THE HACKER'S NEW TARGET – SOFTWARE APPLICATIONS

IBM Software

PCTY2010

Pulse Comes to You

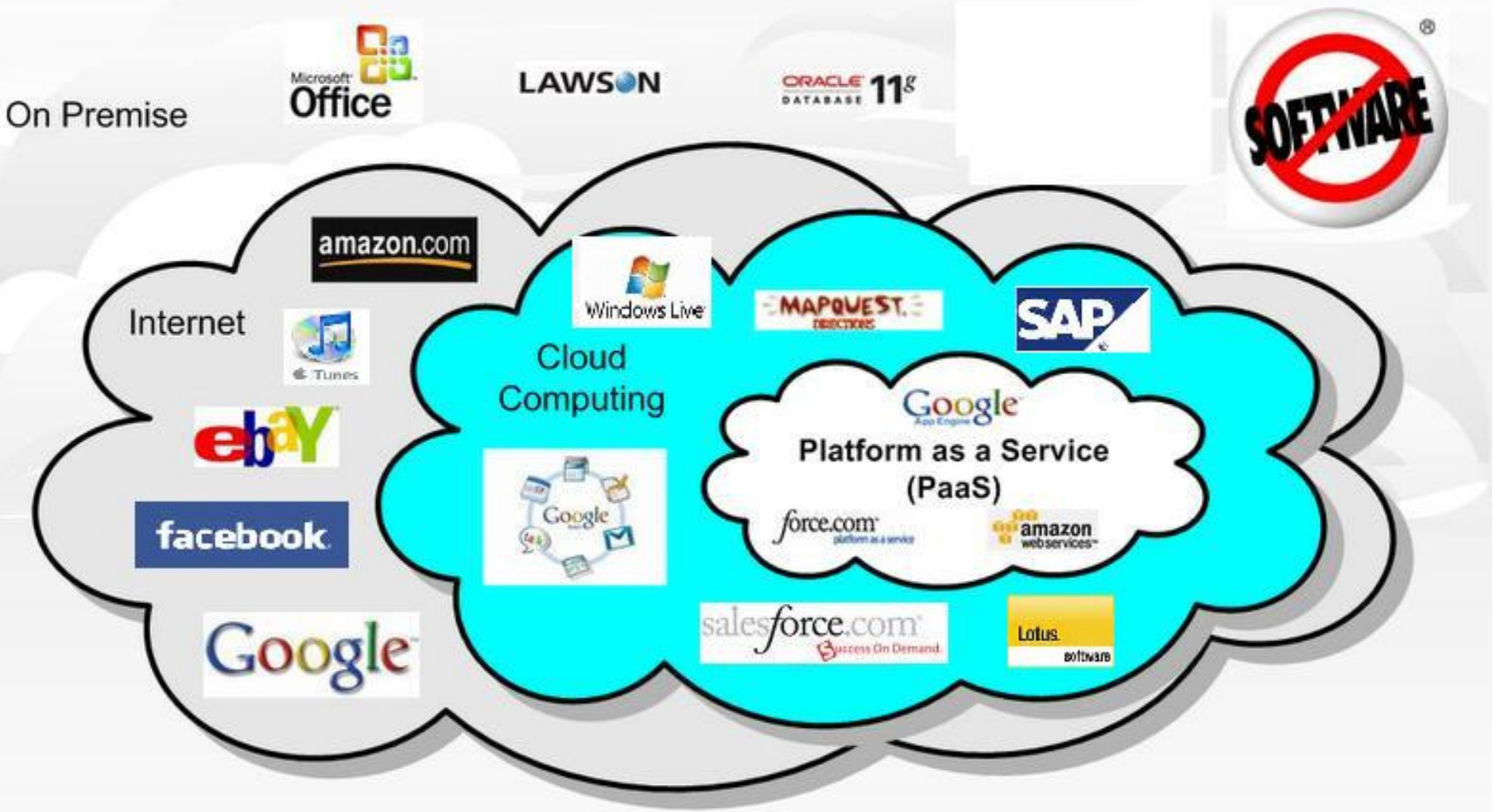
Anthony Lim

MBA CISSP CSSLP FCITIL

Director Asia Pacific, Software Security Solutions, IBM

Singapore Tue 13 Apr 2010

The Wonders of Cloud Computing



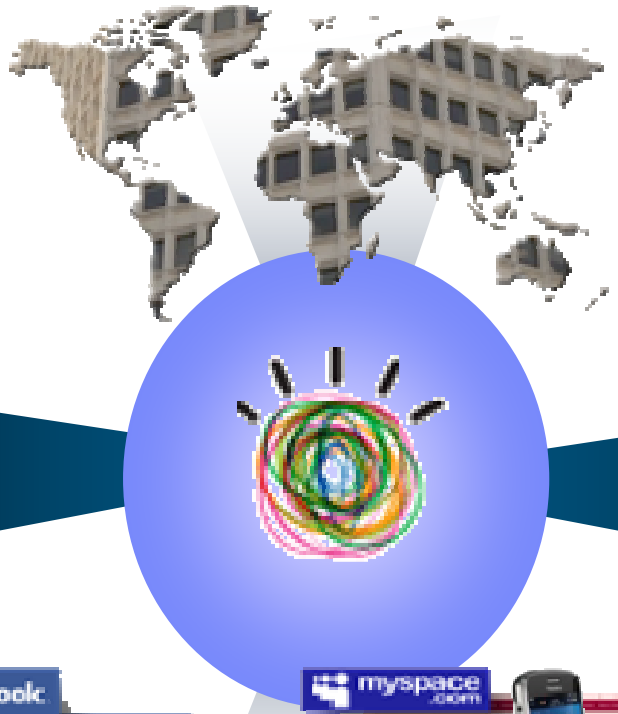
PC Laptop / Netbook Thin Client Mobile Device

Welcome to THE SMARTER PLANET

IBM

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..

PWC 2010 CIO-CSO INFOSEC SURVEY – Some Highlights

Some 2010 CIO-CSO IT Security Priorities

- **Web Content Filters**
- **Data Leakage Prevention**
- **Web 2.0 Security**
- ***Stronger yet Simpler Authentication**
  - Biometrics
  - Disposable Passwords
  - Tokens & Smartcards
  - Reduced Single Sign On
  - IDentity Management

Trends:

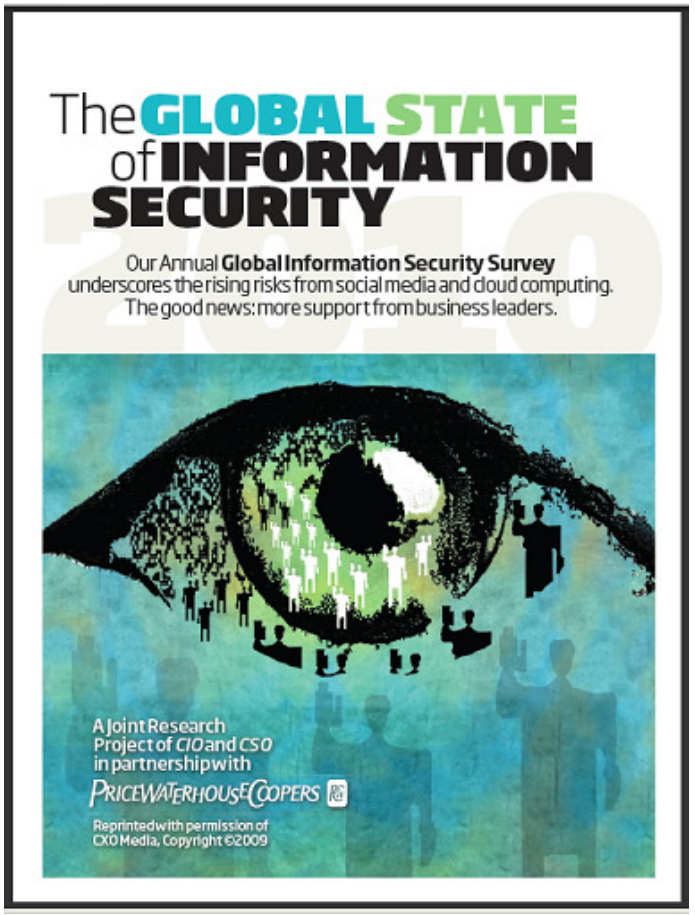
(1) Promise and Peril of SOCIAL NETWORKING

(2) Jumping into the CLOUD (w/o parachute)

(3) INSOURCING Security Management

(4) NEW CORPORATE COMMITMENT

(5) ATTACKS ON DATABASES



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 …

IBM

BBC NEWS

Watch One-Minute World News

News Front Page
Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science/Nature
Technology
Entertainment

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 jobs 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

c|net 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

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

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, chie ecutive of Data Security Sys Solutions, said such accid leaks of confidential info tion could lead to "embarra situations for clients and re tion risks for banks".

"Intentional leakages more serious as the d (could be) used for more cious activities," he said.

kennyc@sph.com.sg

HELPDESK 我的

Glitch: 小故障 xiǎo gù zhàng

Confidential: 私人的 sī rén de

Rectify: 矫正 jiǎo zhèng

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

Cloud Computing Security – The Soft Spot

Application Security Issues

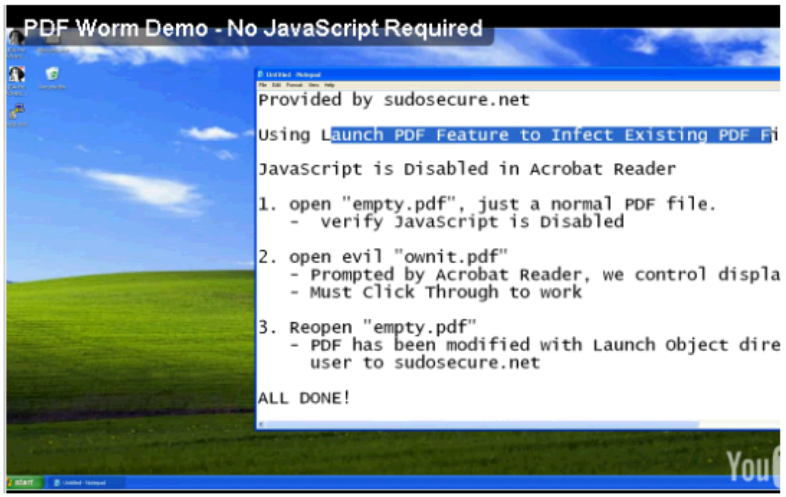
- Applications can be CRASHED to reveal source, logic, script or infrastructure information that can give a hacker intelligence

April 5, 2010 3:32 PM PDT

Exploits not needed to attack via PDF files

by Elinor Mills

77 retweet Share 23



Jeremy Conway created a video to show how his PDF hack works.

