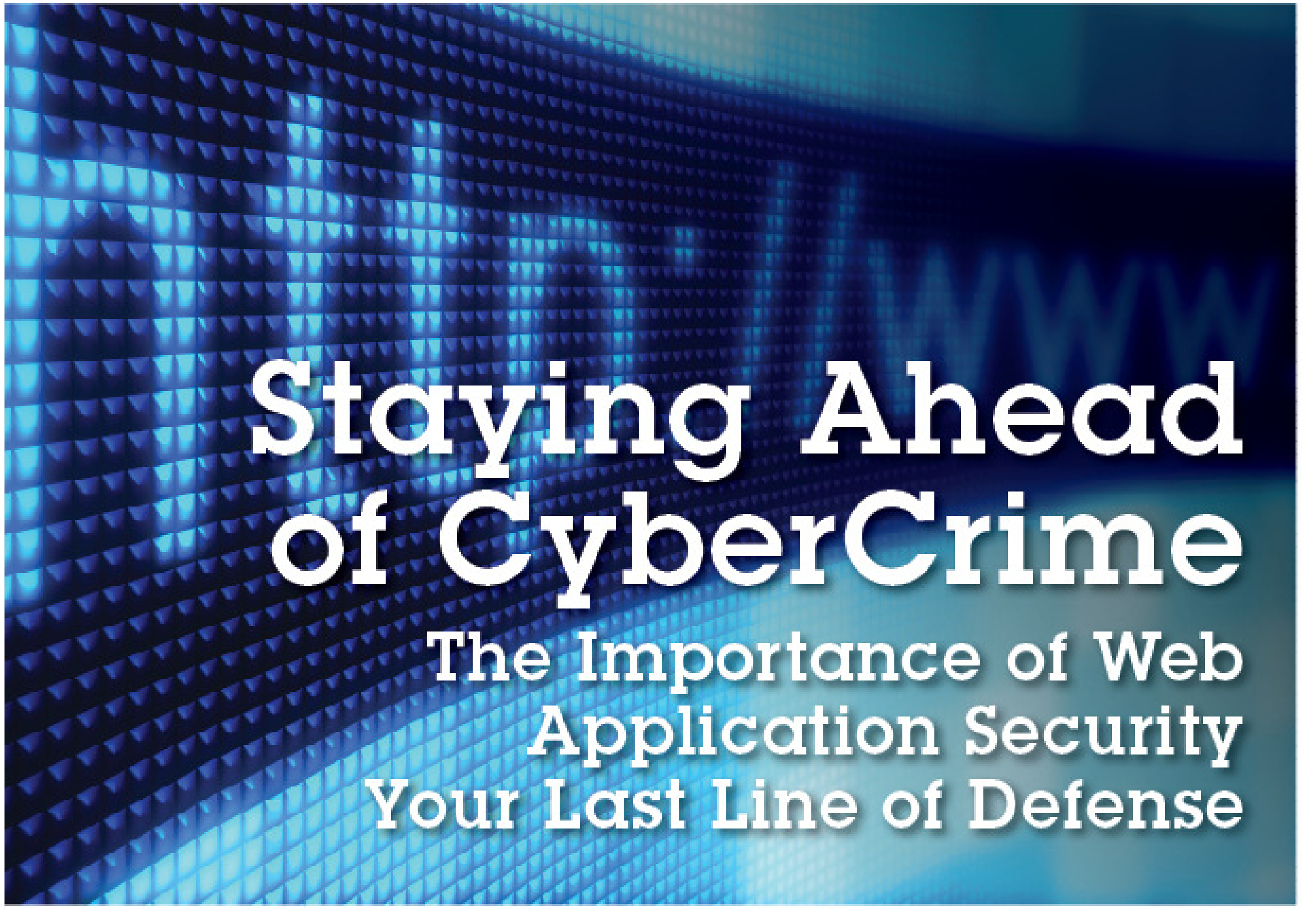


Staying Ahead of CyberCrime

The Importance of Web Application Security Your Last Line of Defense

Anthony Lim

MBA FCITIL CISSP CSSLP

Director, Security
Rational Software
- Asia Pacific

CSSLP

Certified Secure Software Lifecycle Professional

Rational. software

ISC2 SecureSydney 12 November 2009

Welcome to THE SMARTER PLANET

Globalisation 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..

New Forms of Collaboration

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:

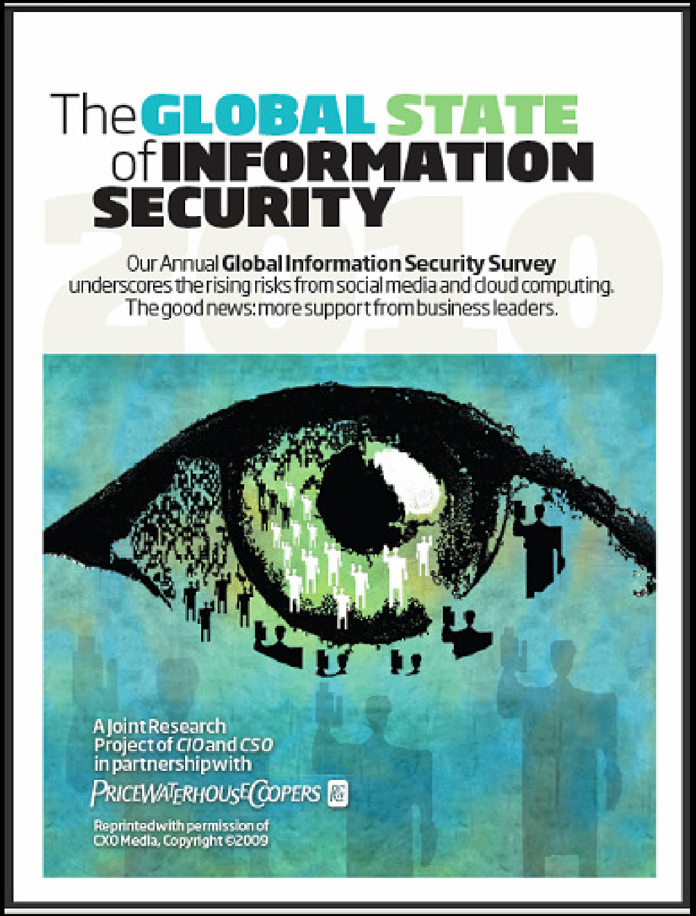
(1) Promise and Peril of SOCIAL NETWORKING

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

(3) INSOURCING Security Management

(4) NEW CORPORATE COMMITMENT

(5) ATTACKS ON DATABASES



The GLOBAL STATE of INFORMATION SECURITY

2010

Our Annual Global Information Security Survey underscores the rising risks from social media and cloud computing. The good news: more support from business leaders.

A Joint Research Project of CIO and CSO in partnership with PRICEWATERHOUSECOOPERS

Reprinted with permission of CXO Media, Copyright ©2009

SMARTER PLANET …. means …

SOFTWARE IS EVERYWHERE – NOT JUST COMPUTERS

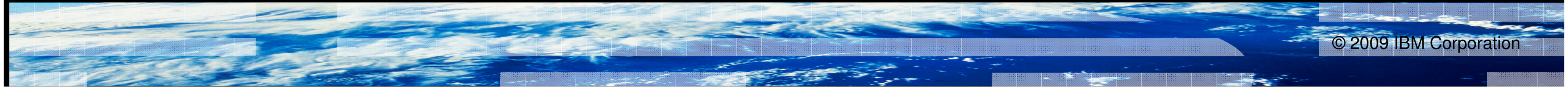
-millions of lines of code everywhere

Mobile ‘smart phones’, home appliances, motor vehicles, planes …
National infrastucture (eg utilities grid, traffic controls)

HIGH AND INCREASING DEPENDENCY ON WEB APPS

For work: Intranet, Extranet, Corporate Services, Accounting, Data …
Communications: email, Instant Messaging, Blog, Web pages …
data transfer … LinkedIn …
Transactions : e-banking, e-trading, SCM, CRM, logistics scheduling,
Research and Education
Recreation : Facebook, Youtube, Second Life … etc

New Possibilities, New Complexities … NEW RISKS!



It Gets Worse

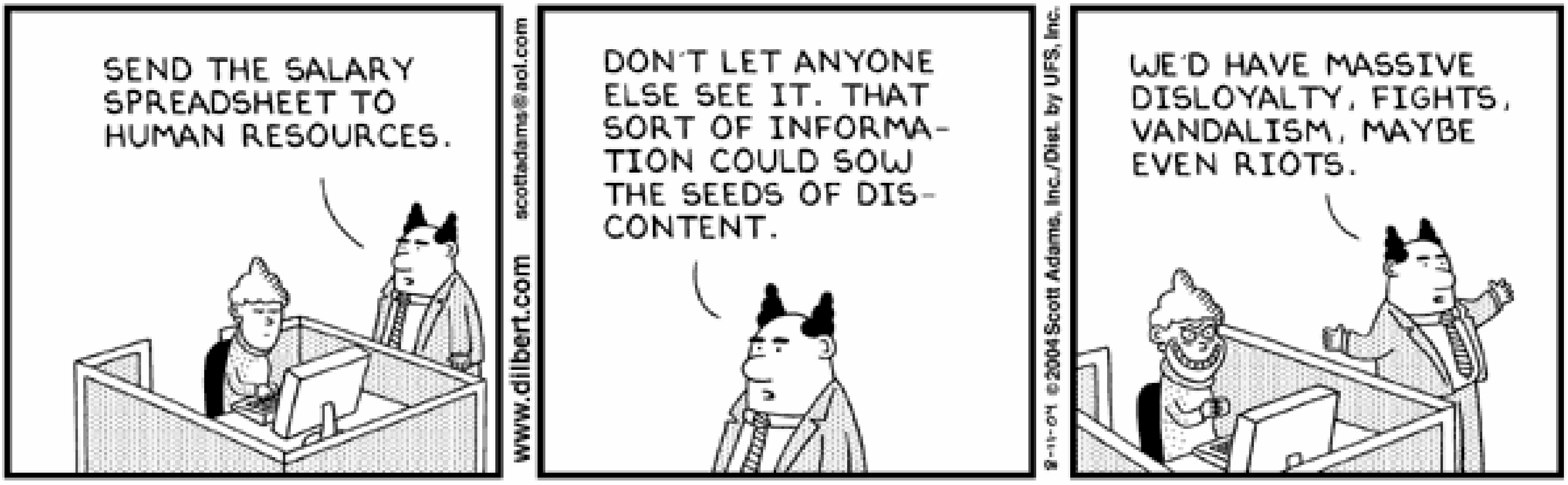
A hacker no longer needs a big machine

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

- It is part of doing business
- Business Continuity
- An environment of TRUST
  - For doing business
  - Ensure Orderliness in Internet world
  - Promote Economic growth

- More than just Confidentiality, Integrity and Availability
- Privacy

3rd Party Customer Data


SEND THE SALARY SPREADSHEET TO HUMAN RESOURCES.
scottadams@aol.com
www.dilbert.com
DON'T LET ANYONE ELSE SEE IT. THAT SORT OF INFORMATION COULD SOW THE SEEDS OF DISCONTENT.
9-11-04 ©2004 Scott Adams, Inc./Dist. by UFS, Inc.
WE'D HAVE MASSIVE DISLOYALTY, FIGHTS, VANDALISM, MAYBE EVEN RIOTS.

© UFS, Inc.

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

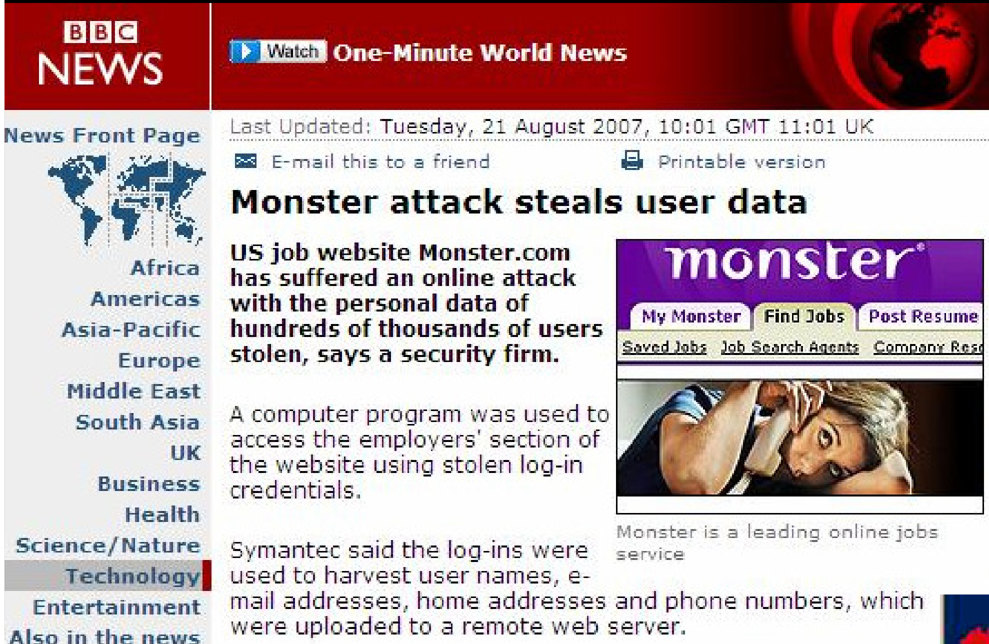
We Use Network Vulnerability Scanners

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

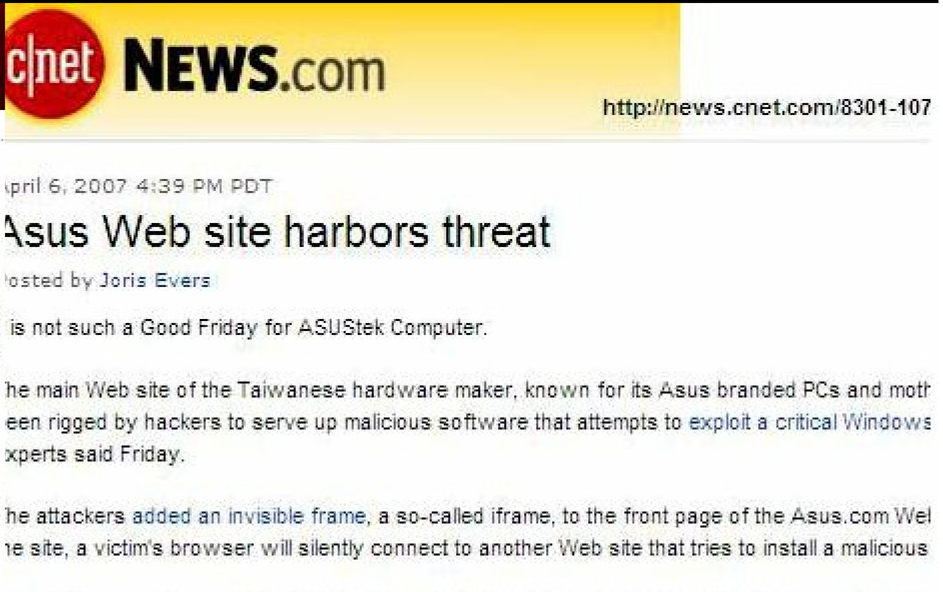
Monster attack steals user data

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.



