Cloud Computing Security – the Soft Spot

Security by Application Development Quality

Anthony Lim
Director, Security, Rational Software
Asia Pacific

CSSLP
Certified Secure Software Lifecycle Professional

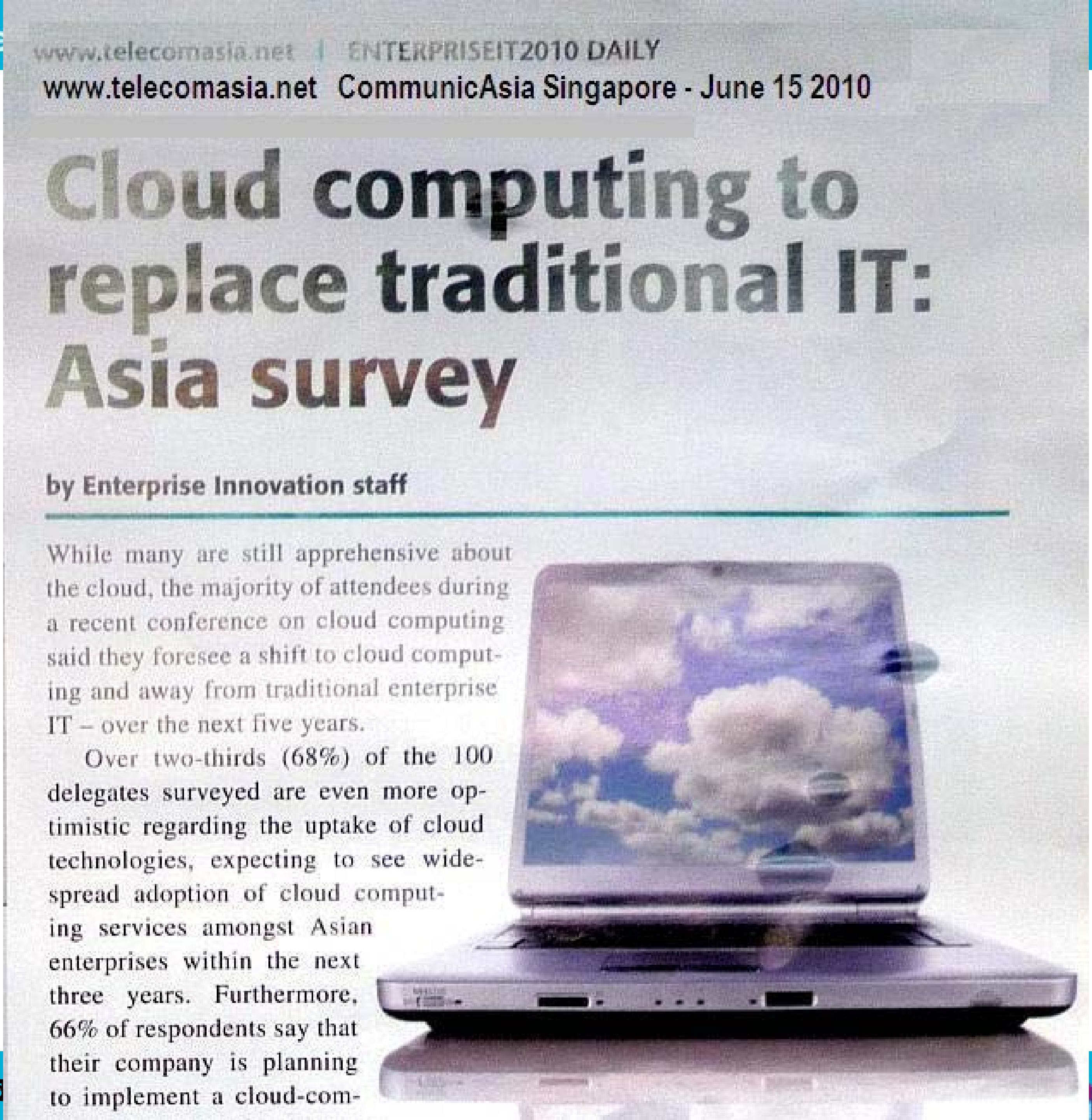
Innovate2010
The Rational Software Conference

Let's build a smarter planet.

The premiere software and product delivery event.
Taipei, ROC, 8-31-2010

IBM

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-

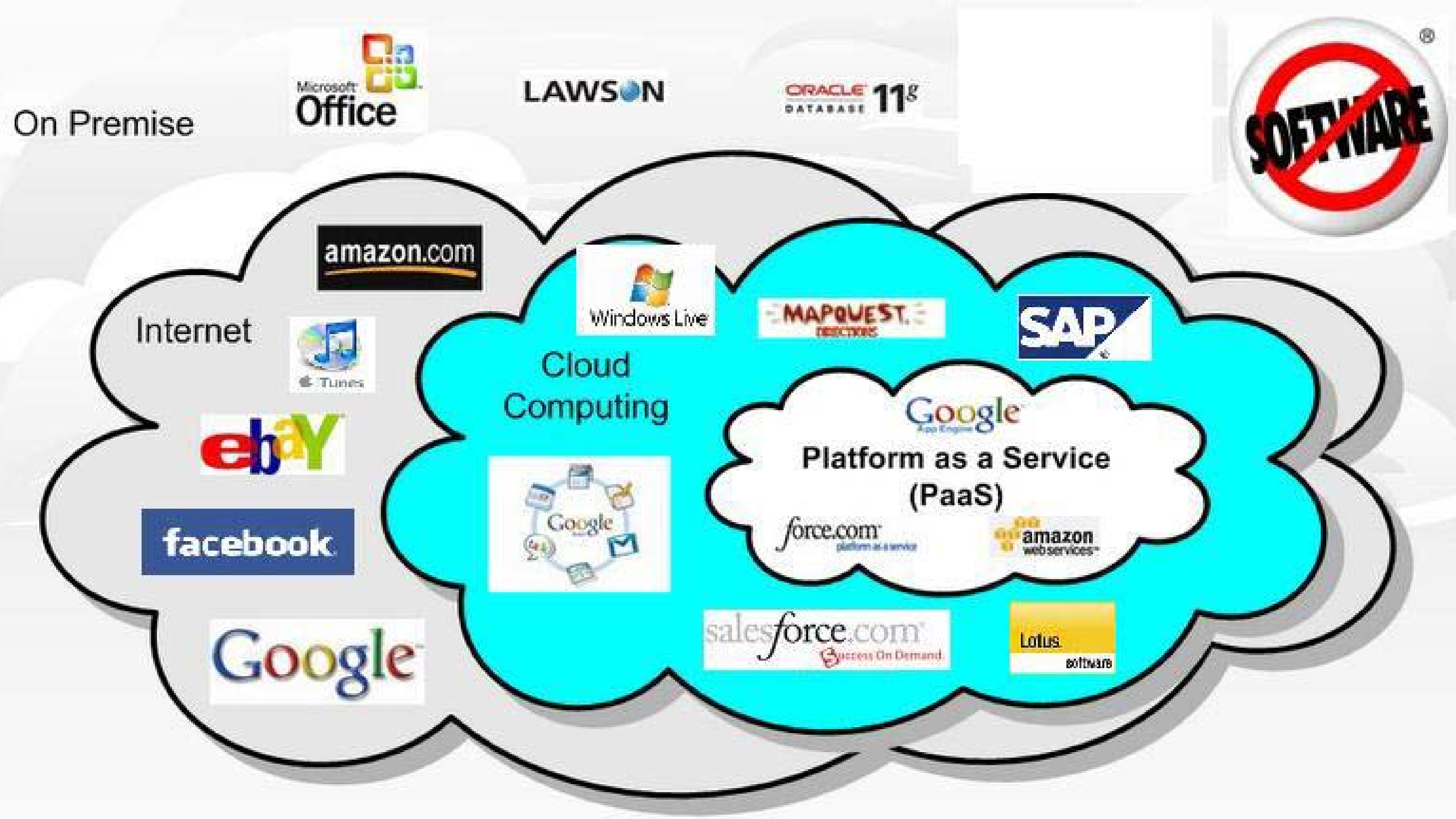
Platform as a service?

Infra as a service?

Appication as a service?

Service as a Service?!

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

- Instrumented, Interconnected, Intelligent

*** Web 2.0**

- **SOA**
- **CLOUD**

facebook
myspace
iTunes
Google
New Forms of Collaboration
facebook
Google Finance
myspace.com

Billions of mobile devices accessing the Web

Access to streams of information in the Real Time

New Possibilities..

ITS ALL ABOUT SOFTWARE!

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.**

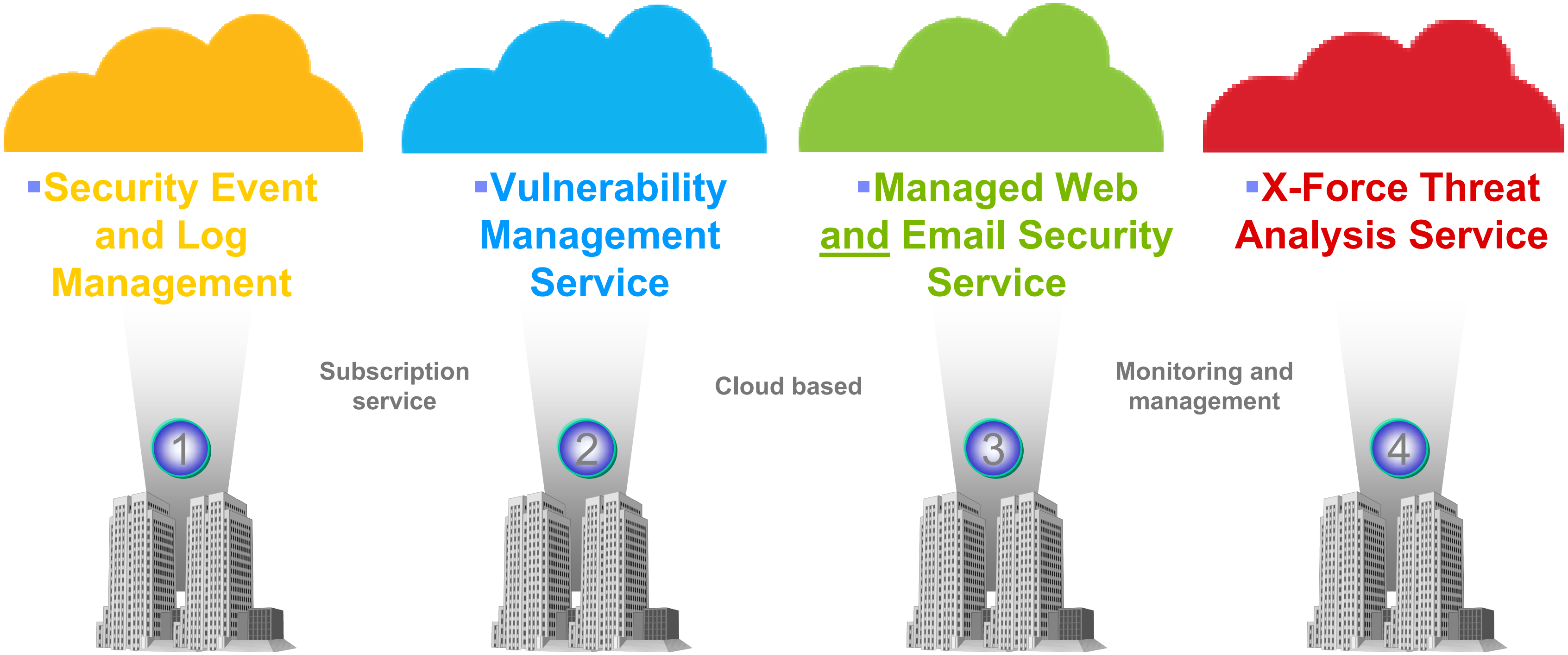
PER GARTNER

- Implement and maintain a security program.
- Build and maintain a secure cloud infrastructure.
- Ensure confidential data protection.
- Implement strong access and identity management.
- Establish application and environment provisioning.
- Implement a governance and audit management program.
- Implement a vulnerability and intrusion management program.
- Maintain environment testing and validation.

Security from the Cloud

Smart Business Security Services delivered from the IBM Cloud

From the Cloud – IBM Security Operations Centers



- **Security Event and Log Management**
- **Vulnerability Management Service**
- **Managed Web and Email Security Service**
- **X-Force Threat Analysis Service**

Subscription service

Cloud based

Monitoring and management

1. Offsite management of logs and events from IPS's, Firewalls and OSs
2. Proactive discovery and remediation of vulnerabilities
3. Protection against spam, worms, viruses, spyware, adware, and offensive content
4. Customized security intelligence based on threat information from X-Force research and development team

To the Customer – Offloading Security Tasks on the Ground

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

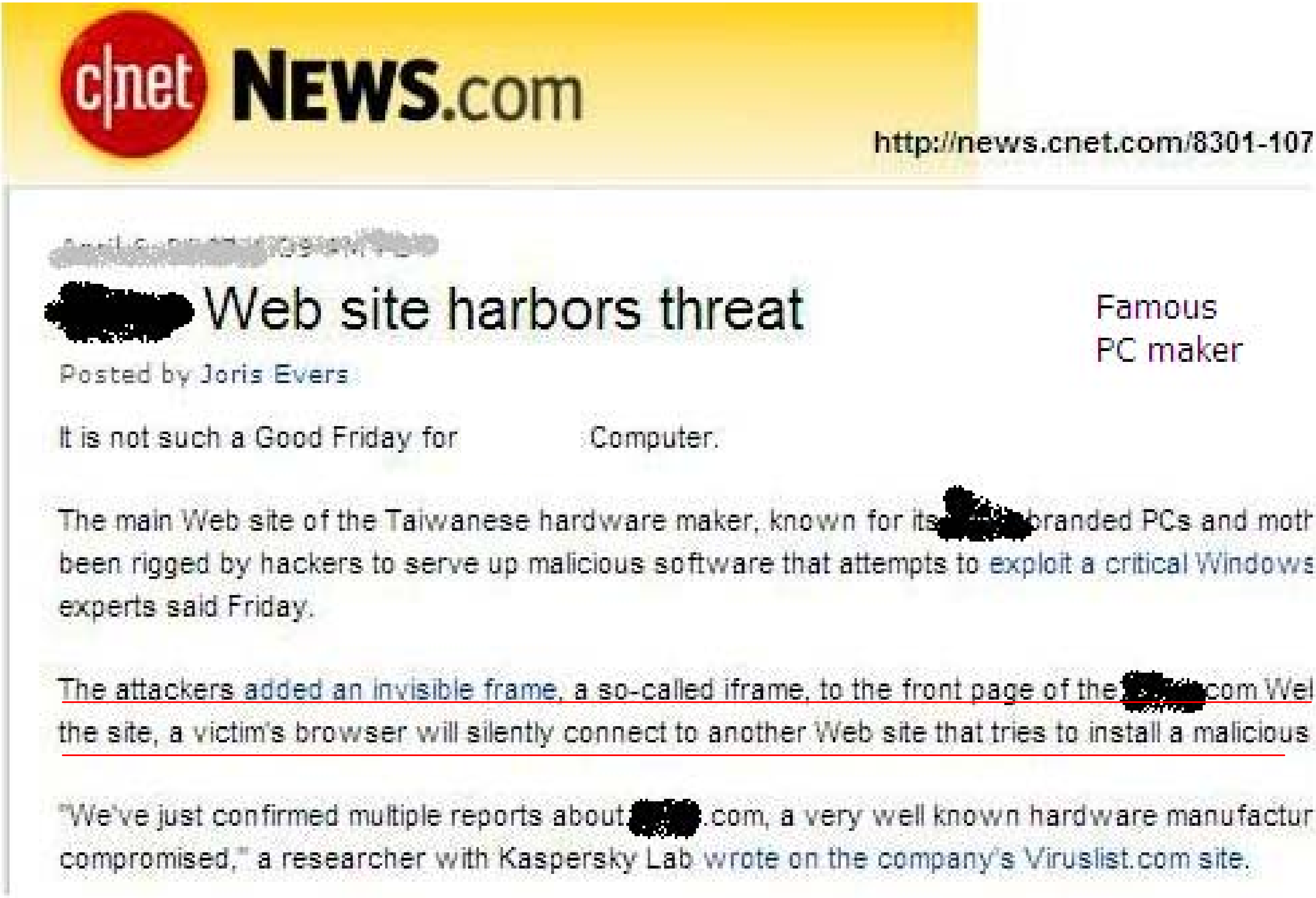
We Use Network Vulnerability Scanners

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

那麼為什麼外面還有鬼？



c|net NEWS.com

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

[redacted]

[redacted] Web site harbors threat

Famous
PC maker

Posted by Joris Evers

It is not such a Good Friday for Computer.