- Applications can be COMPROMISED to make it provide unauthorised entry access or unauthorised access to read, copy or manipulate data stores, or reveal information that it otherwise would not.
  - Eg. Parameter tampering, cookie poisoning
- Applications can be HIJACKED to make it perform its tasks but for an authorised user, or send data to an unauthorised recipient, etc.
  - Eg. Cross-site Scripting, SQL Injection

Cloud Computing - Dangers and Vulnerabilities - The Soft Spot

Security is to save data and program from

Dangers -

- **Disruption of Services.**
- **Lack of Control**
- **Theft /Damage of Information.**
- **Loss of Privacy.**

Fri, Mar 19, 2010
Reuters

New password-stealing virus targets Facebook

BOSTON, US - Hackers have flooded the Internet with virus-tainted spam that targets Facebook's estimated 400 million users in an effort to steal banking passwords and gather other sensitive information.

The emails tell recipients that the passwords on their Facebook accounts have been reset, urging them to click on an attachment to obtain new login credentials, according to anti-virus software maker McAfee Inc.

Vulnerabilities -

- **Hostile Applications eg bot, malware, trojan**
- **Hostile people giving instructions to good applications**
- **Bad guys corrupting or eavesdropping on communications**

WORST CREDIT CARD IDENTITY THEFT CASE

- DONE BY A SOFTWARE ATTACK! ("SQL Injection")

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 20 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.

Those 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

School website tests show up security lapses

Personal data of staff and students [illegible] easily, says [illegible]

By Khushwant [illegible]

FOR a week, membe[rs] mainly known as th[e] Meetup Group (SSMG[)] sites of various sch[ools] with plenty of perso[nal] as addresses and id[entity] phone numbers of st[udents].

SSMG members [have] very hard of[ten].

No hacking, spyw[are] needed. All they did [was] gines such as Google [and] tion fell into their la[ps].

In one case, the [group] word of a system [administrator] popped up. With these, a hacker could use the server at the secondary school to send spam messages or even host an Inter-

SSMG's findings confirm this view.

The issue of data privacy had been raised in Parliament in January by Ms Lee

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 Khng Eu Meng blamed its leak of names, IC numbers and e-mail addresses of 200 students on "human error", and said steps

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

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 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 1.3 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 39.2 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.

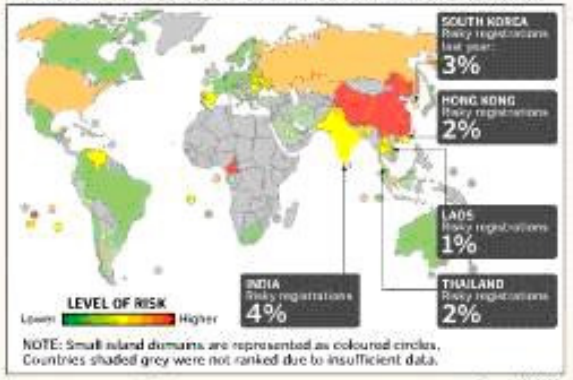
And a domain can be registered with stolen credit card information, too, Web security specialist Mark Gondie of IT solu-

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

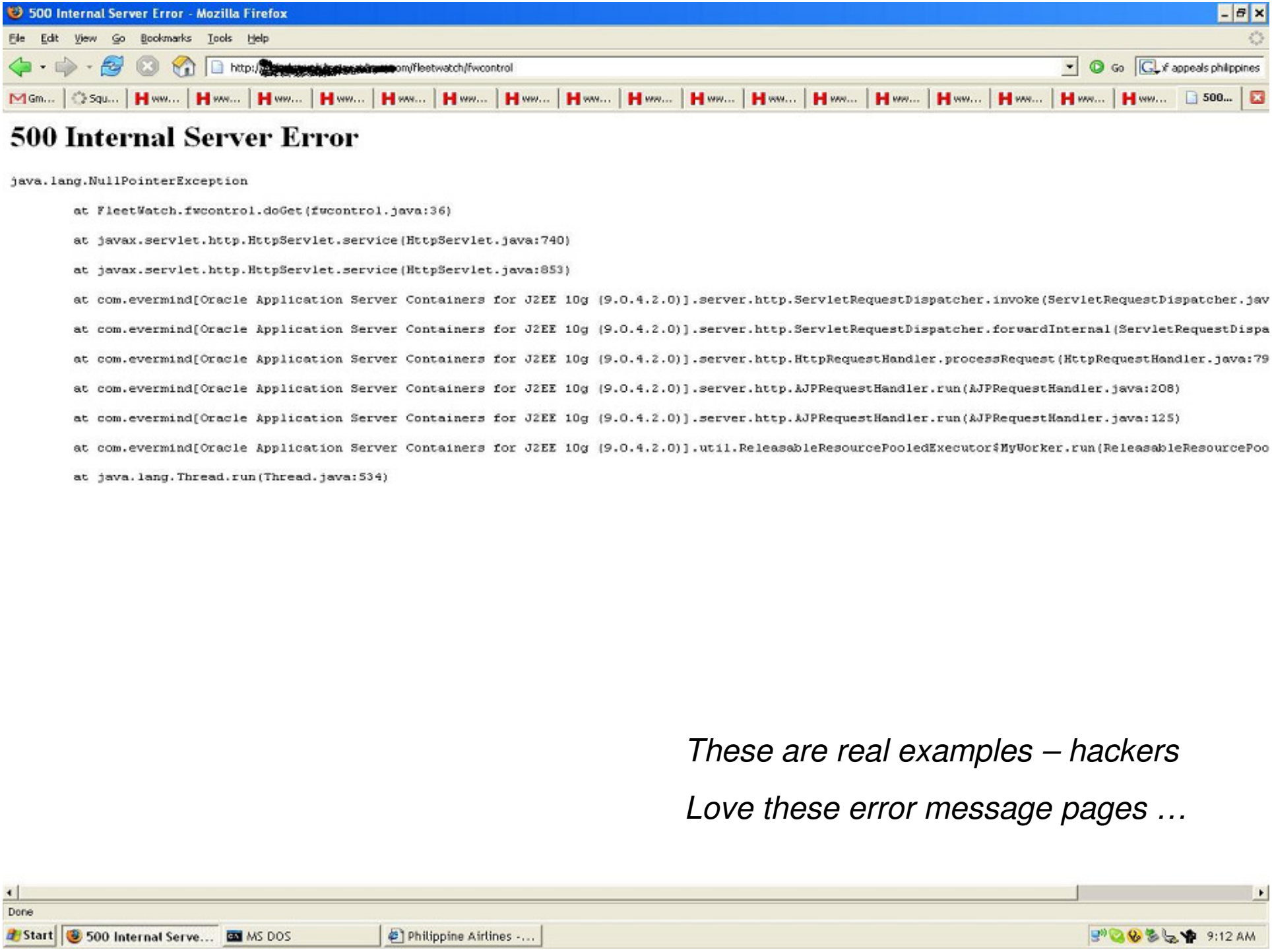
Surfing the Internet is also generally riskier in Asia and the Middle East