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

pril 6, 2007 4:39 PM PDT

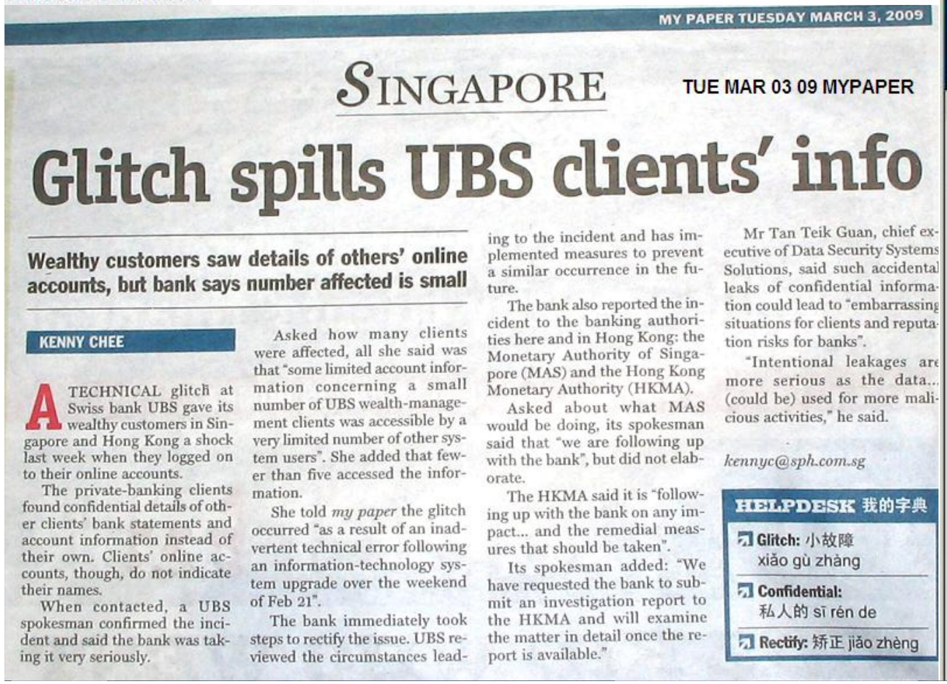
sus Web site harbors threat

osted by Joris Evers

is not such a Good Friday for ASUStek Computer.

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

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



MY PAPER TUESDAY MARCH 3, 2009

SINGAPORE TUE MAR 03 09 MYPAPER

Glitch spills UBS clients' info

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

KENNY CHEE

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

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

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

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

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

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

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

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

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

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

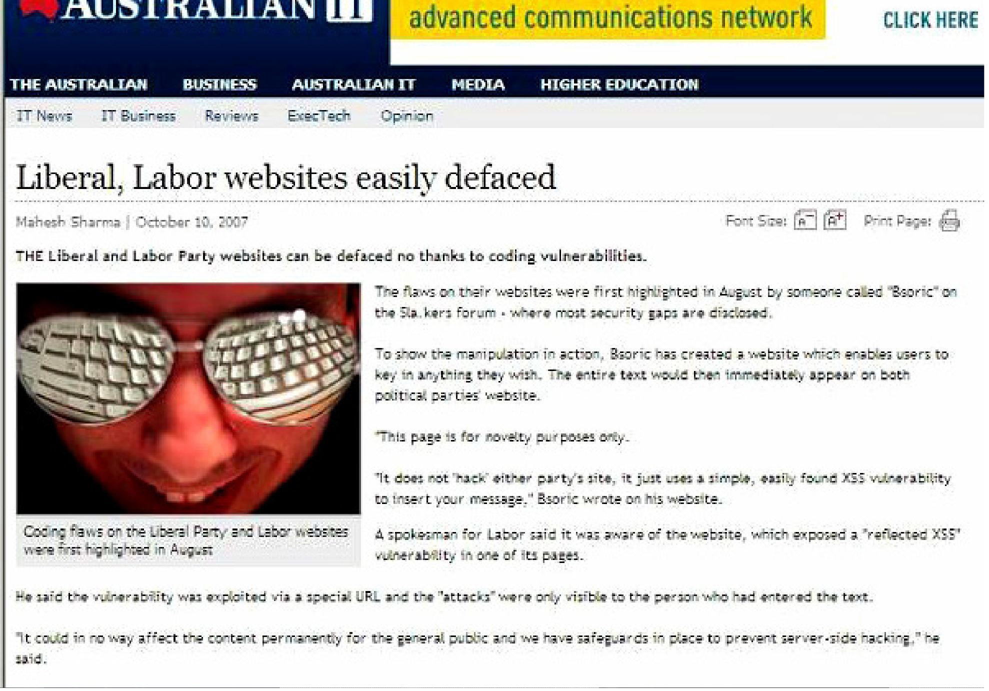
Mr Tan Teik Guan, chief executive of Data Security Systems Solutions, said such accidental leaks of confidential information could lead to "embarrassing situations for clients and reputation risks for banks".

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

kennyc@sph.com.sg

HELPDESK 我的字典

- **Glitch:** 小故障 xiǎo gù zhàng
- **Confidential:** 私人的 sī rén de
- **Rectify:** 矫正 jiǎo zhèng



Liberal, Labor websites easily defaced

Mahesh Sharma | October 10, 2007

THE Liberal and Labor Party websites can be defaced no thanks to coding vulnerabilities.

Coding flaws on the Liberal Party and Labor websites were first highlighted in August

The flaws on their websites were first highlighted in August by someone called "Bsoric" on the Sla.kers forum - where most security gaps are disclosed.

To show the manipulation in action, Bsoric has created a website which enables users to key in anything they wish. The entire text would then immediately appear on both political parties' website.

"This page is for novelty purposes only.

"It does not 'hack' either party's site, it just uses a simple, easily found XSS vulnerability to insert your message," Bsoric wrote on his website.

A spokesman for Labor said it was aware of the website, which exposed a "reflected XSS" vulnerability in one of its pages.

He said the vulnerability was exploited via a special URL and the "attacks" were only visible to the person who had entered the text.

"It could in no way affect the content permanently for the general public and we have safeguards in place to prevent server-side hacking," he said.

STRAITS TIMES SINGAPORE
13 SEP 09

Hackers steal gamers' currency

MapleStory players blame company for lax security

By Tan Weizhen

ith an events section called
Ve are hiring!".
There, it advertises for and
pes to recruit young frontline
rvice staff.
Miss Eileen Ang, 30, the ho-
's human resource manager,
d: "Facebook is also a good
y to keep in touch with old

facebook

Some say Facebook appeals to a younger

in any fashion.
"Professional networks are far better for targeting quality candidates."
On why other recruitment agencies are reluctant to use Facebook for recruitment, Mr Wagenaar explained: "Recruitment over Facebook is still in a

home.

STRAITS TIMES, SINGAPORE FRI FEB 27 09

THE STRAITS TIMES FRIDAY, FEBRUARY 27 2009 PAGE C2

'Errors' on Facebook a cyber trap

Viral application enables perpetrator to access personal data

By Serene Luo

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

sarl@sph.com.sg

FAST-SPREADING

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

Blogger Josh Lim

How to remove it

What you will see

■ Facebook notifications will tell users that their friend "has faced some errors when checking your profile".

■ If they click on the link to "View The Errors Message", a prompt will ask them to "activate" the application to correct the errors. This move allows their information to be accessed.

How to remove the application

■ Click on "Edit" in the Applications pane.

■ Click on the "x" beside the "Error Check System" application.

■ A window will pop up asking the user to confirm the removal.

Are you on Facebook? Beware of hackers

Cyber crooks targeting social networking sites

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

rking sites targeted by hackers

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

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

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

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

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

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

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

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

sandrea@sph.com.sg

May 8, 2009 1:53 PM PDT

UC Berkeley computers hacked, 160,000 at risk

by Michelle Meyers

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

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

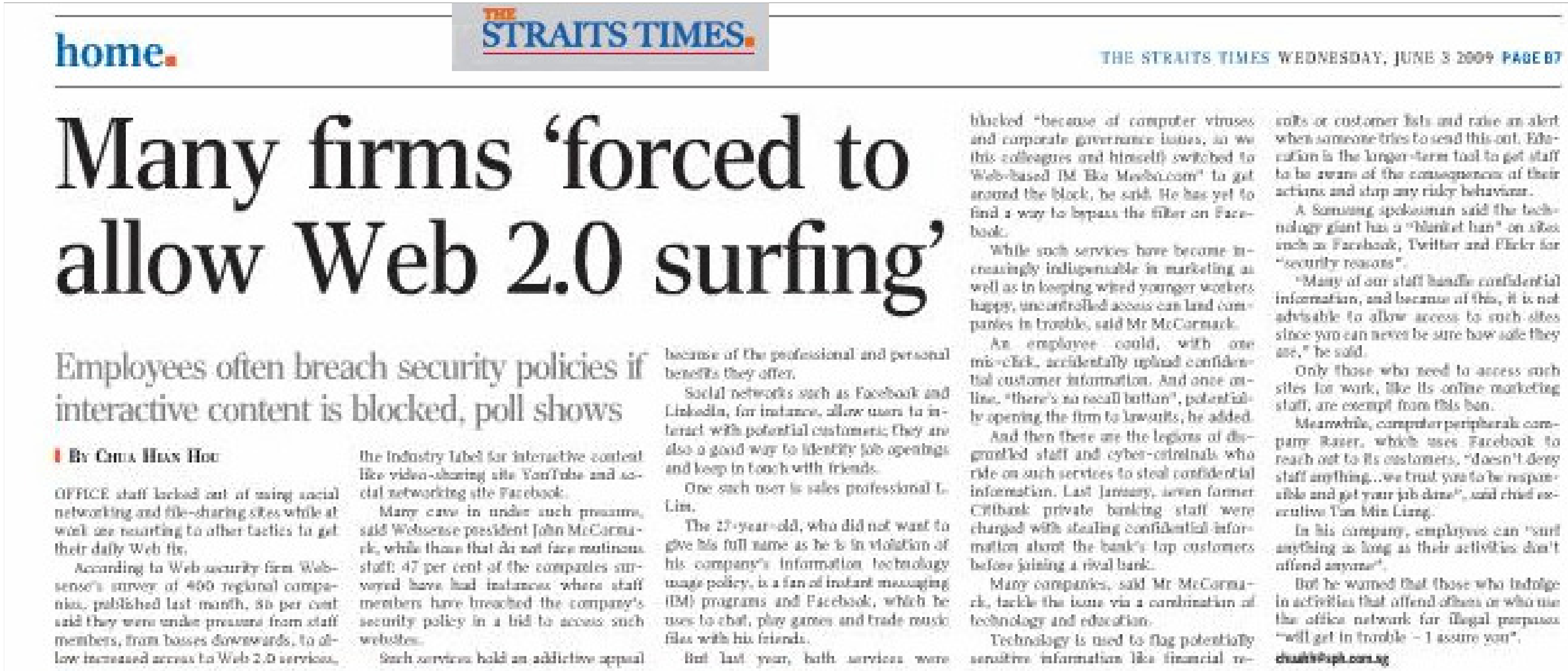
At particular risk of identity theft are some 97,000 individuals whose Social Security numbers were accessed in the breach, but it's still unclear whether hackers were able to match up those SSNs with individual names, Shelton Waggener, UCB's chief technology officer, said in a press conference Friday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

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

(Credit: University of California at Berkeley)

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

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



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 results 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.

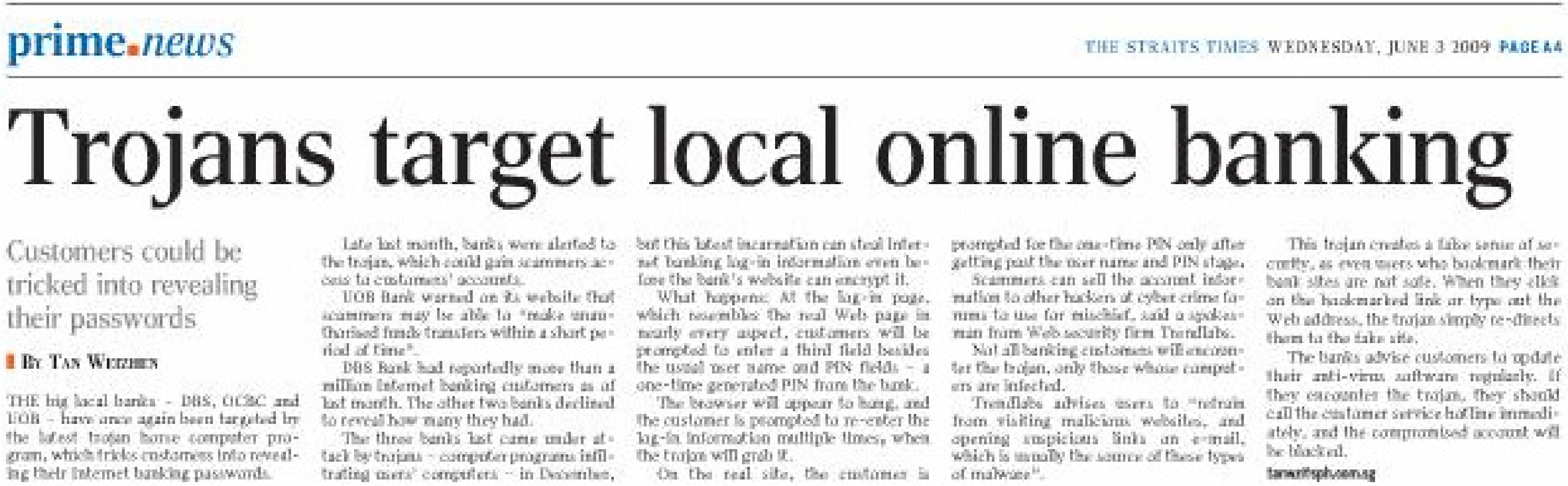
Only those who need to access such sites for work, like its online marketing staff, are exempt from this ban.

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.