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

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

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

[redacted]官網遇駭 彩迷憂頭彩也能改 (2008-11-14)

Another case of malware on web site

上網對獎 電腦就會中毒

〔記者王珮華、鄭琪芳／台北報導〕[redacted]彩券官方網站（http:/[redacted].com.tw/）驚傳遭駭客植入惡意網頁與程式，只要進入該網站對獎就可能「中鏢」，網友在12日凌晨發現後奔相走告，Google、奇摩等入口網站及火狐等瀏覽器也已經將[redacted]官方網站列為警示網站。

[redacted]公司說，10月底就發現駭客入侵，已經清了20多次，所幸得獎號碼未被竄改，投注系統及資料庫都不會受影響；防毒軟體趨勢公司則說，可以免費下載該公司程式掃毒。

[redacted]彩券官方網站驚傳遭駭客攻擊，經查禍首應是來自中國網站。 （記者王珮華翻攝）

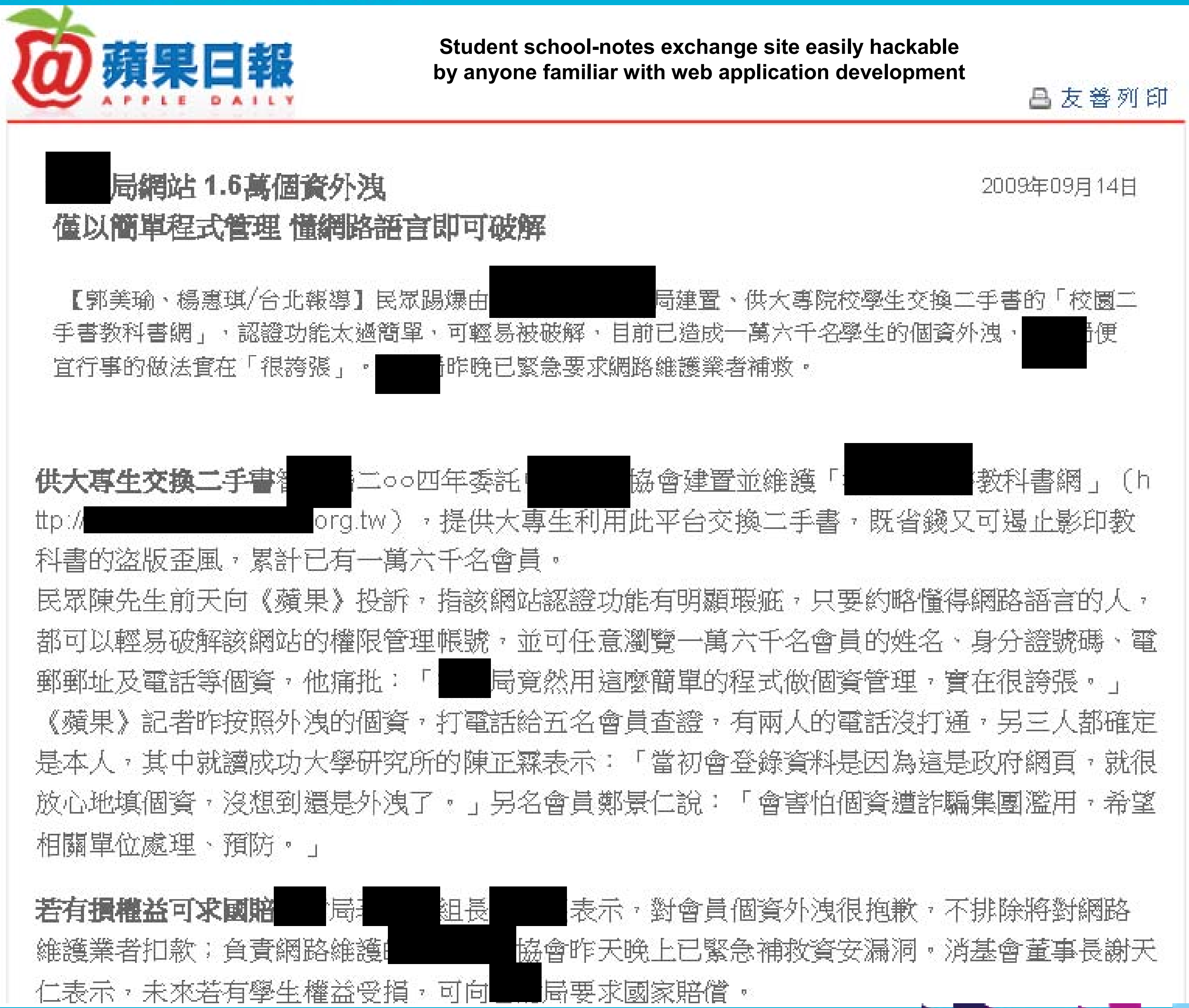
惡意程式 來自中國網站

12日凌晨，一名網友在討論區表示，開啟[redacted]官網同時，會載入一個惡意網站的頁框，該頁框高度被設為「0」，使用者不容易發現；消息經網路流傳後，[redacted]雖立刻清除，但在13日凌晨，網友又依然發現[redacted]網站含毒，截至昨天深夜11點依舊沒有清除。根據Google的資訊安全診斷紀錄顯示，惡意程式的來源都指向兩個中國網站。

根據Google Trends也顯示，[redacted]官網每天約有10萬個不重複使用者到訪，一旦被駭，影響層面相當大。網友質疑，[redacted]頭彩獎金動輒上億，網站安全怎會如此不堪一擊？駭客能在其官網「加料」，是否代表也能竄改開獎數字，甚至將頭彩得主資料曝光？

來源：自由時報 2008.11.14

Student school-notes exchange site easily hackable by anyone familiar with web application development



[redacted]局網站 1.6萬個資外洩 僅以簡單程式管理 懂網路語言即可破解

2009年09月14日

【郭美瑜、楊惠琪/台北報導】民眾踢爆由[redacted]局建置、供大專院校學生交換二手書的「校園二手書教科書網」，認證功能太過簡單，可輕易被破解，目前已造成一萬六千名學生的個資外洩，[redacted]便宜行事的做法實在「很誇張」。[redacted]昨晚已緊急要求網路維護業者補救。

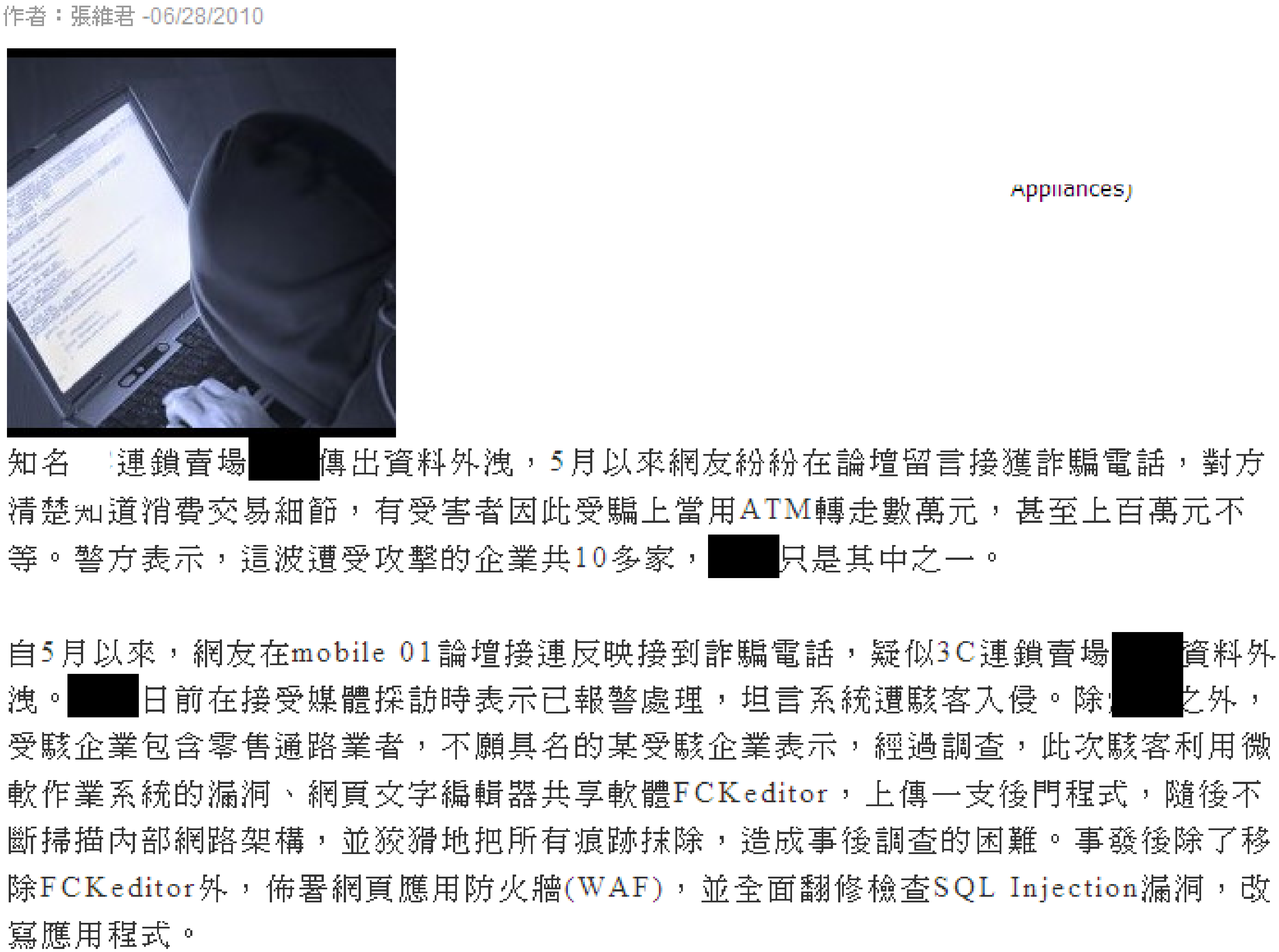
供大專生交換二手書[redacted]二○○四年委託[redacted]協會建置並維護「[redacted]教科書網」（http://[redacted]org.tw），提供大專生利用此平台交換二手書，既省錢又可遏止影印教科書的盜版歪風，累計已有一萬六千名會員。

民眾陳先生前天向《蘋果》投訴，指該網站認證功能有明顯瑕疵，只要約略懂得網路語言的人，都可以輕易破解該網站的權限管理帳號，並可任意瀏覽一萬六千名會員的姓名、身分證號碼、電郵郵址及電話等個資，他痛批：「[redacted]局竟然用這麼簡單的程式做個資管理，實在很誇張。」

《蘋果》記者昨按照外洩的個資，打電話給五名會員查證，有兩人的電話沒打通，另三人都確定是本人，其中就讀成功大學研究所的陳正霖表示：「當初會登錄資料是因為這是政府網頁，就很放心地填個資，沒想到還是外洩了。」另名會員鄭景仁說：「會害怕個資遭詐騙集團濫用，希望相關單位處理、預防。」

若有損權益可求國賠[redacted]局[redacted]組長[redacted]表示，對會員個資外洩很抱歉，不排除將對網路維護業者扣款；負責網路維護[redacted]協會昨天晚上已緊急補救資安漏洞，消基會董事長謝天仁表示，未來若有學生權益受損，可向[redacted]局要求國家賠償。

[redacted]資料外洩: IIS6漏洞加FCKeditor惹禍

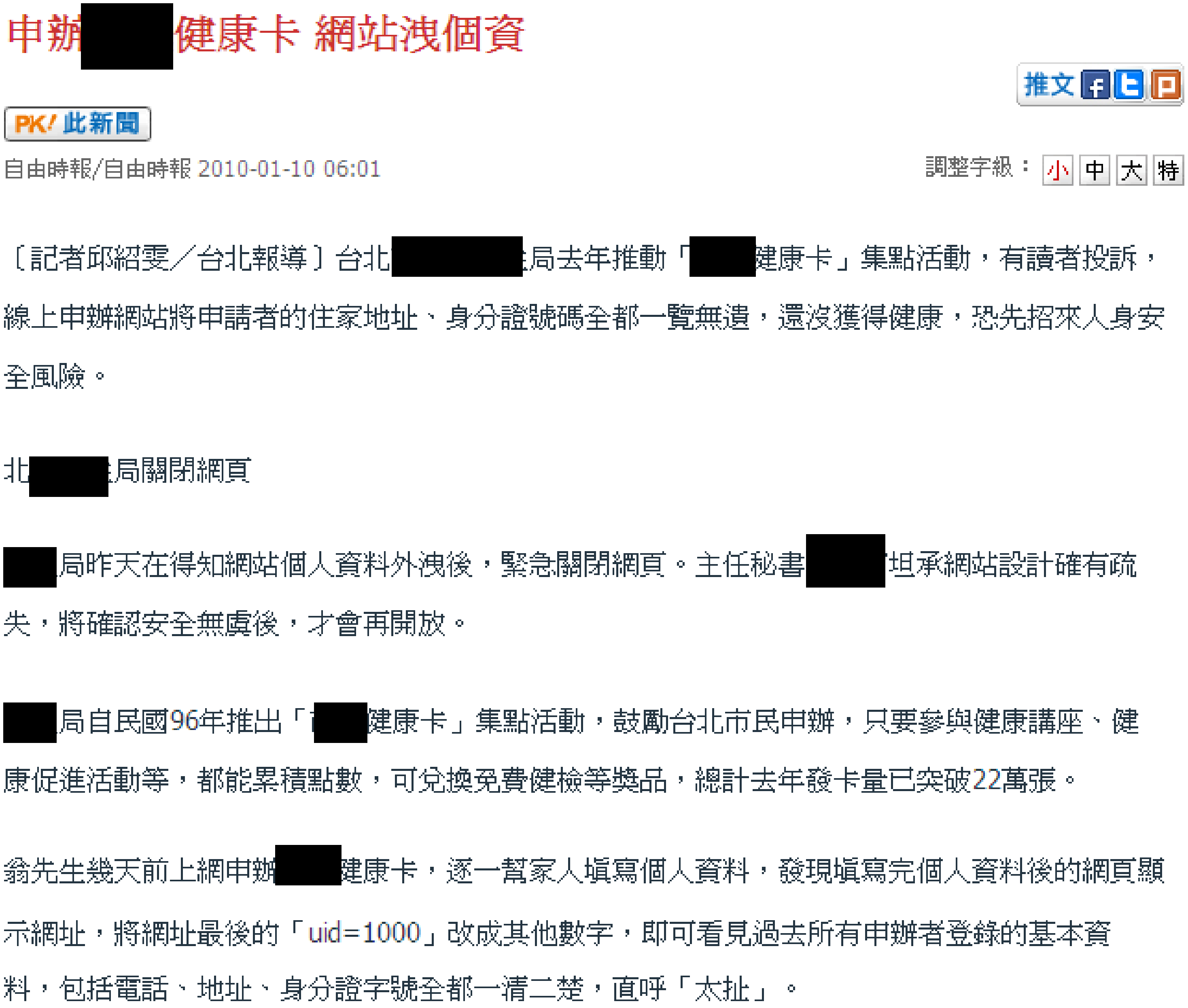


作者：張維君 -06/28/2010

Appliances)

知名 連鎖賣場[redacted]傳出資料外洩，5月以來網友紛紛在論壇留言接獲詐騙電話，對方清楚知道消費交易細節，有受害者因此受騙上當用ATM轉走數萬元，甚至上百萬元不等。警方表示，這波遭受攻擊的企業共10多家，[redacted]只是其中之一。

自5月以來，網友在mobile 01論壇接連反映接到詐騙電話，疑似3C連鎖賣場[redacted]資料外洩。[redacted]日前在接受媒體採訪時表示已報警處理，坦言系統遭駭客入侵。除[redacted]之外，受駭企業包含零售通路業者，不願具名的某受駭企業表示，經過調查，此次駭客利用微軟作業系統的漏洞、網頁文字編輯器共享軟體FCKeditor，上傳一支後門程式，隨後不斷掃描內部網路架構，並狡猾地把所有痕跡抹除，造成事後調查的困難。事發後除了移除FCKeditor外，佈署網頁應用防火牆(WAF)，並全面翻修檢查SQL Injection漏洞，改寫應用程式。