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

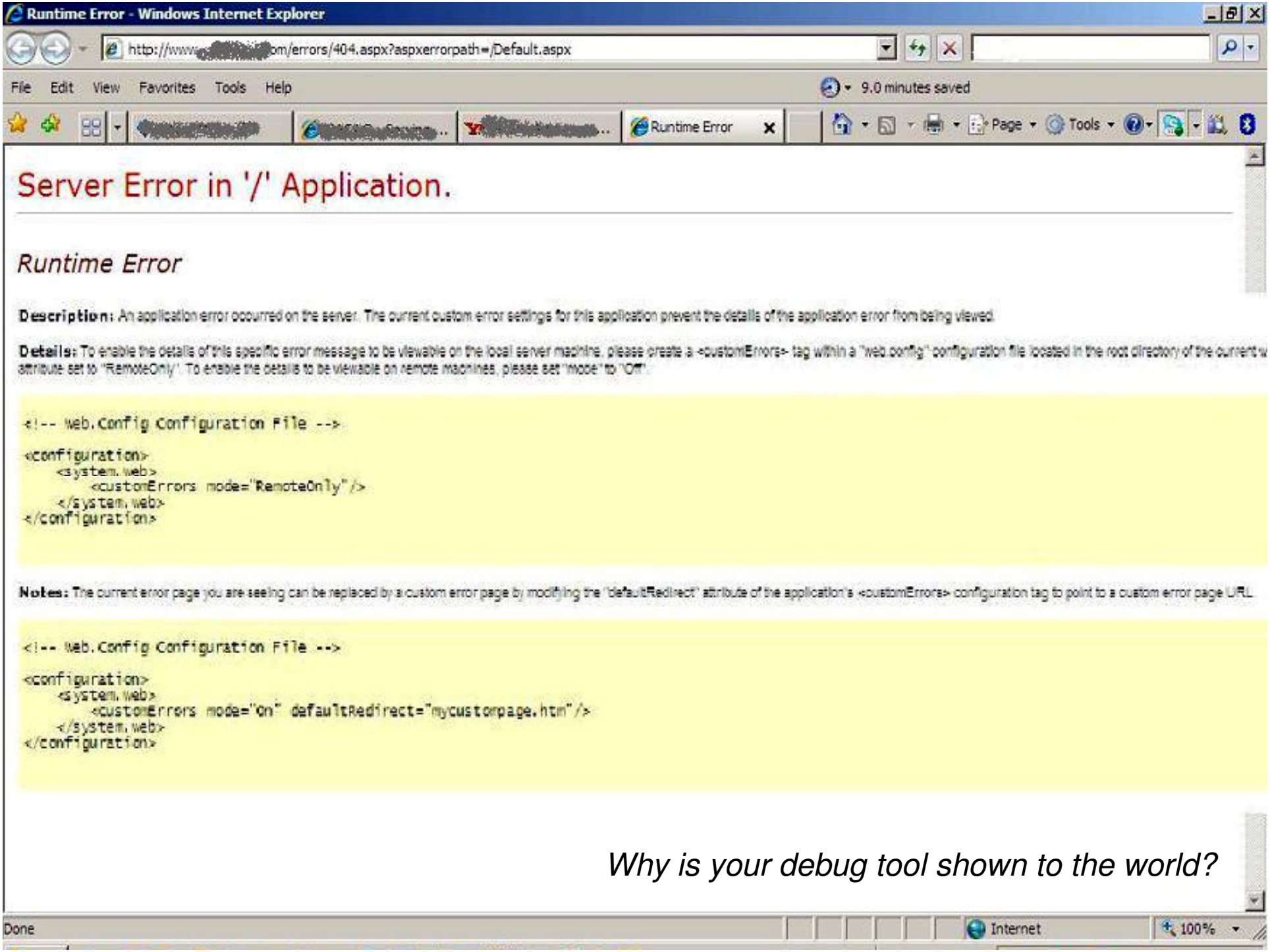
Source: MCAFEE

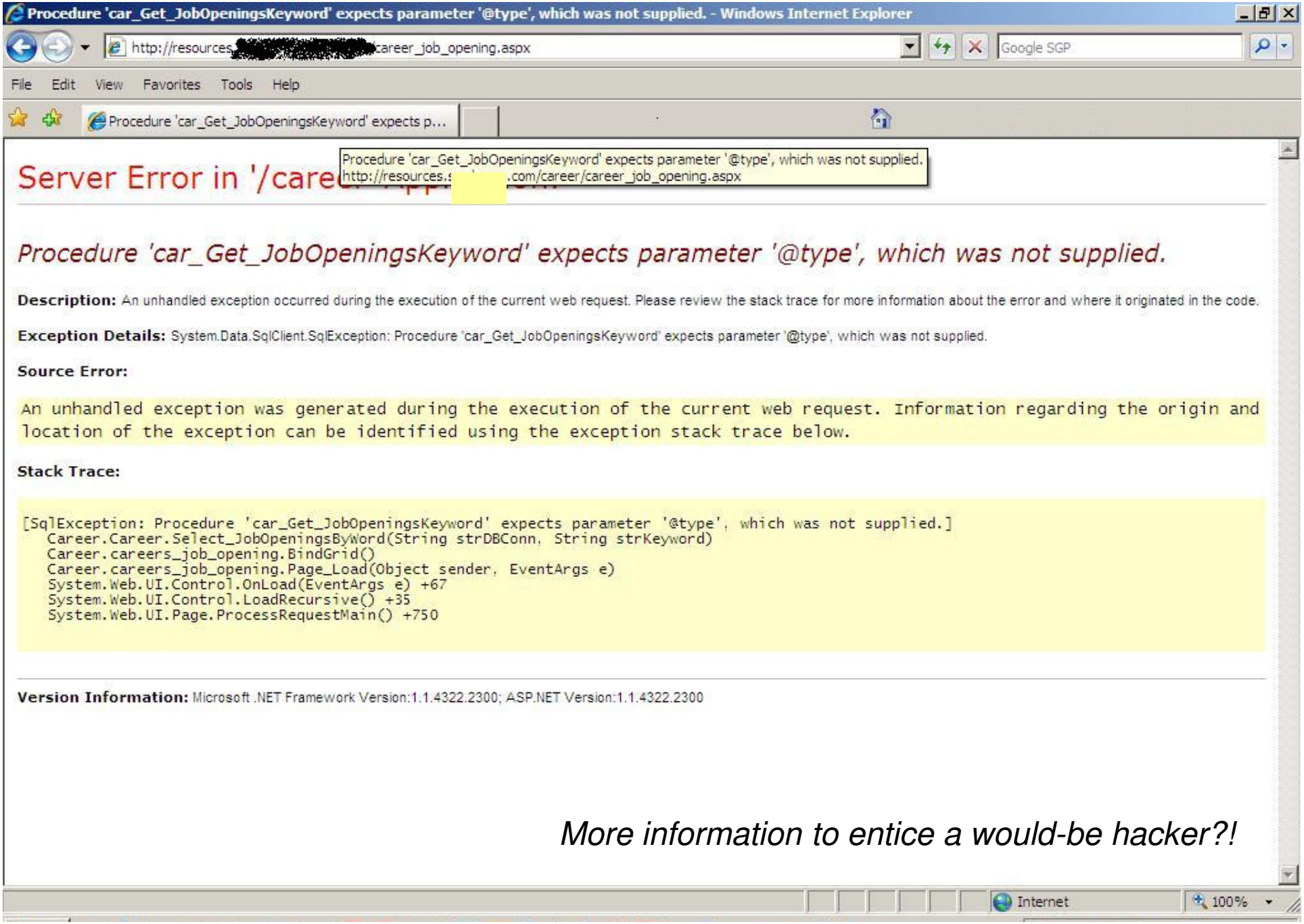
ST GRAPHICS



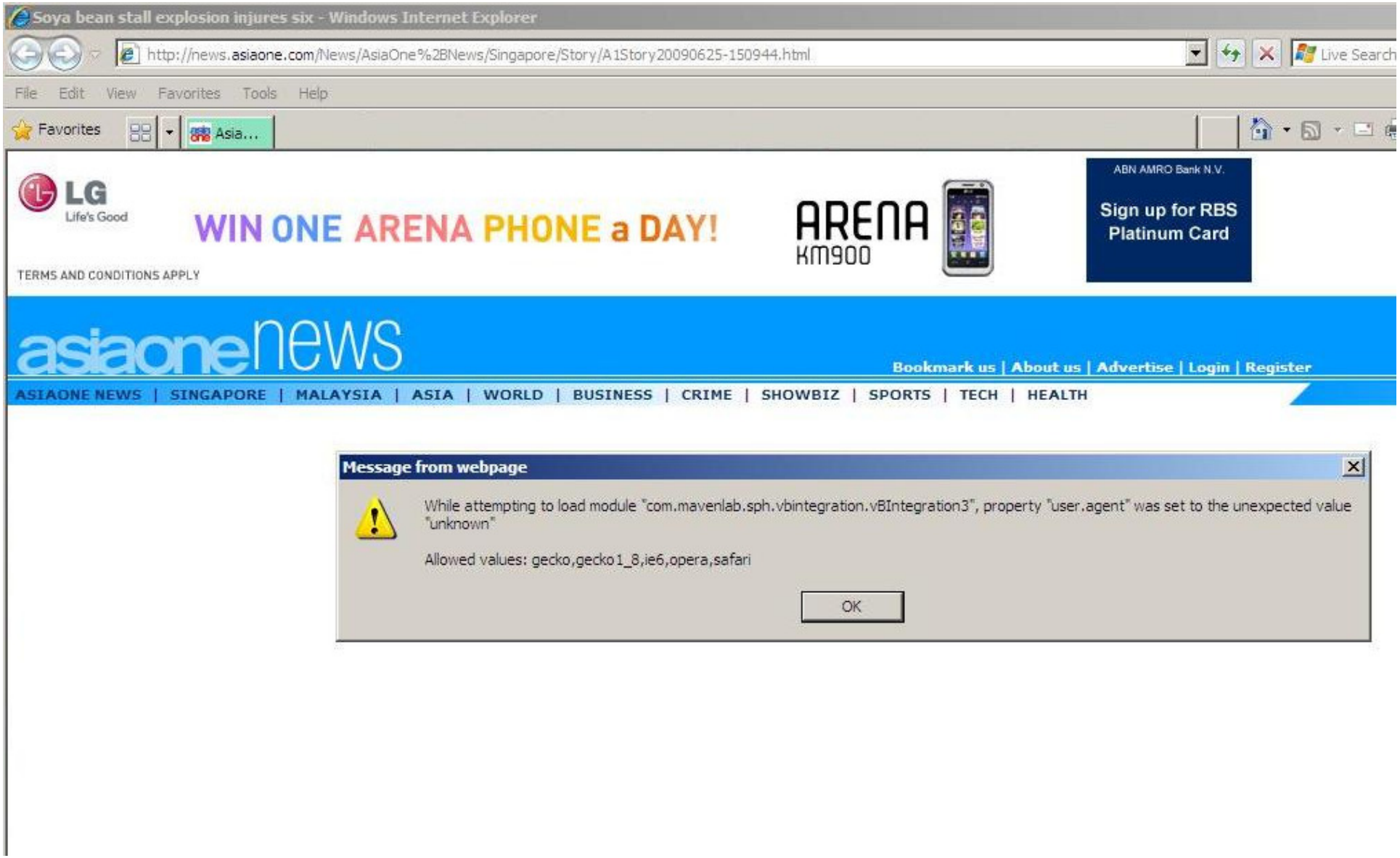
These are real examples – hackers

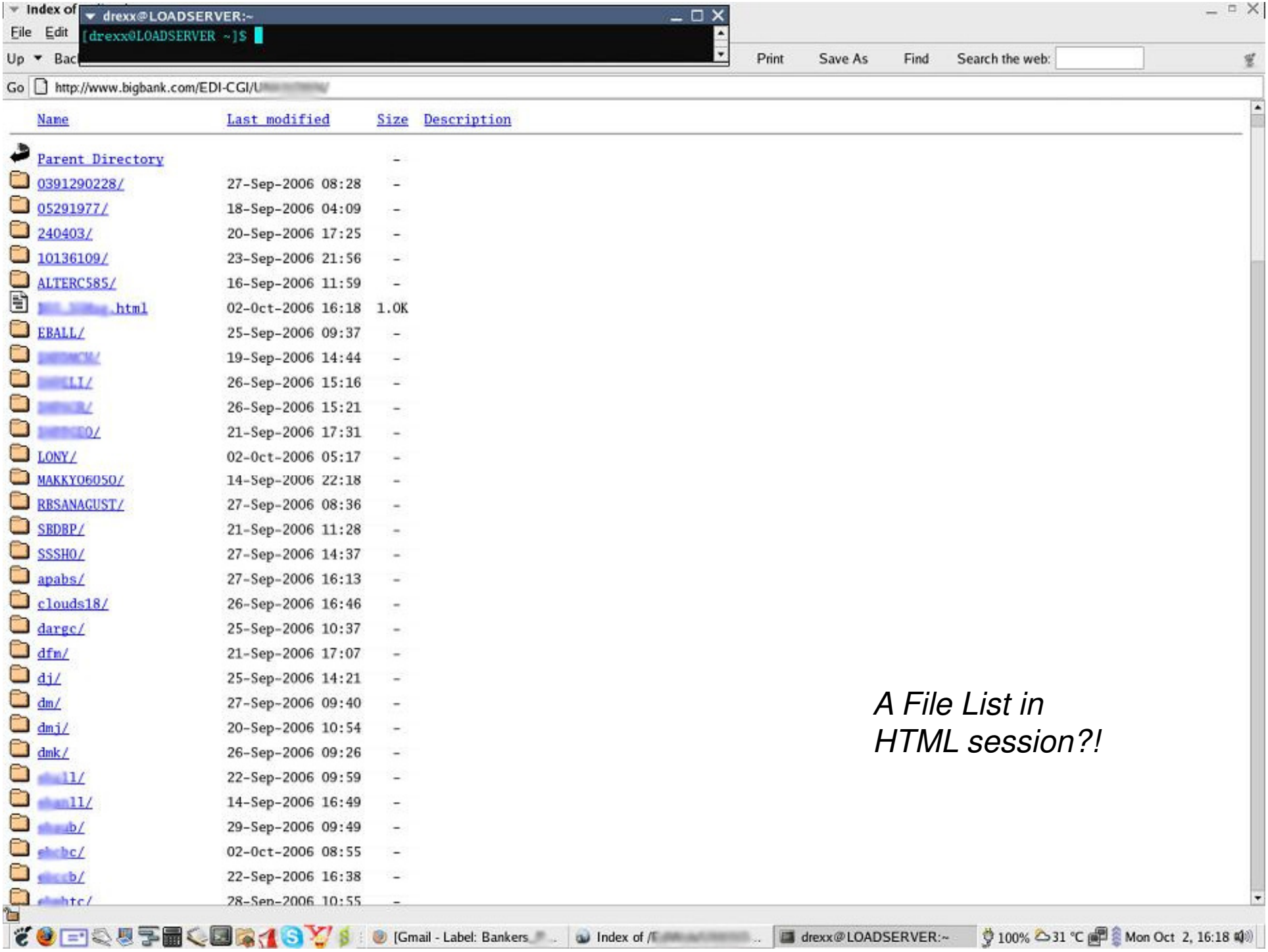
Love these error message pages …