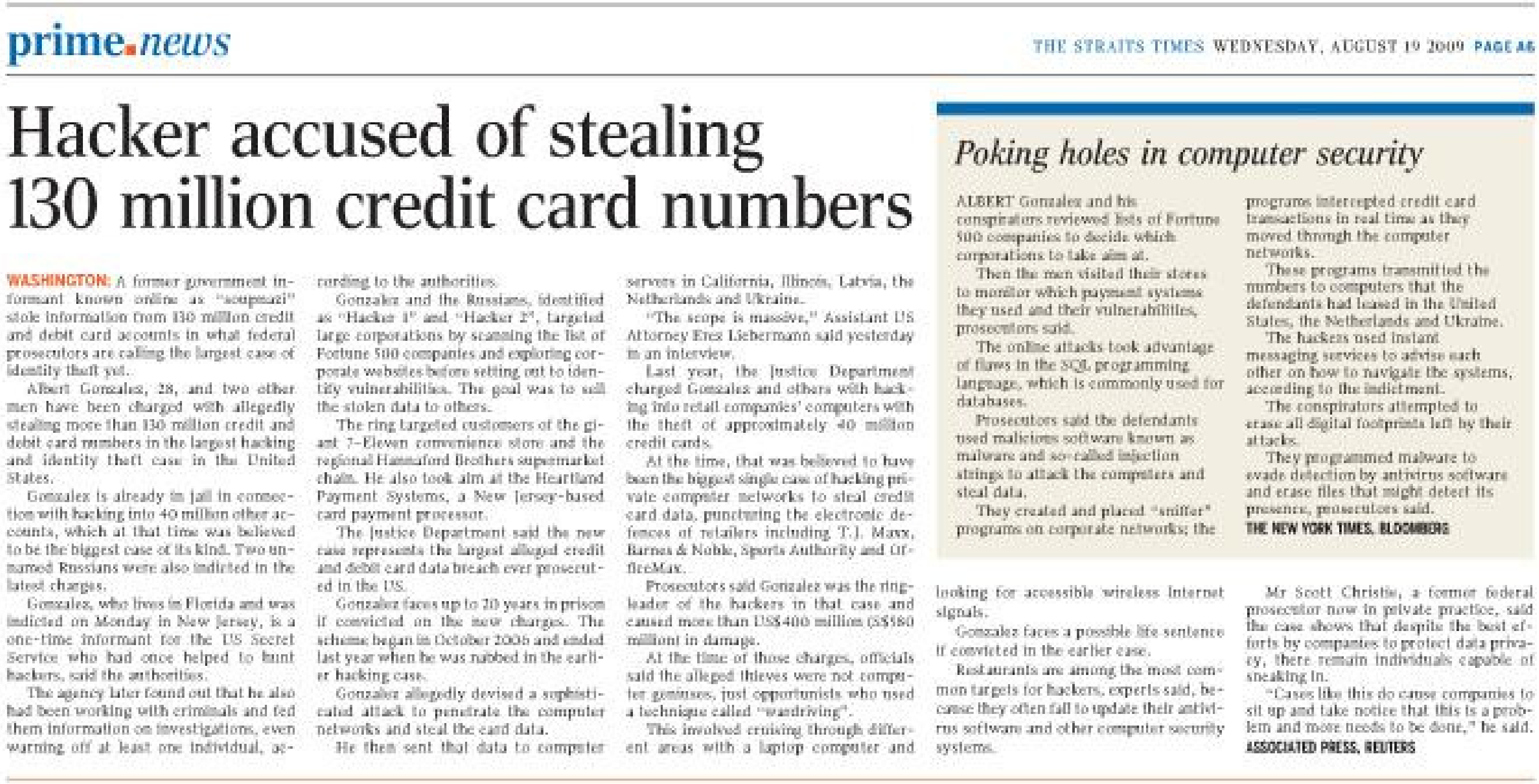
Trendlabs advises users to "refrain from visiting malicious websites, and opening suspicious links on e-mail, which is usually the source of these types of malware".

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 SQL INJECTION : A WEB APP ATTACK!



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

2008 Web Threats Take Center Stage

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

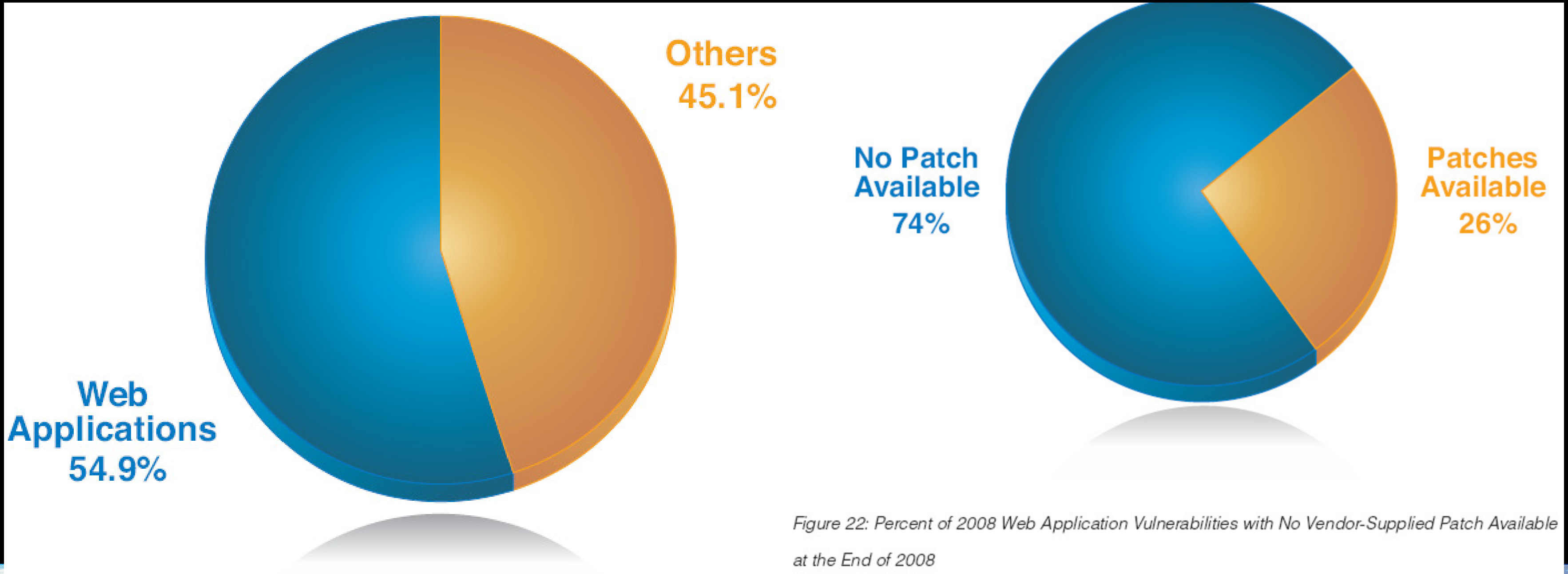
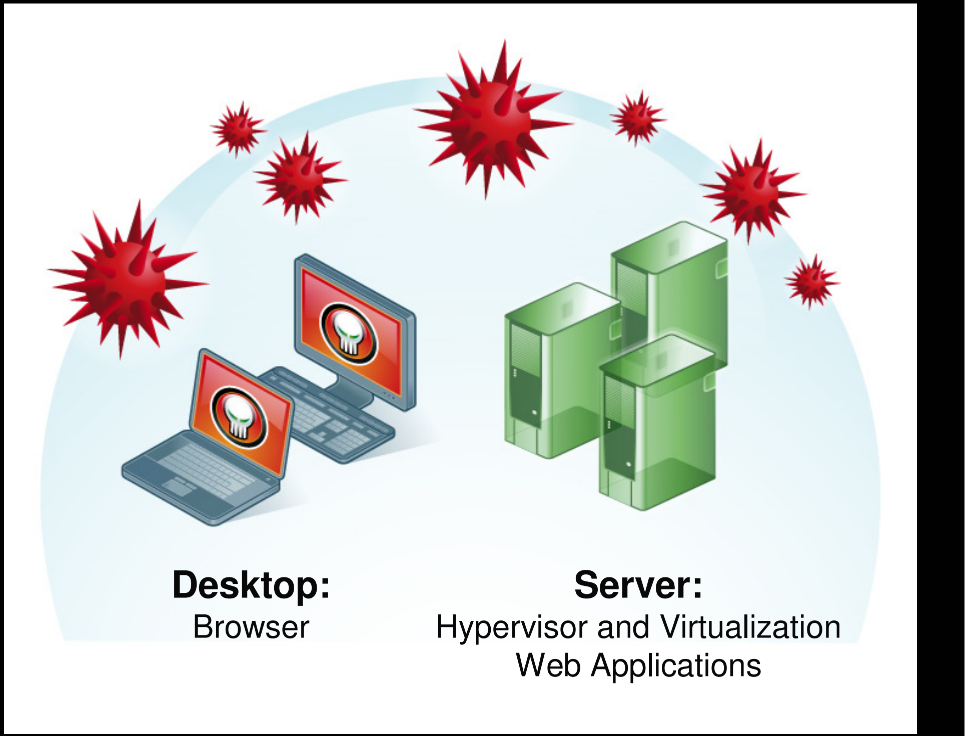


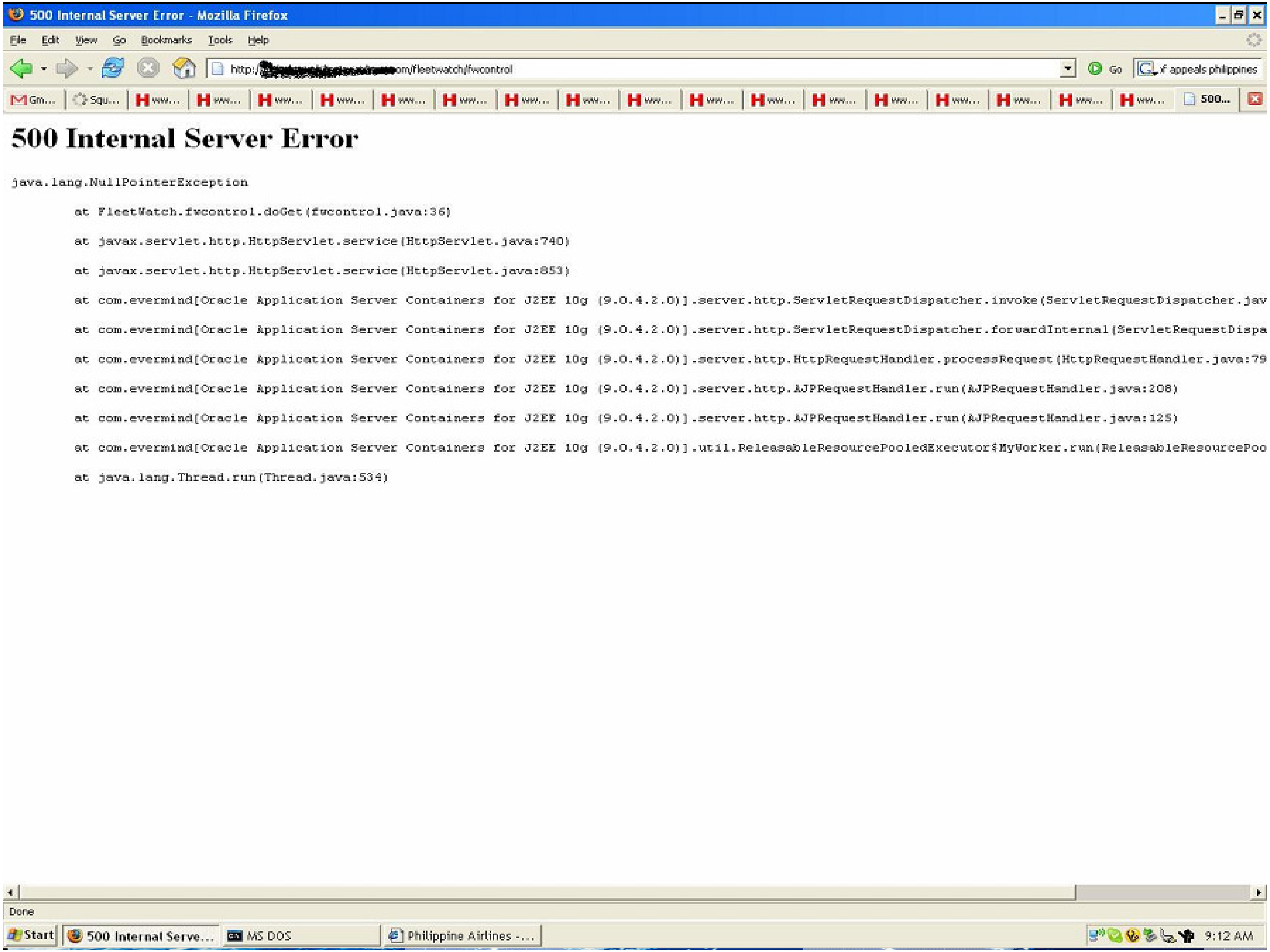
Figure 22: Percent of 2008 Web Application Vulnerabilities with No Vendor-Supplied Patch Available at the End of 2008

Changing security landscape creates complex threats

Web-enabled applications drive the need for security

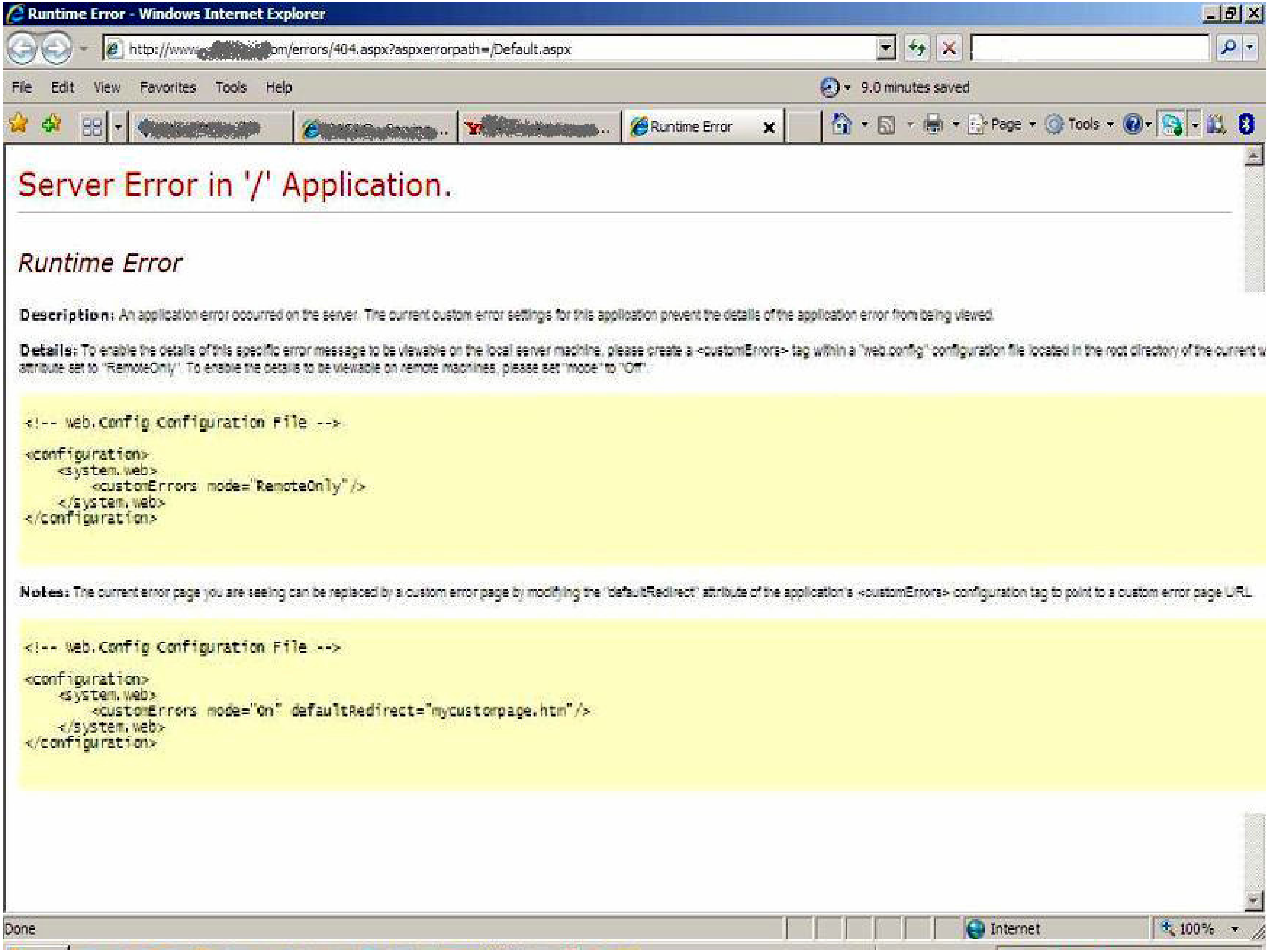
- New applications are increasing the attack surface
- Complex Web applications create complex security risks
- Making applications more available to "good" users, makes them more available to "bad" users
- Web attacks are evolving to blended attacks (i.e. planting of malware on legitimate Web sites)