申辦[redacted]健康卡 網站洩個資

自由時報/自由時報 2010-01-10 06:01

〔記者邱紹雯／台北報導〕台北[redacted]局去年推動「[redacted]健康卡」集點活動，有讀者投訴，線上申辦網站將申請者的住家地址、身分證號碼全都一覽無遺，還沒獲得健康，恐先招來人身安全風險。

北[redacted]局關閉網頁

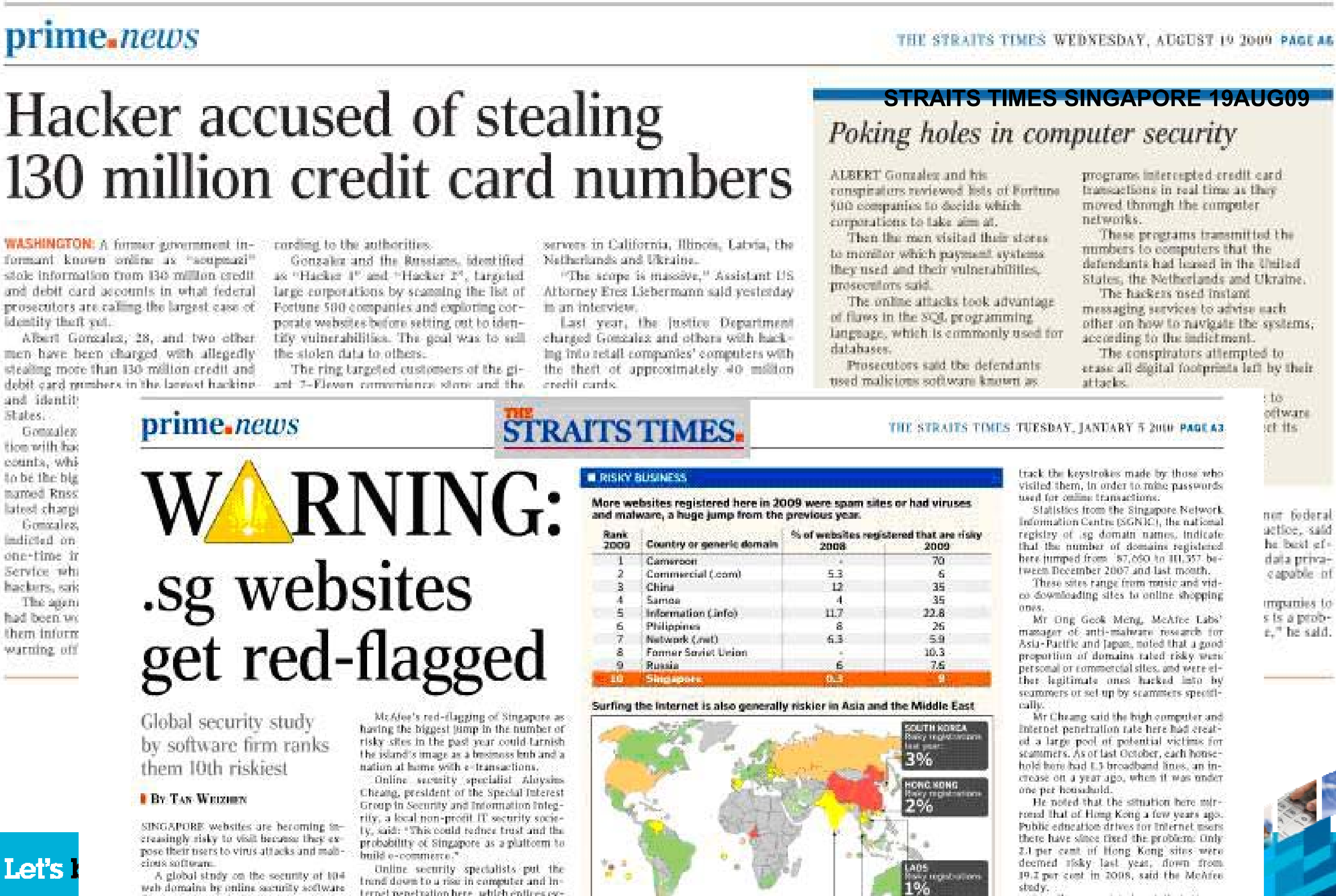
[redacted]局昨天在得知網站個人資料外洩後，緊急關閉網頁。主任秘書[redacted]坦承網站設計確有疏失，將確認安全無虞後，才會再開放。

[redacted]局自民國96年推出「[redacted]健康卡」集點活動，鼓勵台北市民申辦，只要參與健康講座、健康促進活動等，都能累積點數，可兌換免費健檢等獎品，總計去年發卡量已突破22萬張。

翁先生幾天前上網申辦[redacted]健康卡，逐一幫家人填寫個人資料，發現填寫完個人資料後的網頁顯示網址，將網址最後的「uid=1000」改成其他數字，即可看見過去所有申辦者登錄的基本資料，包括電話、地址、身分證字號全都一清二楚，直呼「太扯」。

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 identit

States.

Gonzalez

tion with ha

counts, whi

to be the big

named Russ

latest charg

Gonzalez,

indicted on

one-time in

Service whi

hackers, sai

The agen

had been w

them inform

warning off

cording 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

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.

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

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.

to

oftware

ct its

ner federal

actice, said

he best ef-

data priva-

capable of

mpanies to

s is a prob-

e," he said.

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

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 ex-

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

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

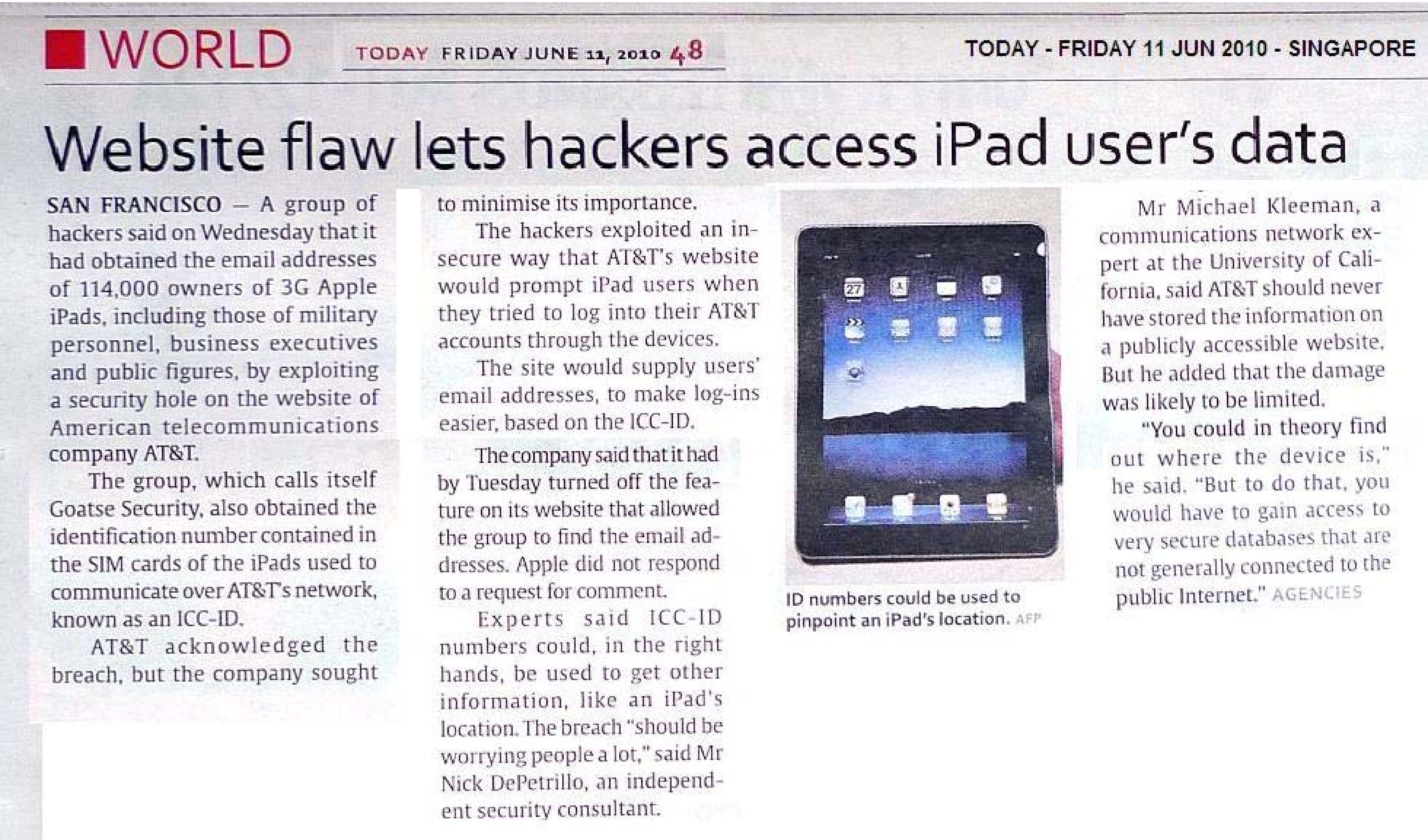
Statistics from the Singapore Network Information Centre (SGNIC), the national registry of .sg domain names, indicate that the number of domains registered here jumped from 87,690 to 111,357 between December 2007 and last month.

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.