Runtime Error - Windows Internet Explorer
http://www[redacted]om/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>
Why is your debug tool shown to the world?
Done
Internet
100%



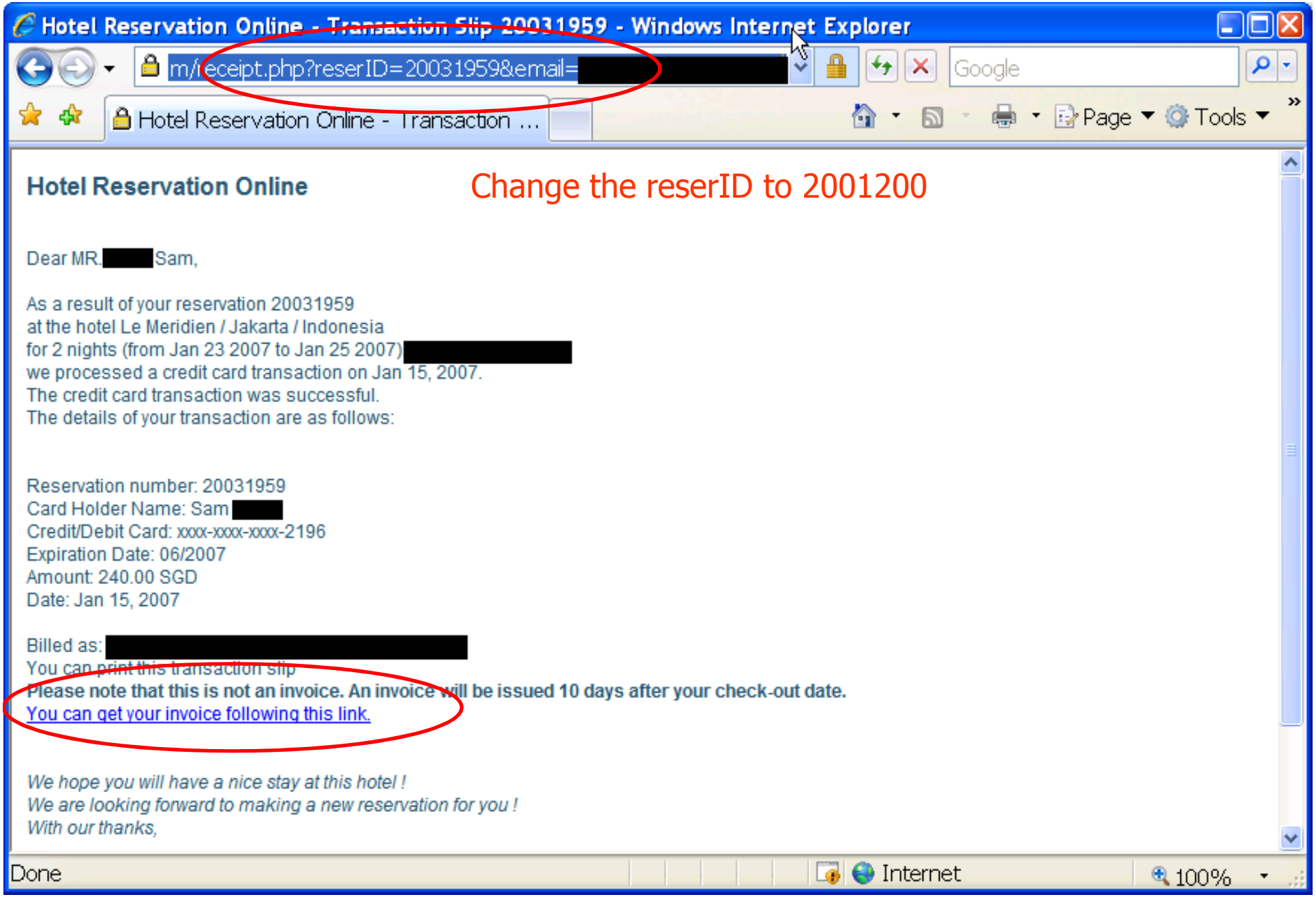
More information to entice a would-be hacker?!





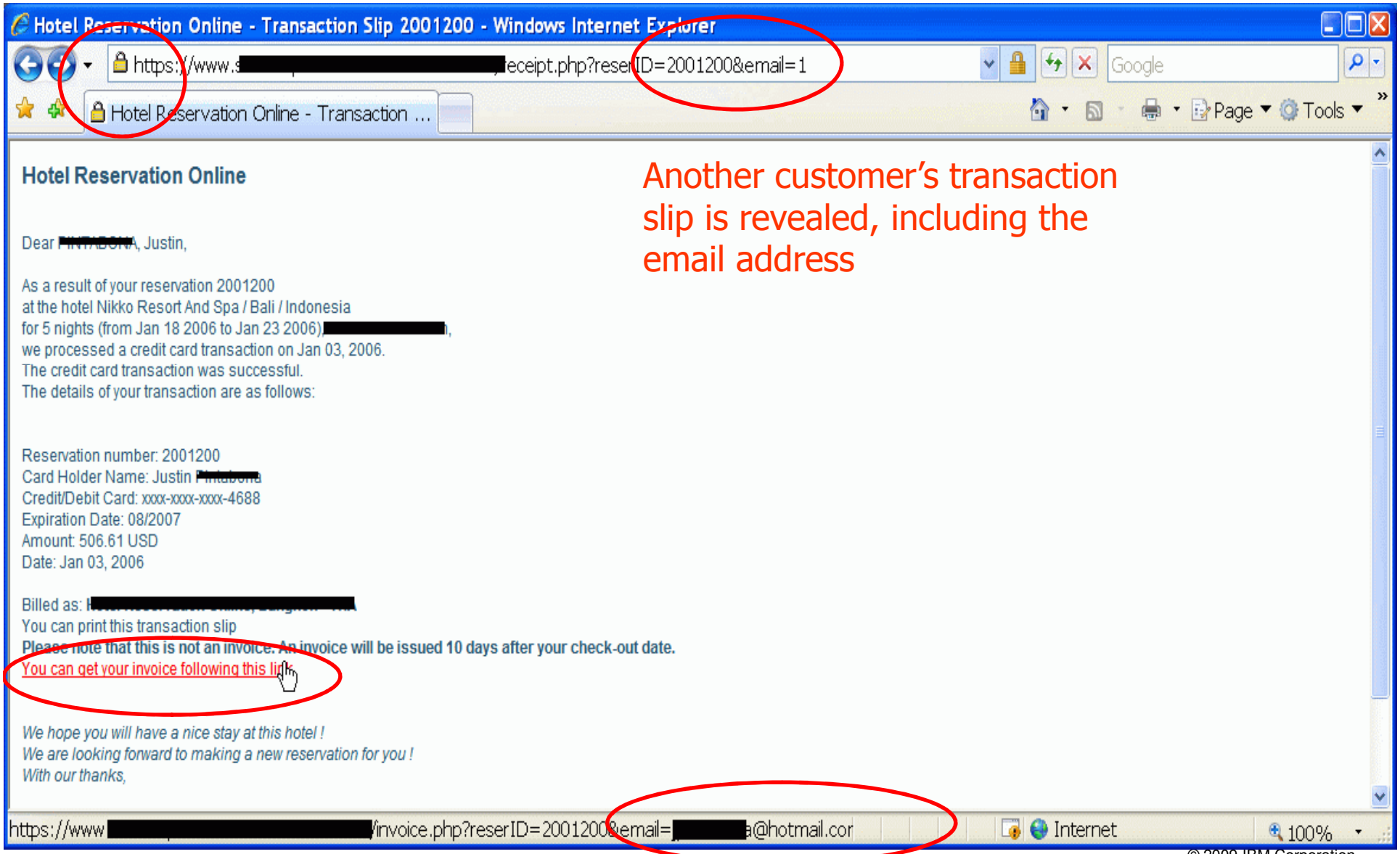
A File List in HTML session?!

