CLOUD COMPUTING SECURITY – THE SOFT SPOT

Security by Application Development Quality Assurance

Anthony Lim

MBA CISSP CSSLP FCITIL

Director, Asia Pacific, Software Security Solutions

IBM, Singapore

Advisor & Secretary, Security & Governance, www.sitf.org.sg

INNOVATE – INDIA – 17 AUG 2010

CSSLP

Certified Secure Software Lifecycle Professional

Prolog: The Security Journey Continues

- Every year - **New, More, Bigger, Better …**
  - **SYSTEMS & ARCHITECTURE**
  - **APPLICATIONS**
  - **SERVICES**

-> New Risks

-> New Vulnerabilities

-> New Hacking methods

- *Viruses, Worms, RATS, Bots …*

(Remote Access TROJANS = Spyware)

->GOVERNANCE & COMPLIANCE!

-> DATA PRIVACY, POLICIES AUDIT

-> MOBILITY

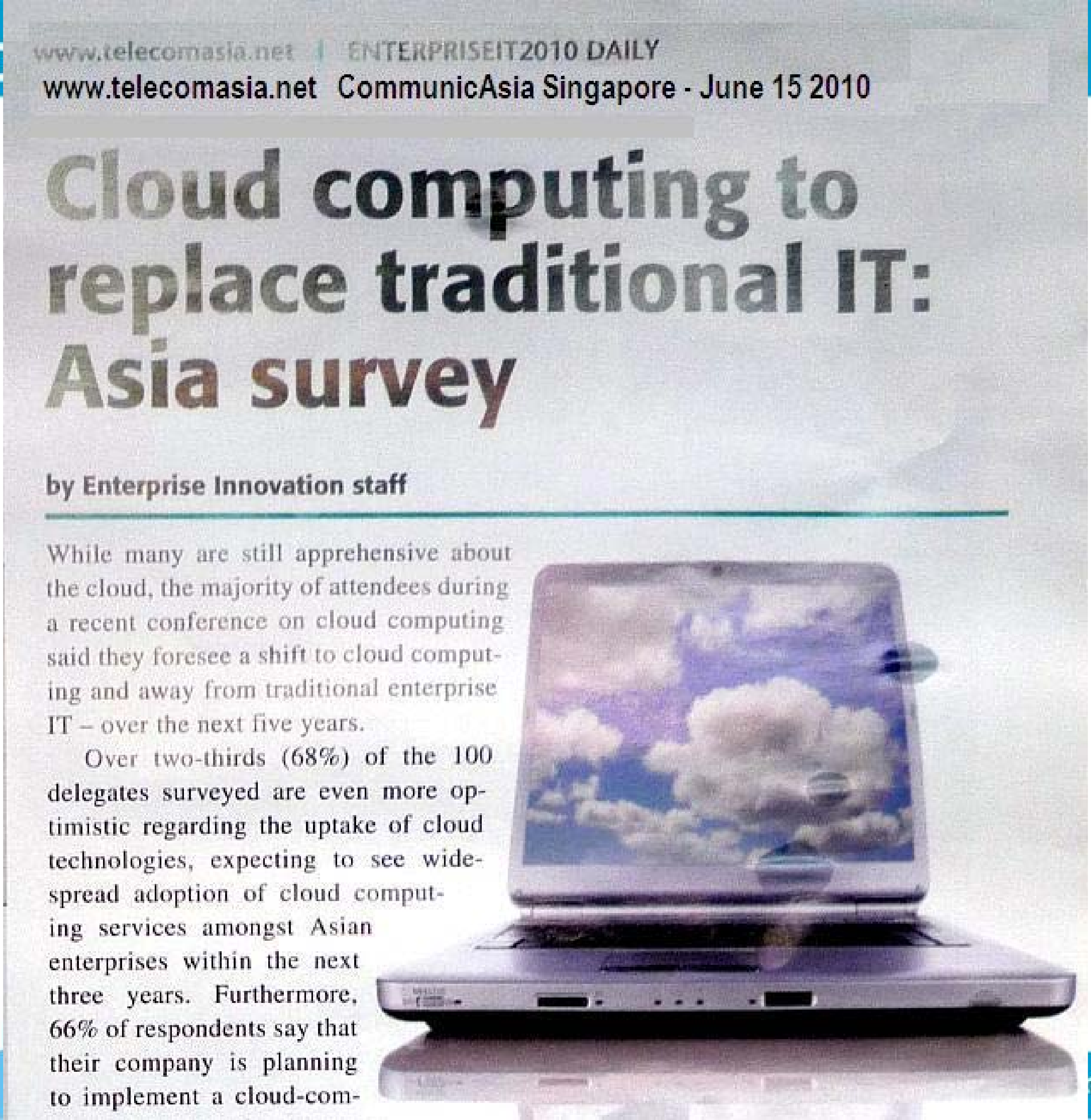
-> DATA LEAKAGE /LOSS

-> S.O.A., S.A.A.S. -> CLOUD COMPUTING

- **APPLICATION AS A SERVICE**
- **PLATFORM AS A SERVICE**
- ***SERVICE AS A SERVICE (?!)***

Inno

IBM



www.telecomasia.net | ENTERPRISEIT2010 DAILY

www.telecomasia.net CommunicAsia Singapore - June 15 2010

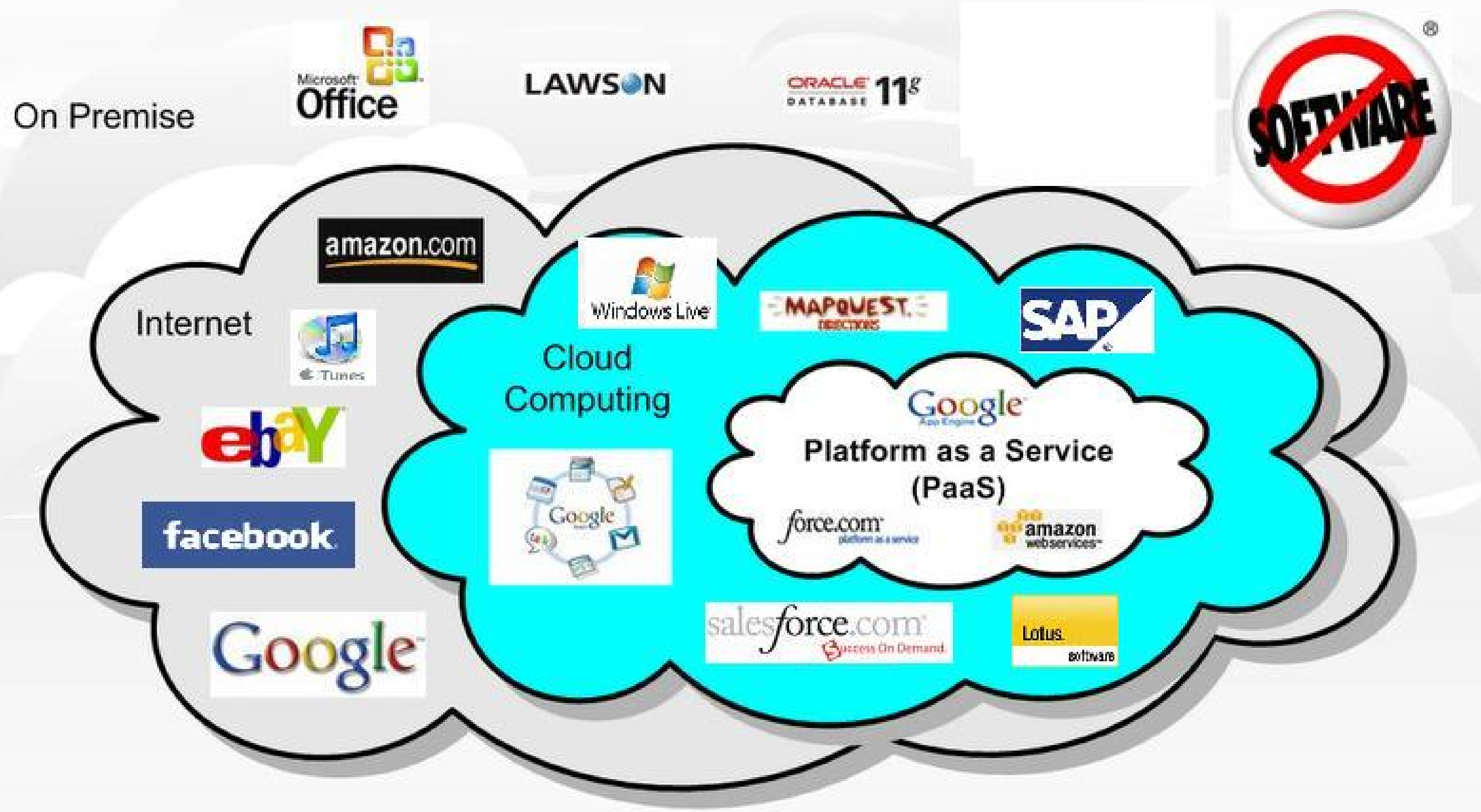
Cloud computing to replace traditional IT: Asia survey

by Enterprise Innovation staff

While many are still apprehensive about the cloud, the majority of attendees during a recent conference on cloud computing said they foresee a shift to cloud computing and away from traditional enterprise IT – over the next five years.

Over two-thirds (68%) of the 100 delegates surveyed are even more optimistic regarding the uptake of cloud technologies, expecting to see widespread adoption of cloud computing services amongst Asian enterprises within the next three years. Furthermore, 66% of respondents say that their company is planning to implement a cloud-com-

The Wonders of Cloud Computing



On Premise

Internet

Cloud Computing

Platform as a Service (PaaS)

PC **Laptop / Netbook** **Thin Client** **Mobile Device**

“The Network is the computer?!”

“The Internet Is The Cloud” (or vice versa?!)

Client-server Architecture? <-> Private Cloud? Virtualization? <-> What’s Where?! Thin Client?!

Welcome to THE SMARTER PLANET

Globalization and Globally Available Resources

- * Web 2.0
- • SOA
- • CLOUD

Billions of mobile devices accessing the Web

Access to streams of information in the Real Time

New Possibilities..

ITS ALL ABOUT SOFTWARE!

It Gets Worse

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

A hacker no longer needs a big machine

CLOUD COMPUTING SECURITY CONSIDERATIONS

Confidentiality:	**Data exposure & leakage**
Integrity:	**Data compromise**
Availability:	**Reliability of service, business continuity**

- Reduced Ability to Demonstrate Compliance:
- **Reduced Ability to Manage the Security Environment:**
- **Storage and Backup, disaster recover**

Can the provider segregate and protect individual groups of data within the remote, distributed shared environment?

- **Firewalls & IPS etc to prevent network/infra hacking attacks**
  - *Standard "perimeter defense" is still first and foremost!*
- **Viruses, worms, trojans, malware, bots …**
- **Identity and access management, user provisioning**
  - Authentication & Encryption
- **Availability – prevent againt Denial of Service**
- **Vigilant monitoring, S.I.E.M.**

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

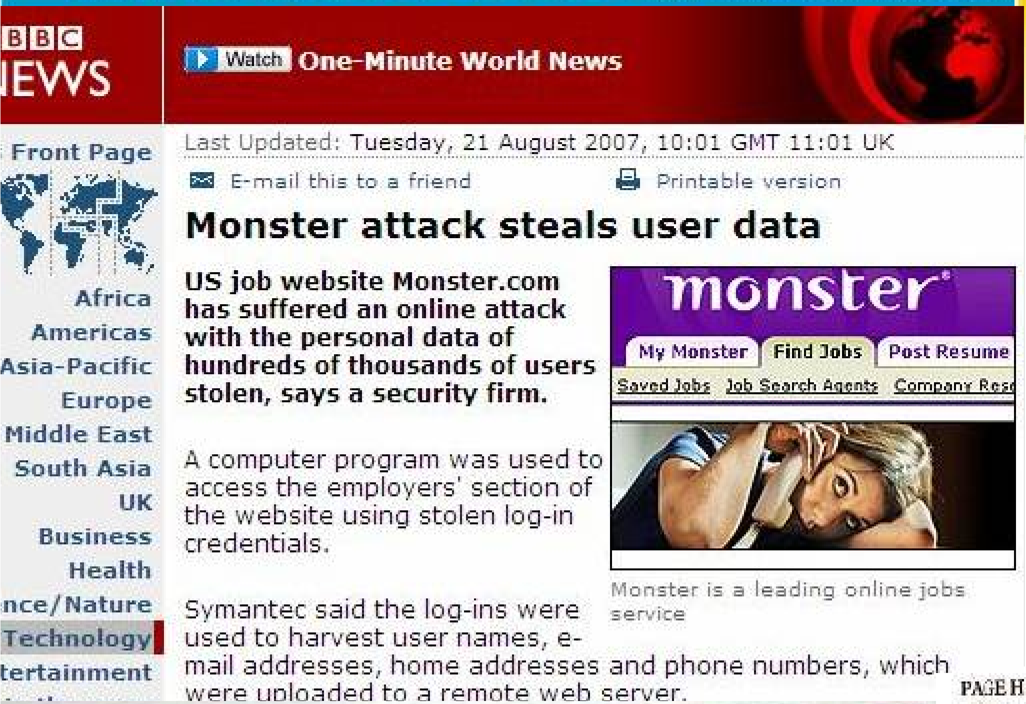
We Use Network Vulnerability Scanners

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 …



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

E-mail this to a friend   Printable version

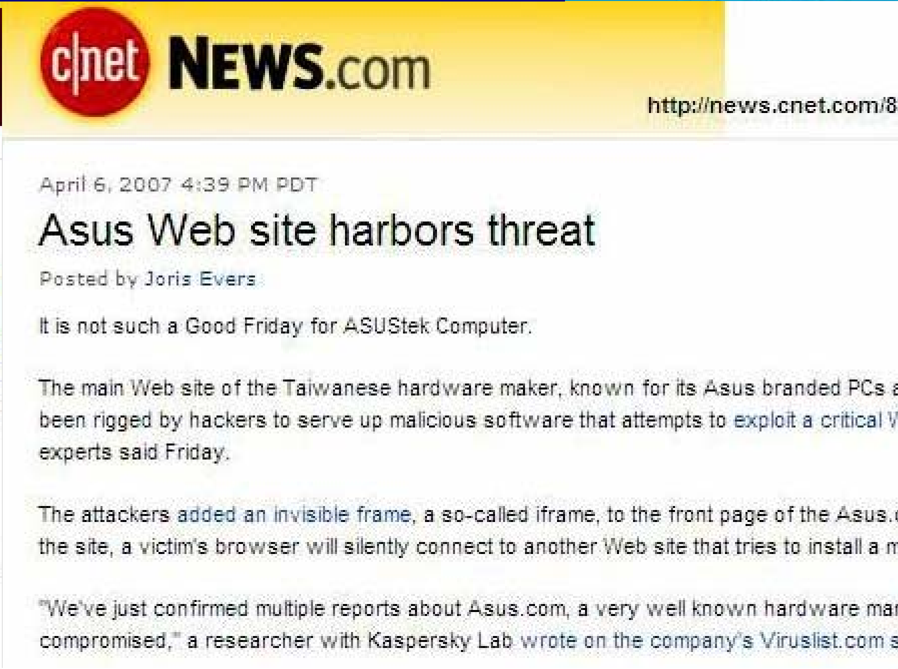
Monster attack steals user data

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.

Monster is a leading online jobs service

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.



April 6, 2007 4:39 PM PDT

Asus Web site harbors threat

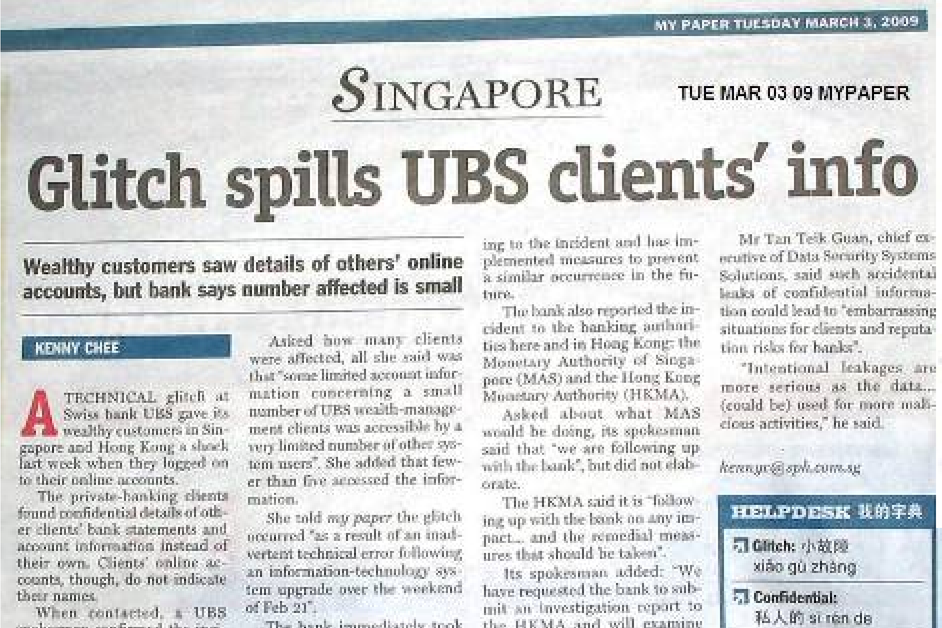
Posted by Joris Evers

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 W experts said Friday.