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)
```



Server Error in '/' Application.

Runtime Error

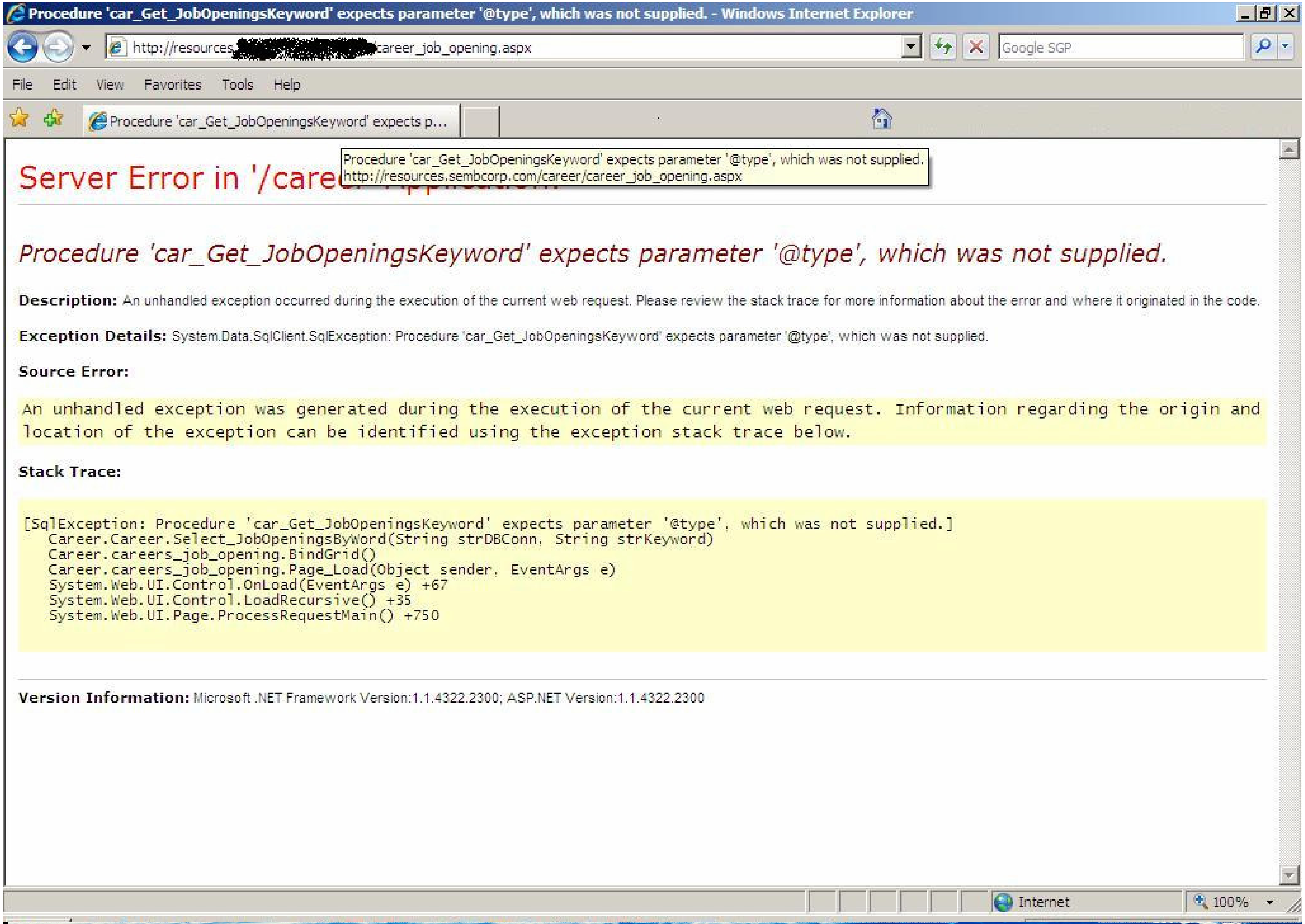
Description: An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed.

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>
```



Procedure 'car_Get_JobOpeningsKeyword' expects parameter '@type', which was not supplied. - Windows Internet Explorer

http://resources[redacted]career_job_opening.aspx

Procedure 'car_Get_JobOpeningsKeyword' expects p...

Procedure 'car_Get_JobOpeningsKeyword' expects parameter '@type', which was not supplied.
http://resources.sembcorp.com/career/career_job_opening.aspx

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.

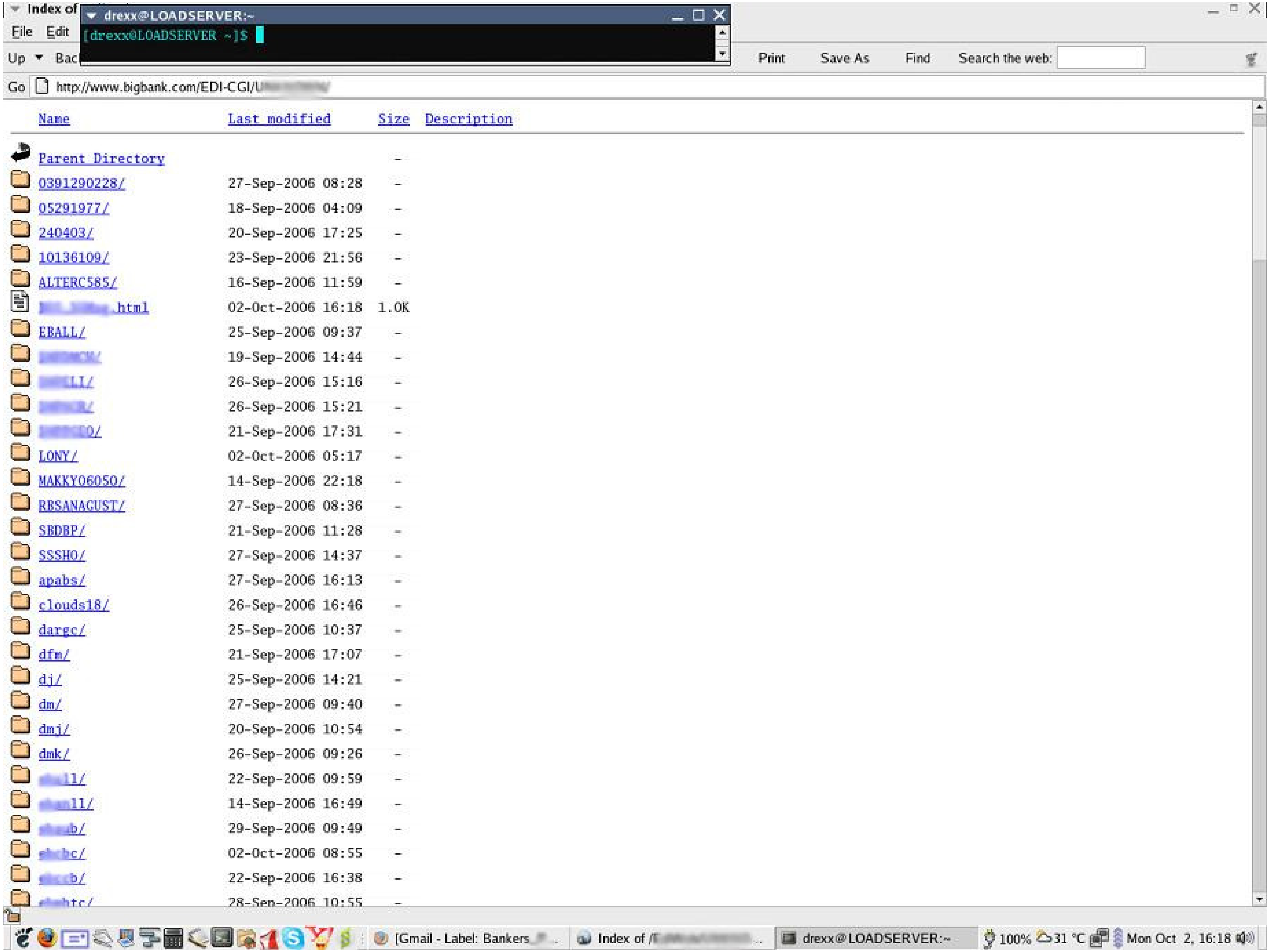
Source Error:

```
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
```

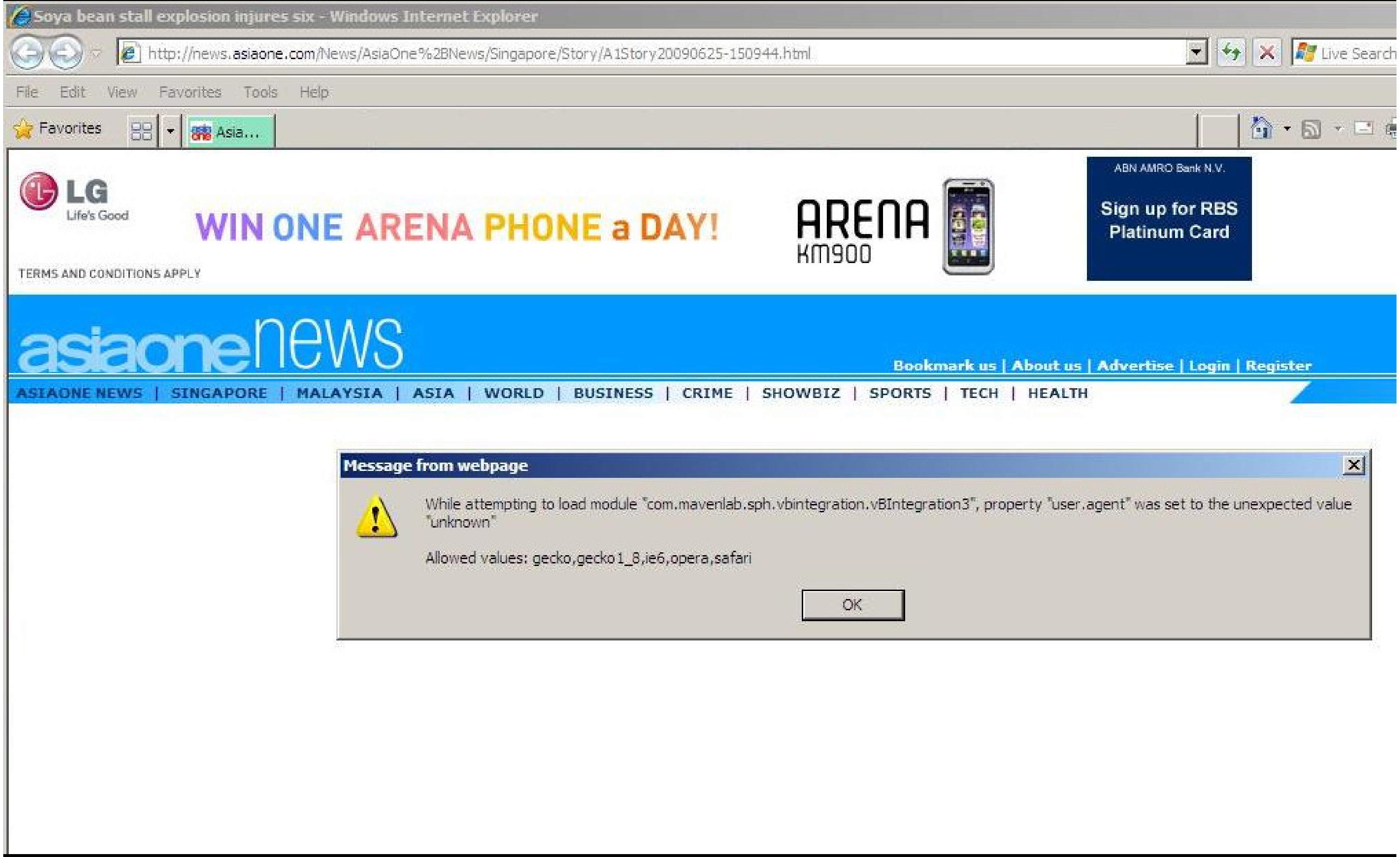
Version Information: Microsoft .NET Framework Version:1.1.4322.2300; ASP.NET Version:1.1.4322.2300



```
[drexx@LOADSERVER ~]$ 
```