Real Example: Online Travel Reservation Portal



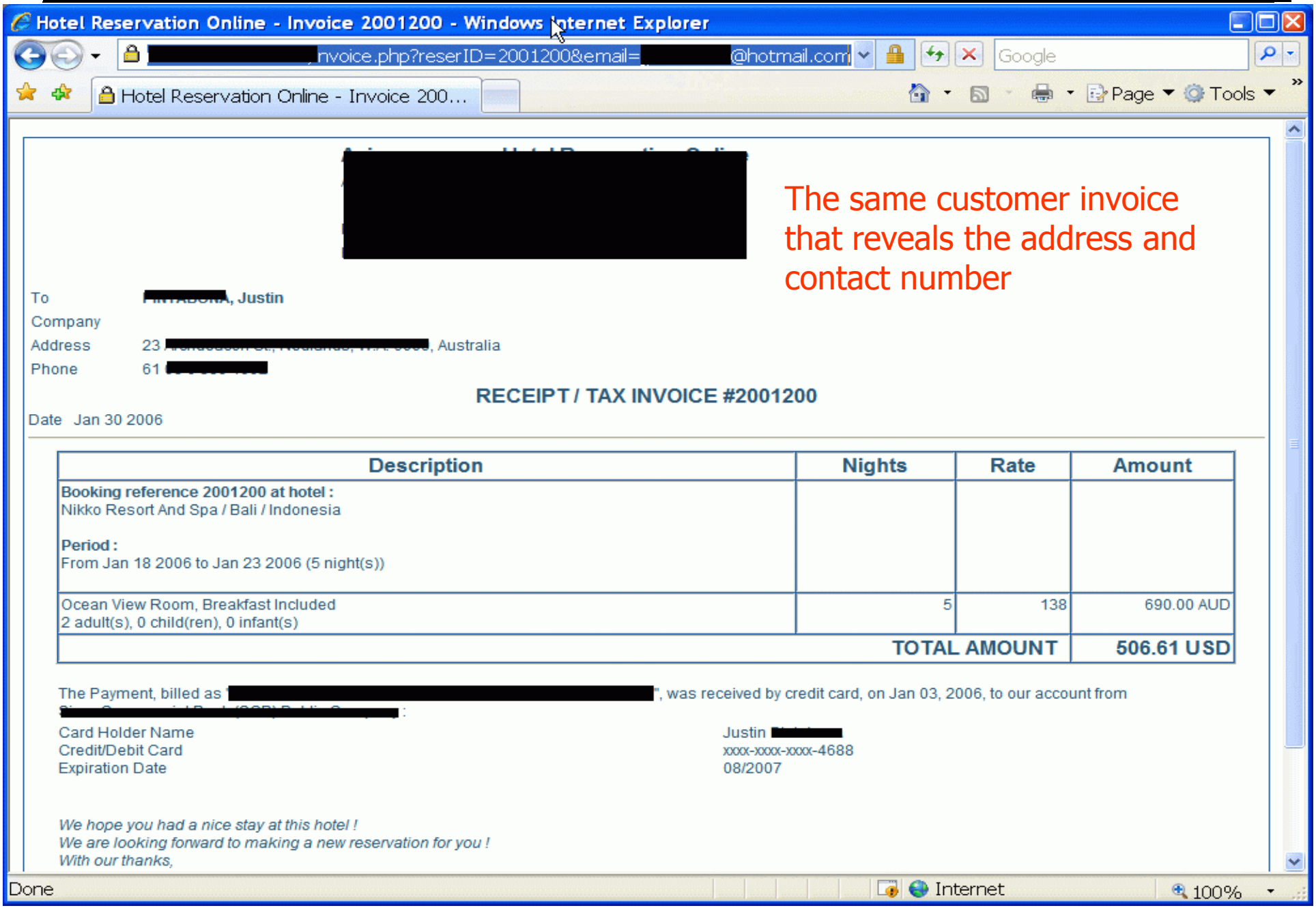
Real Example : Parameter Tampering

Reading another user's transaction – insufficient authorization



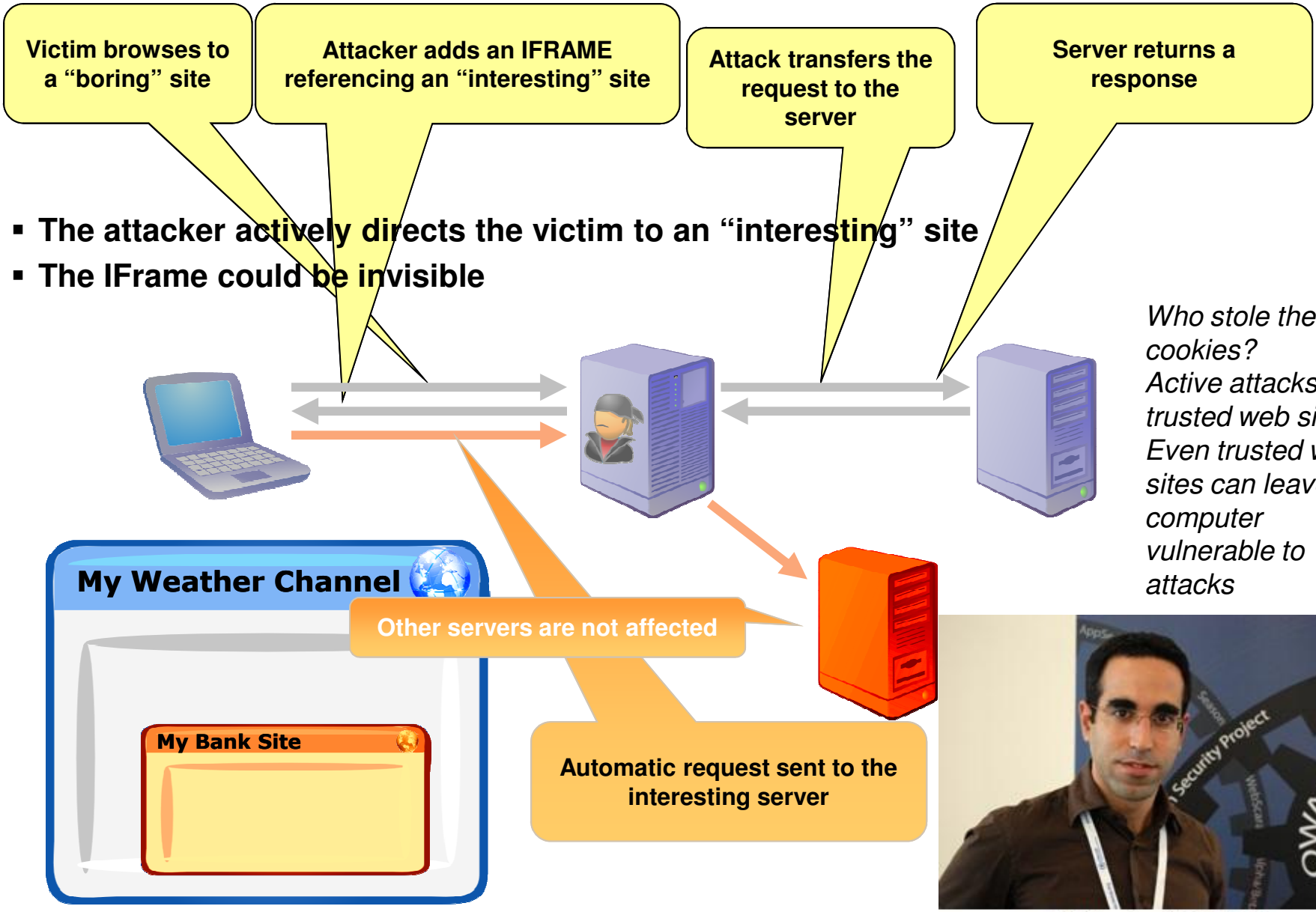
Another customer's transaction slip is revealed, including the email address

Parameter Tampering Reading another user's invoice



The same customer invoice that reveals the address and contact number

“Active” (Web) Man-in-the-Middle Attack



- The attacker actively directs the victim to an “interesting” site
- The IFrame could be invisible

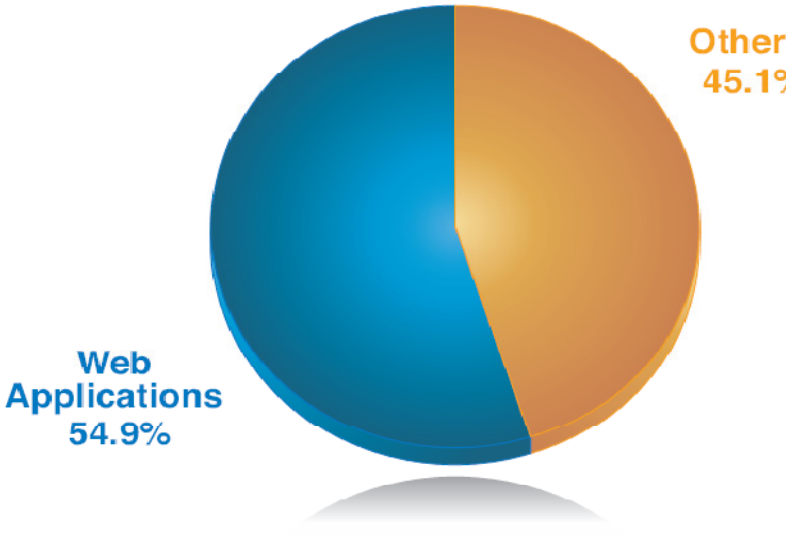
Who stole the cookies?
Active attacks from trusted web sites - Even trusted web sites can leave your computer vulnerable to attacks