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*

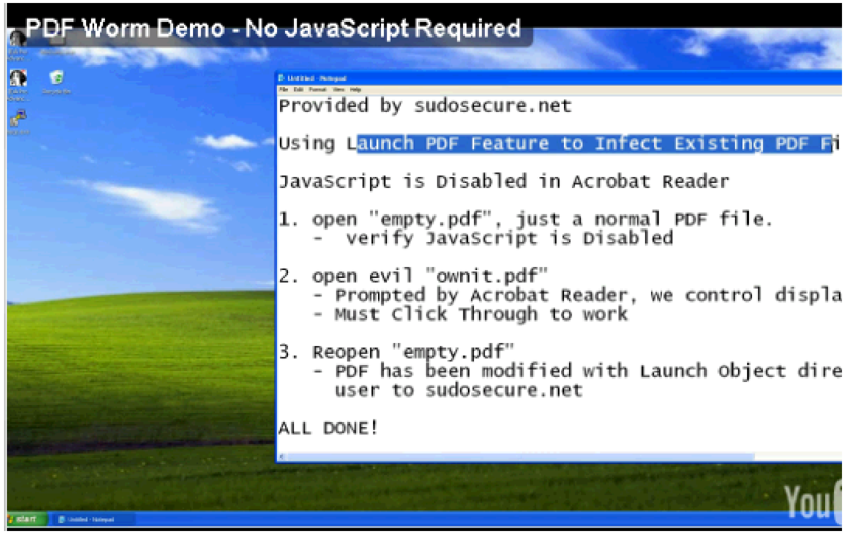
April 5, 2010 3:32 PM PDT

Exploits not needed to attack via PDF files

by Elinor Mills

9 com

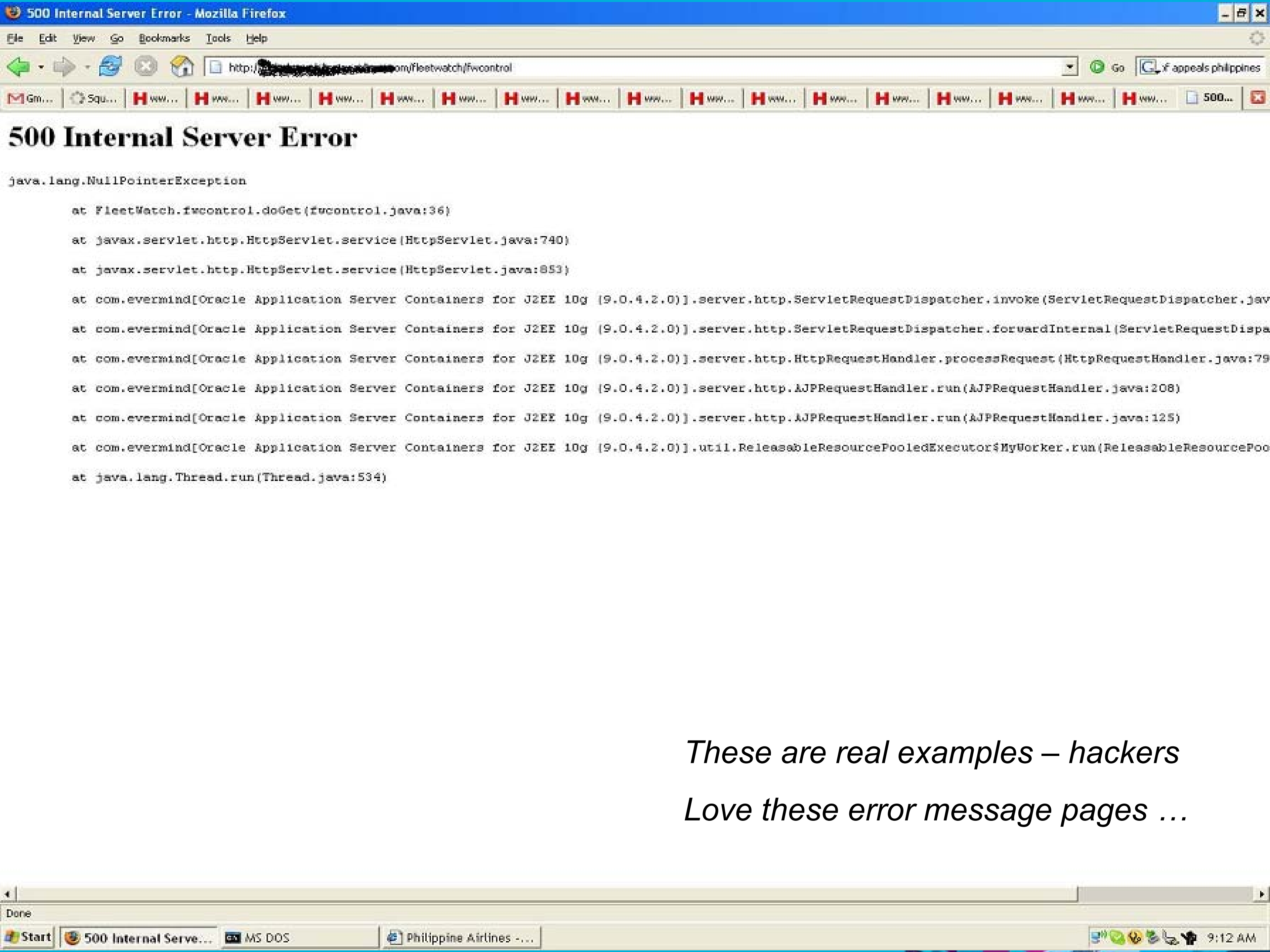
77 retweet Share 23



PDF Worm Demo - No JavaScript Required

```
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.

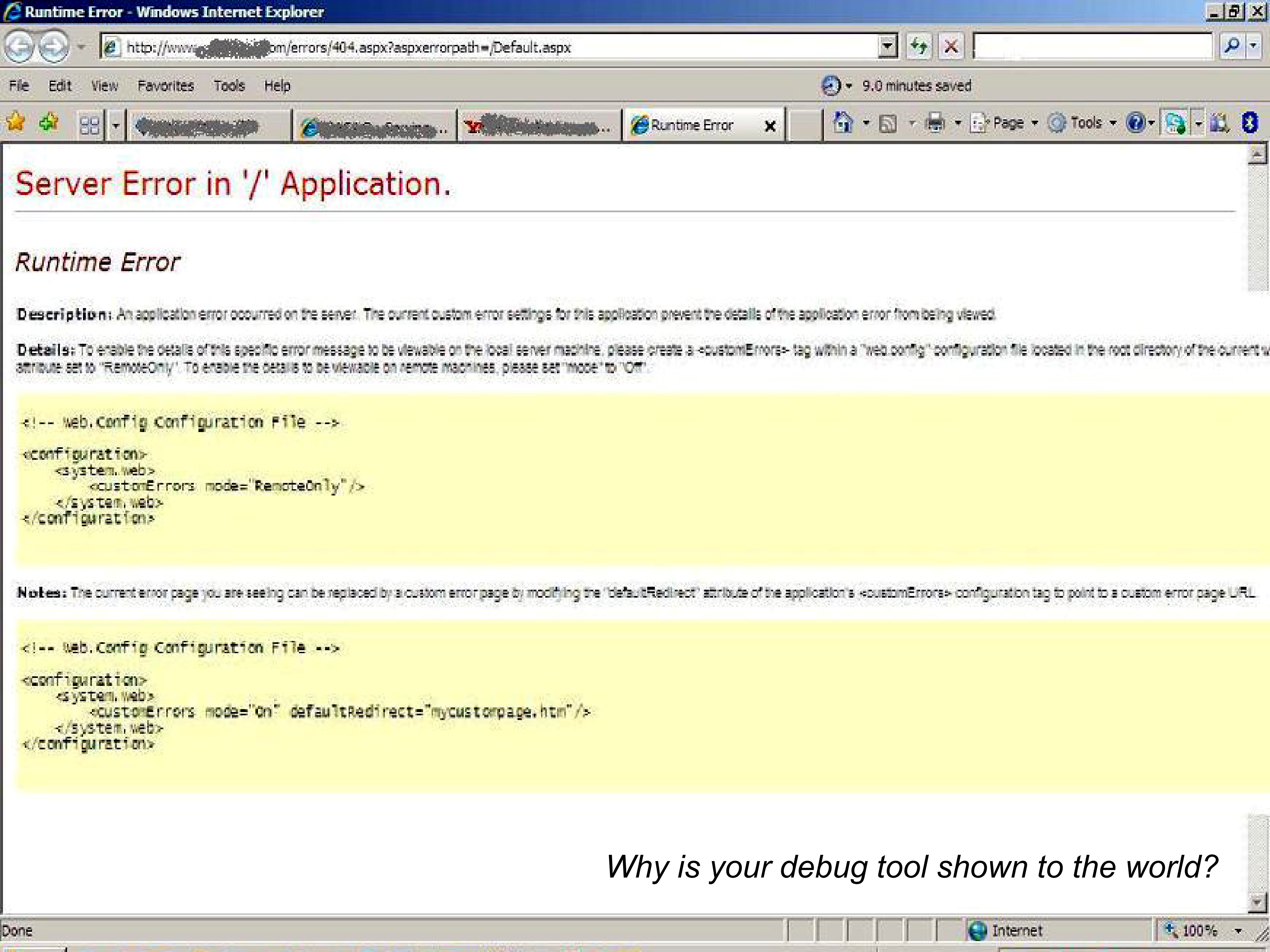

500 Internal Server Error - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://[redacted]om/fleetwatch/fwcontrol
Go
if appeals philippines
Gm... Squ... ww... 500...
Done
Start
500 Internal Serve...
MS DOS
Philippine Airlines -...
9:12 AM

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 …



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.

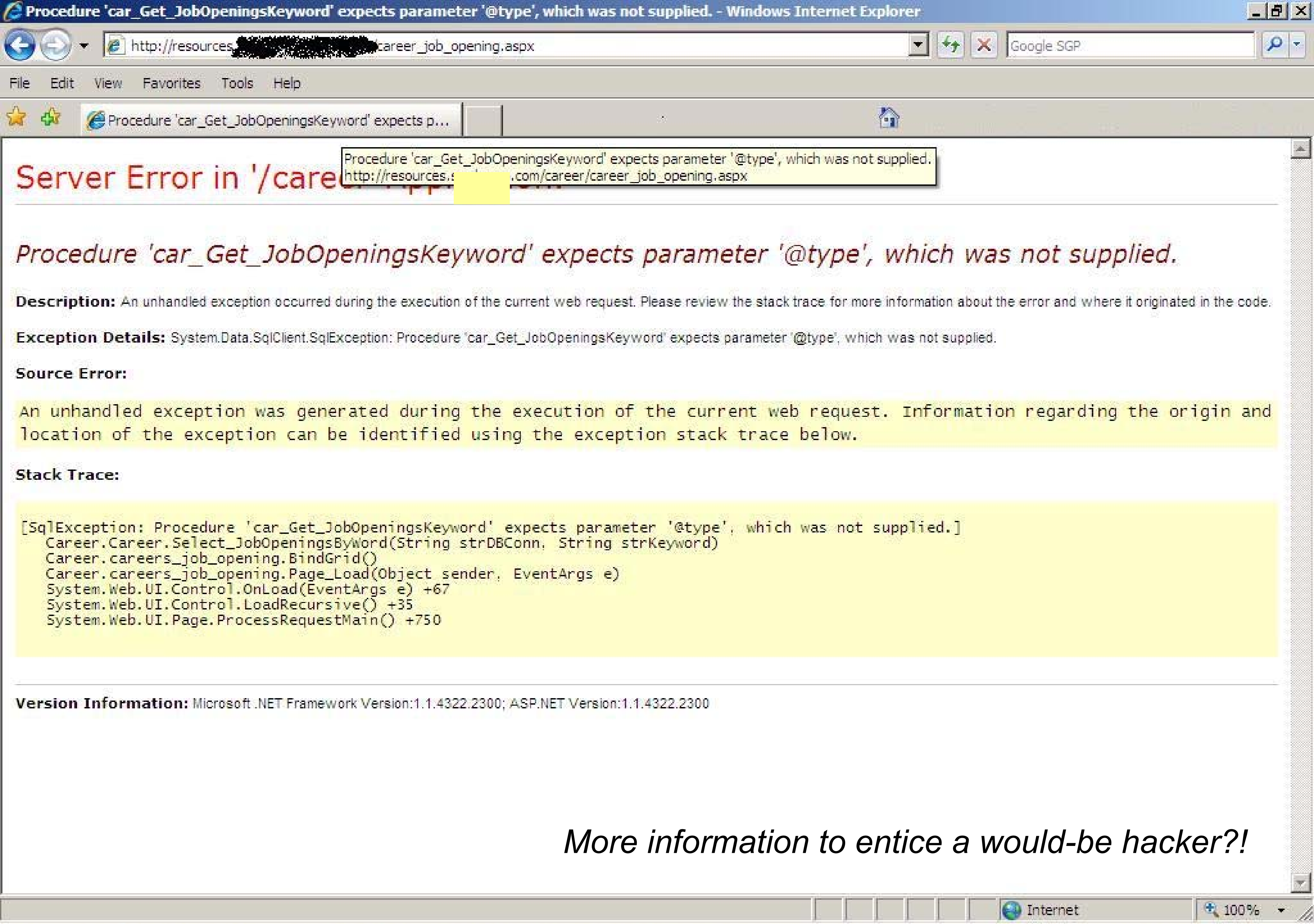
Details: To enable the details of this specific error message to be viewable on the local server machine, please create a <customErrors> tag within a "web.config" configuration file located in the root directory of the current w
attribute set to "RemoteOnly". To enable the details to be viewable on remote 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...
Internet
100%

Procedure 'car_Get_JobOpeningsKeyword' expects parameter '@type', which was not supplied.
http://resources.s[redacted].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:

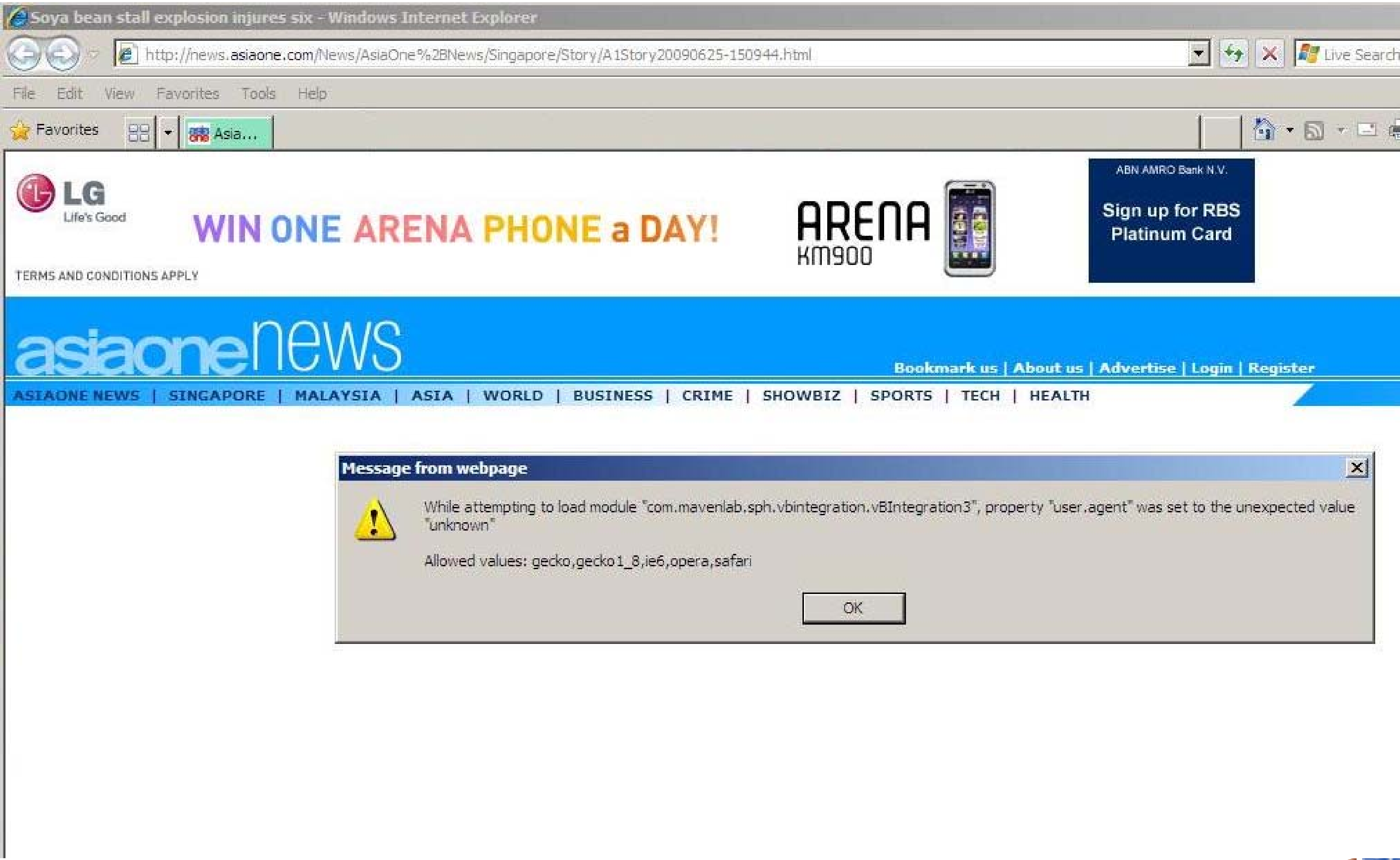
```
An unhandled exception was generated during the execution of the current web request. Information regarding the origin and
location of the exception can be identified using the exception stack trace below.
```

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

More information to entice a would-be hacker?!



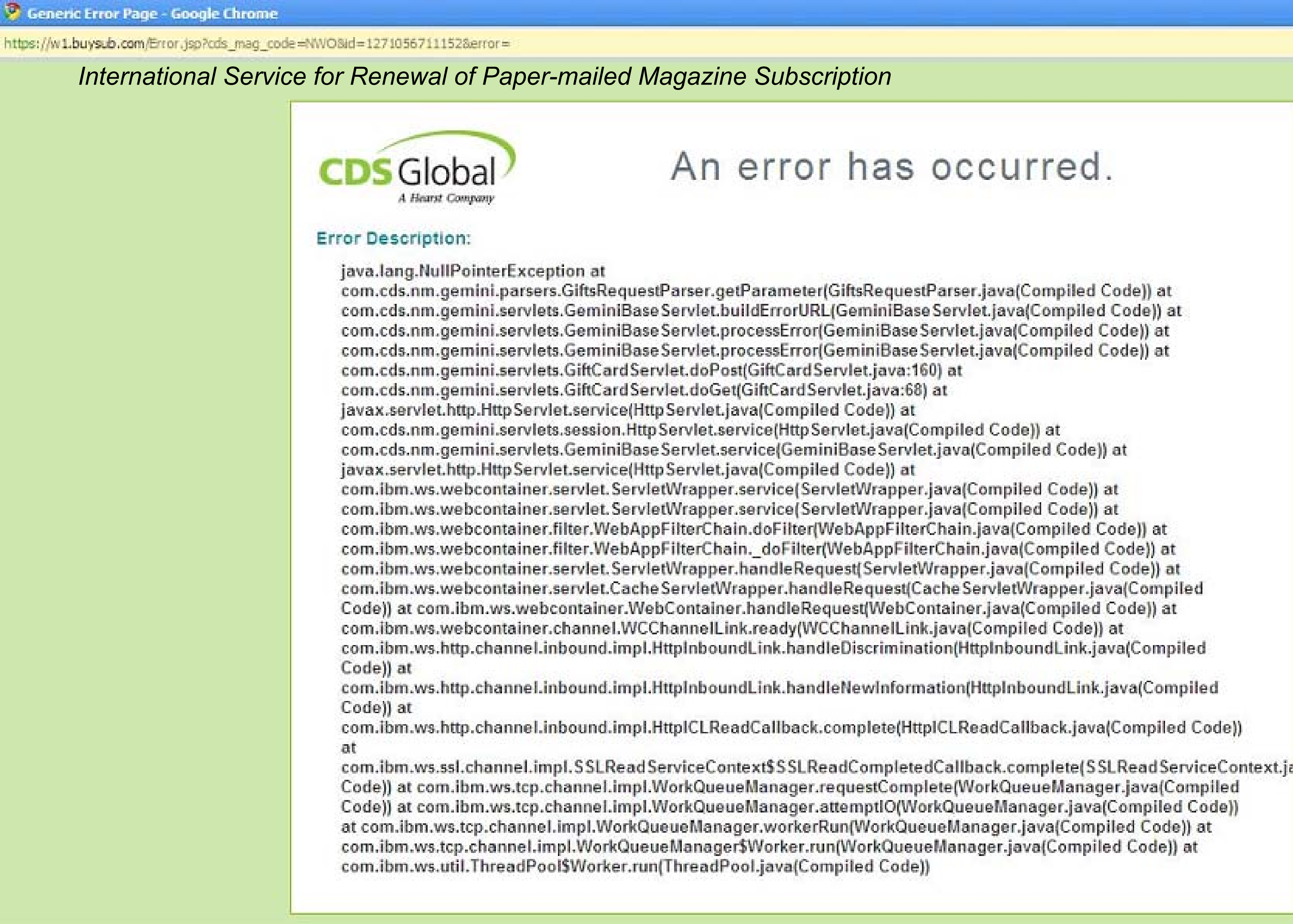
Soya bean stall explosion injures six - Windows Internet Explorer
http://news.asiaone.com/News/AsiaOne%2BNews/Singapore/Story/A1Story20090625-150944.html
Live Search
File Edit View Favorites Tools Help
Favorites
Asia...
LG Life's Good
WIN ONE ARENA PHONE a DAY!
ARENA KM900
TERMS AND CONDITIONS APPLY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

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

International Service for Renewal of Paper-mailed Magazine Subscription



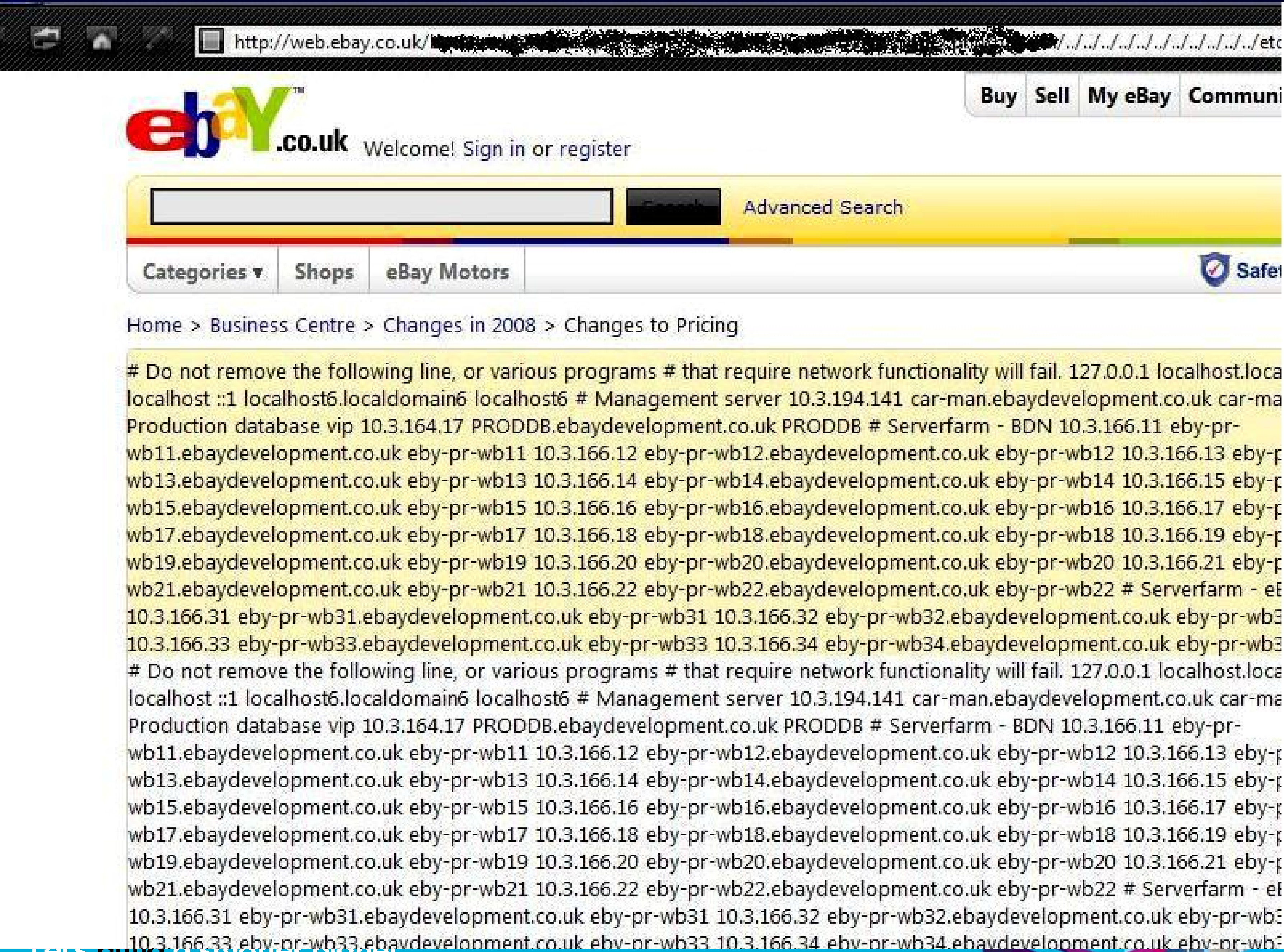
Generic Error Page - Google Chrome
https://w1.buysub.com/Error.jsp?cds_mag_code=NWO&id=1271056711152&error=
CDS Global
A Hearst Company

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))
```