The attackers added an invisible frame, a so-called iframe, to the front page of the Asus. 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 ma 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 [illegible]

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 [illegible] 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 [illegible]

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".

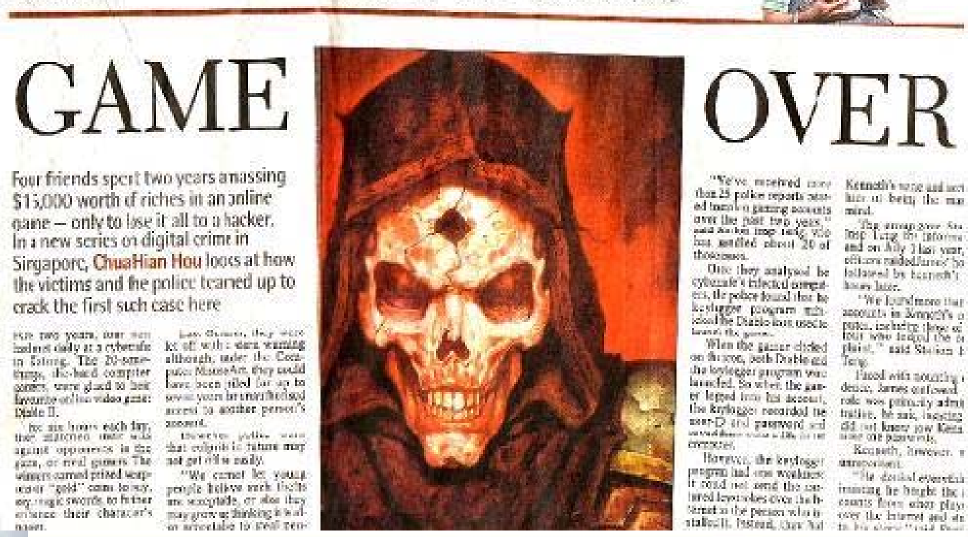
"Intentional leakages are more serious as the data... (could be) used for more malicious activities," he said.

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, Chua Hian Hou looks at how the victims and the police teamed up to crack the first such case here

For two years, four men [illegible] daily at a cybercafe in [illegible]. The 20-something, die-hard computer gamers, were glued to their favourite online video game: Diablo II.

For six hours each day, they matched their skills against opponents in the game, or rival gamers. The winners earned prized weapons, "gold" coins to buy magic swords to further enhance their character's power.

[illegible], they were let off with a stern warning although, under the Computer Misuse Act, they could have been jailed for up to seven years for unauthorised access to another person's account.

However, police warn that culprits in future may not get off so easily.

"We cannot let young people believe such thefts are acceptable, or else they may grow up thinking it is all right to steal [illegible]

"We've received more than 25 police reports related to hacking gaming accounts over the past two years," said [illegible], who has handled about 20 of those cases.

Once they analysed the cybercafe's infected computers, the police found that the keylogger program was linked to the Diablo icon used to launch the game.

When the gamer clicked on the icon, both Diablo and the keylogger program were launched. So when the gamer logged into his account, the keylogger recorded the user-ID and password and [illegible] computer.

However, the keylogger program had one weakness: it could not send the captured keystrokes over the Internet to the person who installed it. Instead, [illegible]

Kenneth's [illegible] mind.

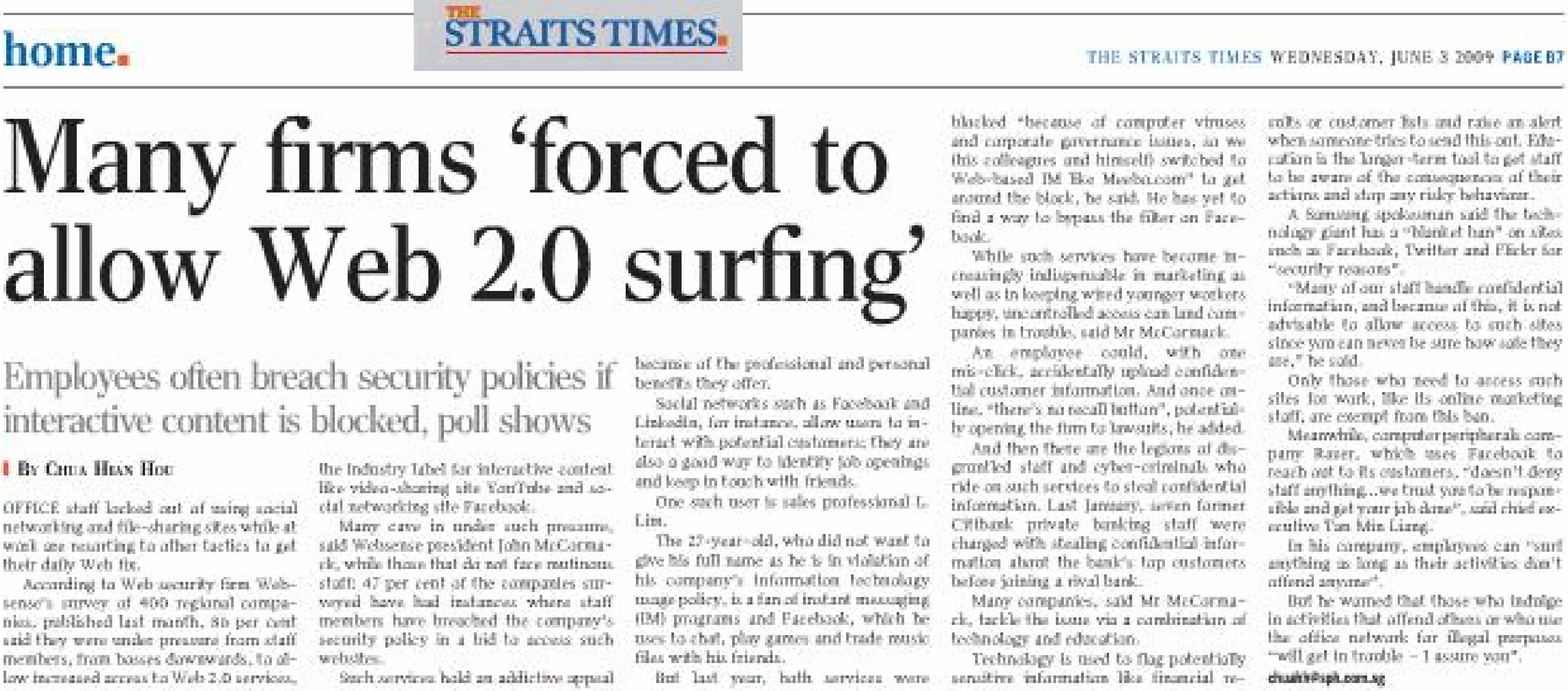
[illegible] and on July 1 last year, officers [illegible] followed by Kenneth's hours later.

"We found more than [illegible] accounts in Kenneth's [illegible], including those of [illegible] four who lodged the [illegible]," said [illegible].

Faced with [illegible], James [illegible] role was primarily [illegible] he said, [illegible] did not know how Kenn[illegible] some [illegible] passwords.

Kenneth, however, [illegible].

"He denied [illegible] he bought the [illegible] counts from other play[illegible] over the Internet and [illegible]



home.

THE STRAITS TIMES

THE STRAITS TIMES WEDNESDAY, JUNE 3 2009 PAGE B7

Many firms 'forced to allow Web 2.0 surfing'

Employees often breach security policies if interactive content is blocked, poll shows

By Chua Hian Hou

OFFICE staff locked out of using social networking and file-sharing sites while at work are resorting to other tactics to get their daily Web fix.

According to Web security firm Websense's survey of 400 regional companies, published last month, 86 per cent said they were under pressure from staff members, from bosses downwards, to allow increased access to Web 2.0 services, the industry label for interactive content like video-sharing site YouTube and social networking site Facebook.

Many cave in under such pressure, said Websense president John McCormack, while those that do not face mutinous staff: 47 per cent of the companies surveyed have had instances where staff members have breached the company's security policy in a bid to access such websites.

Such services hold an addictive appeal because of the professional and personal benefits they offer.

Social networks such as Facebook and LinkedIn, for instance, allow users to interact with potential customers; they are also a good way to identify job openings and keep in touch with friends.

One such user is sales professional L. Lim.

The 27-year-old, who did not want to give his full name as he is in violation of his company's information technology usage policy, is a fan of instant messaging (IM) programs and Facebook, which he uses to chat, play games and trade music files with his friends.

But last year, both services were blocked "because of computer viruses and corporate governance issues, so we (his colleagues and himself) switched to Web-based IM like Meebo.com" to get around the block, he said. He has yet to find a way to bypass the filter on Facebook.

While such services have become increasingly indispensable in marketing as well as in keeping wired younger workers happy, uncontrolled access can land companies in trouble, said Mr McCormack.

An employee could, with one mis-click, accidentally upload confidential customer information. And once online, "there's no recall button", potentially opening the firm to lawsuits, he added.

And then there are the legions of disgruntled staff and cyber-criminals who ride on such services to steal confidential information. Last January, seven former Citibank private banking staff were charged with stealing confidential information about the bank's top customers before joining a rival bank.

Many companies, said Mr McCormack, tackle the issue via a combination of technology and education.

Technology is used to flag potentially sensitive information like financial records or customer lists and raise an alert when someone tries to send this out. Education is the longer-term tool to get staff to be aware of the consequences of their actions and stop any risky behaviour.

A Samsung spokesman said the technology giant has a "blanket ban" on sites such as Facebook, Twitter and Flickr for "security reasons".

"Many of our staff handle confidential information, and because of this, it is not advisable to allow access to such sites since you can never be sure how safe they are," he said.

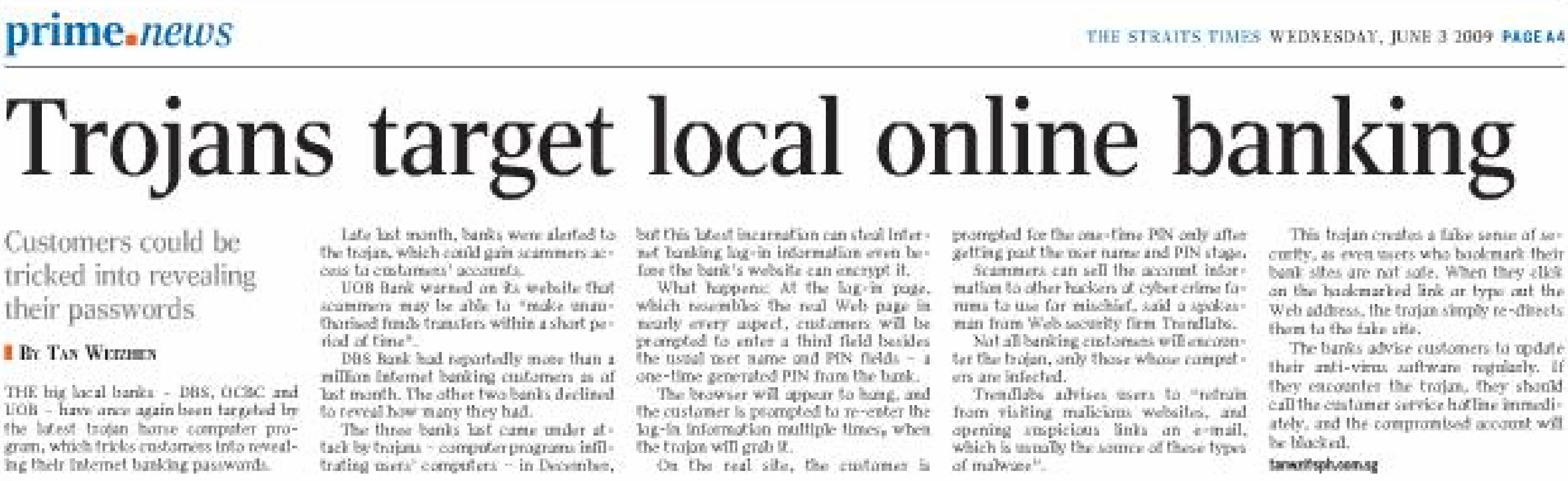
Only those who need to access such sites for work, like its online marketing staff, are exempt from this ban.

Meanwhile, computer peripherals company Razer, which uses Facebook to reach out to its customers, "doesn't deny staff anything...we trust you to be responsible and get your job done", said chief executive Tan Min Liang.

In his company, employees can "surf anything as long as their activities don't offend anyone".

But he warned that those who indulge in activities that offend others or who use the office network for illegal purposes "will get in trouble – I assure you".

chuahh@sph.com.sg



prime.news

THE STRAITS TIMES WEDNESDAY, JUNE 3 2009 PAGE A4

Trojans target local online banking

Customers could be tricked into revealing their passwords

By Tan Weizhen

THE big local banks – DBS, OCBC and UOB – have once again been targeted by the latest trojan horse computer program, which tricks customers into revealing their Internet banking passwords.

Late last month, banks were alerted to the trojan, which could gain scammers access to customers' accounts.

UOB Bank warned on its website that scammers may be able to "make unauthorised funds transfers within a short period of time".

DBS Bank had reportedly more than a million Internet banking customers as of last month. The other two banks declined to reveal how many they had.

The three banks last came under attack by trojans – computer programs infiltrating users' computers – in December, but this latest incarnation can steal Internet banking log-in information even before the bank's website can encrypt it.

What happens: At the log-in page, which resembles the real Web page in nearly every aspect, customers will be prompted to enter a third field besides the usual user name and PIN fields – a one-time generated PIN from the bank.

The browser will appear to hang, and the customer is prompted to re-enter the log-in information multiple times, when the trojan will grab it.

On the real site, the customer is prompted for the one-time PIN only after getting past the user name and PIN stage.

Scammers can sell the account information to other hackers or cyber crime forums to use for mischief, said a spokesman from Web security firm Trendlabs.

Not all banking customers will encounter the trojan, only those whose computers are infected.

Trendlabs advises users to "refrain from visiting malicious websites, and opening suspicious links on e-mail, which is usually the source of these types of malware".

This trojan creates a false sense of security, as even users who bookmark their bank sites are not safe. When they click on the bookmarked link or type out the Web address, the trojan simply re-directs them to the fake site.

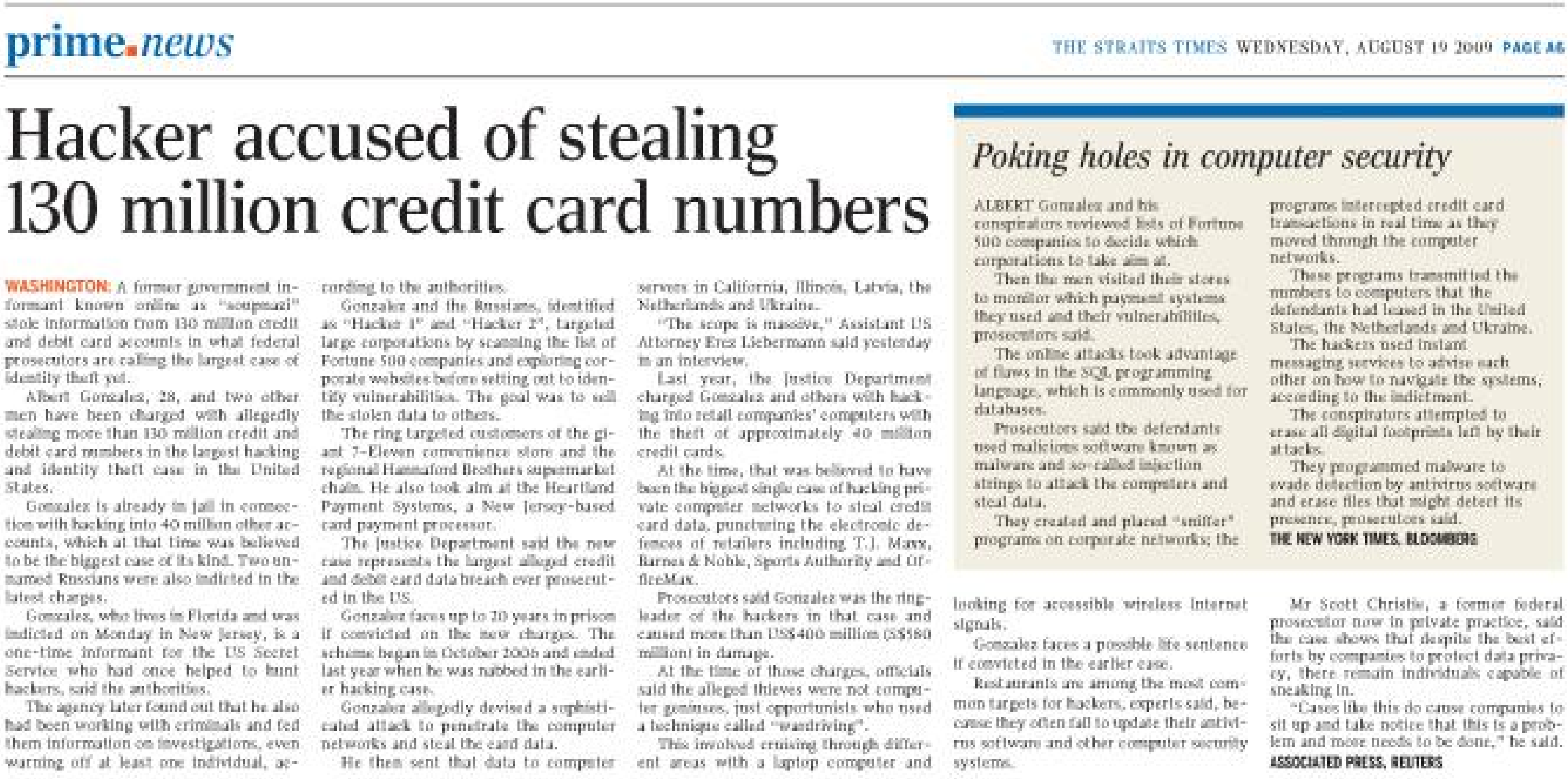
The banks advise customers to update their anti-virus software regularly. If they encounter the trojan, they should call the customer service hotline immediately, and the compromised account will be blocked.

tanwz@sph.com.sg

WORST CREDIT CARD IDENTITY THEFT CASE

- DONE BY A SOFTWARE 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 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.