Adi Sharabani at OWASP

https://www.research.ibm.com/haifa/info/200902_OWASP.shtml

Since 2008 - Web Threats Take Center Stage

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



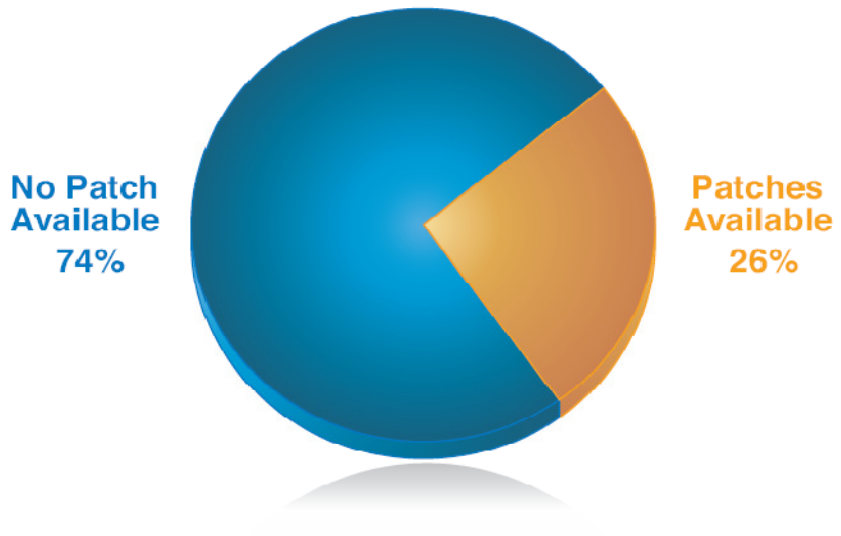


Figure 22: Percent of 2008 Web Application Vulnerabilities with No Vendor-Supplied Patch Available at the End of 2008

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

Top 10 OWASP Critical Web Application Security Issues '09

IBM

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

www.owasp.org

WHY DO APPLICATION SECURITY PROBLEMS EXIST?

IBM

- **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

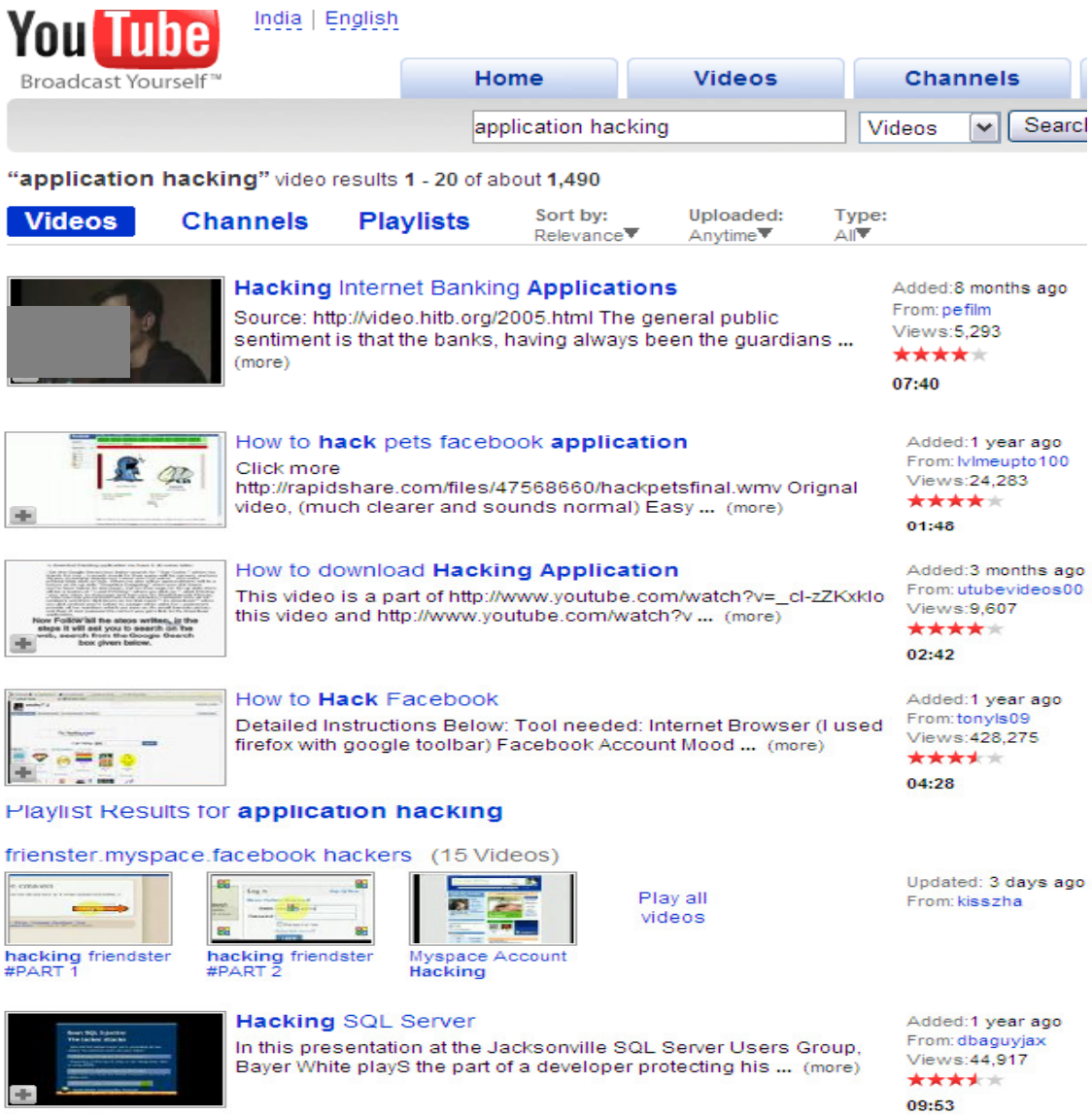
- **Most companies today still do not have an application security QA policy or resource**
  - IT security staff are focused on other things and are swarmed
    - App Sec is their job but they don't understand it and don't want to deal with it
    - Developers think its not their job or problem to have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

DON'T TRY THIS AT HOME!



Conclusion: Application QA for Security

IBM

- **The Application Must Defend Itself**
  - "Traditional" FIREWALLS AND IPS WILL NOT STOP APPLICATION ATTACKS
  - YOU CANNOT STOP AN APPLICATION ATTACK FROM HAPPENING
  - **The best way to protect against an application attack is to ensure the robustness of the application, that its written properly, if not defensively, that it's Q.A'ed for bugs, vulnerabilities, logic errors etc**

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

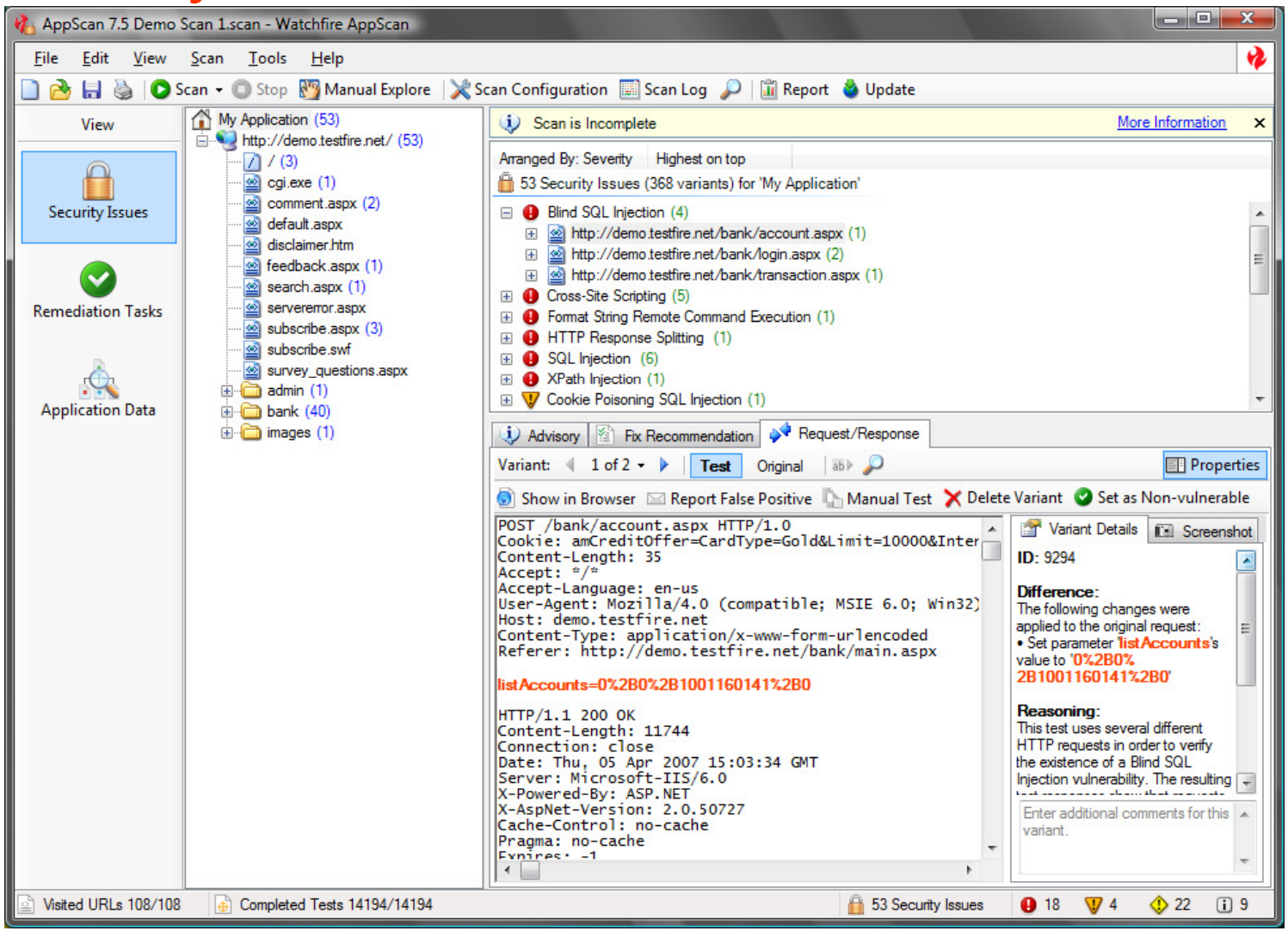
- **QA Testing for Security must now be integrated and strategic**
  - **We need to move security QA testing back to earlier in the SDLC**
  - at production or pre-production stage is late and expensive to fix
  - Developers need to learn to write code defensively and securely