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



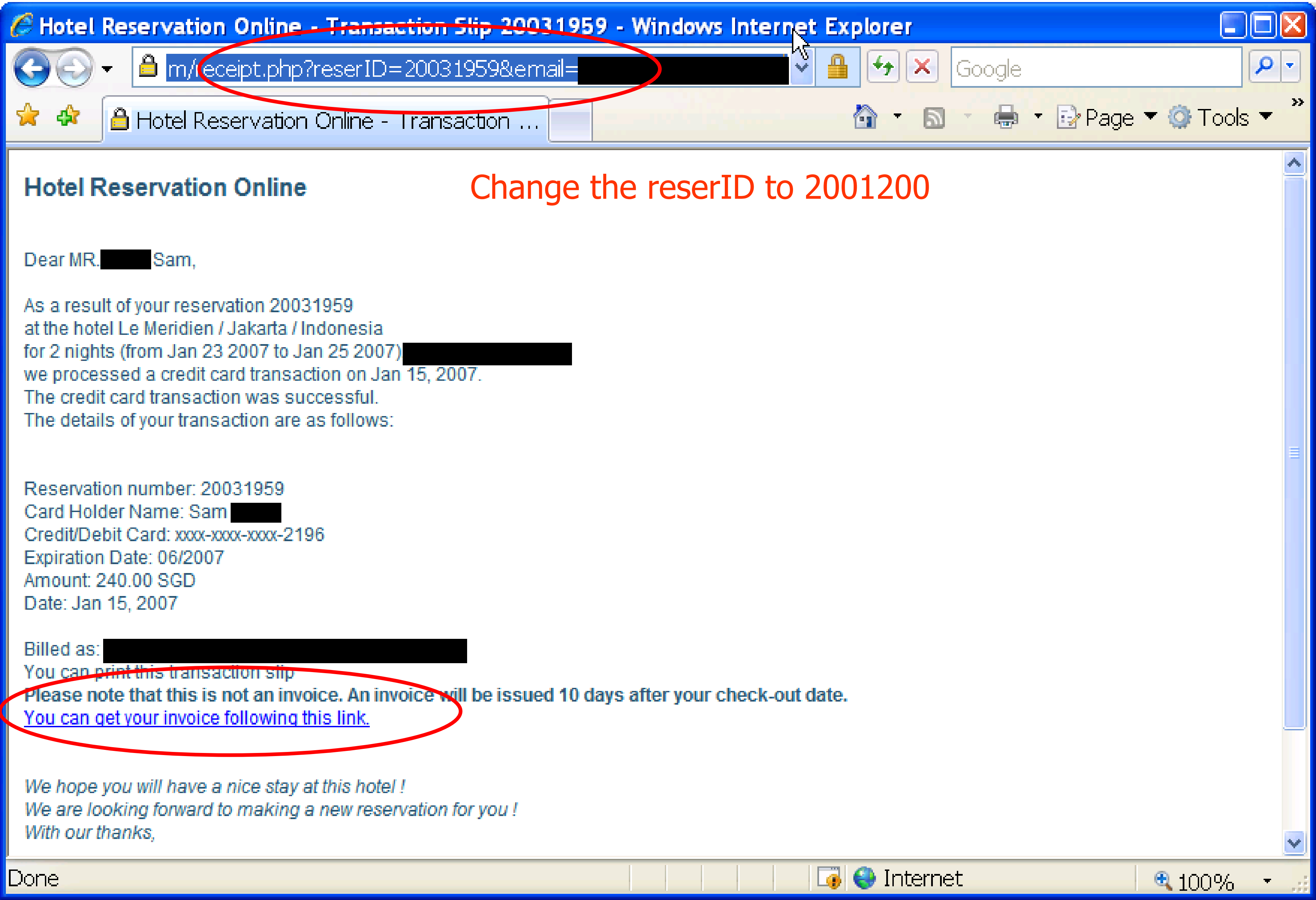
http://web.ebay.co.uk/[redacted]/../../../../../../../../../../../etc