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]EO/              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]anll/            14-Sep-2006 16:49    -
   [redacted]ub/              29-Sep-2006 09:49    -
   [redacted]cbc/             02-Oct-2006 08:55    -
   [redacted]ccb/             22-Sep-2006 16:38    -
   [redacted]htc/             28-Sep-2006 10:55    -
```

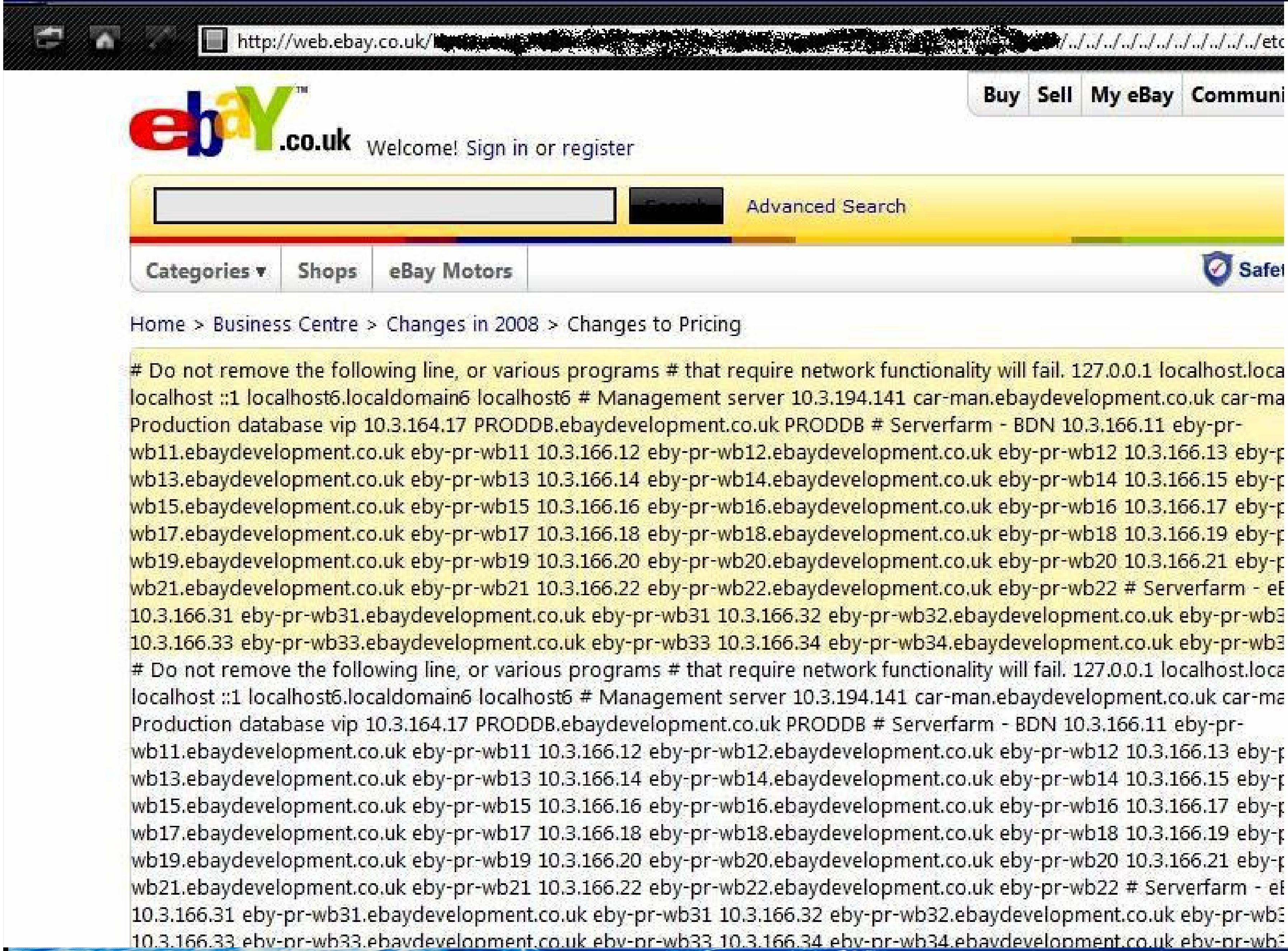


Soya bean stall explosion injures six - Windows Internet Explorer
http://news.asiaone.com/News/AsiaOne%2BNews/Singapore/Story/A1Story20090625-150944.html
Live Search
File
Edit
View
Favorites
Tools
Help
Favorites
Asia...
LG Life's Good
WIN ONE ARENA PHONE a DAY!
ARENA KM900
TERMS AND CONDITIONS APPLY
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
OK

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

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

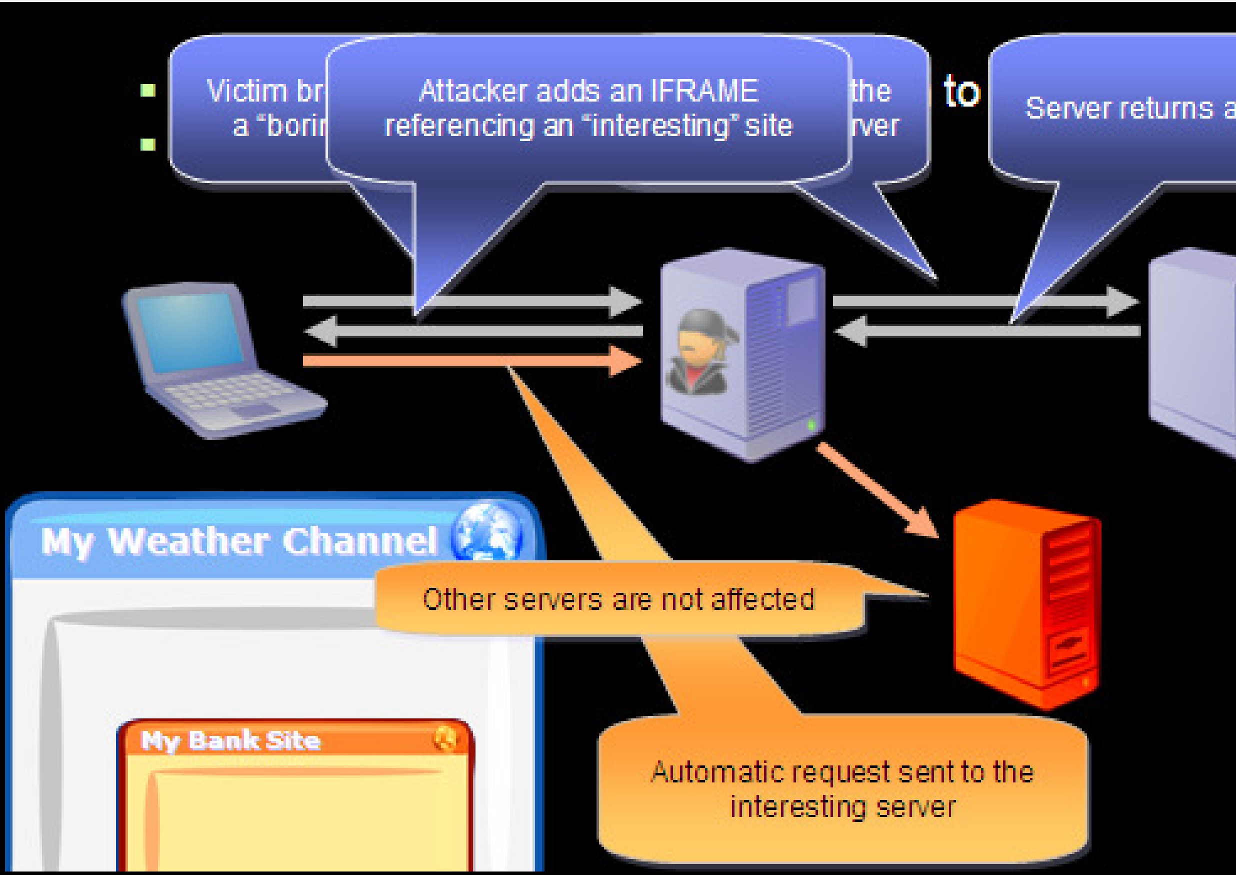


http://web.ebay.co.uk/[redacted]/../../../../../../../../../../../etc

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
```

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



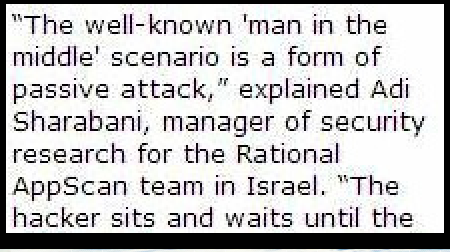
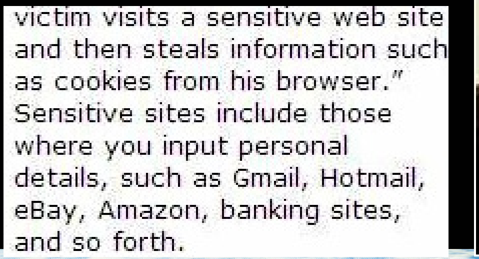
Victim br
a "borin
Attacker adds an IFRAME referencing an "interesting" site
the
rver
to
Server returns a response
My Weather Channel
My Bank Site
Other servers are not affected
Automatic request sent to the interesting server

First presented at

OWASP AP

Conference

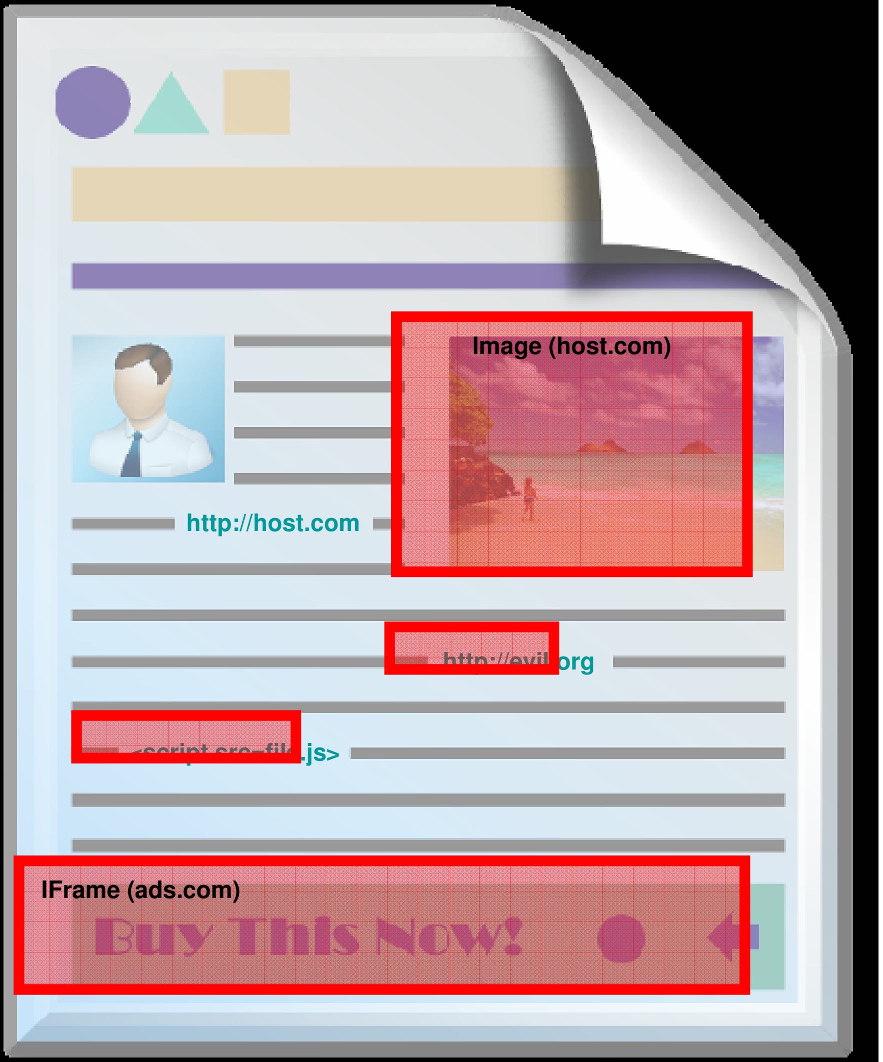
Mar 09 Brisbane

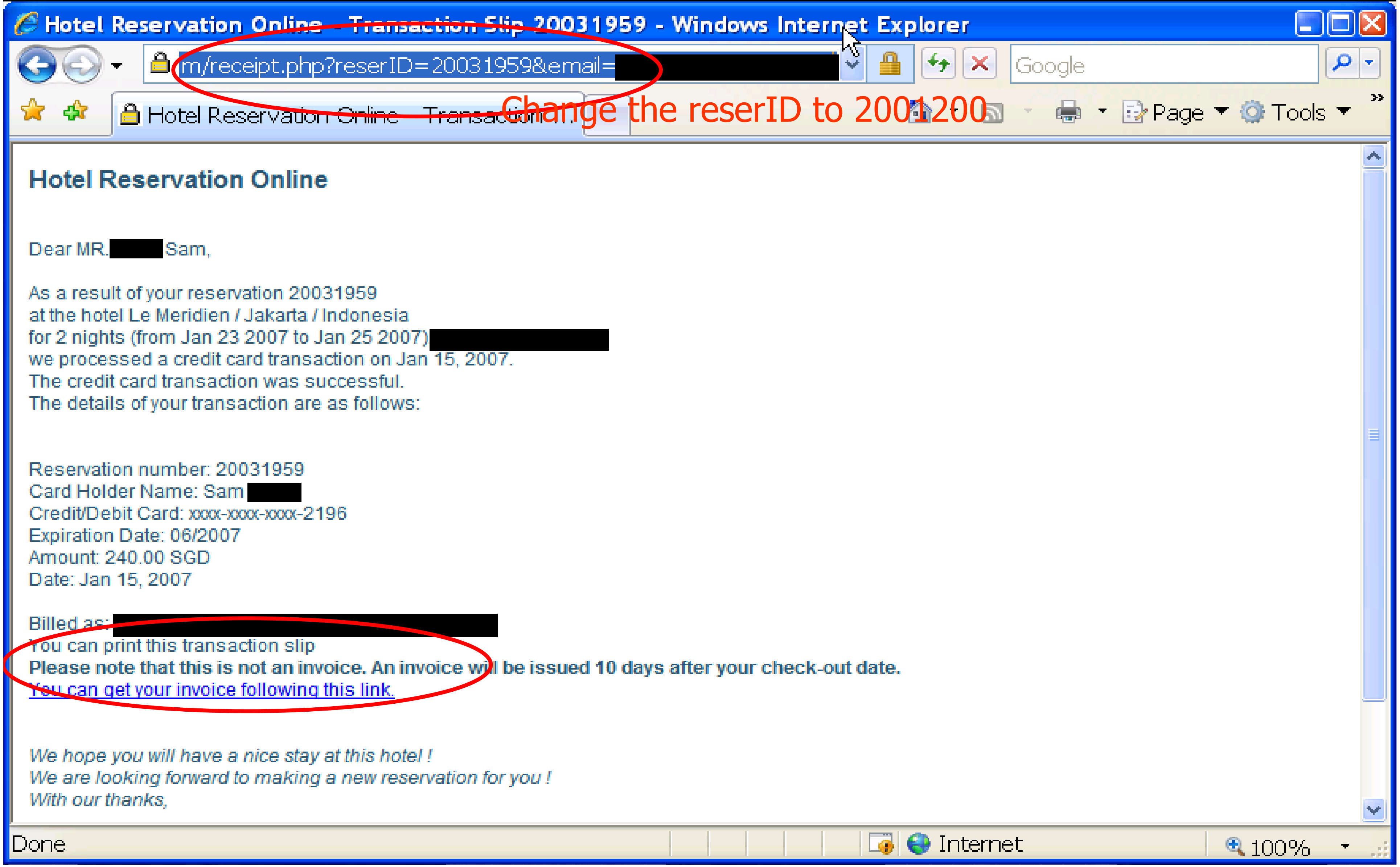
"The well-known 'man in the middle' scenario is a form of passive attack," explained Adi Sharabani, manager of security research for the Rational AppScan team in Israel. "The hacker sits and waits until the victim visits a sensitive web site and then steals information such as cookies from his browser."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

