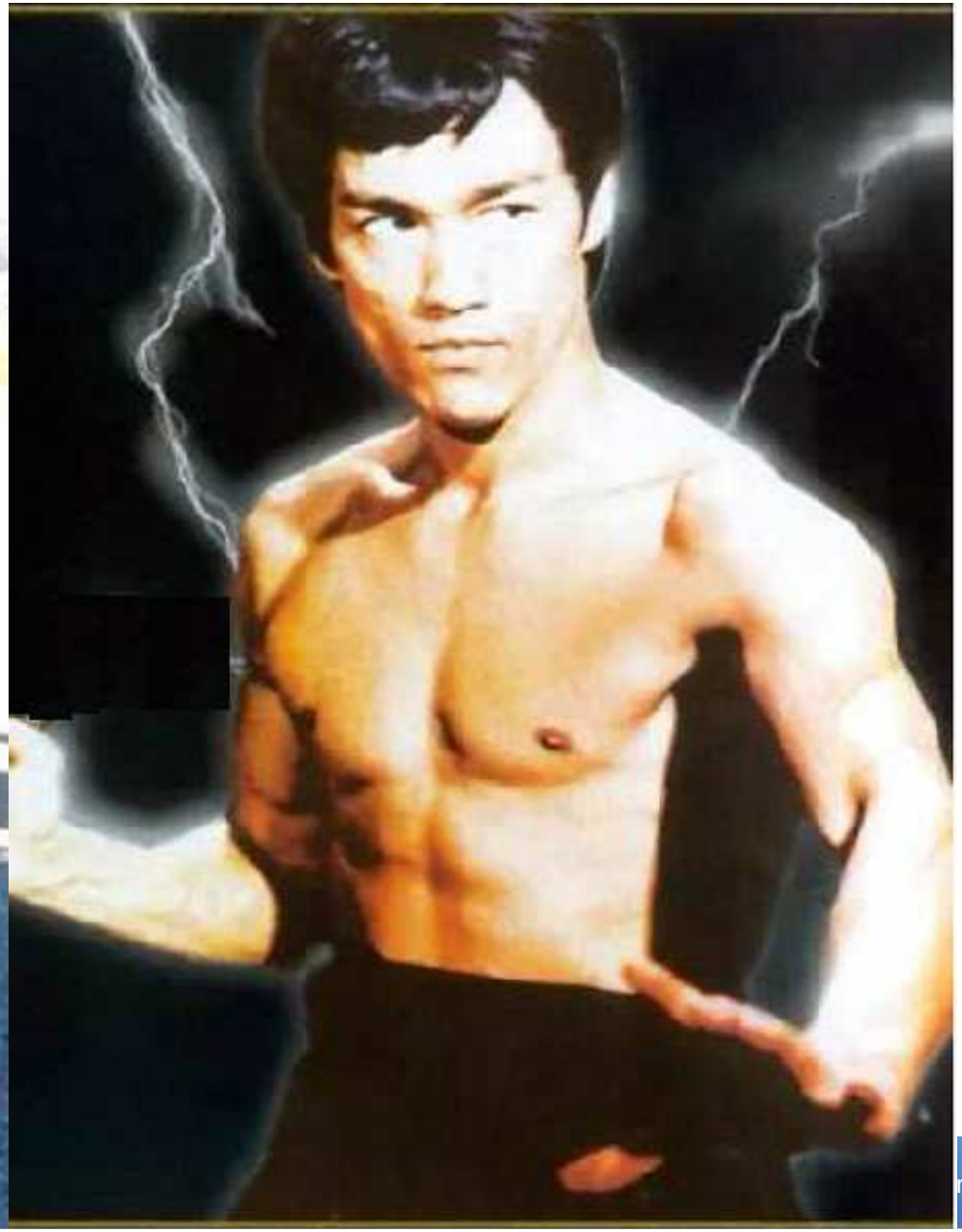


# Conclusion: Application QA for Security

- **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

## *THE HACKER'S NEW TARGET – APPLICATION QUALITY*

**http://www.ibm.com/software/rational/offerings/websecurity/**

# T h a n k  Y o u

**Anthony LIM**

**MBA CISSP CSSLP FCITIL**