Lower Compliance & Security Costs by:

- Ensuring Security Quality in the Application up front
- Not having to do a lot of rework after production
- Automated software security scanning & remediation solution backed by world class R&D

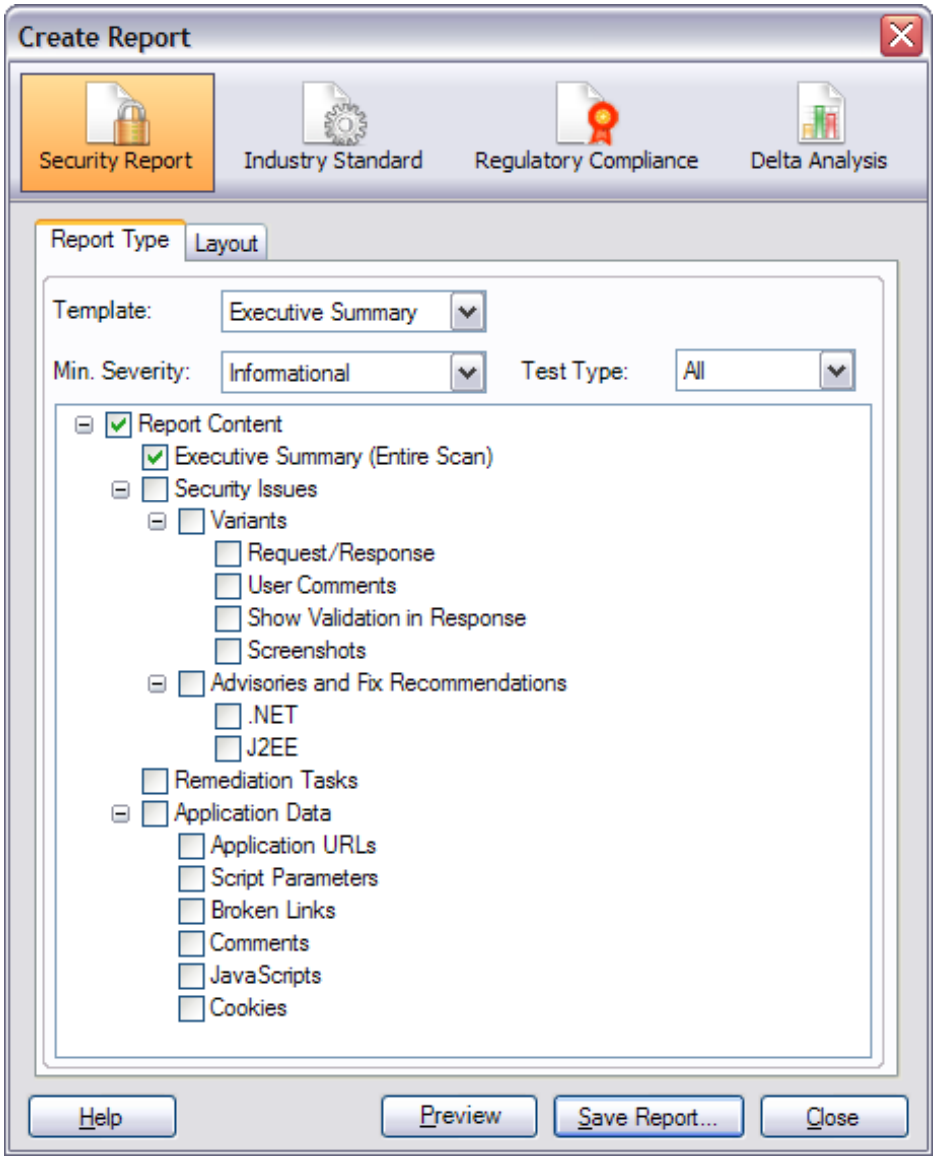
You need a professional solution to

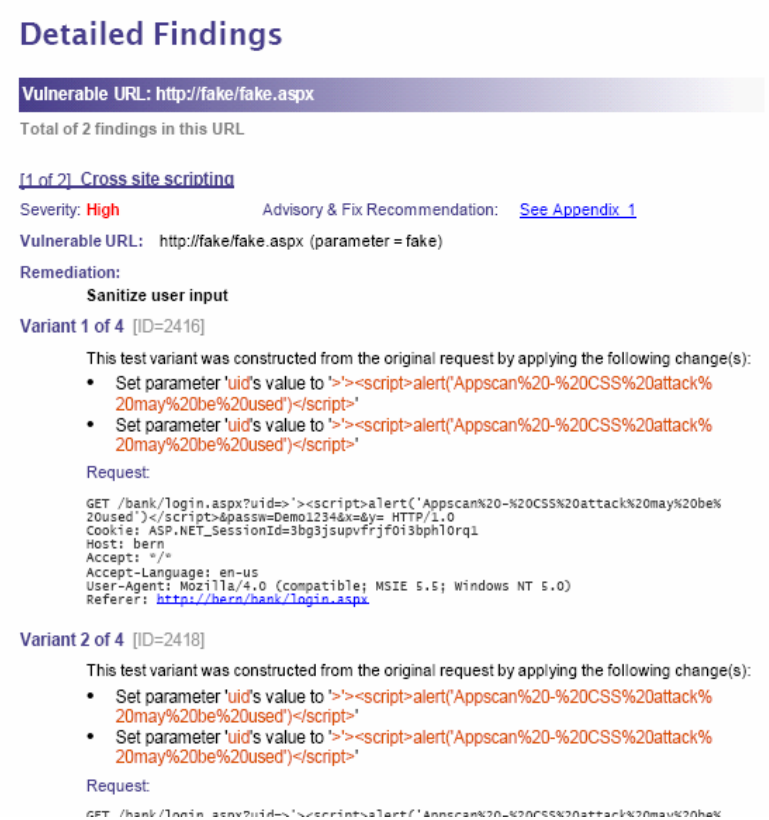
Identify Vulnerabilities



With Rich Report Options

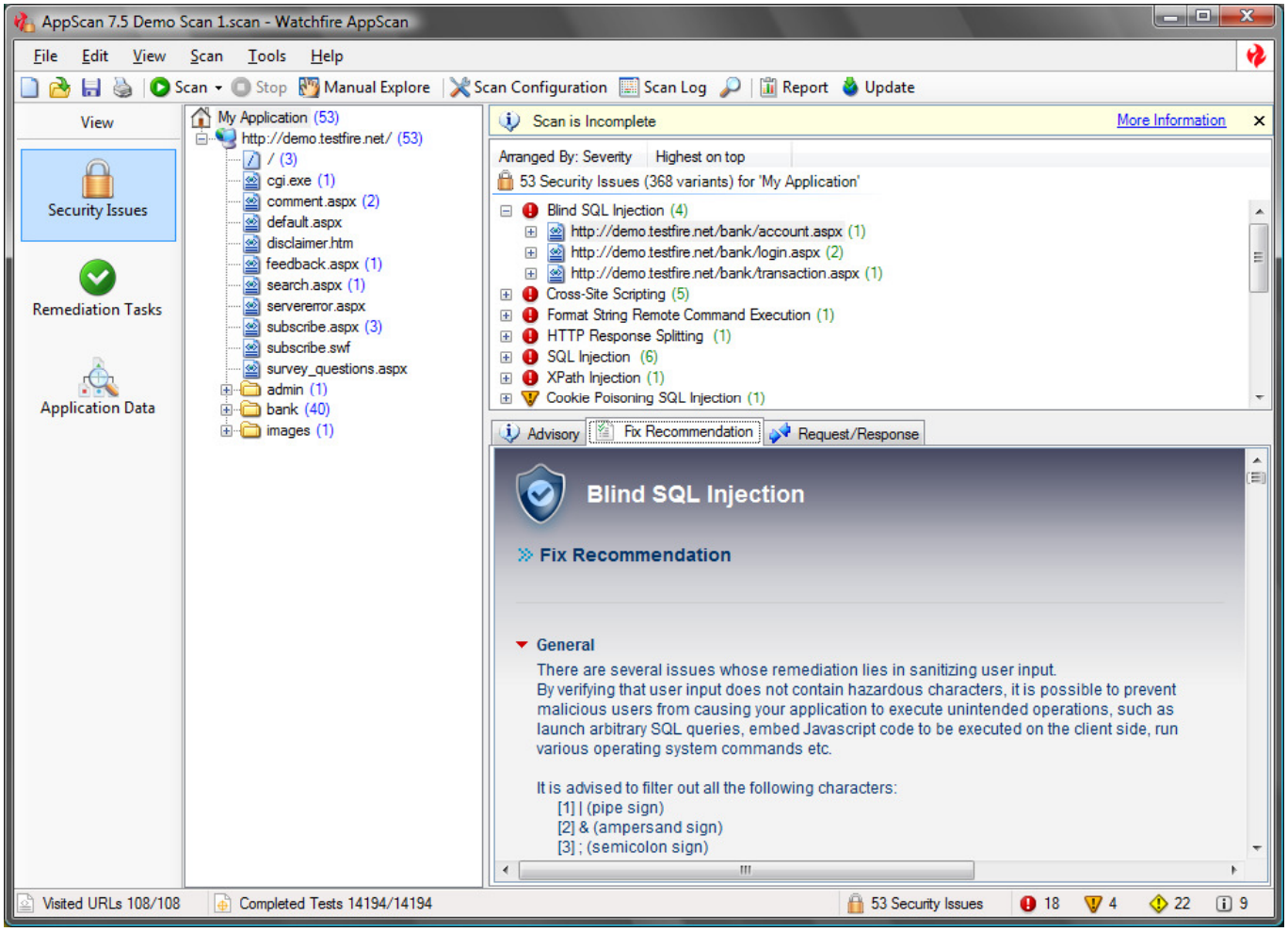
44 Regulatory Compliance Standards, for Executive, Security, Developers.