Malware on Web Applications

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



Real Example:
Online Travel Reservation Portal



Hotel Reservation Online - Transaction Slip 20031959 - Windows Internet Explorer
m/receipt.php?reserID=20031959&email= [redacted]
Google
Hotel Reservation Online - Transaction...
Page
Tools
Done
Internet
100%

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:

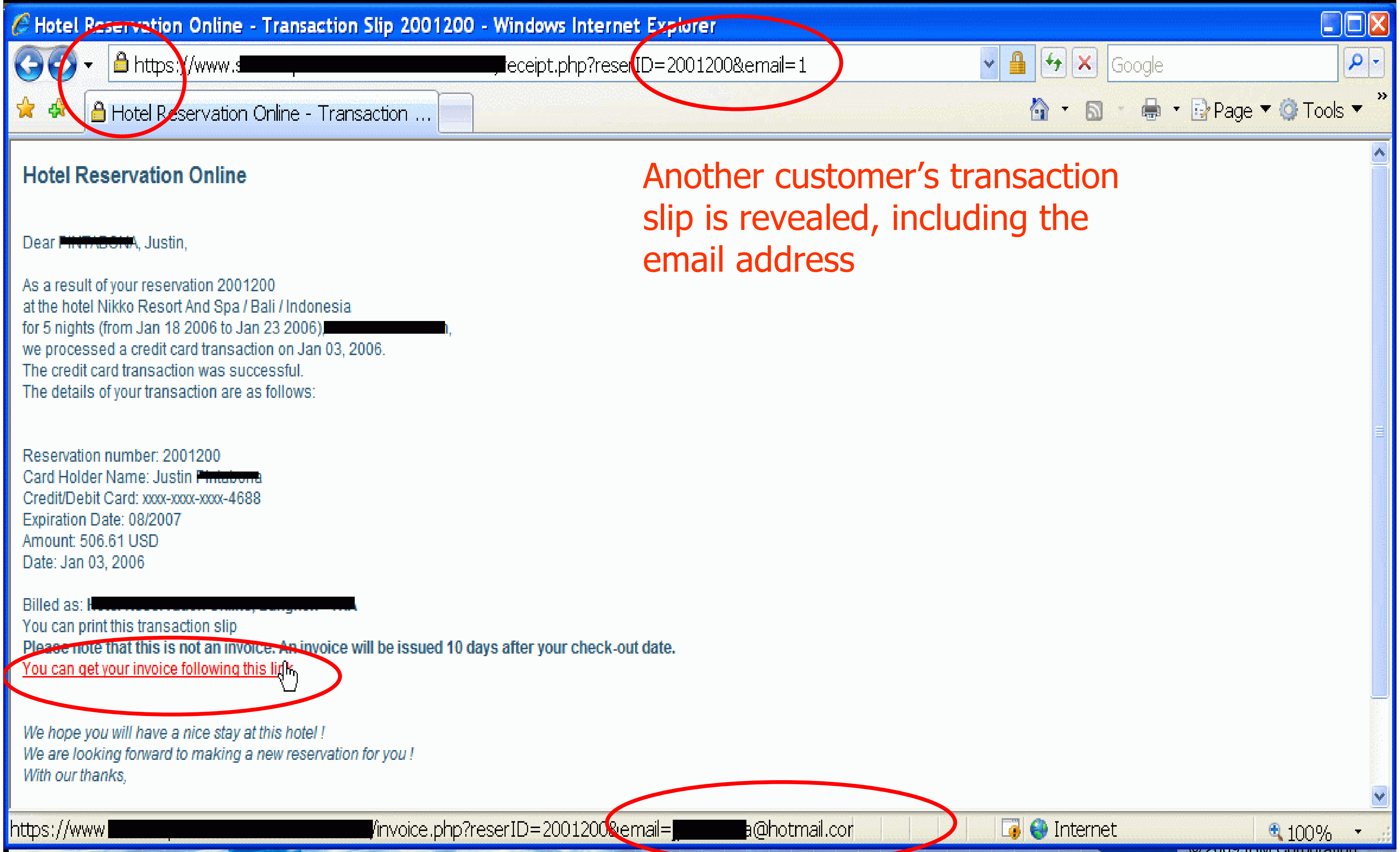
Reservation number: 20031959
Card Holder Name: Sam [redacted]
Credit/Debit Card: xxxx-xxxx-xxxx-2196
Expiration Date: 06/2007
Amount: 240.00 SGD
Date: Jan 15, 2007

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 authorisation



Hotel Reservation Online - Transaction Slip 2001200 - Windows Internet Explorer

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

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

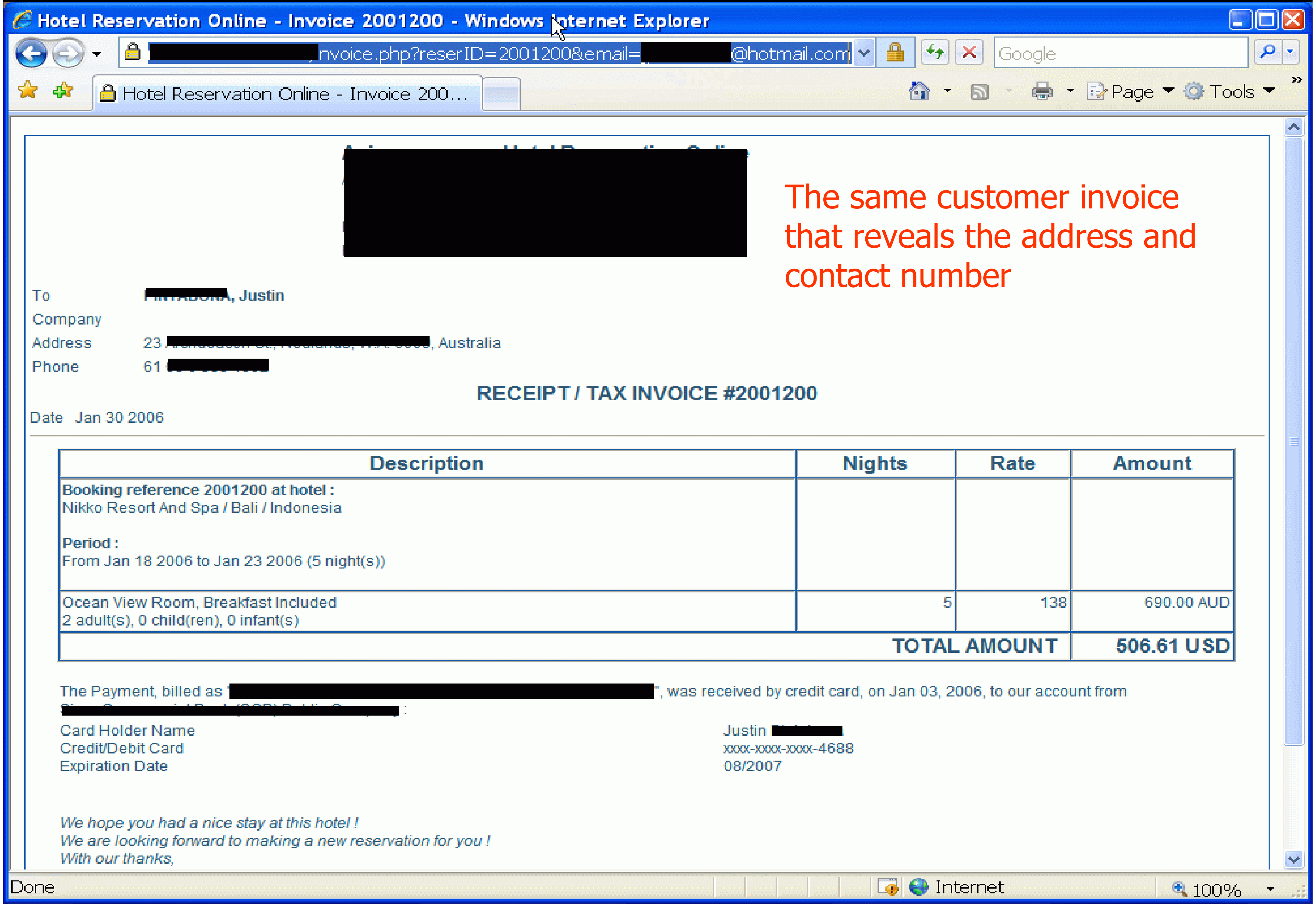
Billed as: [redacted]
You can print this transaction slip
Please note that this is not an invoice. An invoice will be issued 10 days after your check-out date.
You can get your invoice following this link

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]@hotmail.cor

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

Parameter Tampering Reading another user's invoice



Hotel Reservation Online - Invoice 2001200 - Windows Internet Explorer
[redacted]nvoice.php?reserID=2001200&email=[redacted]@hotmail.com
Google
Hotel Reservation Online - Invoice 200…
Page
Tools
Done
Internet
100%

[redacted]

The same customer invoice that reveals the address and contact number

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

RECEIPT / TAX INVOICE #2001200

Date Jan 30 2006

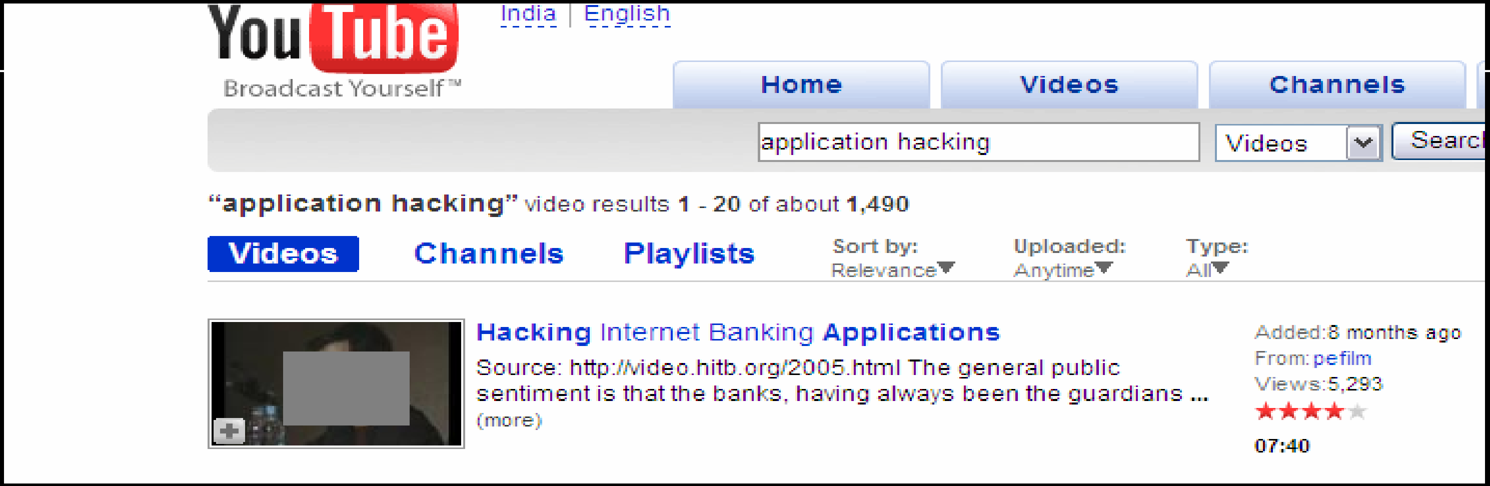
Description	Nights	Rate	Amount
Booking reference 2001200 at hotel : Nikko Resort And Spa / Bali / Indonesia **Period :** From Jan 18 2006 to Jan 23 2006 (5 night(s))			
Ocean View Room, Breakfast Included 2 adult(s), 0 child(ren), 0 infant(s)	5	138	690.00 AUD
		TOTAL AMOUNT	**506.61 USD**

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

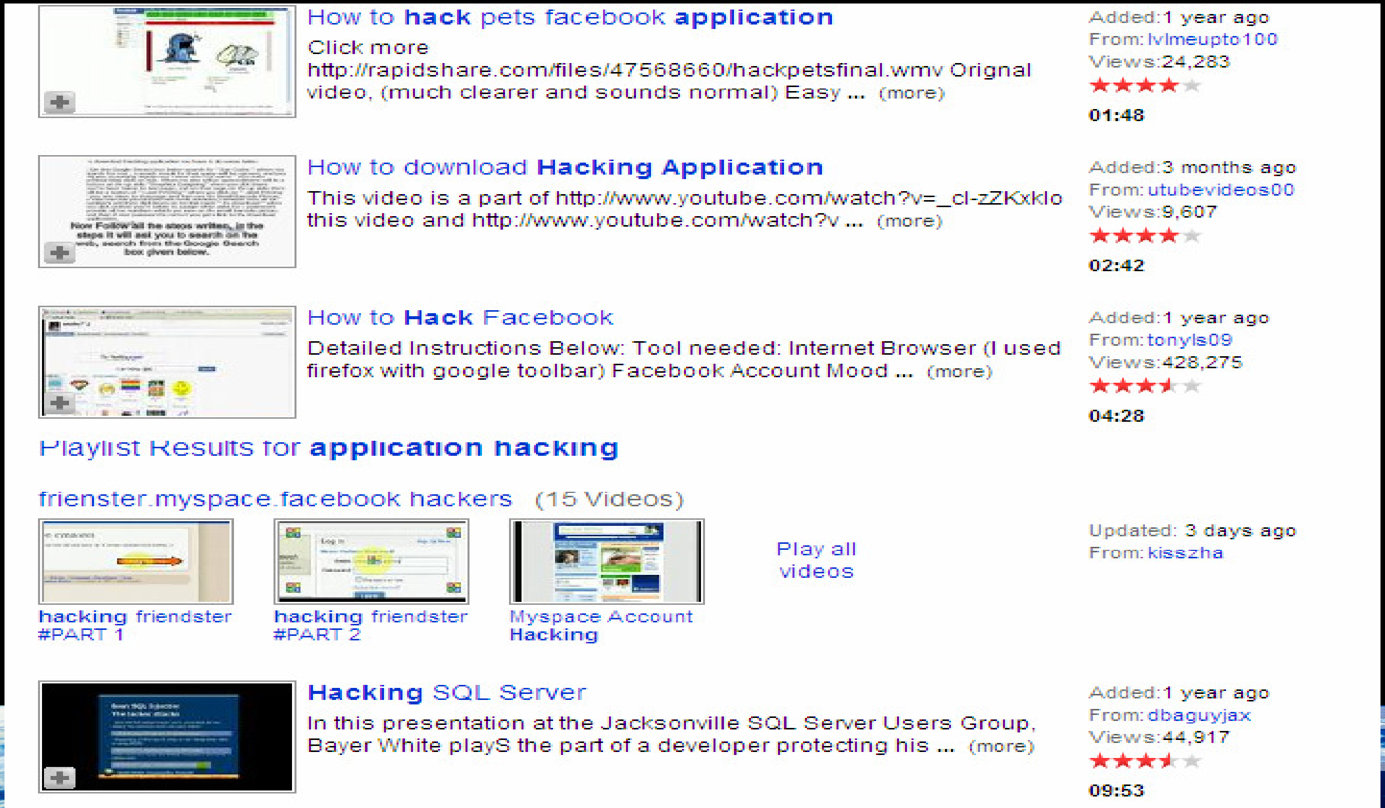
We hope you had a nice stay at this hotel !
We are looking forward to making a new reservation for you !
With our thanks,

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**

friensterr.myspace.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

Top 10 OWASP
Critical Web Application Security Issues ‘09

1 Unvalidated Input

2 Broken Access Control

3 Broken Authentication and Session Management

4 Cross Site Scripting Flaws

5 Buffer Overflows

6 Injection Flaws

7 Improper Error Handling

8 Insecure Storage

9 *Denial of Service*

10 Insecure Configuration Management

Why do hackers today target applications?