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

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
sites of vari
with plenty
as addresses
phone numb

SSMG me
very hard

No hacki
needed. All
gines such as
tion fell into

In one ca
word of a

popped up. With these, a hacker could use the server of 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.

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."

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 300 students on "human error", and said steps have been taken to prevent any recurrence.

Mr Tjoe, 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

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

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

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".

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 19.2 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.

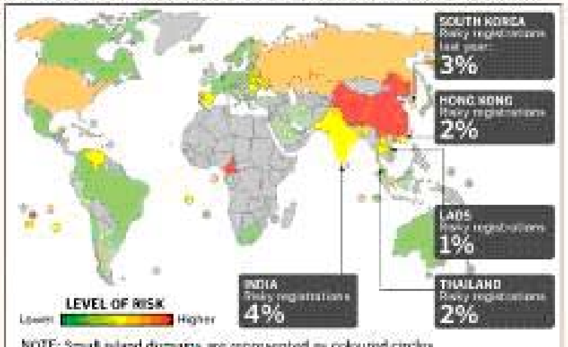
Another factor lies in the ease of the

RISKY BUSINESS

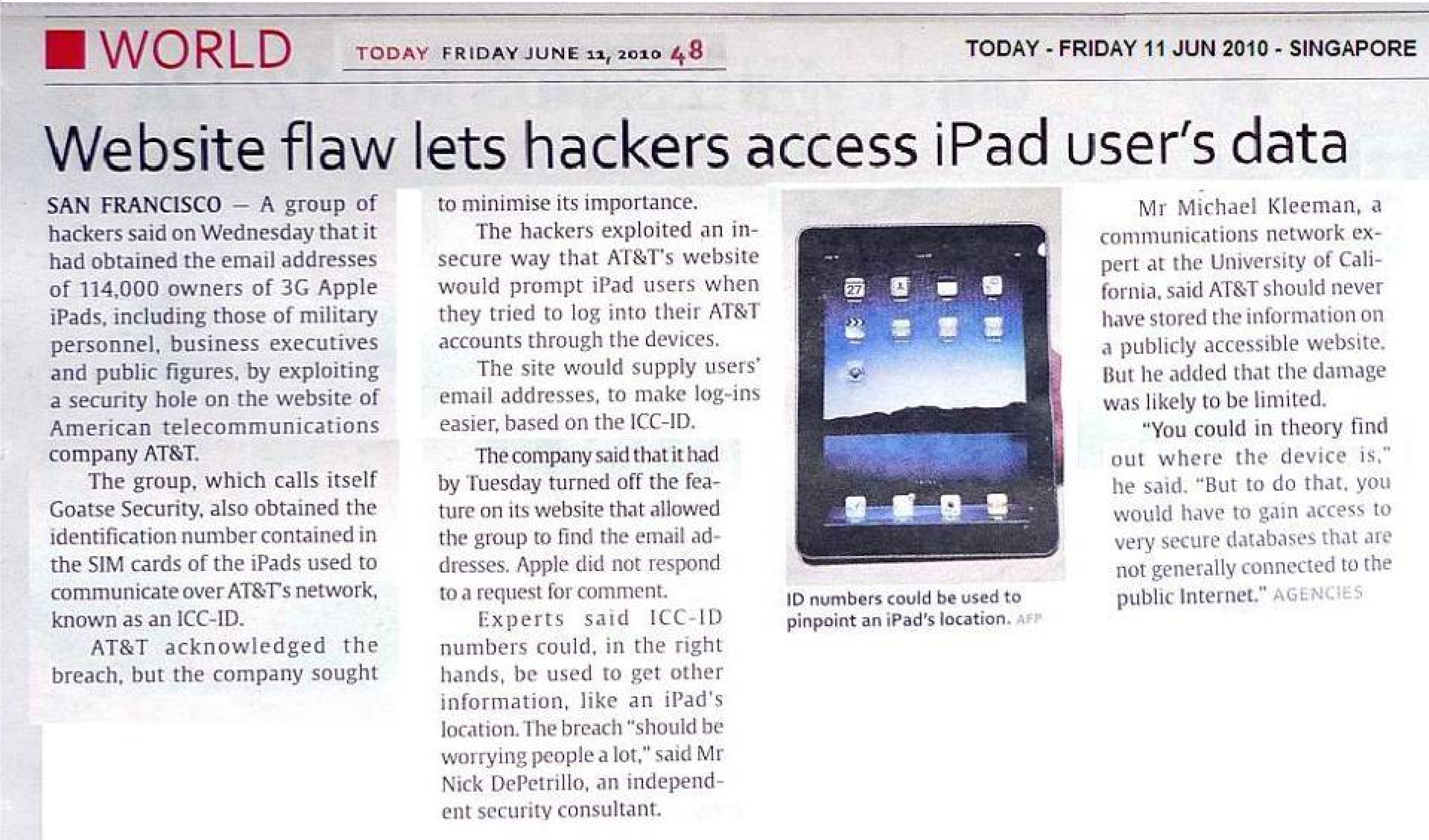
More websites registered here in 2009 were spam sites or had viruses and malware, a huge jump from the previous year.

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.



WORLD TODAY FRIDAY JUNE 11, 2010 48

TODAY - FRIDAY 11 JUN 2010 - SINGAPORE

Website flaw lets hackers access iPad user's data

SAN FRANCISCO — A group of hackers said on Wednesday that it had obtained the email addresses of 114,000 owners of 3G Apple iPads, including those of military personnel, business executives and public figures, by exploiting a security hole on the website of American telecommunications company AT&T.

The group, which calls itself Goatse Security, also obtained the identification number contained in the SIM cards of the iPads used to communicate over AT&T's network, known as an ICC-ID.

AT&T acknowledged the breach, but the company sought to minimise its importance.

The hackers exploited an insecure way that AT&T's website would prompt iPad users when they tried to log into their AT&T accounts through the devices.

The site would supply users' email addresses, to make log-ins easier, based on the ICC-ID.

The company said that it had by Tuesday turned off the feature on its website that allowed the group to find the email addresses. Apple did not respond to a request for comment.

Experts said ICC-ID numbers could, in the right hands, be used to get other information, like an iPad's location. The breach "should be worrying people a lot," said Mr Nick DePetrillo, an independent security consultant.

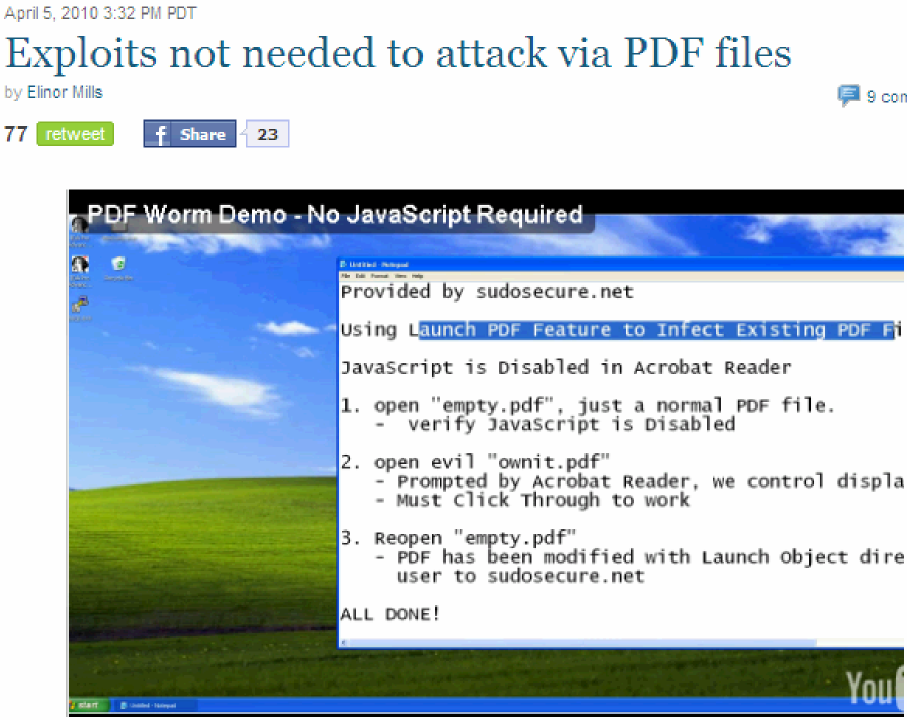
ID numbers could be used to pinpoint an iPad's location. AFP

Mr Michael Kleeman, a communications network expert at the University of California, said AT&T should never have stored the information on a publicly accessible website. But he added that the damage was likely to be limited.

"You could in theory find out where the device is," he said. "But to do that, you would have to gain access to very secure databases that are not generally connected to the public Internet." AGENCIES

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
- 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*



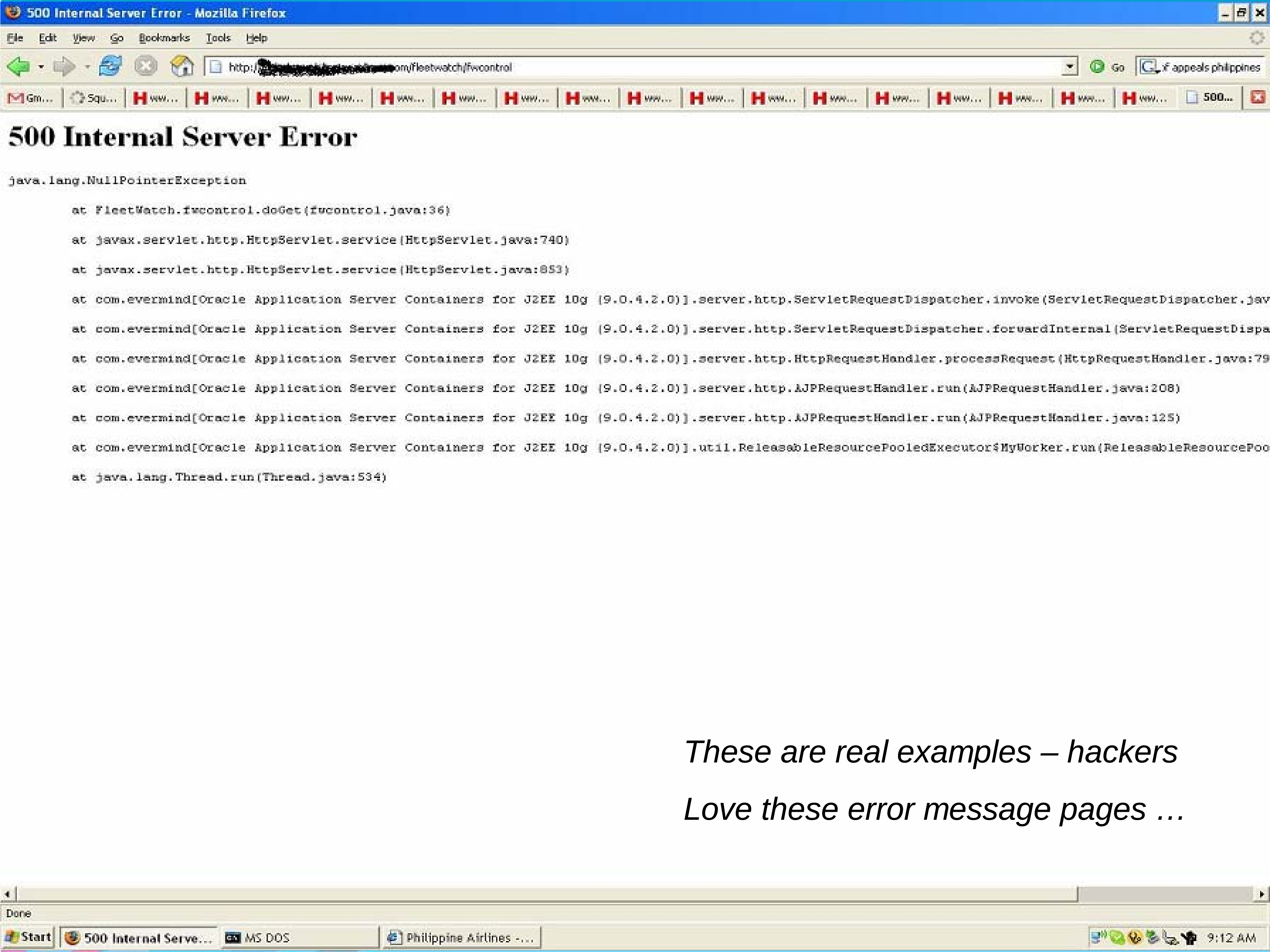
April 5, 2010 3:32 PM PDT

Exploits not needed to attack via PDF files

by Elinor Mills

```
Provided by sudosecure.net

Using Launch PDF Feature to Infect Existing PDF Fi

JavaScript is Disabled in Acrobat Reader

1. open "empty.pdf", just a normal PDF file.
   - verify JavaScript is Disabled

2. open evil "ownit.pdf"
   - Prompted by Acrobat Reader, we control displa
   - Must Click Through to work

3. Reopen "empty.pdf"
   - PDF has been modified with Launch object dire
     user to sudosecure.net

ALL DONE!
```

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



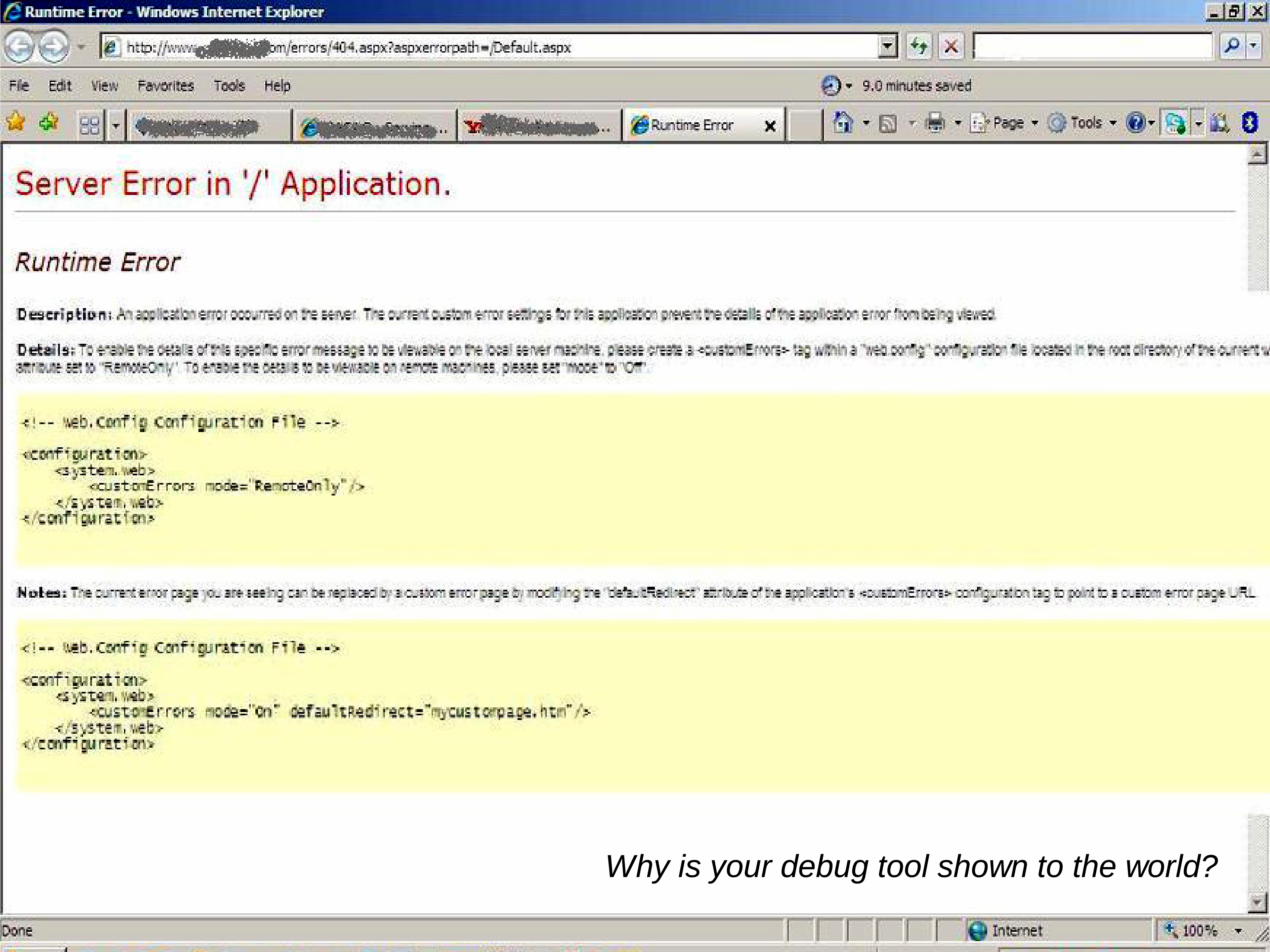
500 Internal Server Error - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://[redacted]om/fleetwatch/fwcontrol
Go
f appeals philippines
Gm... Squ... ww... ww... ww... ww... ww... ww... ww... ww... ww... ww... ww... ww... ww... ww... ww... ww... ww... 500...
Done
Start
500 Internal Serve...
MS DOS
Philippine Airlines -...
9:12 AM