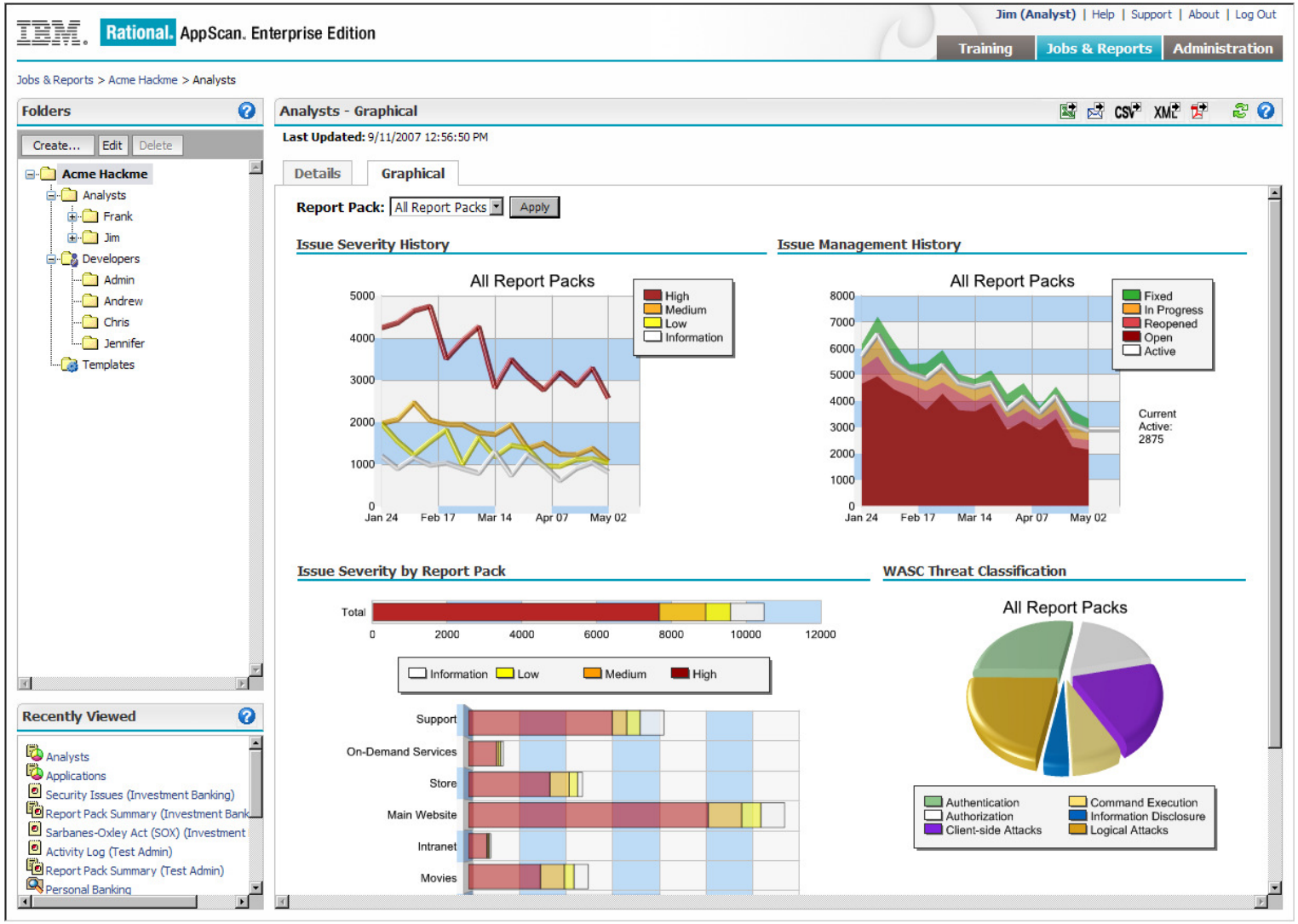


And Most Important :

Actionable Fix Recommendations



AppScan Enterprise – Dashboards and Metrics

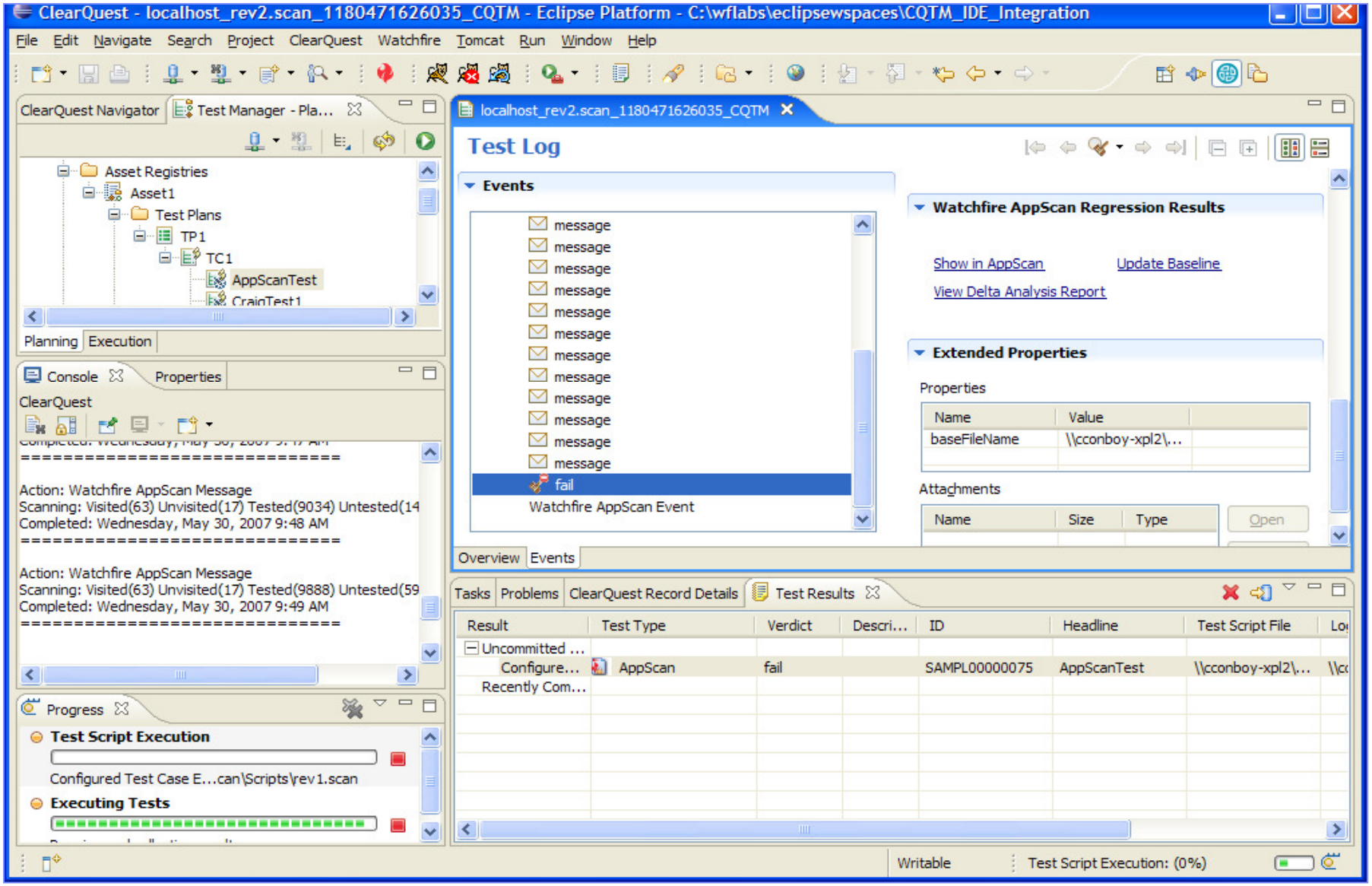


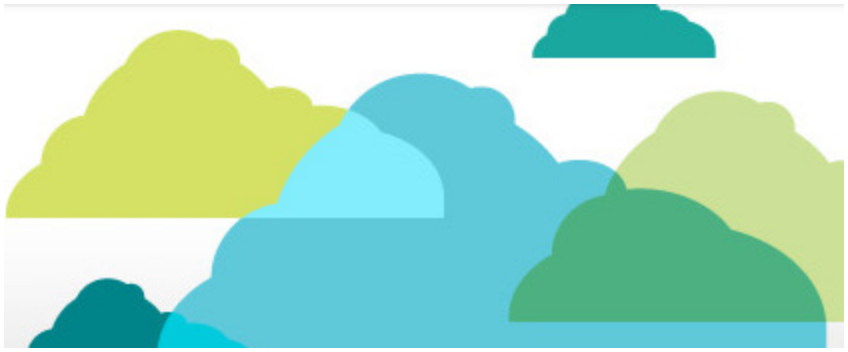
Policies

Controls

Compliance

AppScan - CQTM & RQM Integration *Protect Your Investment*





Thank You

Anthony LIM

MBA CISSP CSSLP FCITIL

The Hacker's New Target – Software Applications

www.isc2.org **www.owasp.org**

www.ibm.com/security