- Because they know you have firewalls
  - So its not very convenient to attack the network anymore
  - But they still want to attack 'cos they still want to steal data …

- Because firewalls do not protect against app attacks!
  - So the hackers are having a field day!
  - Very few people are actively aware of application security issues

- Because web sites have a large footprint
  - No need to worry anymore about cumbersome IP addresses

- Because they can!
  - **It is difficult or impossible to write a comprehensively robust application**

    Developers are yet to have secure coding as second nature

    Developers think differently from hackers

    Cheap, Fast, Good – choose two, you can't have it all

    It is a nightmare to manually QA the application

    Many companies today still do not have a software security QA policy or resource

Software Application Development Pressures

Today I’m being asked to:

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

Cheap

Fast

Good

- Choose 2

OUR GOAL IS TO WRITE BUG-FREE SOFTWARE. I'LL PAY A TEN-DOLLAR BONUS FOR EVERY BUG YOU FIND AND FIX.
S. Adams E-mail: SCOTTADAMS@AOL.COM
YAHOO!
WE'RE RICH
YES!!! YES!!! YES!!!
11/13 © 1995 United Feature Syndicate, Inc.(NYC)
I HOPE THIS DRIVES THE RIGHT BEHAVIOR.
I'M GONNA WRITE ME A NEW SUV THIS AFTER-NOON!

Why do application security problems exist ?

- IT security solutions and professionals are normally from the network /infrastructure /sysadmin side
  - They usually have little or no experience in application development
  - And developers typically don't know or don't care about security or networking

- Most companies today still do not have an application security QA policy or resource
  - IT security staff are focused on other things and are swarmed
    - App Sec is their job but they don't understand it and don't want to deal with it
    - Developers think its not their job or problem to have security in coding
    - People who outsource expect the 3rd party to security-QA for them

- It is cultural currently to not associate security with coding
  - "Buffer Overflow" has been around for 25 years!
  - "Input Validation" is still often overlooked.

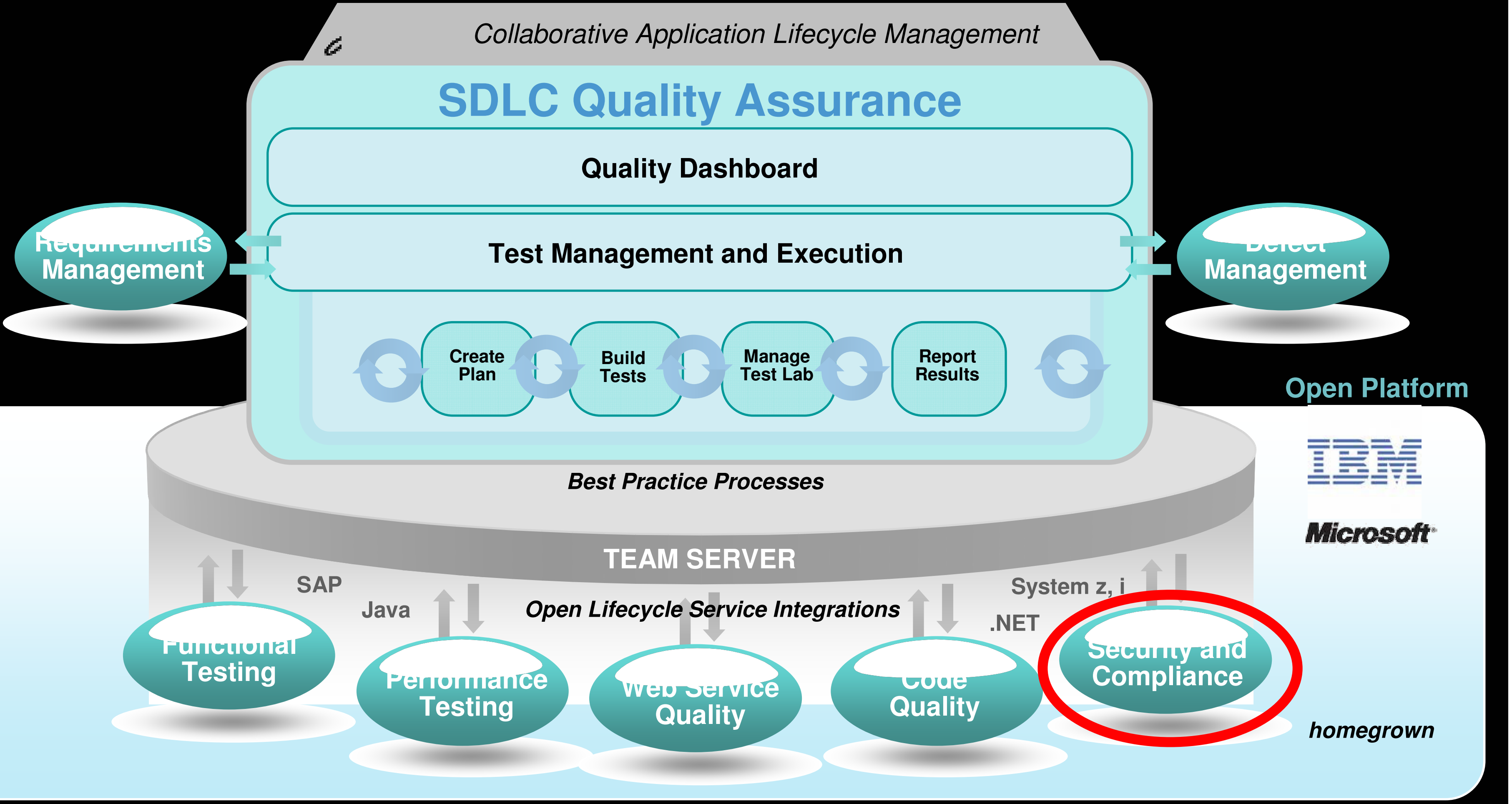
Back then coding was done by engineers …

Then came Y2K …

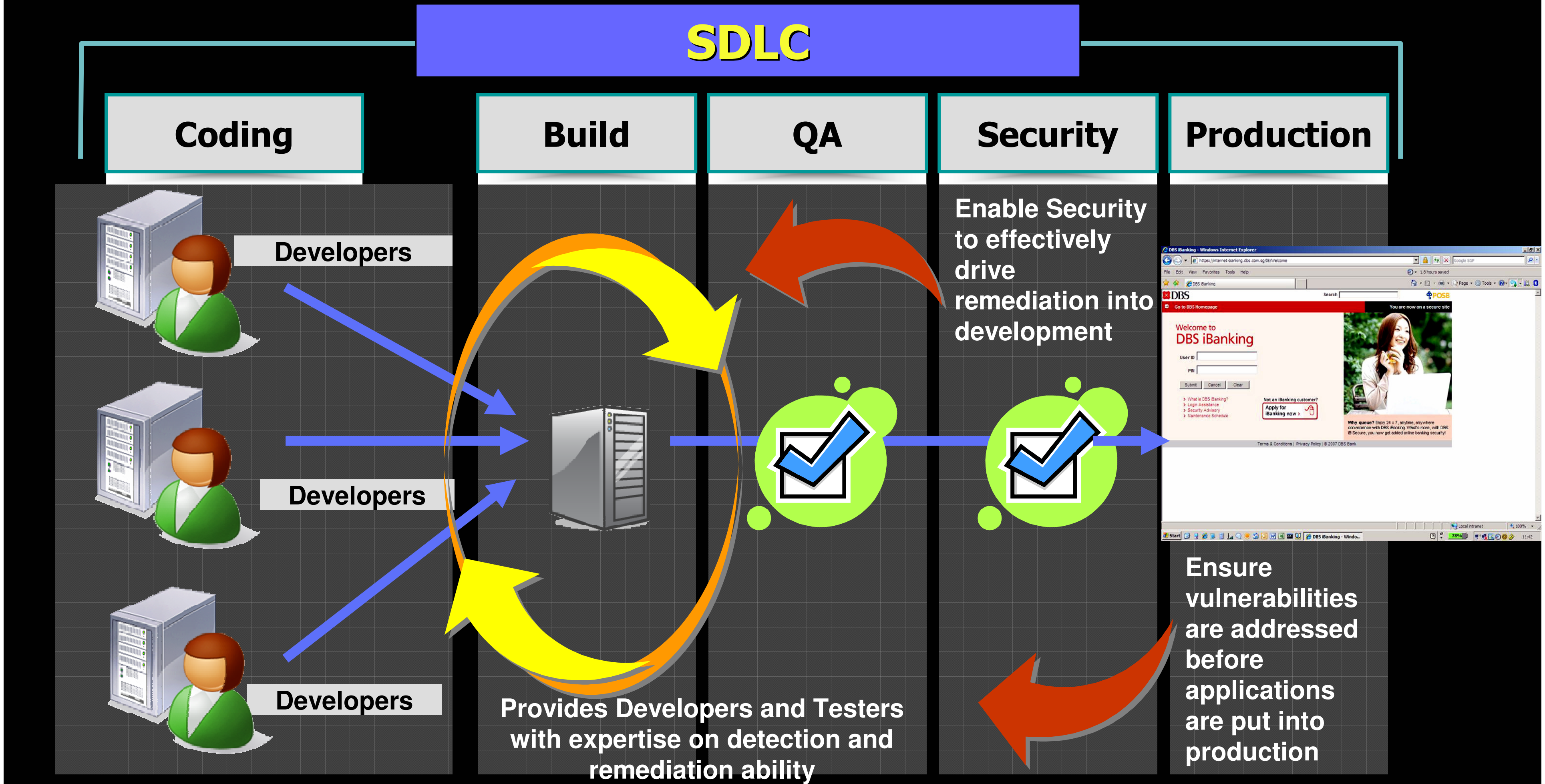
Web Application Secuirty - Solution Strategy

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

Security testing is part of SDLC quality testing



Building security & compliance into the SDLC – further back



SDLC

Coding

Build

QA

Security

Production

Developers

Developers

Developers

Enable Security to effectively drive remediation into development

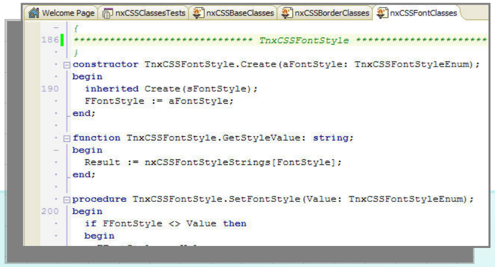
Provides Developers and Testers with expertise on detection and remediation ability

Ensure vulnerabilities are addressed before applications are put into production

Software Security Testing Technologies Primer

Static Code Analysis = Whitebox

- Looking at the code for security issues (code-level scanning)

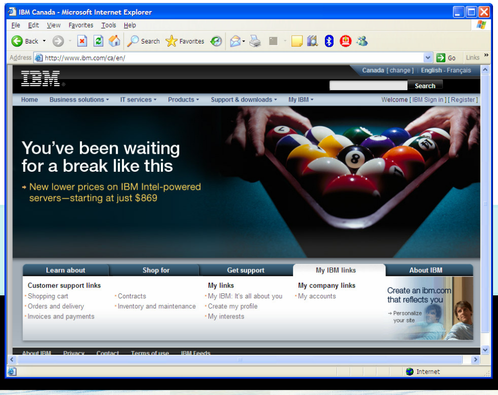


```
{
****************************** TnxCSSFontStyle **********************
}
constructor TnxCSSFontStyle.Create(aFontStyle: TnxCSSFontStyleEnum);
begin
  inherited Create(sFontStyle);
  FFontStyle := aFontStyle;
end;

function TnxCSSFontStyle.GetStyleValue: string;
begin
  Result := nxCSSFontStyleStrings[FontStyle];
end;

procedure TnxCSSFontStyle.SetFontStyle(Value: TnxCSSFontStyleEnum);
begin
  if FFontStyle <> Value then
  begin
```

Code integrity

Dynamic Analysis = Blackbox

- Sending tests to a functioning application



You've been waiting for a break like this

→ New lower prices on IBM Intel-powered servers—starting at just $869

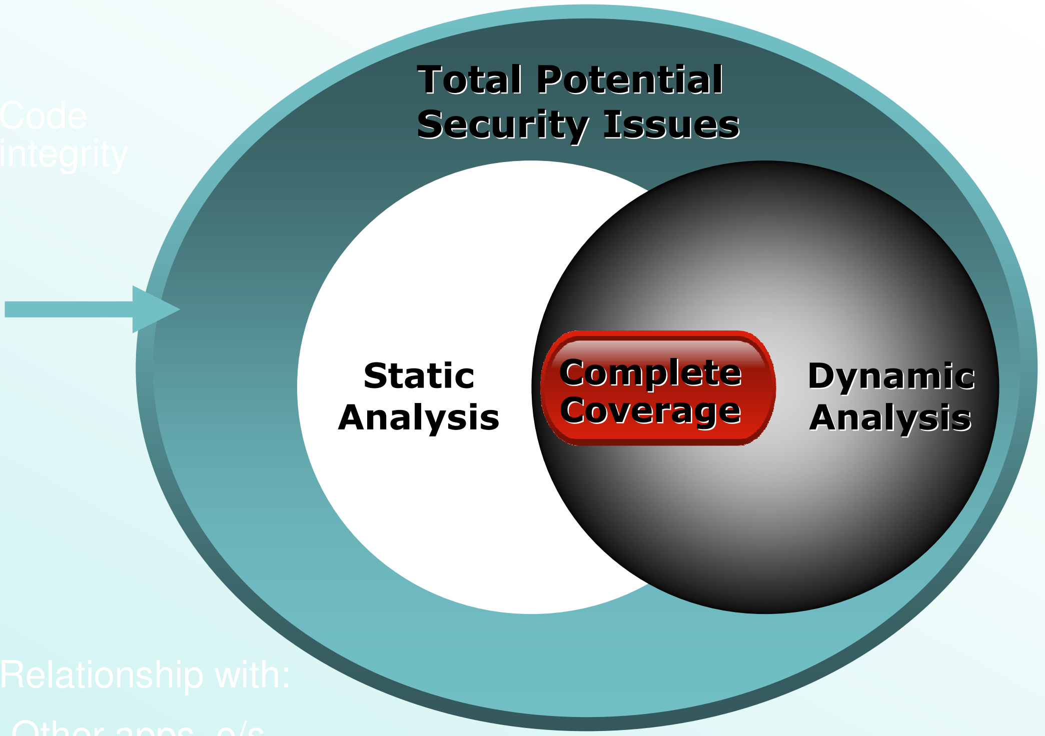
Customer support links
- Shopping cart
- Orders and delivery
- Invoices and payments
- Contracts
- Inventory and maintenance