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)
```

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
[redacted]
[redacted]
[redacted]
Runtime Error
Page
Tools
Done
Internet
100%

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.

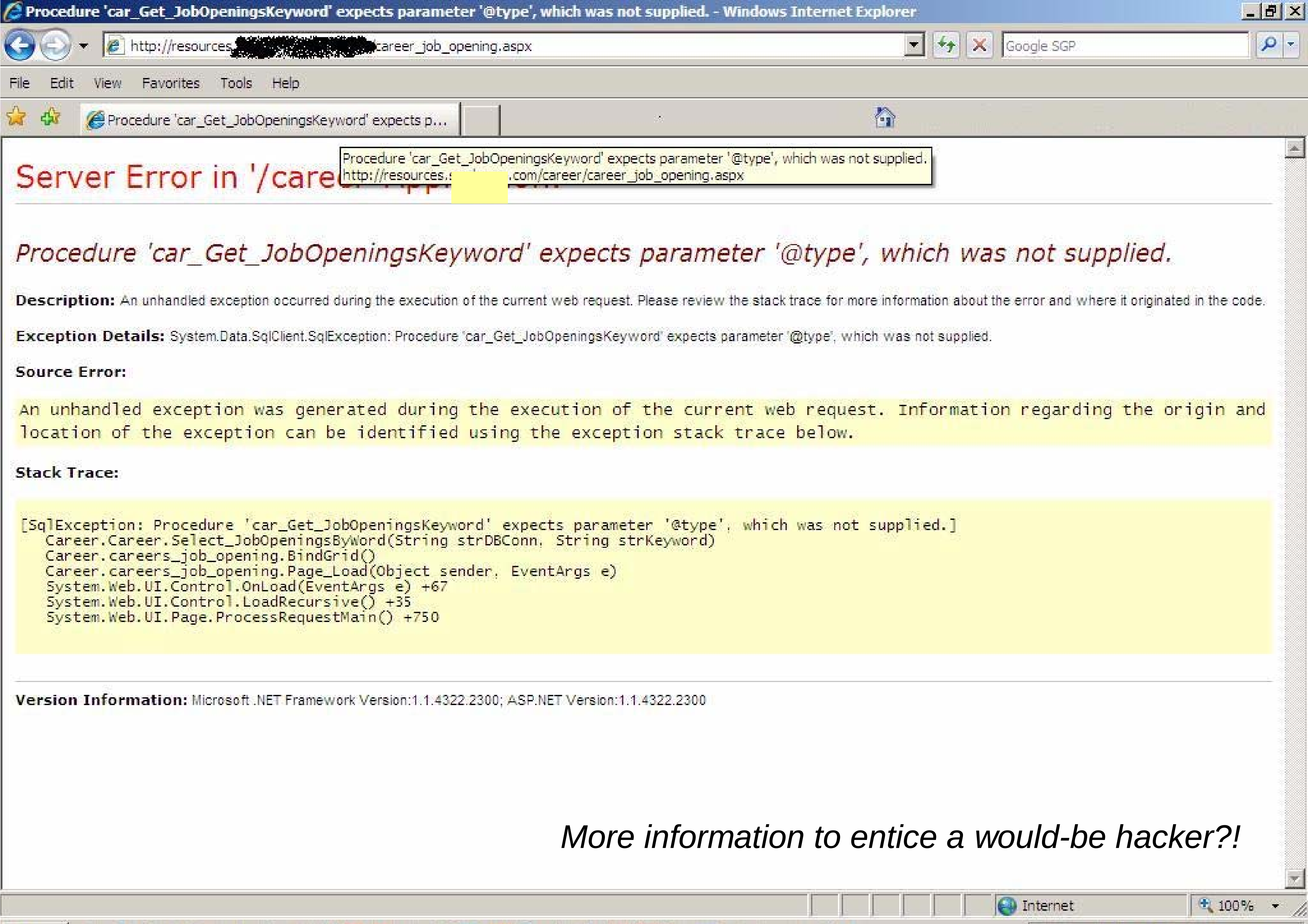
Details: To enable the details of this specific error message to be viewable on the local server machine, please create a <customErrors> tag within a "web.config" configuration file located in the root directory of the current w
attribute set to "RemoteOnly". To enable the details to be viewable on remote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


Procedure 'car_Get_JobOpeningsKeyword' expects parameter '@type', which was not supplied. - Windows Internet Explorer
http://resources[redacted]career_job_opening.aspx
Google SGP
File
Edit
View
Favorites
Tools
Help
Procedure 'car_Get_JobOpeningsKeyword' expects p...
Procedure 'car_Get_JobOpeningsKeyword' expects parameter '@type', which was not supplied.
http://resources.s[redacted].com/career/career_job_opening.aspx
Internet
100%

Server Error in '/care

Procedure 'car_Get_JobOpeningsKeyword' expects parameter '@type', which was not supplied.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Procedure 'car_Get_JobOpeningsKeyword' expects parameter '@type', which was not supplied.

Source Error:

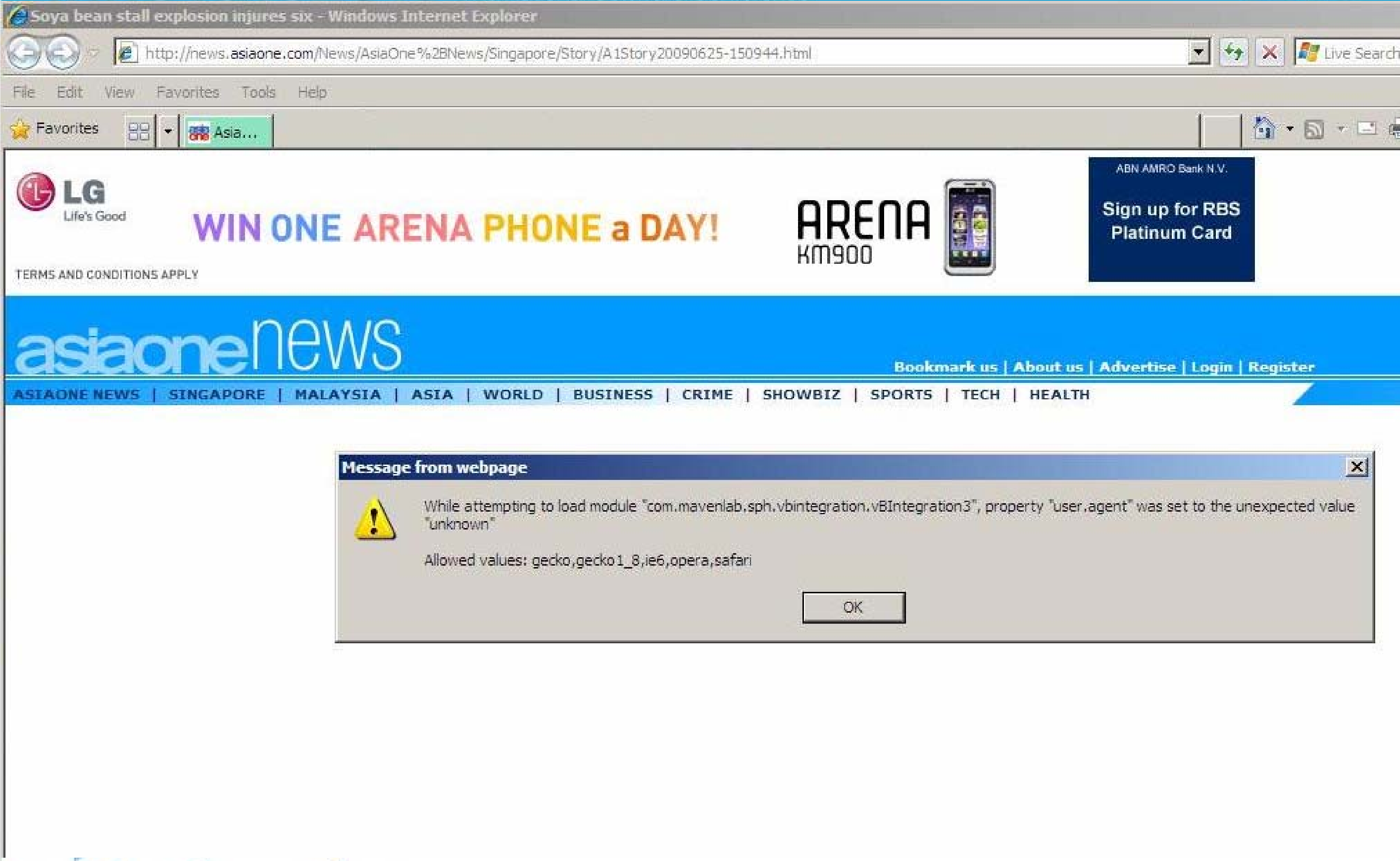
```
An unhandled exception was generated during the execution of the current web request. Information regarding the origin and
location of the exception can be identified using the exception stack trace below.
```

Stack Trace:

```
[SqlException: Procedure 'car_Get_JobOpeningsKeyword' expects parameter '@type', which was not supplied.]
   Career.Career.Select_JobOpeningsByWord(String strDBConn, String strKeyword)
   Career.careers_job_opening.BindGrid()
   Career.careers_job_opening.Page_Load(Object sender, EventArgs e)
   System.Web.UI.Control.OnLoad(EventArgs e) +67
   System.Web.UI.Control.LoadRecursive() +35
   System.Web.UI.Page.ProcessRequestMain() +750
```

Version Information: Microsoft .NET Framework Version:1.1.4322.2300; ASP.NET Version:1.1.4322.2300

More information to entice a would-be hacker?!



Soya bean stall explosion injures six - Windows Internet Explorer

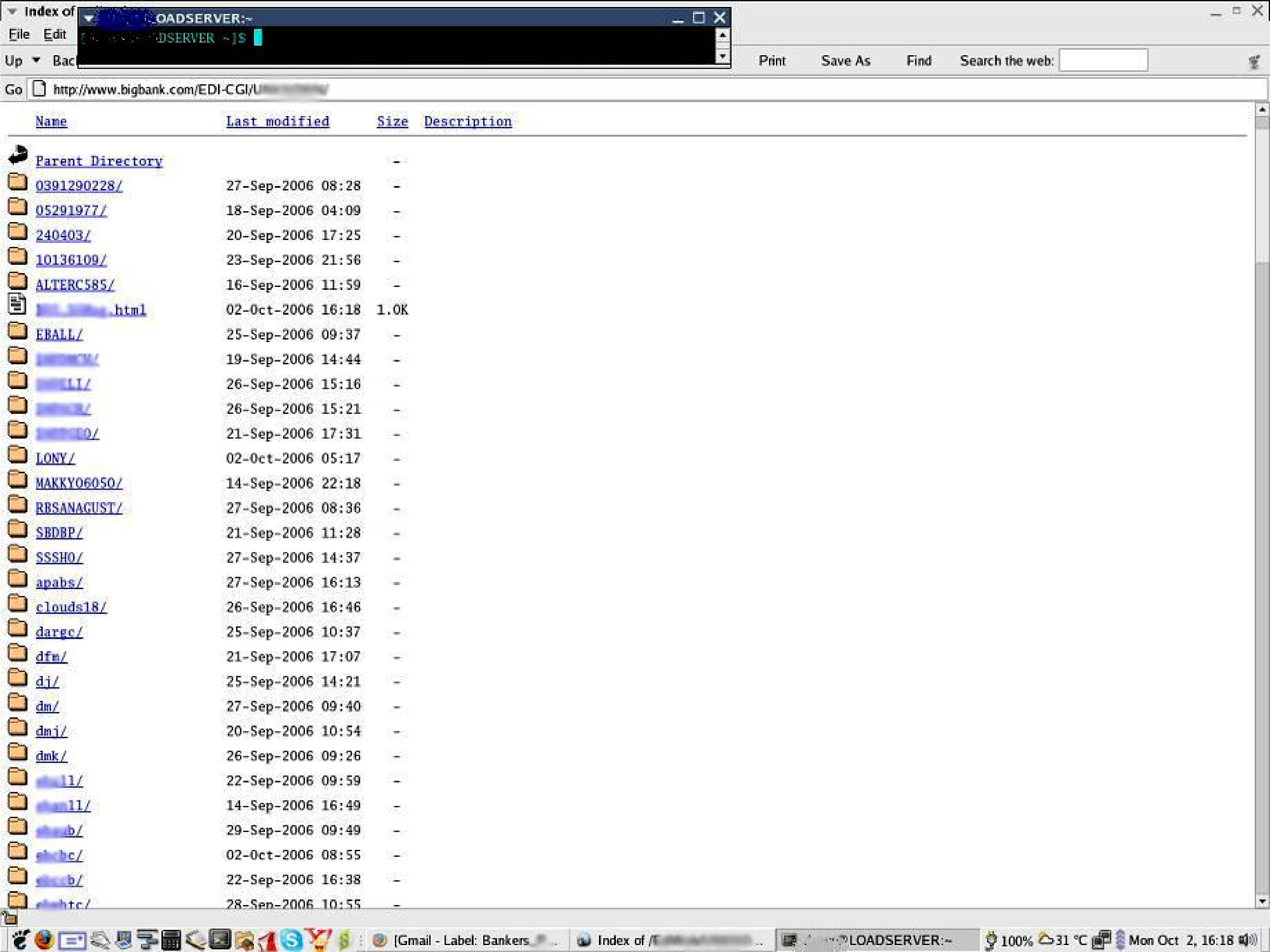
http://news.asiaone.com/News/AsiaOne%2BNews/Singapore/Story/A1Story20090625-150944.html

Live Search
File
Edit
View
Favorites
Tools
Help
Favorites
Asia...
LG Life's Good
WIN ONE ARENA PHONE a DAY!
TERMS AND CONDITIONS APPLY
ARENA KM900
ABN AMRO Bank N.V.
Sign up for RBS Platinum Card
asiaonenews
Bookmark us | About us | Advertise | Login | Register
ASIAONE NEWS | SINGAPORE | MALAYSIA | ASIA | WORLD | BUSINESS | CRIME | SHOWBIZ | SPORTS | TECH | HEALTH

Message from webpage

While attempting to load module "com.mavenlab.sph.vbintegration.vBIntegration3", property "user.agent" was set to the unexpected value "unknown"

Allowed values: gecko,gecko1_8,ie6,opera,safari

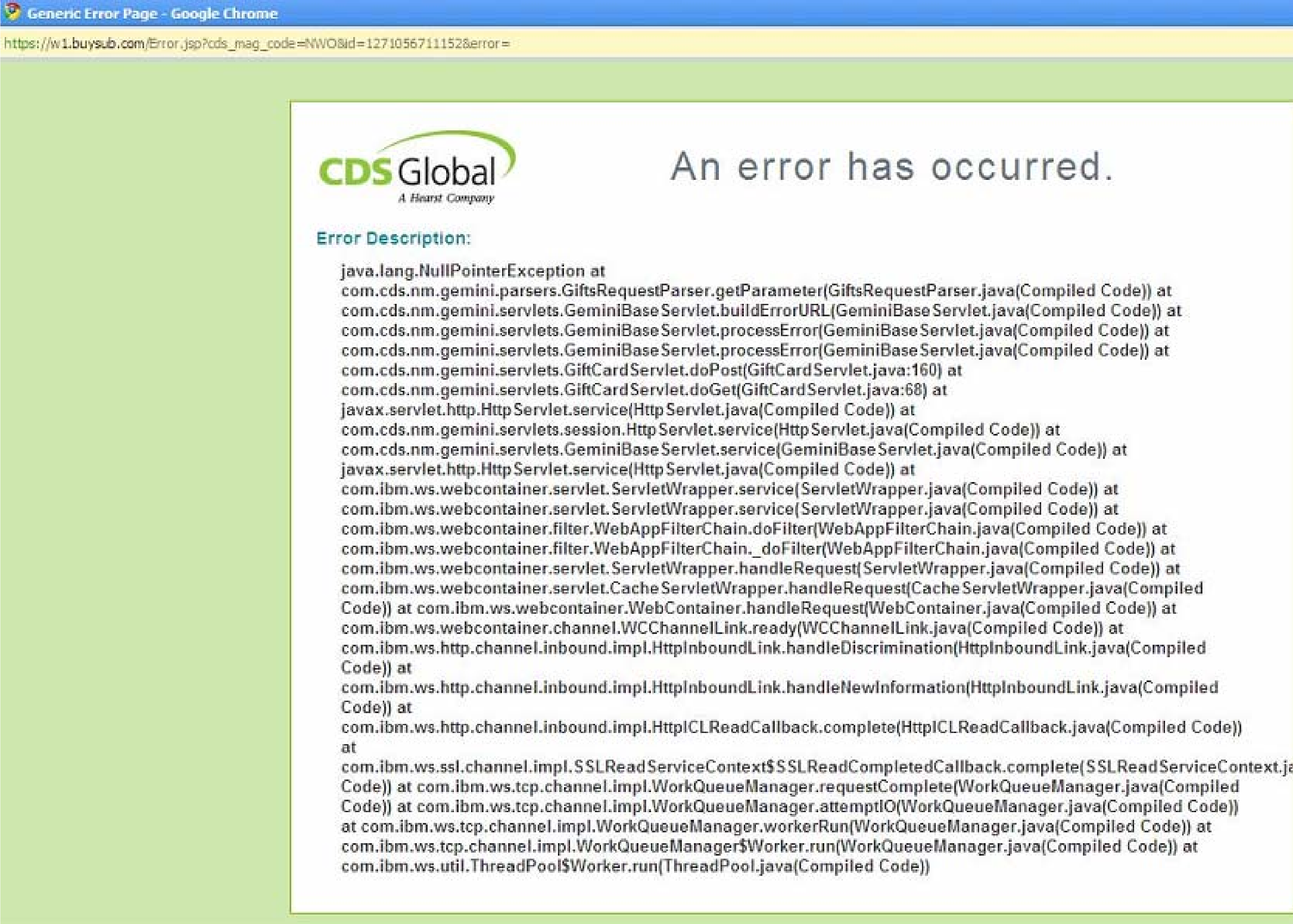


[redacted]LOADSERVER:~