My links
- My IBM: It's all about you
- Create my profile
- My interests

My company links
- My accounts

Create an ibm.com that reflects you

→ Personalize your site



Relationship with:

-Other apps, o/s

-Middleware, infra

SOFTWARE APPLICATION SECURITY – two Areas

BLACK BOX

(Dynamic APP Analysis)

- **don’t need to worry about code (good for security folks who are not into code)**

- **Test for relationship between App and**
  - **other apps (eg SOA, Web 2.0)**
  - **network / OS / infra**
  - **middleware**

- Like IPS : tests for ‘unknown”

WHITE BOX

(State CODE Analysis)

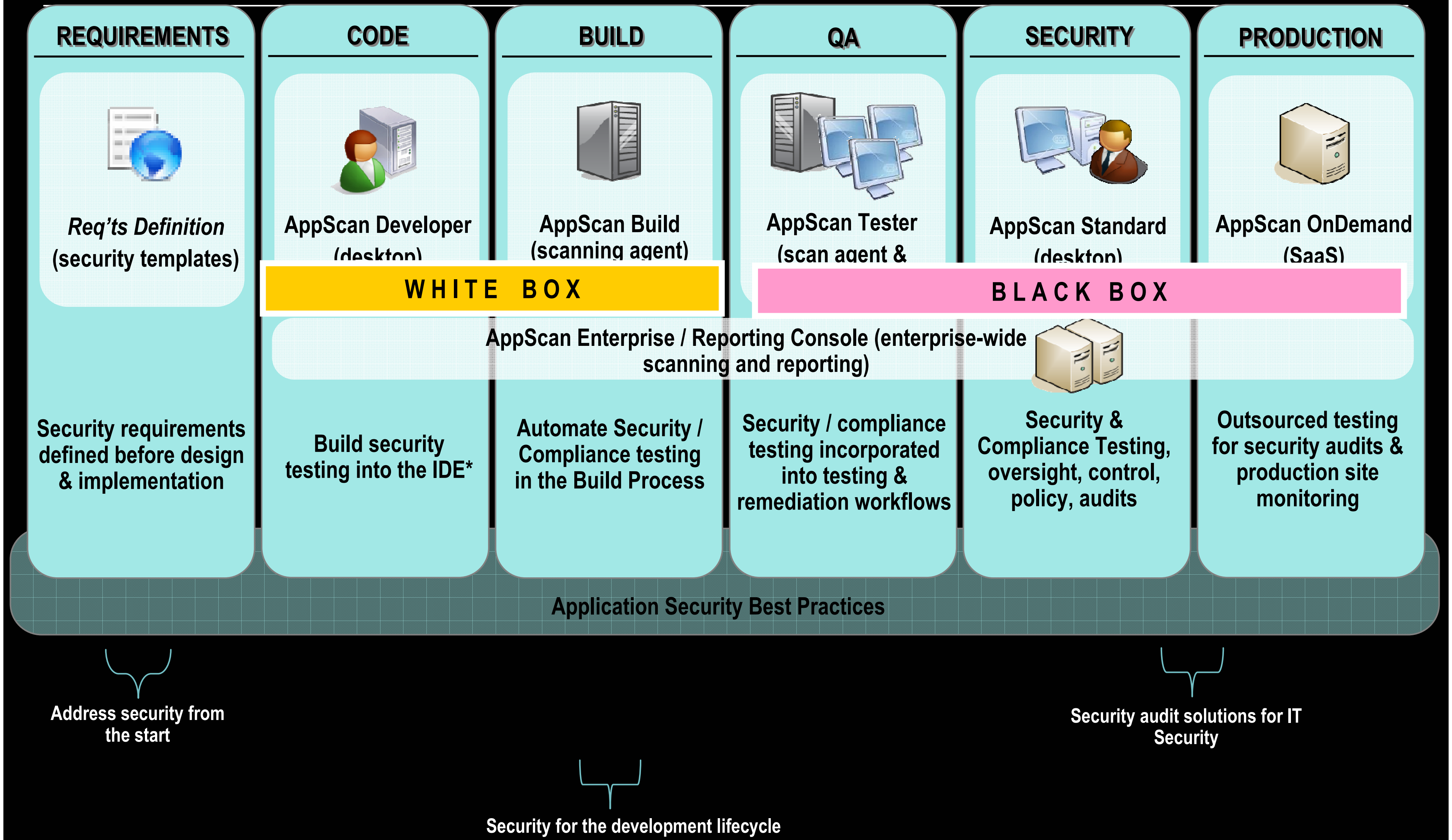
- good for developers who are not into security

- good for interim audit

- test for more than just HTML/HTTP code

- Like Firewall: checks for “known”

Rational End-to-End Application Security… at the Source



REQUIREMENTS

Req'ts Definition (security templates)

Security requirements defined before design & implementation

CODE

AppScan Developer (desktop)

Build security testing into the IDE*

BUILD

AppScan Build (scanning agent)

Automate Security / Compliance testing in the Build Process

QA

AppScan Tester (scan agent &

Security / compliance testing incorporated into testing & remediation workflows

SECURITY

AppScan Standard (desktop)

Security & Compliance Testing, oversight, control, policy, audits

PRODUCTION

AppScan OnDemand (SaaS)

Outsourced testing for security audits & production site monitoring

WHITE BOX

BLACK BOX

AppScan Enterprise / Reporting Console (enterprise-wide scanning and reporting)

Application Security Best Practices

Address security from the start

Security for the development lifecycle

Security audit solutions for IT Security

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

IBM

www.isc2.org

CISSP

CSSLP CM
Certified Secure Software Lifecycle Professional
(ISC)2®
SECURITY TRANSCENDS TECHNOLOGY®

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

Conclusion: Application QA for Security

- The Application Must Defend Itself
  - You cannot depend on firewall or infrastructure security to do so

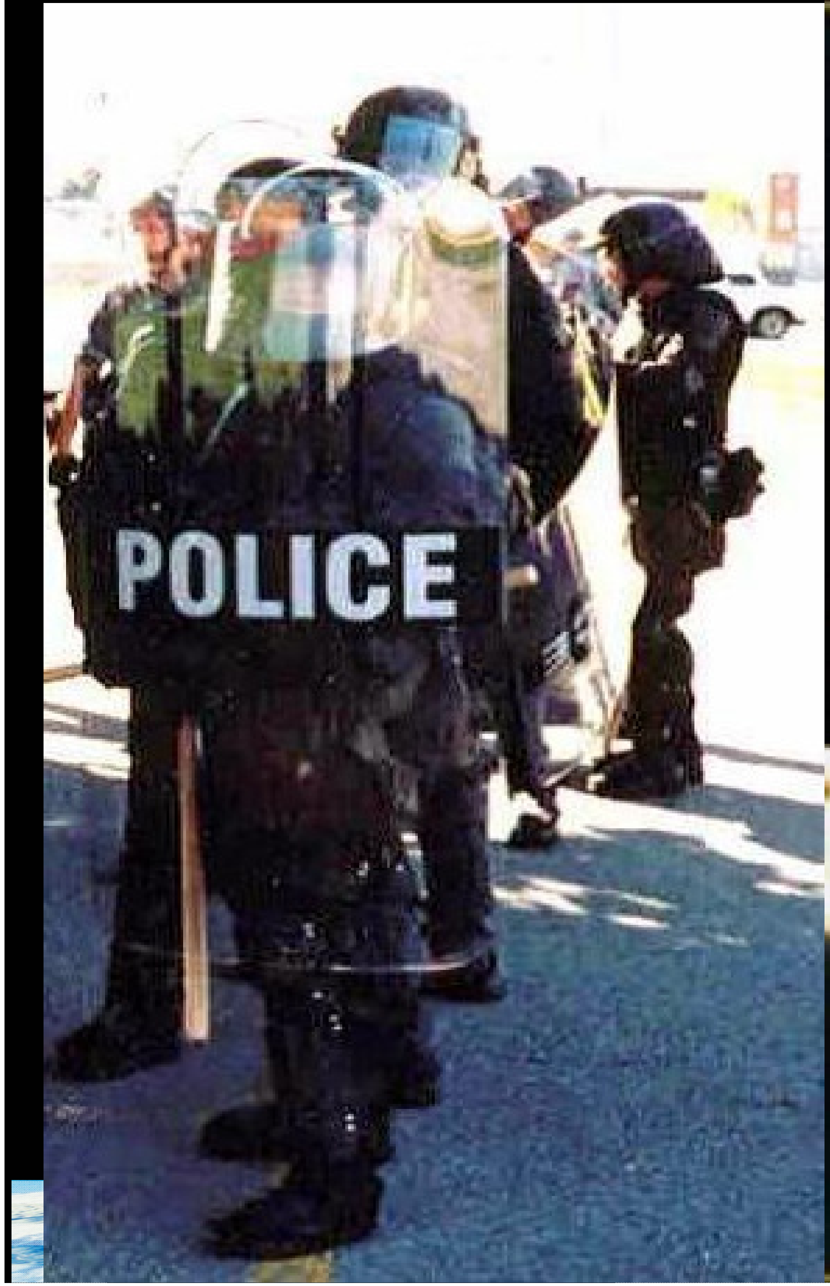
- Bridging the GAP between Software development and Information Security

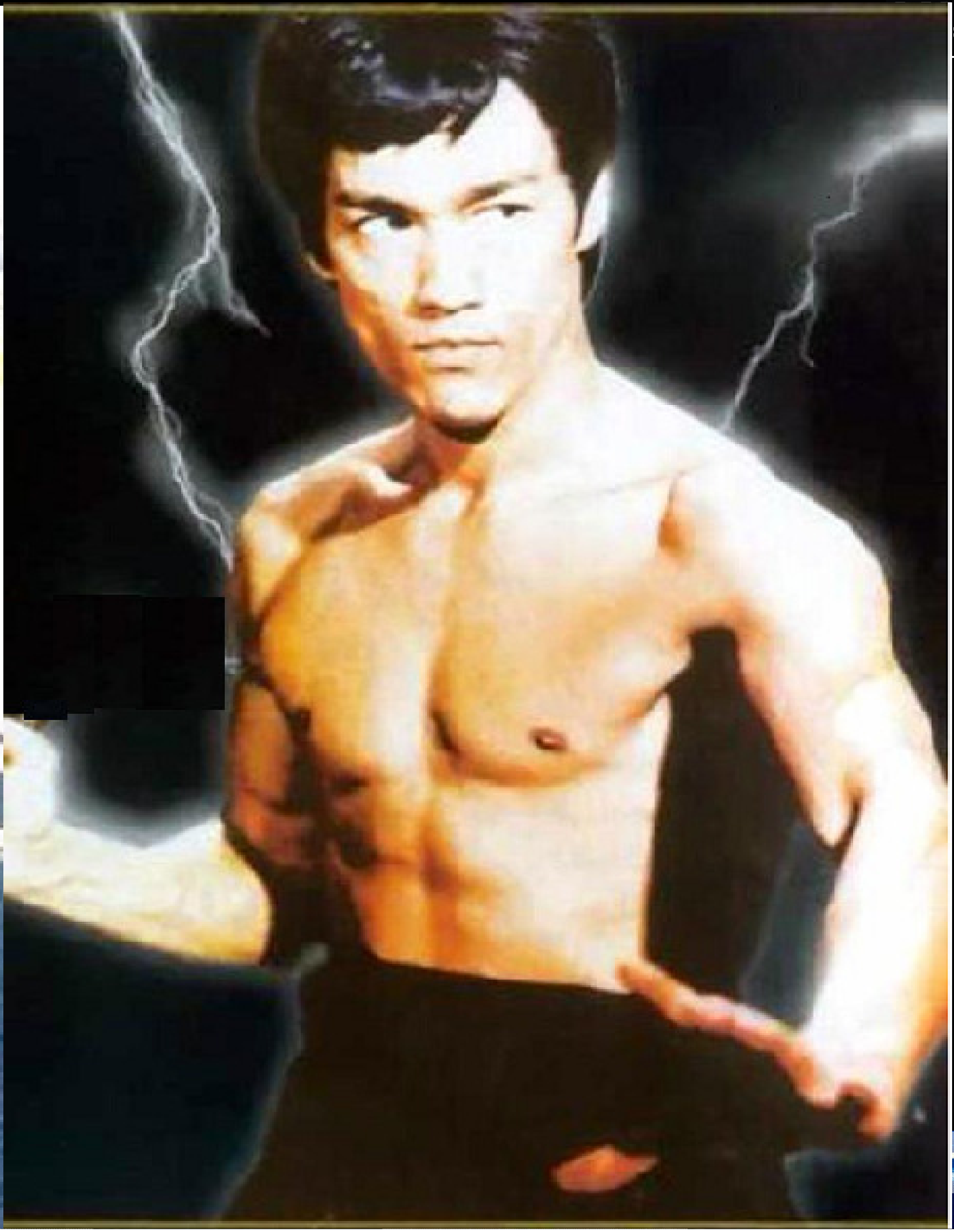
- QA Testing for Security must now be integrated and strategic

- We need to move security QA testing back to earlier in the SDLC
  - at production or pre-production stage is late and expensive to fix
  - Developers need to learn to write code defensively and securely

- Lower Compliance & Security Costs by:
- Ensuring Security Quality in the Application up front
- Not having to do a lot of rework after production

SDLC QA - YOUR LAST LINE OF DEFENSE





CSSLP

Certified Secure Software Lifecycle Professional

THANK YOU

Staying Ahead Of CyberCrime Today – Software Quality

Anthony Lim
MBA FCITIL
CISSP CSSLP

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