```
[redacted]DSERVER ~]$
```

http://www.bigbank.com/EDI-CGI/U[redacted]

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	-	
[redacted].html	02-Oct-2006 16:18	1.0K	
EBALL/	25-Sep-2006 09:37	-	
[redacted]/	19-Sep-2006 14:44	-	
[redacted]LI/	26-Sep-2006 15:16	-	
[redacted]/	26-Sep-2006 15:21	-	
[redacted]O/	21-Sep-2006 17:31	-	
LONY/	02-Oct-2006 05:17	-	
MAKKY06050/	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	-	
[redacted]ll/	22-Sep-2006 09:59	-	
[redacted]ll/	14-Sep-2006 16:49	-	
[redacted]b/	29-Sep-2006 09:49	-	
[redacted]bc/	02-Oct-2006 08:55	-	
[redacted]b/	22-Sep-2006 16:38	-	
[redacted]tc/	28-Sep-2006 10:55	-	



https://w1.buysub.com/Error.jsp?cds_mag_code=NWO&id=1271056711152&error=

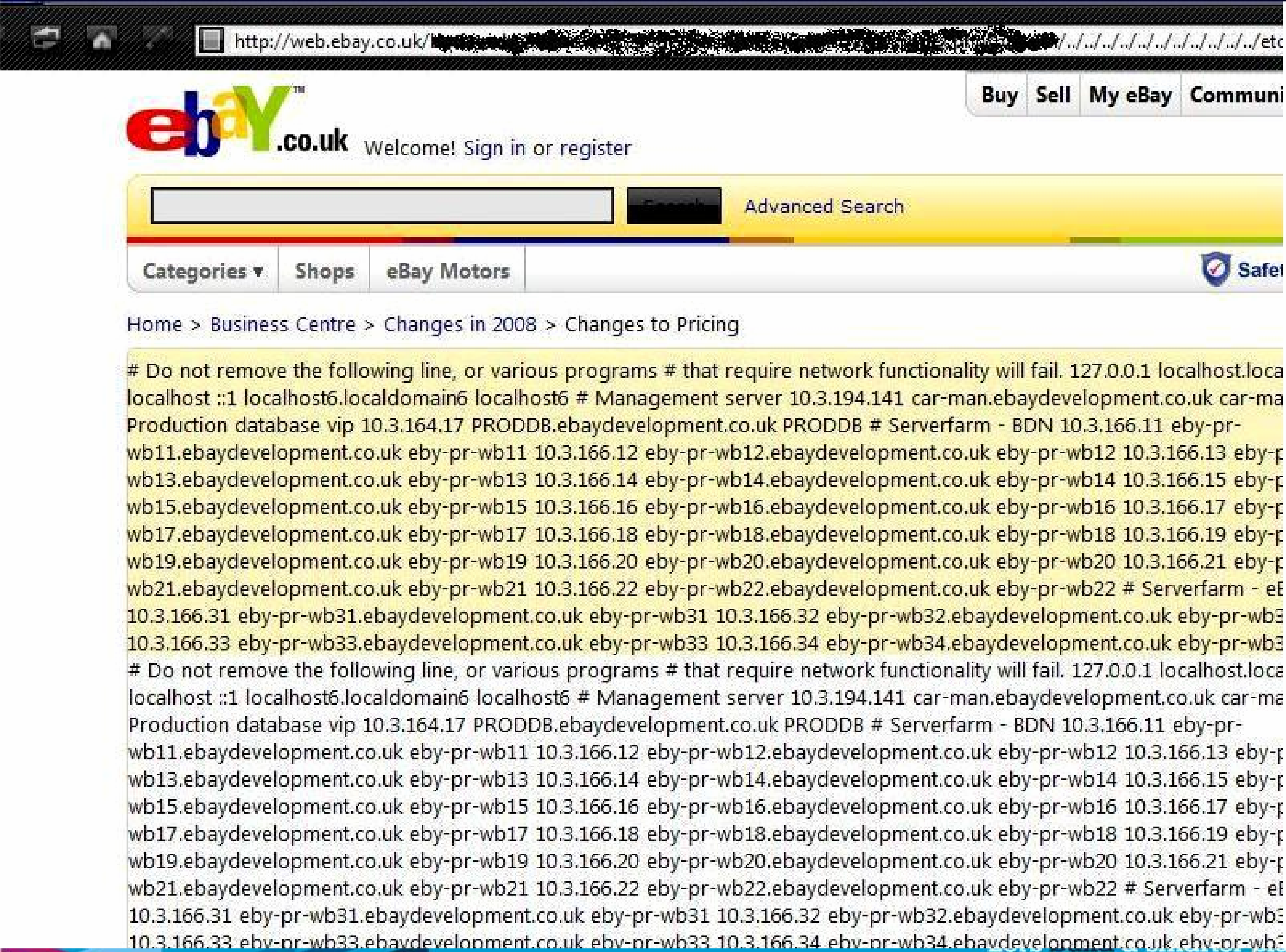
An error has occurred.

Error Description:

```
java.lang.NullPointerException at
com.cds.nm.gemini.parsers.GiftsRequestParser.getParameter(GiftsRequestParser.java(Compiled Code)) at
com.cds.nm.gemini.servlets.GeminiBaseServlet.buildErrorURL(GeminiBaseServlet.java(Compiled Code)) at
com.cds.nm.gemini.servlets.GeminiBaseServlet.processError(GeminiBaseServlet.java(Compiled Code)) at
com.cds.nm.gemini.servlets.GeminiBaseServlet.processError(GeminiBaseServlet.java(Compiled Code)) at
com.cds.nm.gemini.servlets.GiftCardServlet.doPost(GiftCardServlet.java:160) at
com.cds.nm.gemini.servlets.GiftCardServlet.doGet(GiftCardServlet.java:68) at
javax.servlet.http.HttpServlet.service(HttpServlet.java(Compiled Code)) at
com.cds.nm.gemini.servlets.session.HttpServlet.service(HttpServlet.java(Compiled Code)) at
com.cds.nm.gemini.servlets.GeminiBaseServlet.service(GeminiBaseServlet.java(Compiled Code)) at
javax.servlet.http.HttpServlet.service(HttpServlet.java(Compiled Code)) at
com.ibm.ws.webcontainer.servlet.ServletWrapper.service(ServletWrapper.java(Compiled Code)) at
com.ibm.ws.webcontainer.servlet.ServletWrapper.service(ServletWrapper.java(Compiled Code)) at
com.ibm.ws.webcontainer.filter.WebAppFilterChain.doFilter(WebAppFilterChain.java(Compiled Code)) at
com.ibm.ws.webcontainer.filter.WebAppFilterChain._doFilter(WebAppFilterChain.java(Compiled Code)) at
com.ibm.ws.webcontainer.servlet.ServletWrapper.handleRequest(ServletWrapper.java(Compiled Code)) at
com.ibm.ws.webcontainer.servlet.CacheServletWrapper.handleRequest(CacheServletWrapper.java(Compiled
Code)) at com.ibm.ws.webcontainer.WebContainer.handleRequest(WebContainer.java(Compiled Code)) at
com.ibm.ws.webcontainer.channel.WCChannelLink.ready(WCChannelLink.java(Compiled Code)) at
com.ibm.ws.http.channel.inbound.impl.HttpInboundLink.handleDiscrimination(HttpInboundLink.java(Compiled
Code)) at
com.ibm.ws.http.channel.inbound.impl.HttpInboundLink.handleNewInformation(HttpInboundLink.java(Compiled
Code)) at
com.ibm.ws.http.channel.inbound.impl.HttpICLReadCallback.complete(HttpICLReadCallback.java(Compiled Code))
at
com.ibm.ws.ssl.channel.impl.SSLReadServiceContext$SSLReadCompletedCallback.complete(SSLReadServiceContext.ja
Code)) at com.ibm.ws.tcp.channel.impl.WorkQueueManager.requestComplete(WorkQueueManager.java(Compiled
Code)) at com.ibm.ws.tcp.channel.impl.WorkQueueManager.attemptIO(WorkQueueManager.java(Compiled Code))
at com.ibm.ws.tcp.channel.impl.WorkQueueManager.workerRun(WorkQueueManager.java(Compiled Code)) at
com.ibm.ws.tcp.channel.impl.WorkQueueManager$Worker.run(WorkQueueManager.java(Compiled Code)) at
com.ibm.ws.util.ThreadPool$Worker.run(ThreadPool.java(Compiled Code))
```

International Service for Renewal of Paper-mailed Magazine Subscription

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



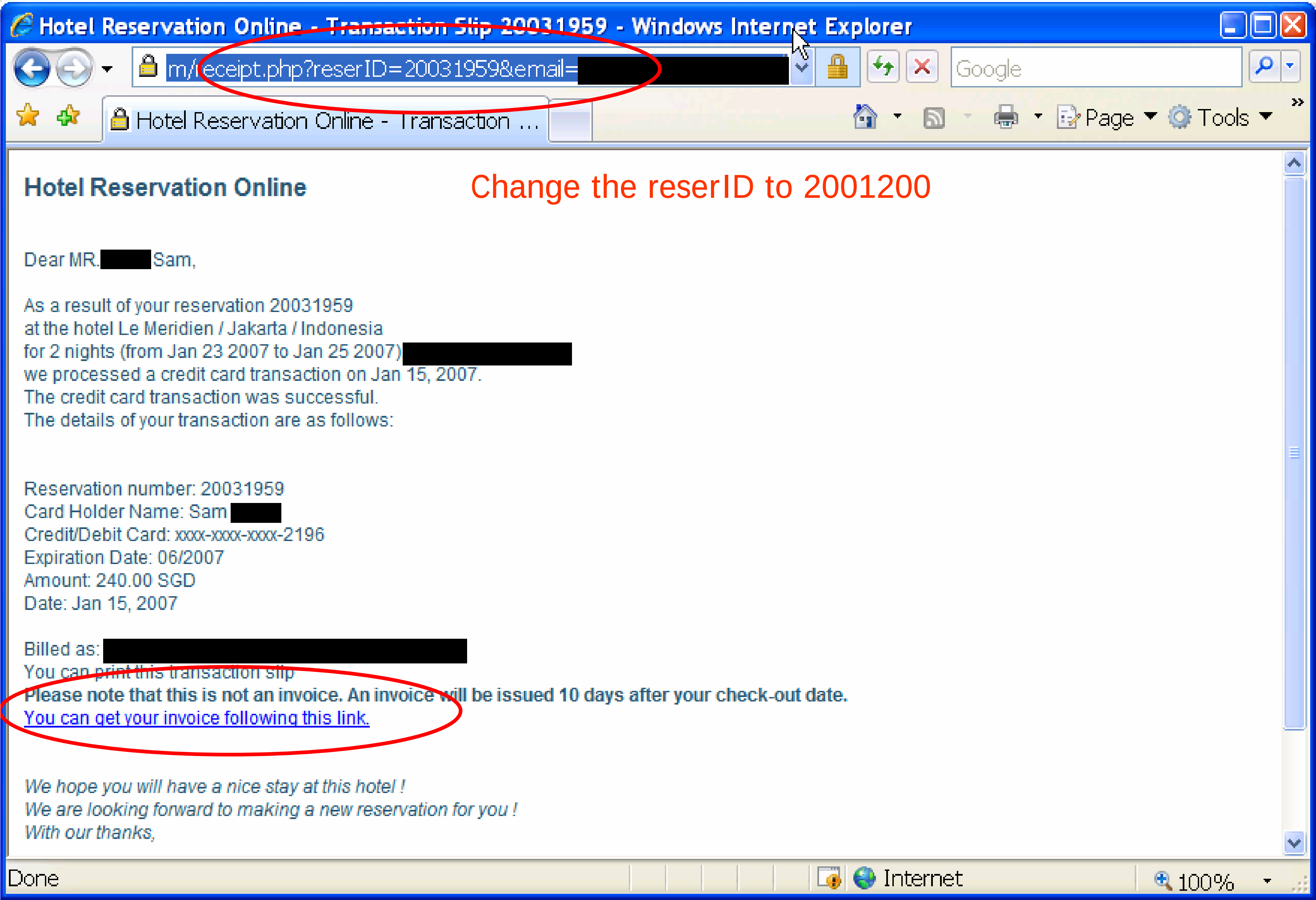
http://web.ebay.co.uk/[redacted]/../../../../../../../../../../../etc
Buy
Sell
My eBay
Communi
ebay.co.uk
Welcome! Sign in or register
Advanced Search
Categories ▾
Shops
eBay Motors
Safe

Home > Business Centre > Changes in 2008 > Changes to Pricing

```
# Do not remove the following line, or various programs # that require network functionality will fail. 127.0.0.1 localhost.loca
localhost ::1 localhost6.localdomain6 localhost6 # Management server 10.3.194.141 car-man.ebaydevelopment.co.uk car-ma
Production database vip 10.3.164.17 PRODDB.ebaydevelopment.co.uk PRODDB # Serverfarm - BDN 10.3.166.11 eby-pr-
wb11.ebaydevelopment.co.uk eby-pr-wb11 10.3.166.12 eby-pr-wb12.ebaydevelopment.co.uk eby-pr-wb12 10.3.166.13 eby-p
wb13.ebaydevelopment.co.uk eby-pr-wb13 10.3.166.14 eby-pr-wb14.ebaydevelopment.co.uk eby-pr-wb14 10.3.166.15 eby-p
wb15.ebaydevelopment.co.uk eby-pr-wb15 10.3.166.16 eby-pr-wb16.ebaydevelopment.co.uk eby-pr-wb16 10.3.166.17 eby-p
wb17.ebaydevelopment.co.uk eby-pr-wb17 10.3.166.18 eby-pr-wb18.ebaydevelopment.co.uk eby-pr-wb18 10.3.166.19 eby-p
wb19.ebaydevelopment.co.uk eby-pr-wb19 10.3.166.20 eby-pr-wb20.ebaydevelopment.co.uk eby-pr-wb20 10.3.166.21 eby-p
wb21.ebaydevelopment.co.uk eby-pr-wb21 10.3.166.22 eby-pr-wb22.ebaydevelopment.co.uk eby-pr-wb22 # Serverfarm - eE
10.3.166.31 eby-pr-wb31.ebaydevelopment.co.uk eby-pr-wb31 10.3.166.32 eby-pr-wb32.ebaydevelopment.co.uk eby-pr-wb3
10.3.166.33 eby-pr-wb33.ebaydevelopment.co.uk eby-pr-wb33 10.3.166.34 eby-pr-wb34.ebaydevelopment.co.uk eby-pr-wb3
```

```
# Do not remove the following line, or various programs # that require network functionality will fail. 127.0.0.1 localhost.loca
localhost ::1 localhost6.localdomain6 localhost6 # Management server 10.3.194.141 car-man.ebaydevelopment.co.uk car-ma
Production database vip 10.3.164.17 PRODDB.ebaydevelopment.co.uk PRODDB # Serverfarm - BDN 10.3.166.11 eby-pr-
wb11.ebaydevelopment.co.uk eby-pr-wb11 10.3.166.12 eby-pr-wb12.ebaydevelopment.co.uk eby-pr-wb12 10.3.166.13 eby-p
wb13.ebaydevelopment.co.uk eby-pr-wb13 10.3.166.14 eby-pr-wb14.ebaydevelopment.co.uk eby-pr-wb14 10.3.166.15 eby-p
wb15.ebaydevelopment.co.uk eby-pr-wb15 10.3.166.16 eby-pr-wb16.ebaydevelopment.co.uk eby-pr-wb16 10.3.166.17 eby-p
wb17.ebaydevelopment.co.uk eby-pr-wb17 10.3.166.18 eby-pr-wb18.ebaydevelopment.co.uk eby-pr-wb18 10.3.166.19 eby-p
wb19.ebaydevelopment.co.uk eby-pr-wb19 10.3.166.20 eby-pr-wb20.ebaydevelopment.co.uk eby-pr-wb20 10.3.166.21 eby-p
wb21.ebaydevelopment.co.uk eby-pr-wb21 10.3.166.22 eby-pr-wb22.ebaydevelopment.co.uk eby-pr-wb22 # Serverfarm - eE
10.3.166.31 eby-pr-wb31.ebaydevelopment.co.uk eby-pr-wb31 10.3.166.32 eby-pr-wb32.ebaydevelopment.co.uk eby-pr-wb3
10.3.166.33 eby-pr-wb33.ebaydevelopment.co.uk eby-pr-wb33 10.3.166.34 eby-pr-wb34.ebaydevelopment.co.uk eby-pr-wb3
```

Real Example: Online Travel Reservation Portal


Hotel Reservation Online - Transaction Slip 20031959 - Windows Internet Explorer
Google
Hotel Reservation Online - Transaction ...
Page
Tools
Done
Internet
100%

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

Change the reserID to 2001200

Hotel Reservation Online

Dear MR.[redacted] Sam,

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

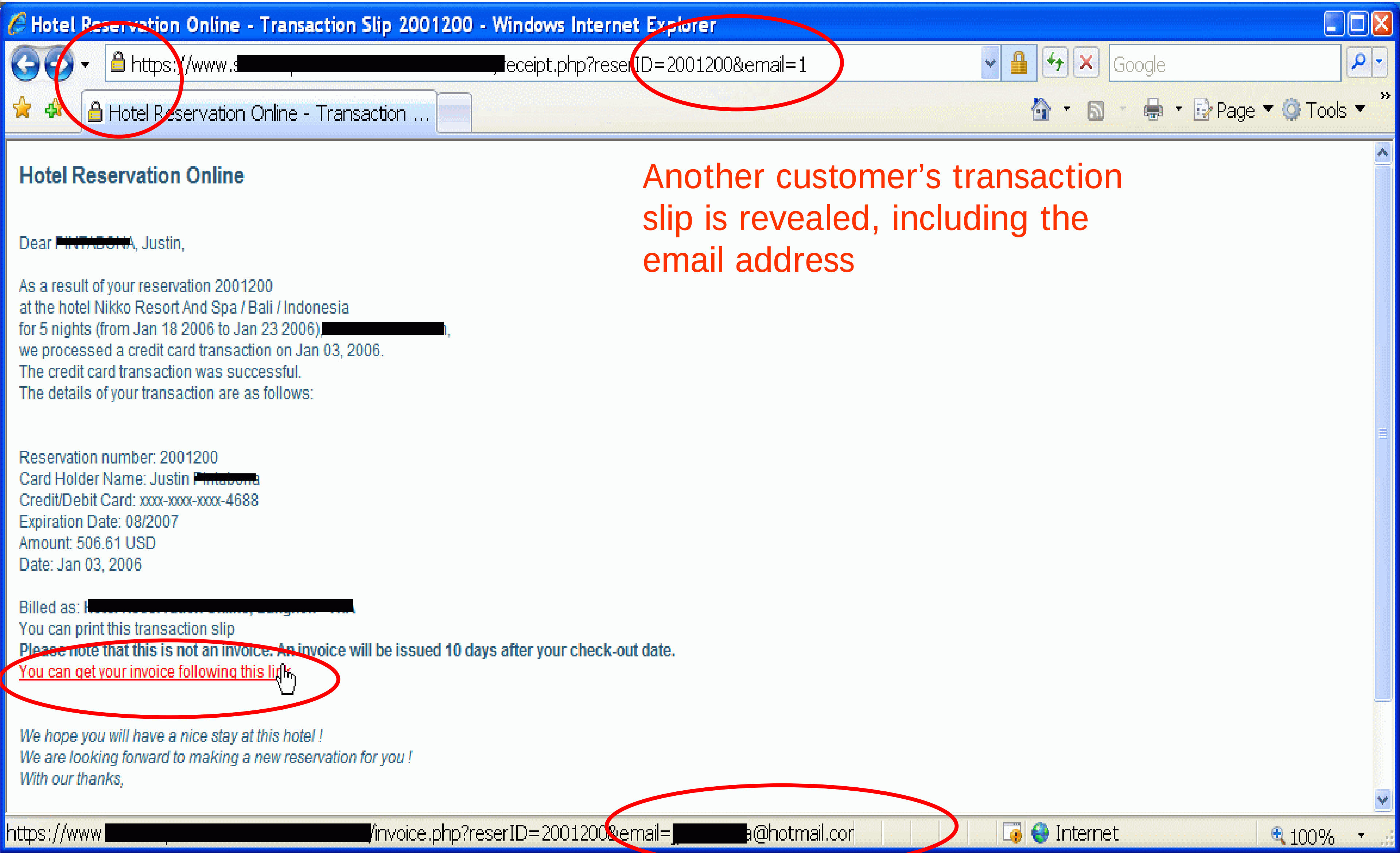
Reservation number: 20031959
Card Holder Name: Sam [redacted]
Credit/Debit Card: xxxx-xxxx-xxxx-2196
Expiration Date: 06/2007
Amount: 240.00 SGD
Date: Jan 15, 2007

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

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

Real Example : Parameter Tampering

Reading another user's transaction – insufficient authorization


Hotel Reservation Online - Transaction Slip 2001200 - Windows Internet Explorer
Google
Hotel Reservation Online - Transaction ...
Page
Tools
Internet
100%

https://www.s[redacted]eceipt.php?reserID=2001200&email=1

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

Hotel Reservation Online

Dear [redacted], Justin,

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

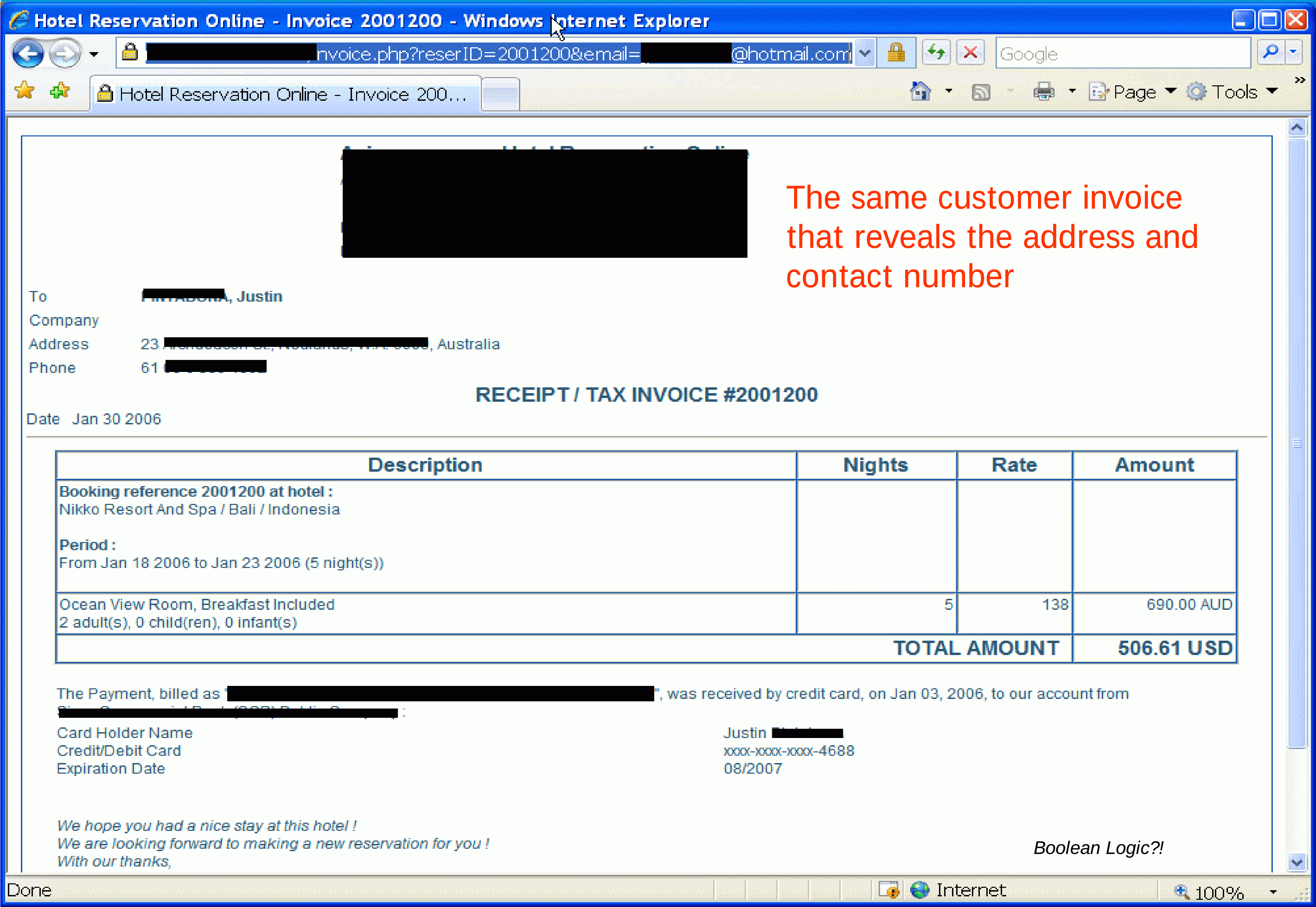
Reservation number: 2001200
Card Holder Name: Justin [redacted]
Credit/Debit Card: xxxx-xxxx-xxxx-4688
Expiration Date: 08/2007
Amount: 506.61 USD
Date: Jan 03, 2006

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

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

https://www[redacted]/invoice.php?reserID=2001200&email=[redacted]a@hotmail.cor

Parameter Tampering Reading another user's invoice


Hotel Reservation Online - Invoice 2001200 - Windows Internet Explorer
Google
Hotel Reservation Online - Invoice 200...
Page
Tools
Done
Internet
100%

[redacted]nvoice.php?reserID=2001200&email=[redacted]@hotmail.com

[redacted]

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

RECEIPT / TAX INVOICE #2001200

Date Jan 30 2006

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

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

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

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

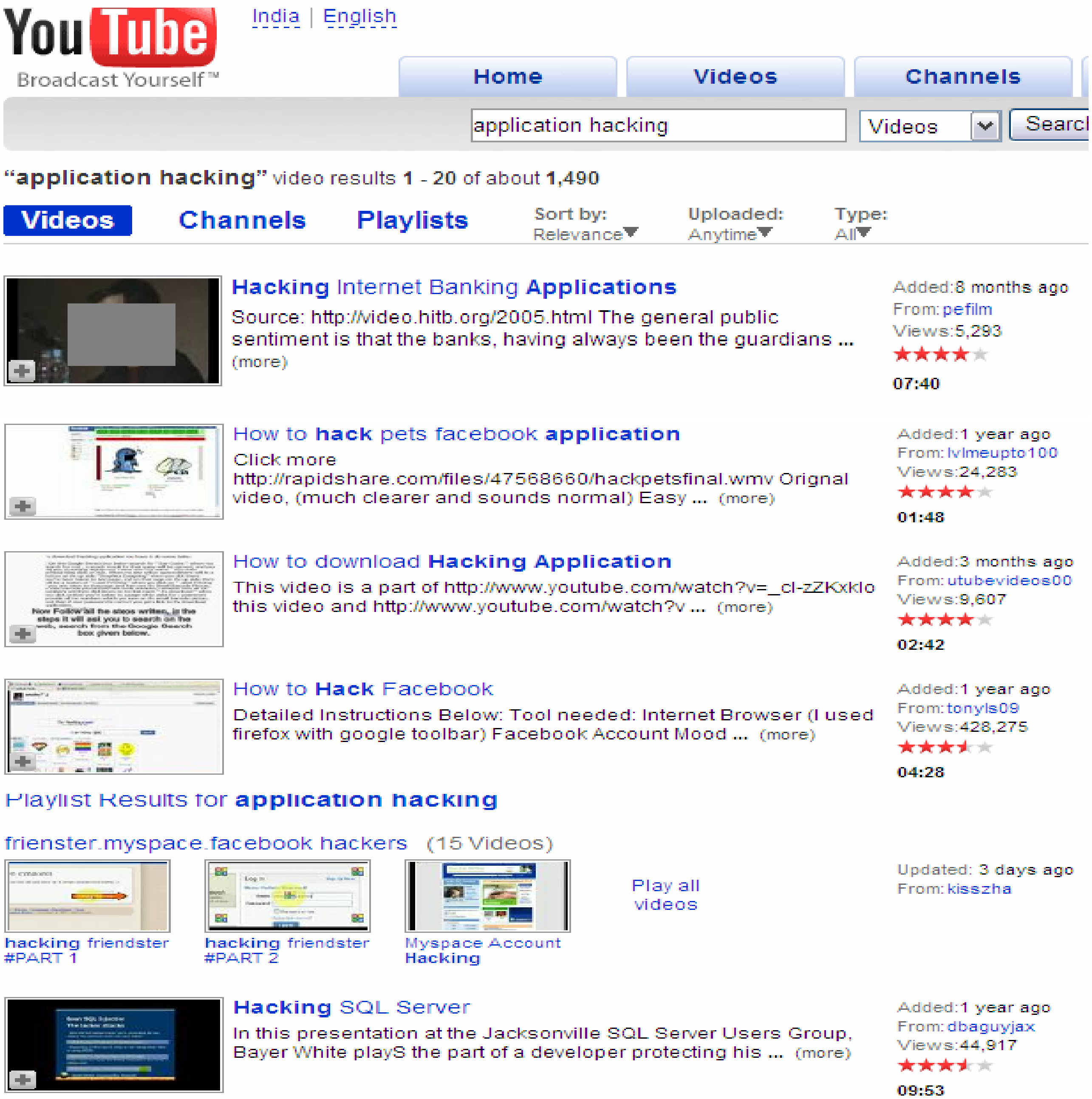
The same customer invoice that reveals the address and contact number

Boolean Logic?!

A Sample Of The ‘low hanging fruits’...

- Shell Command Execution
- HTTP PUT Defacement
- Backup Files
- Blind SQL Injection
- Debug files and Test pages
- Directory Listing
- Insecure HTTP Methods
- HTTP Response Splitting
- SOAP Web Services Issues
- XPath Injection
- Path Traversal in Parameters
- Server Side Includes
- File Upload
- Phishing Through URL redirection
- Poison Null Byte
- Buffer Overflows
- Administration Pages
- SQL Injection
- LDAP Injection
- MS FrontPage Issues
- Email Spoofing
- Cross Site Scripting
- Path Traversal in URL
- BEA WebLogic Issues
- SUN iPlanet Issues
- Oracle iAS Issues
- Format Strings
- ColdFusion Issues
- IBM WebSphere
- PHP Issues
- Apache HTTPd Issues
- Microsoft IIS Issues
- Privacy Issues
- Credentials Enumeration
- Tomcat Issues
- Cookie Poisoning SQL Injection

DON’T TRY THIS AT HOME!



“application hacking” video results **1** - **20** of about **1,490**

Hacking Internet Banking **Applications**
Source: http://video.hitb.org/2005.html The general public sentiment is that the banks, having always been the guardians ... (more)
Added: 8 months ago
From: pefilm
Views: 5,293
★★★★☆
07:40

How to **hack** pets facebook **application**
Click more http://rapidshare.com/files/47568660/hackpetsfinal.wmv Orignal video, (much clearer and sounds normal) Easy ... (more)
Added: 1 year ago
From: lvlmeupto100
Views: 24,283
★★★★☆
01:48

How to download **Hacking Application**
This video is a part of http://www.youtube.com/watch?v=_cl-zZKxklo this video and http://www.youtube.com/watch?v ... (more)
Added: 3 months ago
From: utubevideos00
Views: 9,607
★★★★☆
02:42

How to **Hack** Facebook
Detailed Instructions Below: Tool needed: Internet Browser (I used firefox with google toolbar) Facebook Account Mood ... (more)
Added: 1 year ago
From: tonyls09
Views: 428,275
★★★½☆
04:28

Playlist Results for **application hacking**

friensterˌmyspace.facebook hackers (15 Videos)
hacking friendster #PART 1
hacking friendster #PART 2
Myspace Account **Hacking**
Play all videos
Updated: 3 days ago
From: kisszha

Hacking SQL Server
In this presentation at the Jacksonville SQL Server Users Group, Bayer White playS the part of a developer protecting his ... (more)
Added: 1 year ago
From: dbaguyjax
Views: 44,917
★★★½☆
09:53

WHY DO HACKERS TODAY ATTACK 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 (?)**

Singapore

Mercedes

- ***Cheap***
- ***Fast***
- ***Good***

-> Choose 2

OUR GOAL IS TO WRITE BUG-FREE SOFTWARE. I'LL PAY A TEN-DOLLAR BONUS FOR EVERY BUG YOU FIND AND FIX.
YAHOO!
WE'RE RICH
YES!!! YES!!! YES!!!
I HOPE THIS DRIVES THE RIGHT BEHAVIOR.
I'M GONNA WRITE ME A NEW SUV THIS AFTERNOON!

S. Adams E-mail: SCOTTADAMS@AOL.COM

11/13 © 1995 United Feature Syndicate, Inc.(NYC)

Top 10 OWASP Critical Web Application Security Issues ’09 www.owasp.org

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

2010

1 Injection

2 Cross-Site Scripting (XSS)

3 Broken Authentication and Session Management

4 Insecure Direct Object References

5 Cross-Site Request Forgery (CSRF)

6 Security Misconfiguration

7 Insecure Cryptographic Storage

8 Failure to Restrict URL Access

9 Insufficient Transport Layer Protection

10 Unvalidated Redirects and Forwards

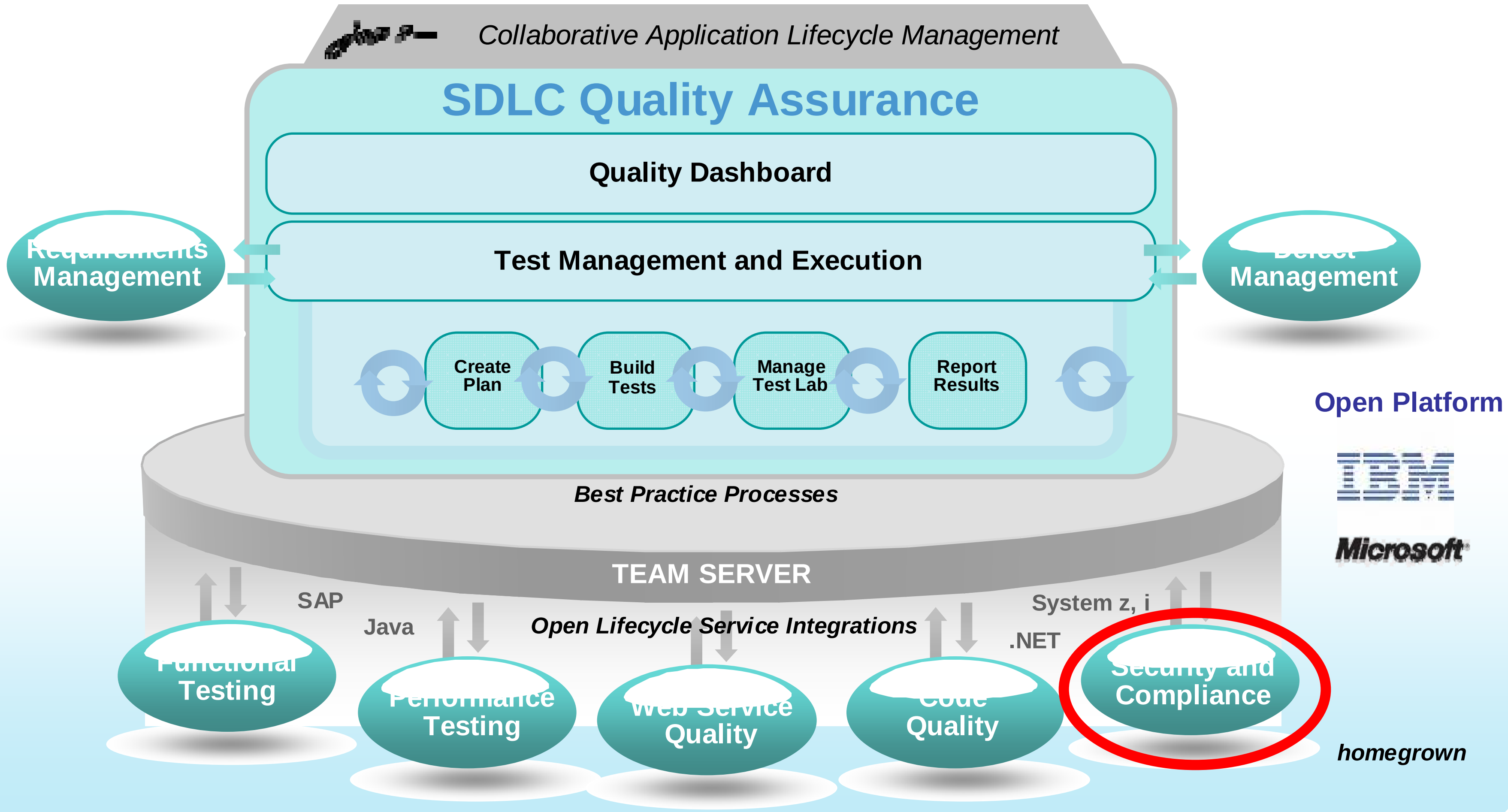
WHY DO APPLICATION SECURITY PROBLEMS EXIST?

- **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

Back then coding was done by engineers …

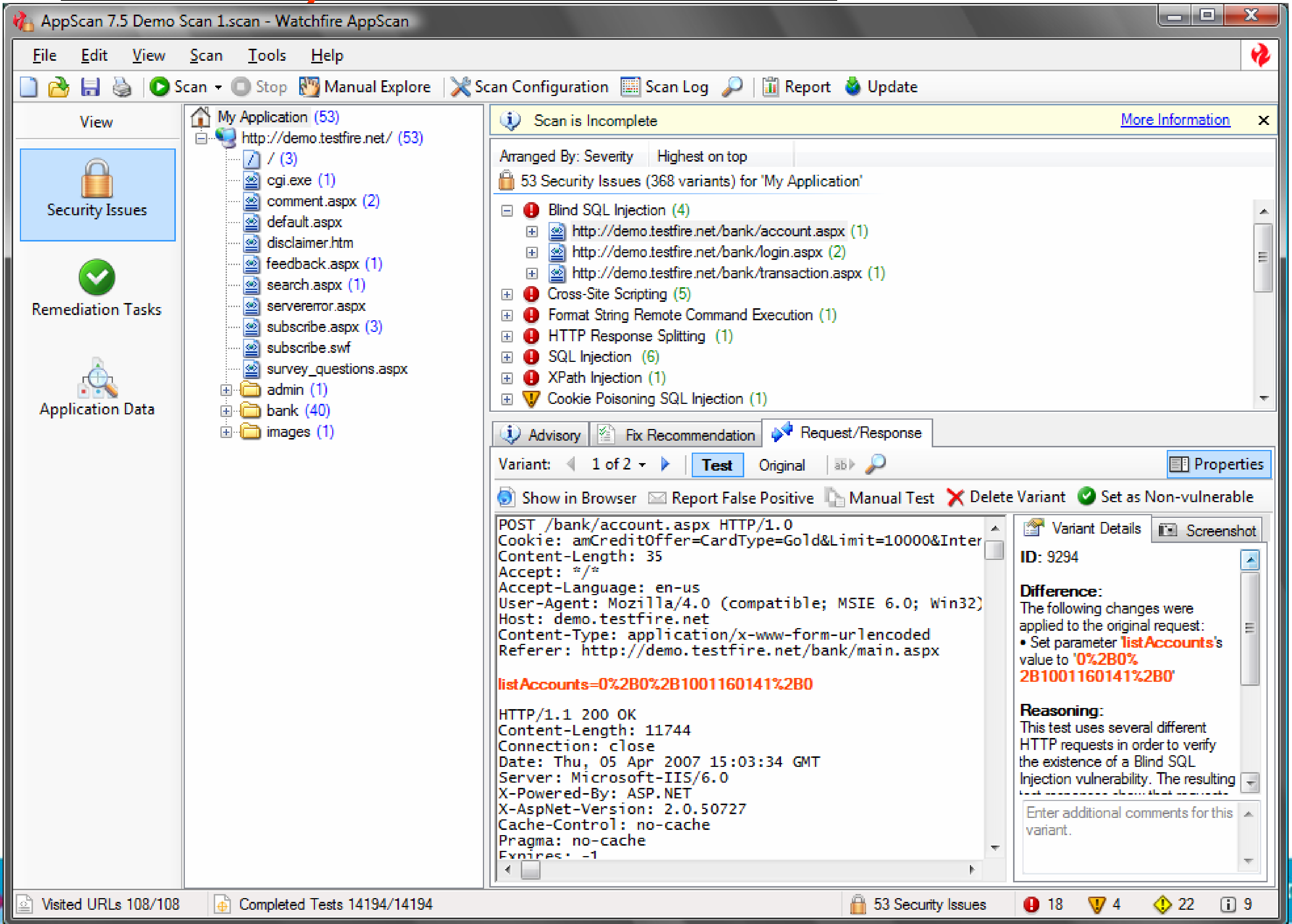
Then came Y2K … Dotcom boom … etc

SECURITY TESTING IS PART OF SDLC QUALITY TESTING



You need a professional solution to

Identify Vulnerabilities



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

Scan is Incomplete

Arranged By: Severity | Highest on top

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

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

```
POST /bank/account.aspx HTTP/1.0
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Inter
Content-Length: 35
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: demo.testfire.net
Content-Type: application/x-www-form-urlencoded
Referer: http://demo.testfire.net/bank/main.aspx

listAccounts=0%2B0%2B1001160141%2B0

HTTP/1.1 200 OK
Content-Length: 11744
Connection: close
Date: Thu, 05 Apr 2007 15:03:34 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
Pragma: no-cache
Expires: -1
```

ID: 9294

Difference:
The following changes were applied to the original request:
- Set parameter 'listAccounts''s value to '0%2B0%2B1001160141%2B0'

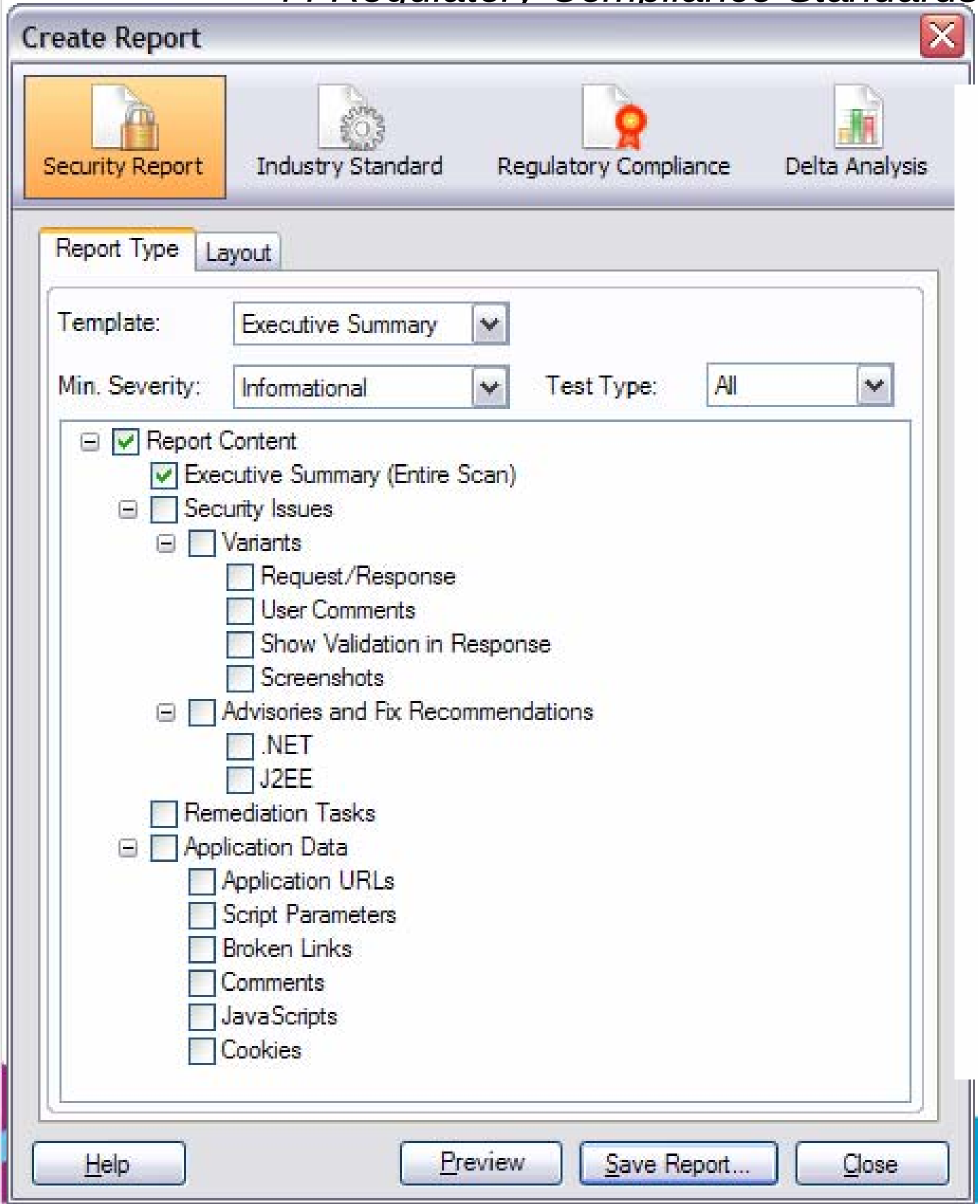
Reasoning:
This test uses several different HTTP requests in order to verify the existence of a Blind SQL Injection vulnerability. The resulting

Enter additional comments for this variant.

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

With Rich Report Options

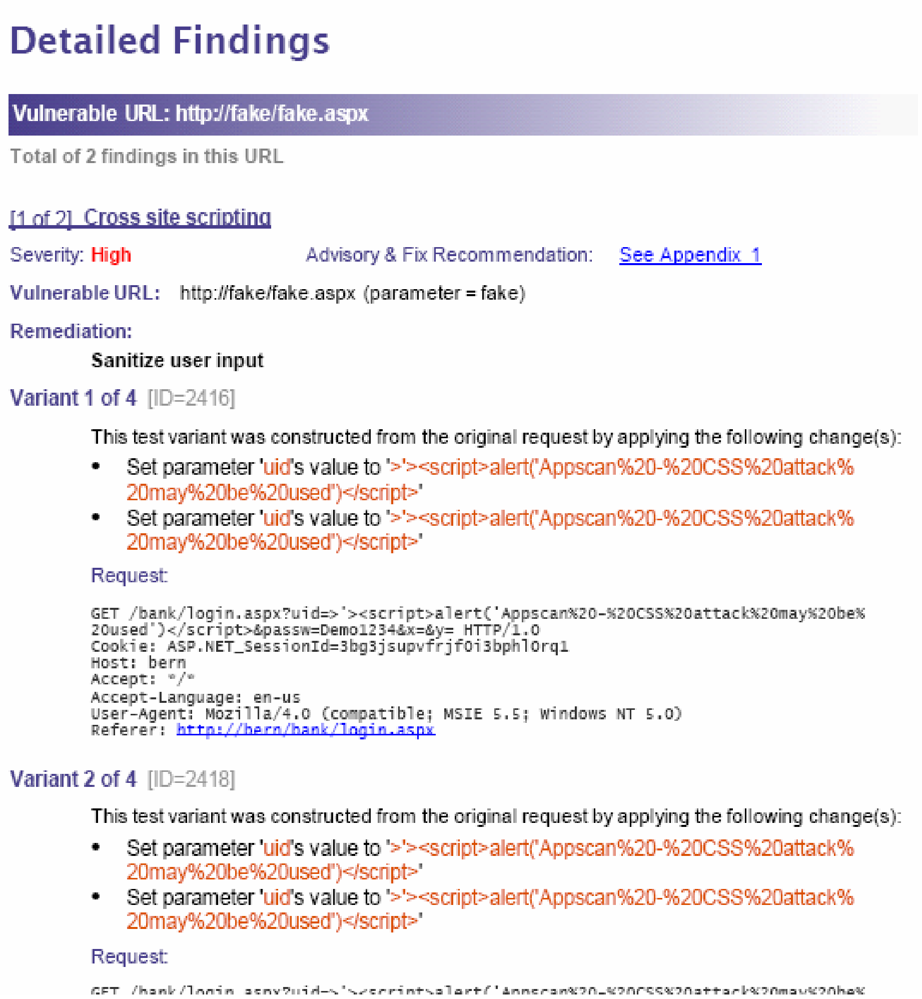
44 Regulatory Compliance Standards, for Executive, Security, Developers.



Template: Executive Summary

Min. Severity: Informational   Test Type: All

- ☑ Report Content
  - ☑ Executive Summary (Entire Scan)
  - □ Security Issues
    - □ Variants
      - □ Request/Response
      - □ User Comments
      - □ Show Validation in Response
      - □ Screenshots
    - □ Advisories and Fix Recommendations
      - □ .NET
      - □ J2EE
  - □ Remediation Tasks
  - □ Application Data
    - □ Application URLs
    - □ Script Parameters
    - □ Broken Links
    - □ Comments
    - □ JavaScripts
    - □ Cookies



Detailed Findings

Vulnerable URL: http://fake/fake.aspx

Total of 2 findings in this URL

[1 of 2] Cross site scripting

Severity: High   Advisory & Fix Recommendation: See Appendix 1

Vulnerable URL: http://fake/fake.aspx (parameter = fake)

Remediation:

Sanitize user input

Variant 1 of 4 [ID=2416]

This test variant was constructed from the original request by applying the following change(s):

- Set parameter 'uid's value to '>'><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>'
- Set parameter 'uid's value to '>'><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>'

Request:

```
GET /bank/login.aspx?uid=>'><script>alert('Appscan%20-%20CSS%20attack%20may%20be%
20used')</script>&passw=Demo1234&x=&y= HTTP/1.0
Cookie: ASP.NET_SessionId=3bg3jsupvfrjf0i3bphl0rq1
Host: bern
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
Referer: http://bern/bank/login.aspx
```

Variant 2 of 4 [ID=2418]

This test variant was constructed from the original request by applying the following change(s):

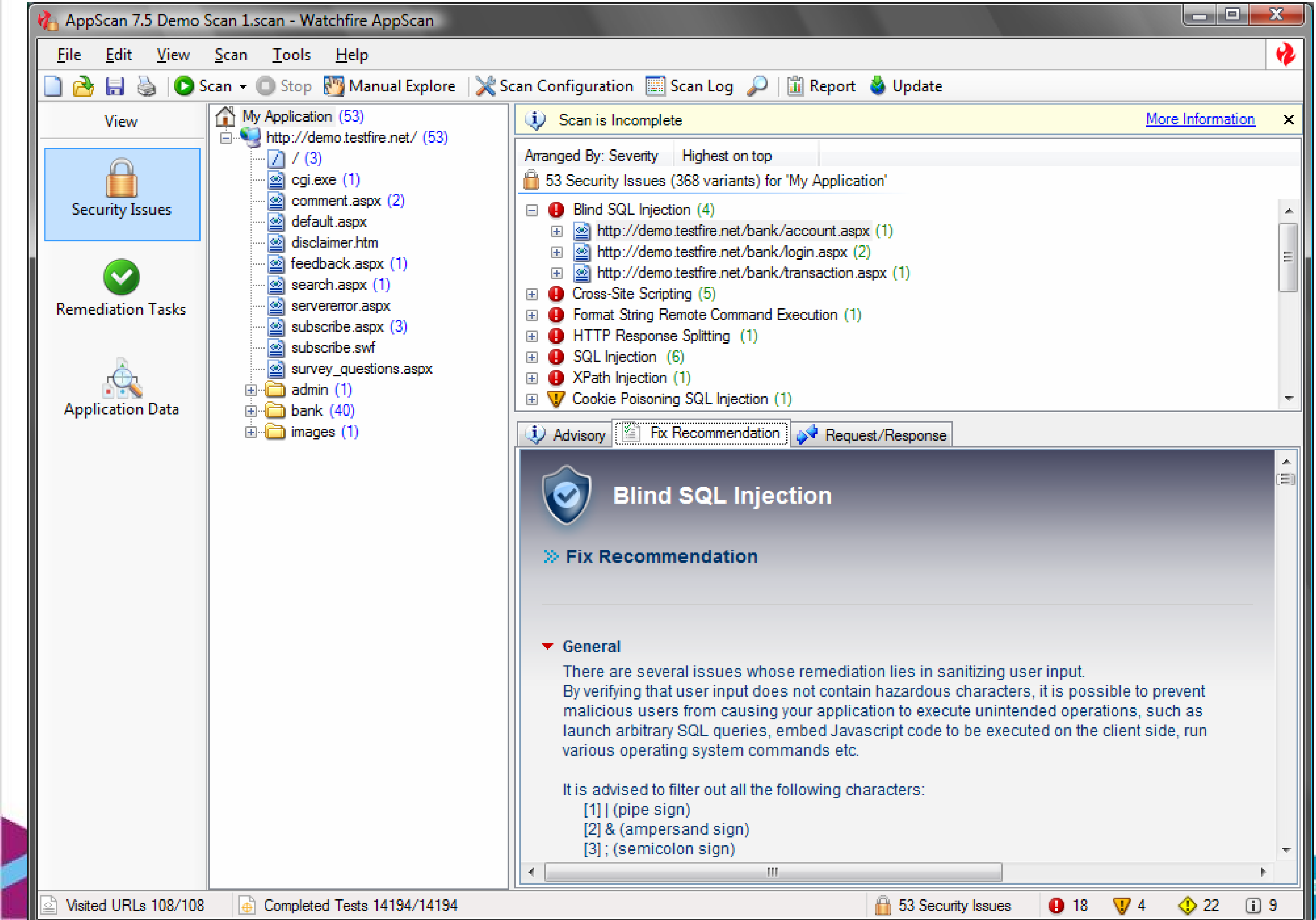
- Set parameter 'uid's value to '>'><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>'
- Set parameter 'uid's value to '>'><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>'

Request:

```
GET /bank/login.aspx?uid=>'><script>alert('Appscan%20-%20CSS%20attack%20may%20be%
```

And Most Important :

Actionable Fix Recommendations



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

Scan is Incomplete

Arranged By: Severity Highest on top

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

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

Blind SQL Injection

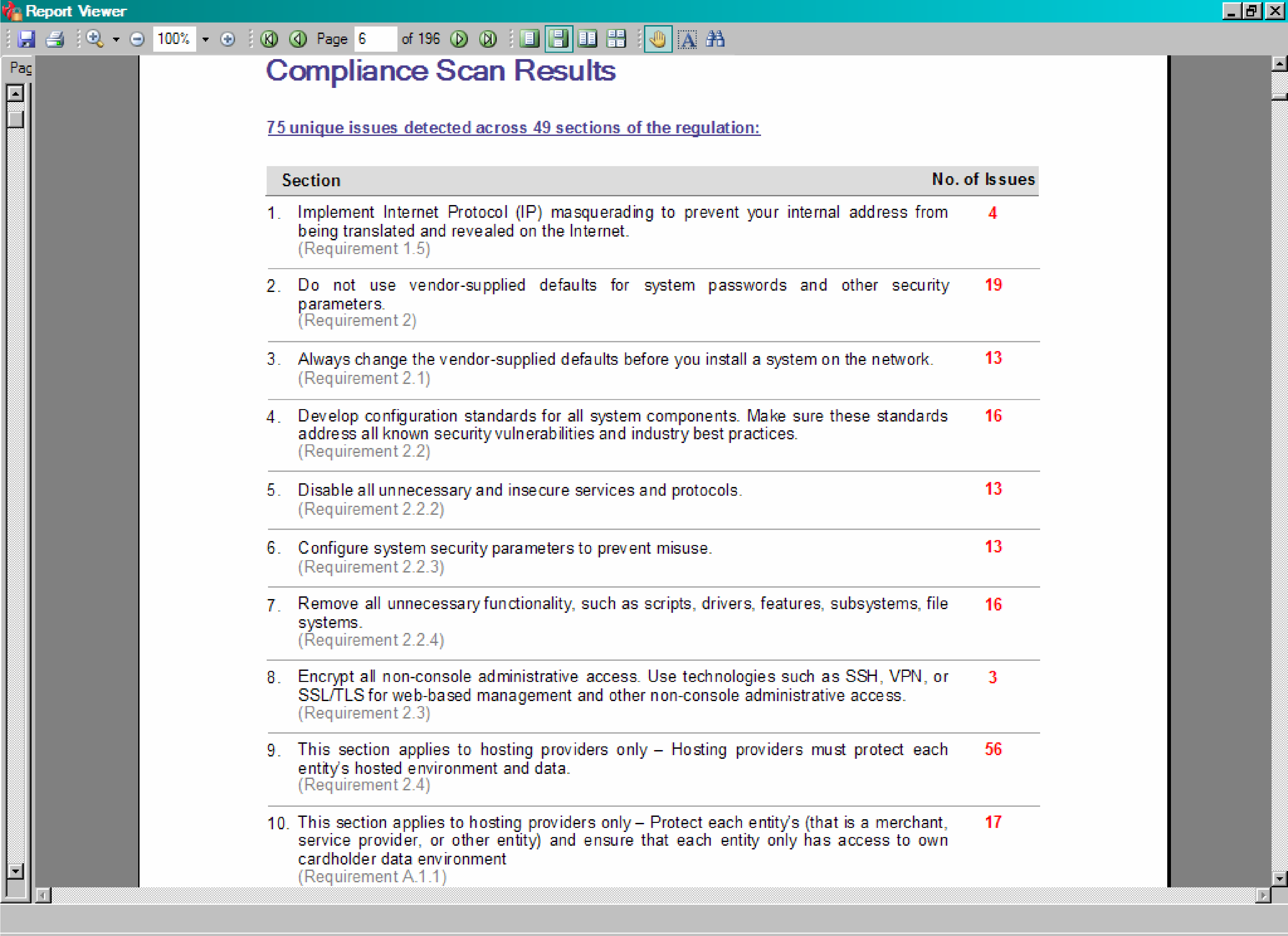
Fix Recommendation

General

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

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

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

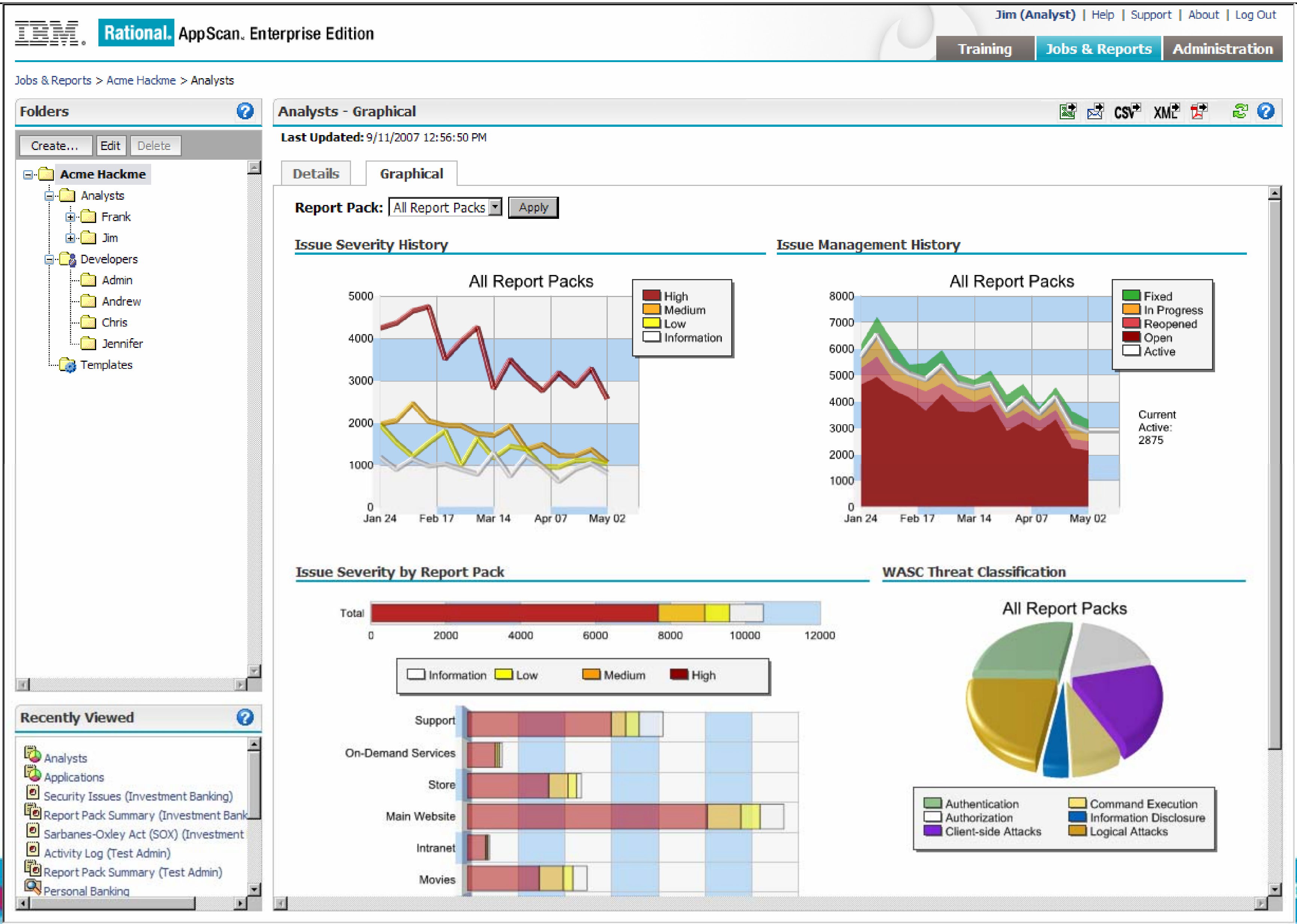


Compliance Scan Results

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

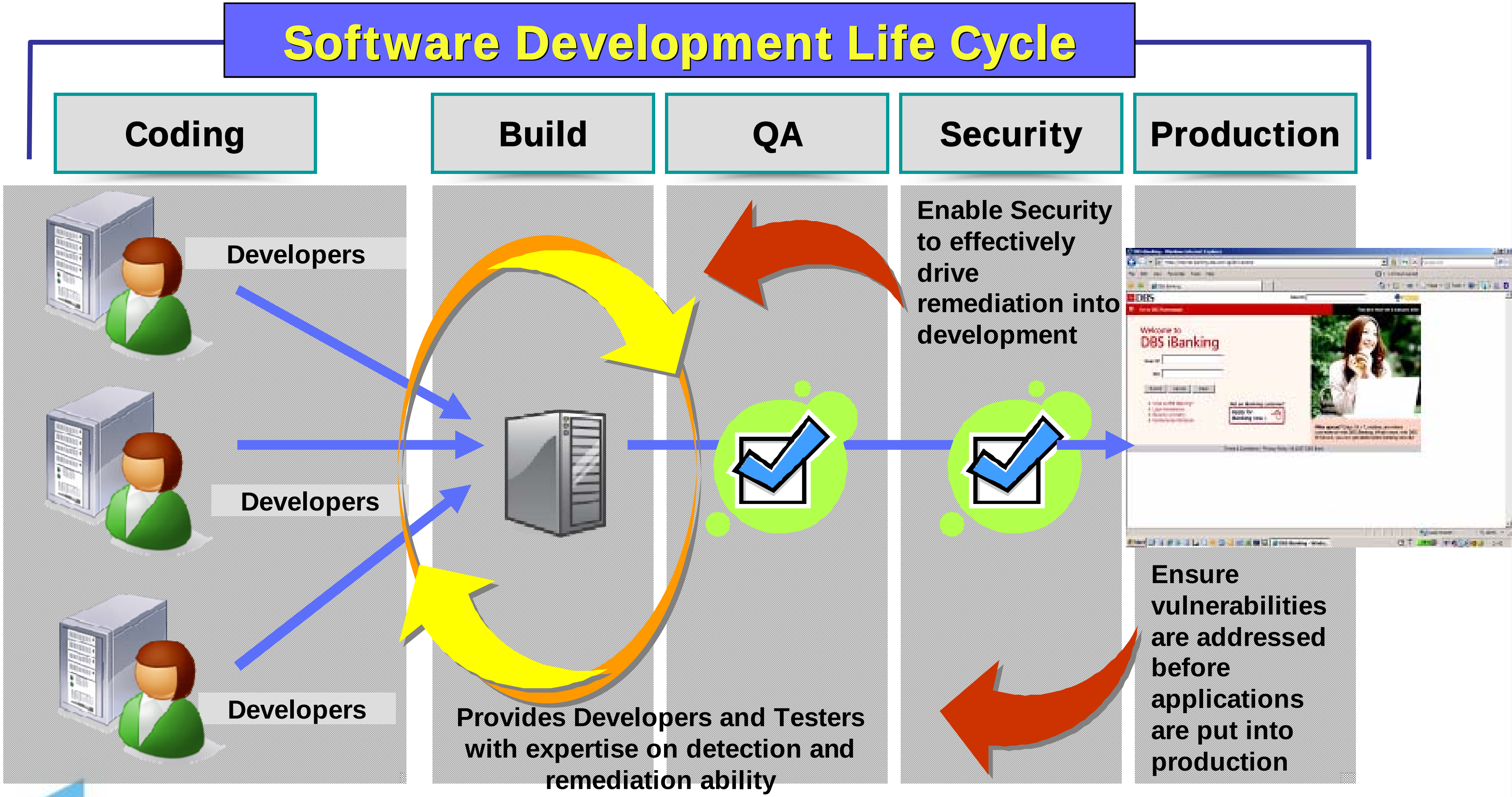
Enterprise Software QA Solution – Dashboards and Metrics



Last Updated: 9/11/2007 12:56:50 PM

Report Pack: All Report Packs

Building security & compliance into the SDLC – further back



Software Development Life Cycle

Coding

Build

QA

Security

Production

Developers

Developers

Developers

Enable Security to effectively drive remediation into development

Provides Developers and Testers with expertise on detection and remediation ability

Ensure vulnerabilities are addressed before applications are put into production

Application Development Security Testing Domains

"BLACK BOX *IBM Rational Appscan Source Edition*	WHITE BOX *IBM Rational Appscan Standard Edition*
Dynamic APPLICATION Analysis	**State CODE Analysis**
Good for security folks who are not experienced in application development	***Good for developers who are not experienced in security***
Don't need to worry about code	***Provides learning for developers***
Simulates real-world exploit attack	***Good for interim audit of half-written code***
Tests for relation between App and other apps, O/S, middleware, network	***Can test for more than just HTTP /HTML code - eg. C, C++, C#, Perl, Codefusion, Javascript …***
Like IPS, checks for "unknown" threats	***Like Firewall, checks for "known" threats***

Conclusion: Application Develppment Quality for Security

- **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**

Thank You

Anthony LIM

MBA CISSP CSSLP FCITIL

ISC2

CLOUD COMPUTING SECURITY – THE SOFT SPOT

www.isc2.org

www.owasp.org

www.ibm.com/security