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
```

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:

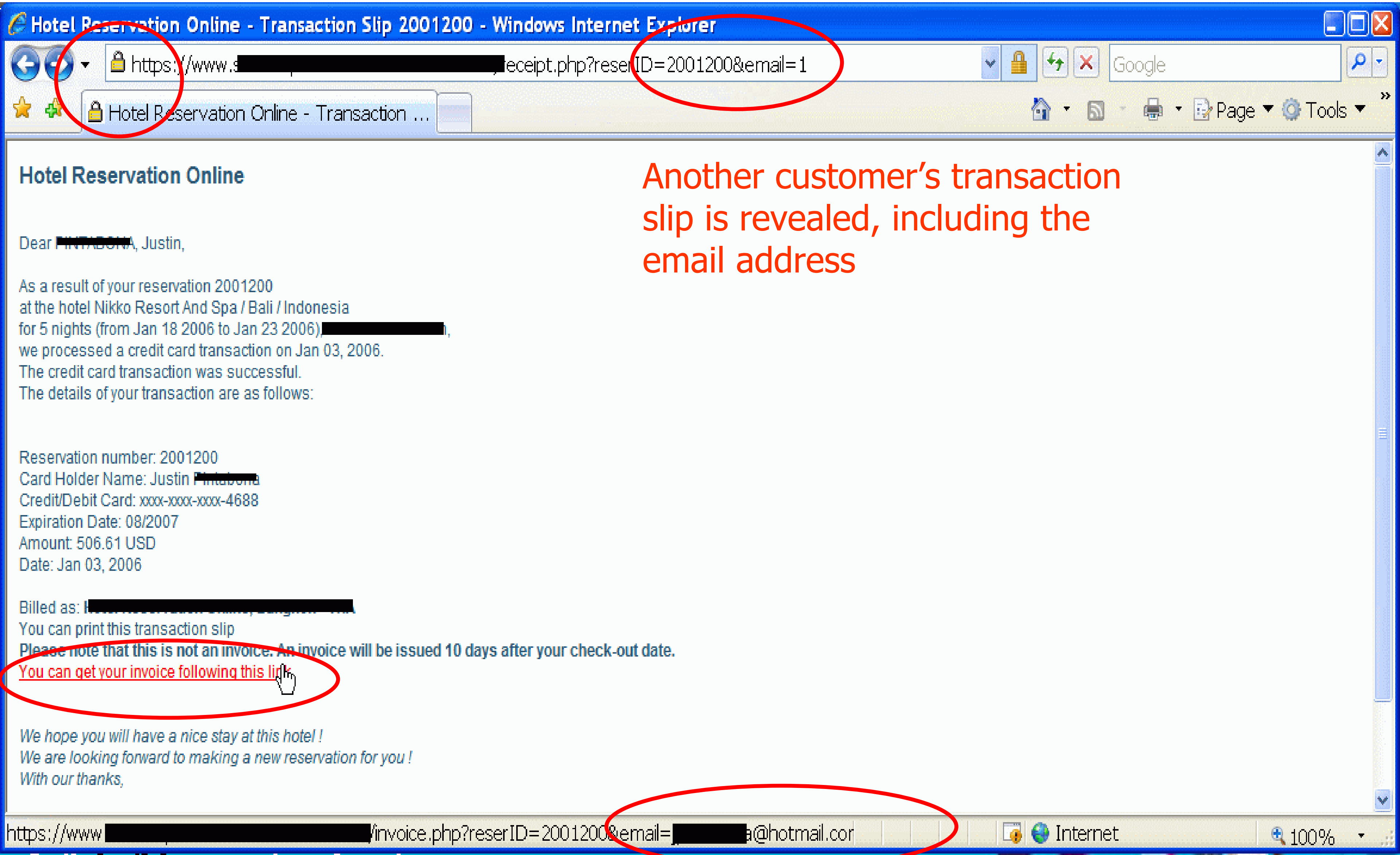
Reservation number: 20031959
Card Holder Name: Sam [redacted]
Credit/Debit Card: xxxx-xxxx-xxxx-2196
Expiration Date: 06/2007
Amount: 240.00 SGD
Date: Jan 15, 2007

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 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

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

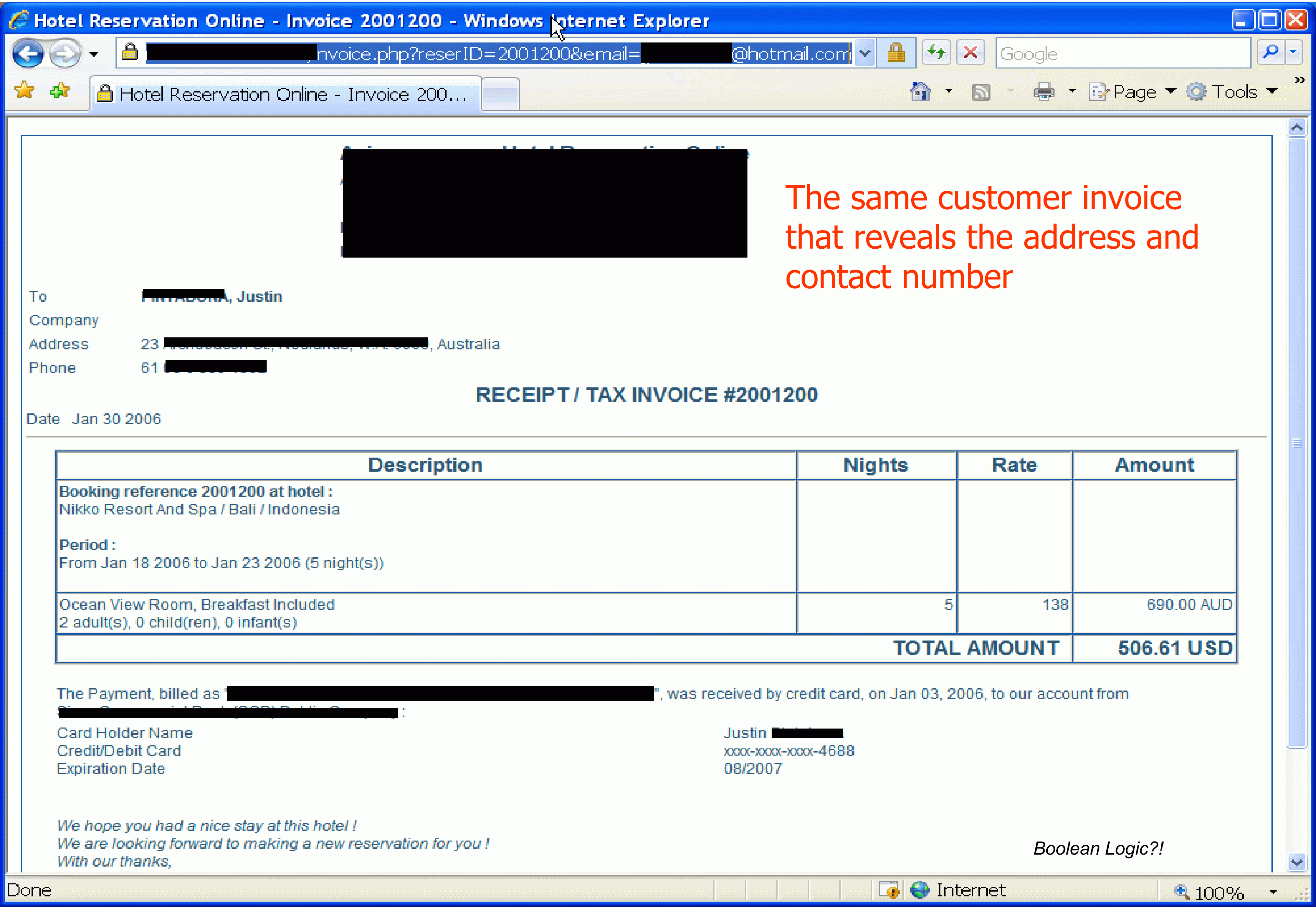
Billed as: [redacted]
You can print this transaction slip
Please note that this is not an invoice. An invoice will be issued 10 days after your check-out date.
You can get your invoice following this link

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

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]

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

LDAP Injection

SQL Injection

Email Spoofing

MS FrontPage Issues

Cross Site Scripting

Path Traversal in URL

BEA WebLogic Issues

SUN iPlanet Issues

Oracle iAS Issues

Format Strings

ColdFusion Issues

VALIDATE INPUT

PHP Issues

Apache HTTPd Issues

Microsoft IIS Issues

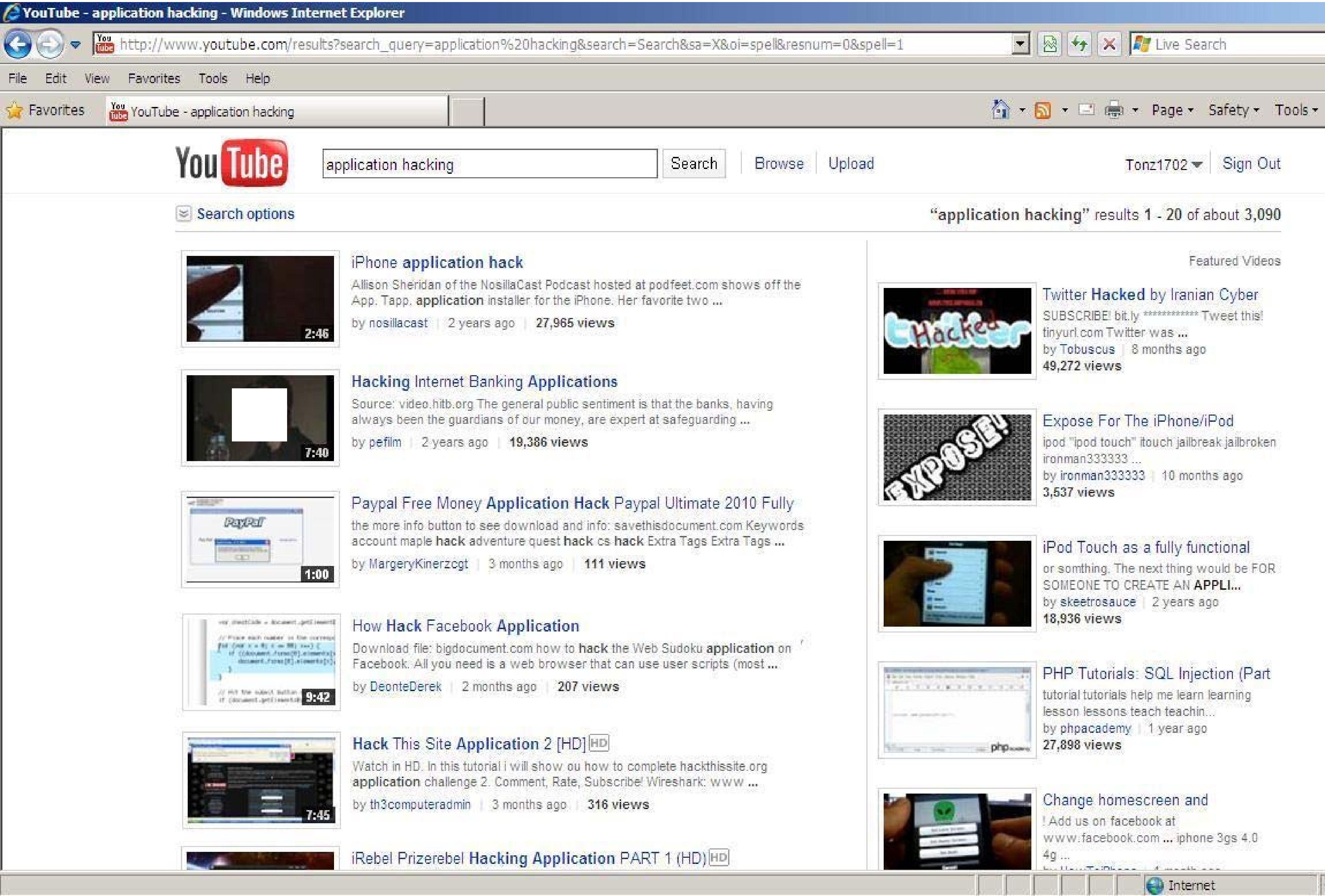
Privacy Issues

Credentials Enumeration

Tomcat Issues

Cookie Poisoning SQL Injection

不要在家嘗試, 啊!


YouTube - application hacking - Windows Internet Explorer
http://www.youtube.com/results?search_query=application%20hacking&search=Search&sa=X&oi=spell&resnum=0&spell=1
Live Search
File
Edit
View
Favorites
Tools
Help
Favorites
YouTube - application hacking
Page
Safety
Tools
YouTube
application hacking
Search
Browse
Upload
Tonz1702
Sign Out
Search options
Internet

"application hacking" results 1 - 20 of about 3,090

iPhone application hack
Allison Sheridan of the NosillaCast Podcast hosted at podfeet.com shows off the App. Tapp. application installer for the iPhone. Her favorite two ...
by nosillacast | 2 years ago | 27,965 views (2:46)

Hacking Internet Banking Applications
Source: video.hitb.org The general public sentiment is that the banks, having always been the guardians of our money, are expert at safeguarding ...
by pefilm | 2 years ago | 19,386 views (7:40)

Paypal Free Money Application Hack Paypal Ultimate 2010 Fully
the more info button to see download and info: savethisdocument.com Keywords account maple hack adventure quest hack cs hack Extra Tags Extra Tags ...
by MargeryKinerzcgt | 3 months ago | 111 views (1:00)

How Hack Facebook Application
Download file: bigdocument.com how to hack the Web Sudoku application on Facebook. All you need is a web browser that can use user scripts (most ...
by DeonteDerek | 2 months ago | 207 views (9:42)

Hack This Site Application 2 [HD] HD
Watch in HD. In this tutorial i will show ou how to complete hackthissite.org application challenge 2. Comment, Rate, Subscribe! Wireshark: www ...
by th3computeradmin | 3 months ago | 316 views (7:45)

iRebel Prizerebel Hacking Application PART 1 (HD) HD

Featured Videos

Twitter Hacked by Iranian Cyber
SUBSCRIBE! bit.ly ************ Tweet this! tinyurl.com Twitter was ...
by Tobuscus | 8 months ago
49,272 views

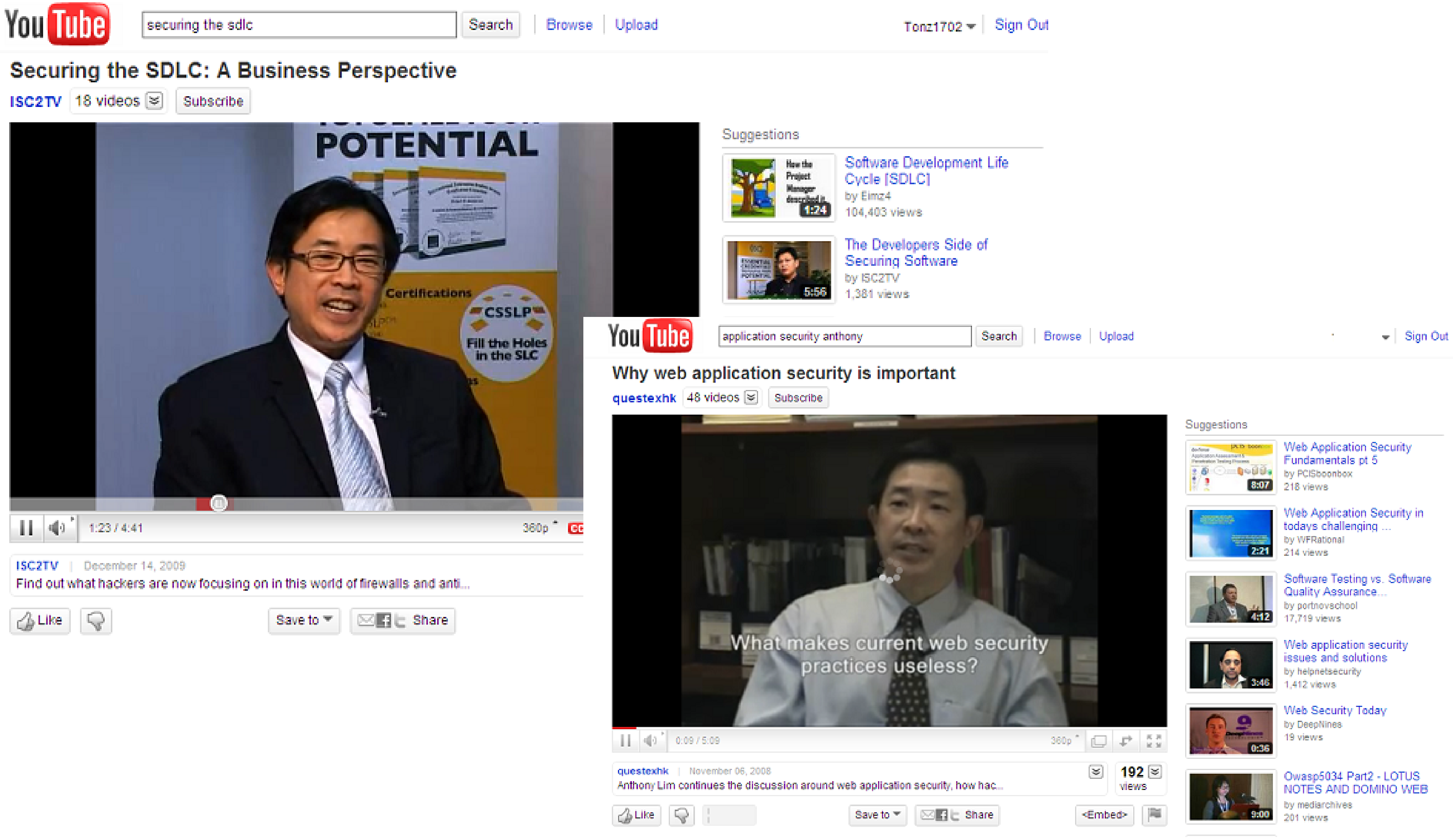
Expose For The iPhone/iPod
ipod "ipod touch" itouch jailbreak jailbroken ironman333333 ...
by ironman333333 | 10 months ago
3,537 views

iPod Touch as a fully functional
or somthing. The next thing would be FOR SOMEONE TO CREATE AN APPLI...
by skeetrosauce | 2 years ago
18,936 views

PHP Tutorials: SQL Injection (Part
tutorial tutorials help me learn learning lesson lessons teach teachin...
by phpacademy | 1 year ago
27,898 views

Change homescreen and
! Add us on facebook at www.facebook.com ... iphone 3gs 4.0 4g ...

不要害怕，這裡是救援



Securing the SDLC: A Business Perspective

ISC2TV | December 14, 2009
Find out what hackers are now focusing on in this world of firewalls and anti...

Software Development Life Cycle [SDLC]
by Eimz4
104,403 views

The Developers Side of Securing Software
by ISC2TV
1,381 views

Why web application security is important

What makes current web security practices useless?

questexhk | November 06, 2008
Anthony Lim continues the discussion around web application security, how hac...

Web Application Security Fundamentals pt 5
by PCISboonbox
218 views

Web Application Security in todays challenging ...
by WFRational
214 views

Software Testing vs. Software Quality Assurance...
by portnovschool
17,719 views

Web application security issues and solutions
by helpnetsecurity
1,412 views

Web Security Today
by DeepNines
19 views

Owasp5034 Part2 - LOTUS NOTES AND DOMINO WEB
by mediarchives
201 views

為什麼黑客可以打軟體？

- **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 do not normally code defensively
    - Developers think differently from hackers
    - Developers have increasingly long and sophisticated applications, and often can be short on resources, knowledge or experience
    - **It is a nightmare to manually QA the application**

為什麼軟體會有漏洞？

Singapore
Mercedes

**Do more
with less**

**200,000
lines**

Today I’m being asked to:

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

- ***Fast*** 快
- ***Good*** 好
- ***Cheap*** 便宜

-> Choose 2 only

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!

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 WE HAVE APPLICATION SECURITY ISSUES?

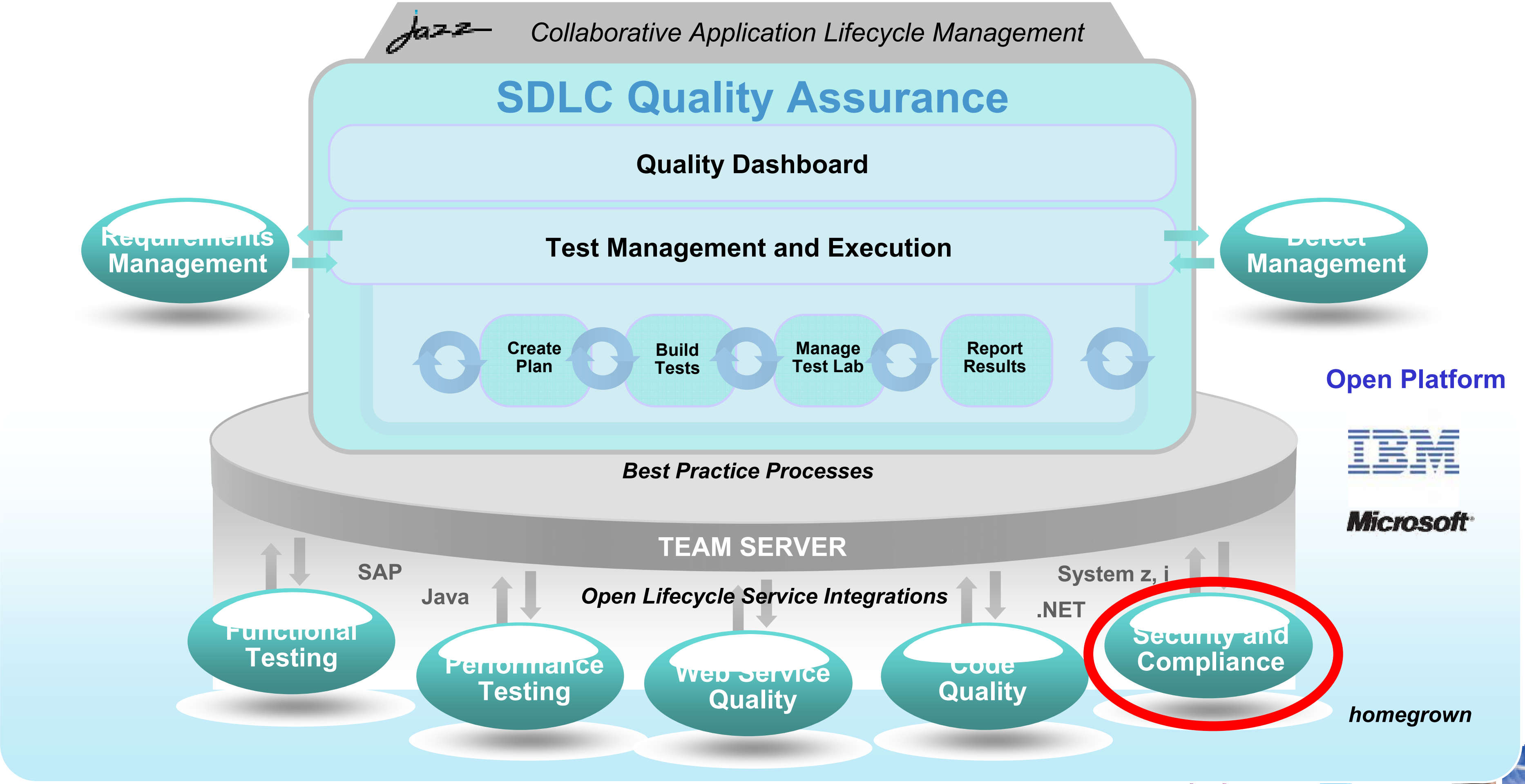
- **IT security solutions and professionals are normally from the network /infrastructure /sysadmin side**
  - They usually have little or no experience in application development
  - **And developers typically don’t know or don’t care about security or networking**

- **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 currently still not “cultural” for developers to write code defensively

Back then coding was done by engineers …

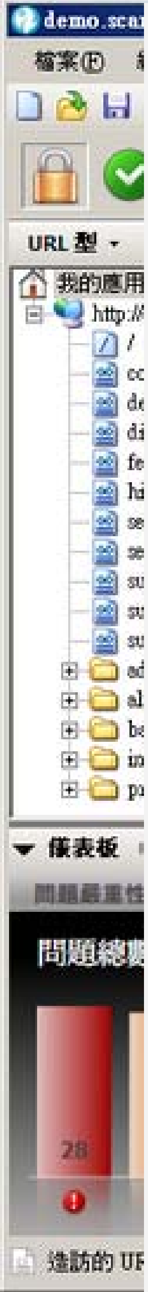
Then came Y2K … Dotcom boom … etc

SECURITY TESTING IS PART OF SDLC QUALITY TESTING



You need a professional solution to

Identify Vulnerabilities

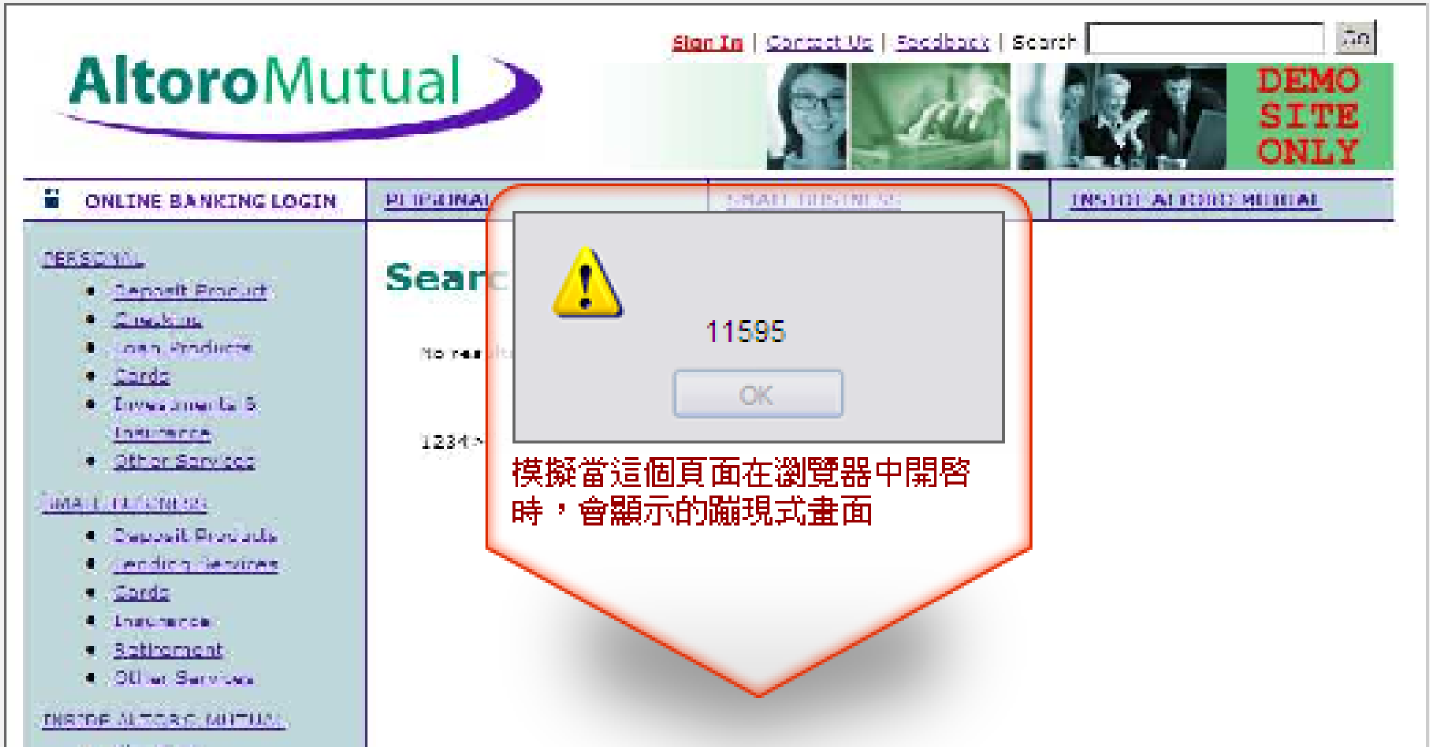


注入的 Script AppScan 似乎會包含在回應中。如果以下畫面顯示模擬產生注入 Script 的蹦現式畫面，即證明應用程式容易遭受「跨網站編寫 Script」的侵害。否則，如果要驗證這個漏洞：1) 開啓「要求/回應」標籤，然後按一下「顯示在瀏覽器中」，看看是否會出現蹦現式畫面。請注意，某些 Script 語法是瀏覽器專屬的，因此如果未蹦現注入的警示，請嘗試不同的瀏覽器（用滑鼠右鍵按一下瀏覽器 > 檢視來源 > 另存新檔...）。2) 檢查原始測試回應中警示 Script 的有效性。

用者，讓駭客可以檢

呈現的測試回應

新視窗

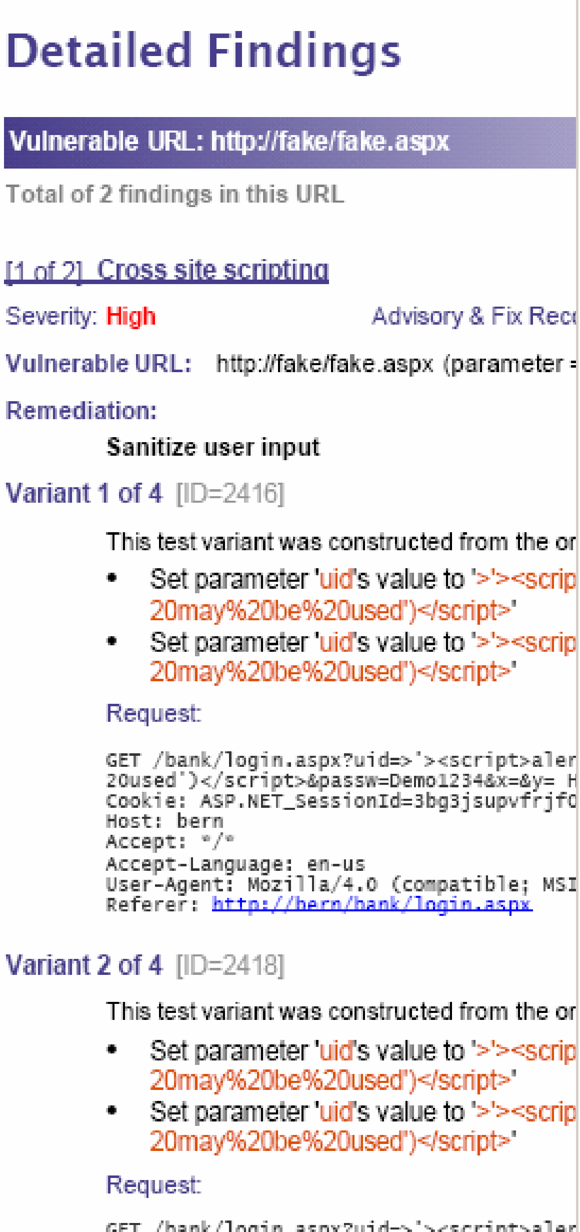


11595

模擬當這個頁面在瀏覽器中開啓時，會顯示的蹦現式畫面

With Rich Report Options

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



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 Reco

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

Remediation:

Sanitize user input

Variant 1 of 4 [ID=2416]

This test variant was constructed from the or

- Set parameter 'uid's value to '>'><scrip 20may%20be%20used')</script>'
- Set parameter 'uid's value to '>'><scrip 20may%20be%20used')</script>'

Request:

```
GET /bank/login.aspx?uid=>'><script>aler
20used')</script>&passw=Demo1234&x=&y= H
Cookie: ASP.NET_SessionId=3bg3jsupvfrjf0
Host: bern
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSI
Referer: http://bern/bank/login.aspx
```

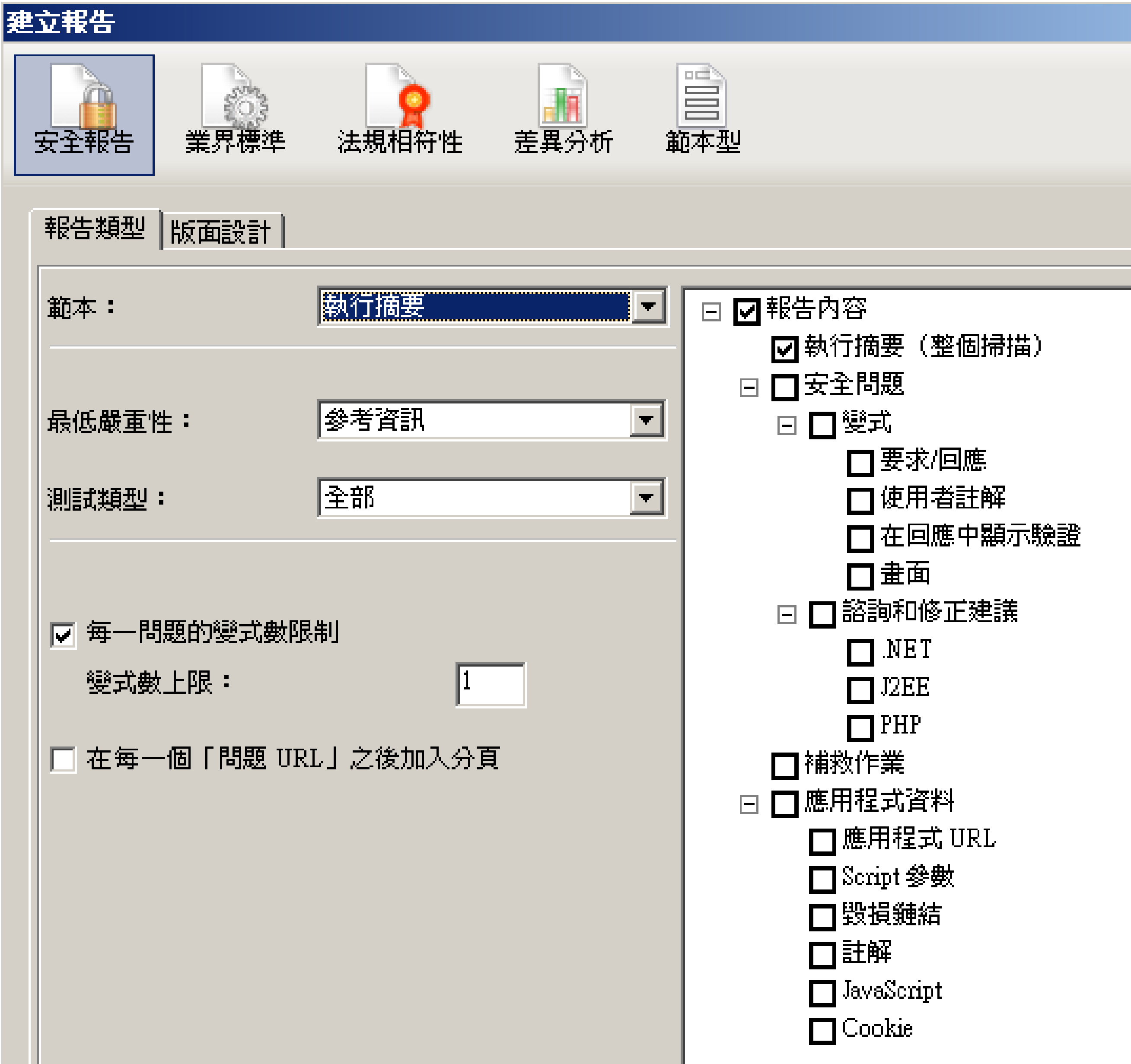
Variant 2 of 4 [ID=2418]

This test variant was constructed from the or

- Set parameter 'uid's value to '>'><scrip 20may%20be%20used')</script>'
- Set parameter 'uid's value to '>'><scrip 20may%20be%20used')</script>'

Request:

```
GET /bank/login.aspx?uid=>'><script>aler
```



建立報告

範本： 執行摘要

最低嚴重性： 參考資訊

測試類型： 全部

☑ 每一問題的變式數限制

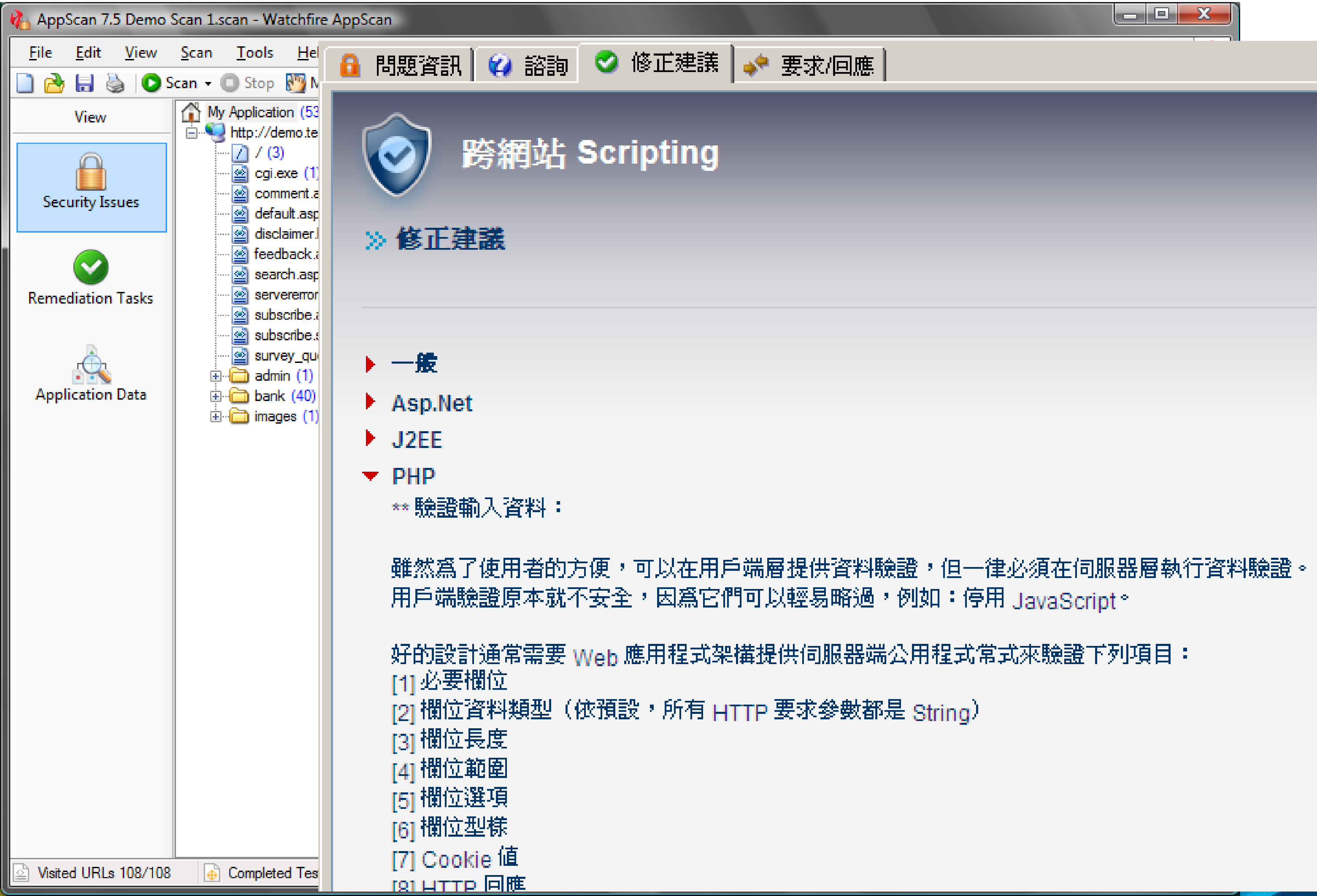
變式數上限： 1

□ 在每一個「問題 URL」之後加入分頁

- ☑ 報告內容
  - ☑ 執行摘要（整個掃描）
  - □ 安全問題
    - □ 變式
      - □ 要求/回應
      - □ 使用者註解
      - □ 在回應中顯示驗證
      - □ 畫面
    - □ 諮詢和修正建議
      - □ .NET
      - □ J2EE
      - □ PHP
  - □ 補救作業
  - □ 應用程式資料
    - □ 應用程式 URL
    - □ Script 參數
    - □ 毀損鏈結
    - □ 註解
    - □ JavaScript
    - □ Cookie

And Most Important :

Actionable Fix Recommendations



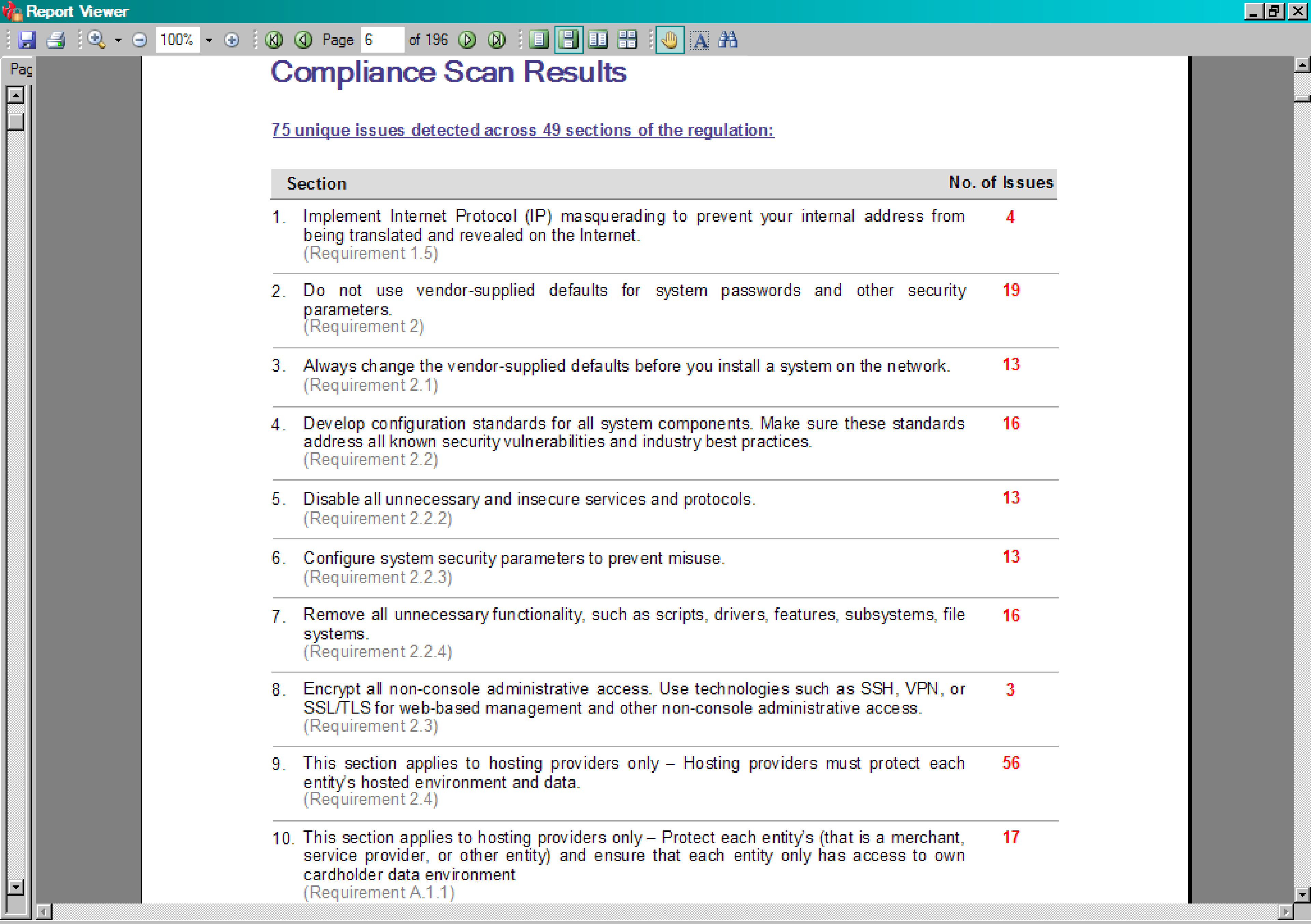
跨網站 Scripting

修正建議

** 驗證輸入資料：

雖然為了使用者的方便，可以在用戶端層提供資料驗證，但一律必須在伺服器層執行資料驗證。用戶端驗證原本就不安全，因為它們可以輕易略過，例如：停用 JavaScript。

好的設計通常需要 Web 應用程式架構提供伺服器端公用程式常式來驗證下列項目：
[1] 必要欄位
[2] 欄位資料類型（依預設，所有 HTTP 要求參數都是 String）
[3] 欄位長度
[4] 欄位範圍
[5] 欄位選項
[6] 欄位型樣
[7] Cookie 值
[8] HTTP 回應

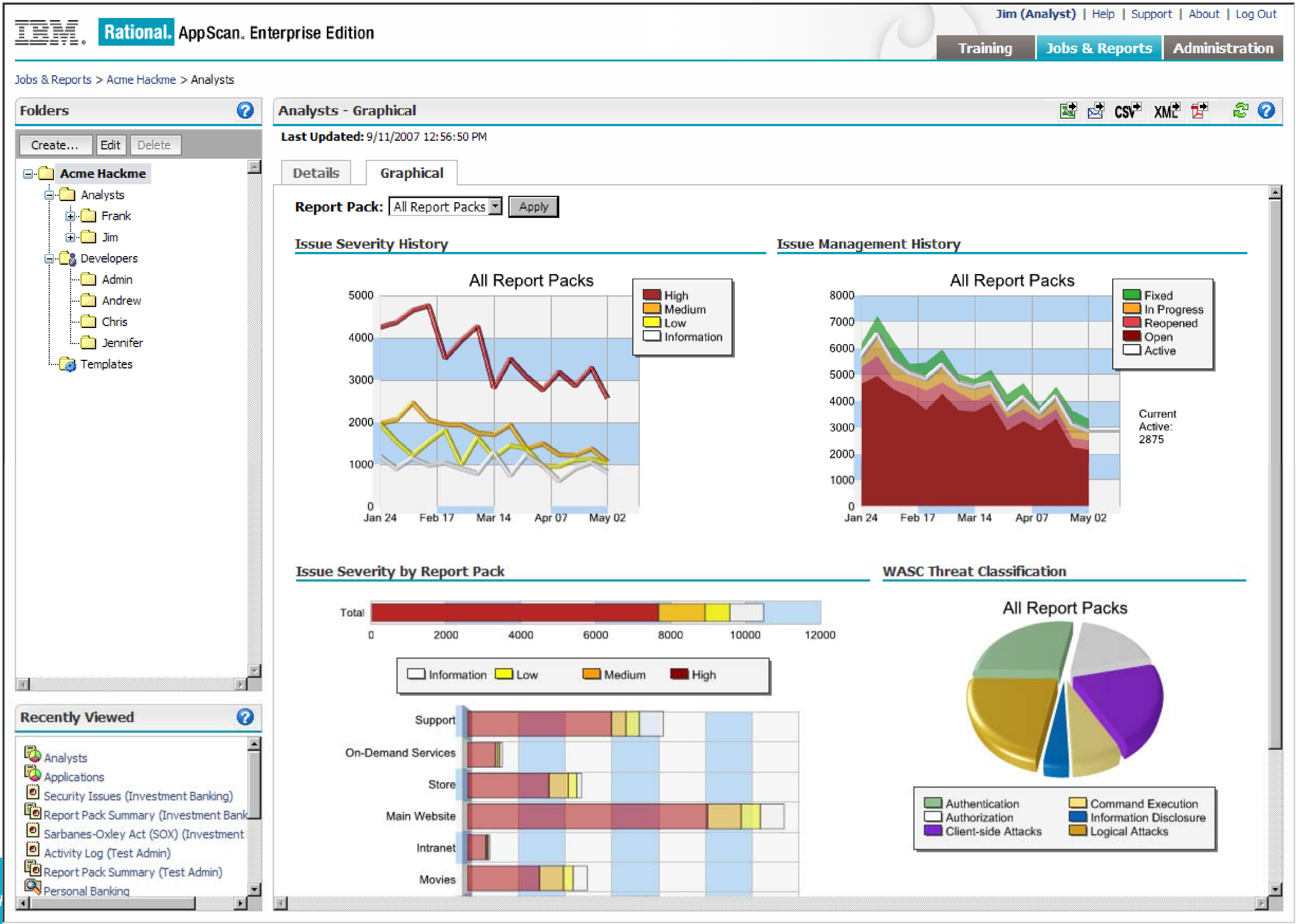


Compliance Scan Results

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



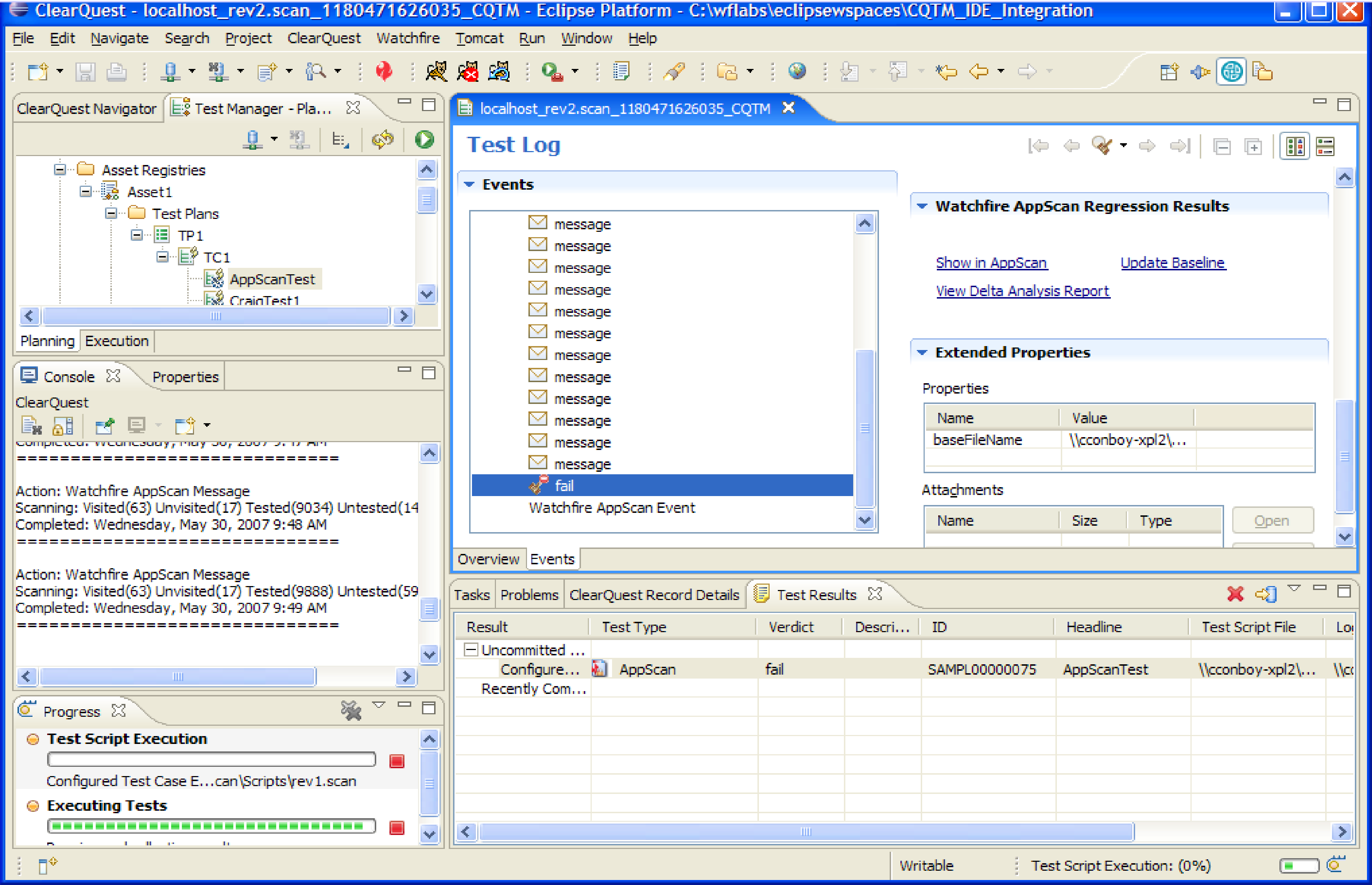
Last Updated: 9/11/2007 12:56:50 PM

Report Pack: All Report Packs

Current Active: 2875

L

AppScan - CQTM & RQM Integration, also with RTC


ClearQuest - localhost_rev2.scan_1180471626035_CQTM - Eclipse Platform - C:\wflabs\eclipsewspaces\CQTM_IDE_Integration
File Edit Navigate Search Project ClearQuest Watchfire Tomcat Run Window Help
ClearQuest Navigator
Test Manager - Pla...
Asset Registries
Asset1
Test Plans
TP1
TC1
AppScanTest
CraigTest1
Planning
Execution
Console
Properties
ClearQuest
Progress
localhost_rev2.scan_1180471626035_CQTM
Test Log
Events
Watchfire AppScan Regression Results
Show in AppScan
Update Baseline
View Delta Analysis Report
Extended Properties
Properties
Attachments
Open
Overview
Events
Tasks
Problems
ClearQuest Record Details
Test Results
Writable
Test Script Execution: (0%)

```
==============================
Action: Watchfire AppScan Message
Scanning: Visited(63) Unvisited(17) Tested(9034) Untested(14
Completed: Wednesday, May 30, 2007 9:48 AM
==============================

Action: Watchfire AppScan Message
Scanning: Visited(63) Unvisited(17) Tested(9888) Untested(59
Completed: Wednesday, May 30, 2007 9:49 AM
==============================
```

Test Script Execution

Configured Test Case E...can\Scripts\rev1.scan

Executing Tests

Events:

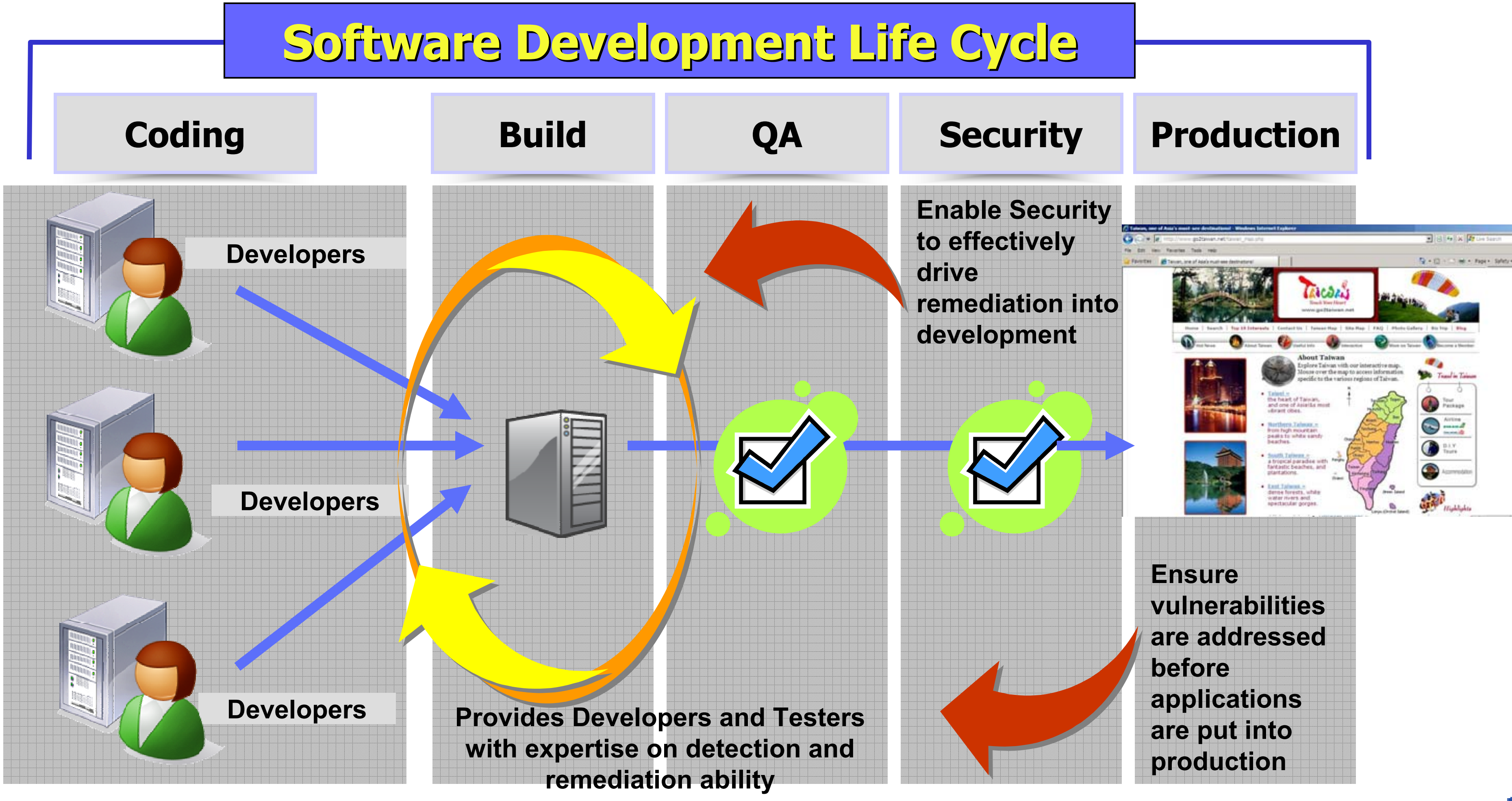
- message
- message
- message
- message
- message
- message
- message
- message
- message
- message
- message
- message
- fail
- Watchfire AppScan Event

Name	Value
baseFileName	\\cconboy-xpl2\...

Name	Size	Type

Result	Test Type	Verdict	Descri...	ID	Headline	Test Script File	Lo
Uncommitted ...							
Configure...	AppScan	fail		SAMPL00000075	AppScanTest	\\cconboy-xpl2\...	\\c
Recently Com...							

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

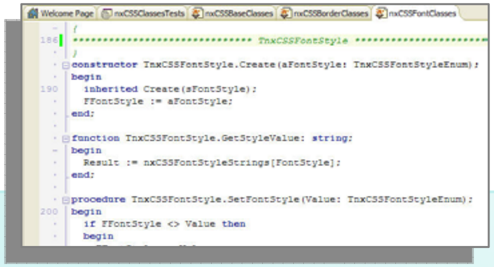
Provides Developers and Testers with expertise on detection and remediation ability

Ensure vulnerabilities are addressed before applications are put into production

Software Security Testing Technologies

Static Code Analysis = Whitebox

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

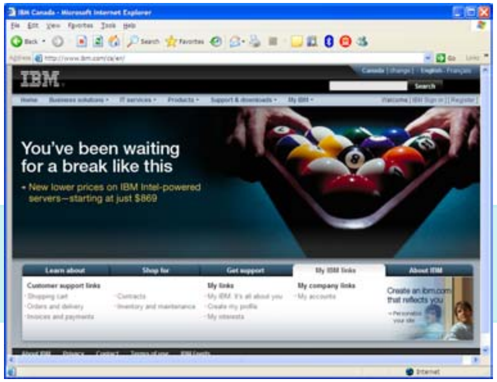


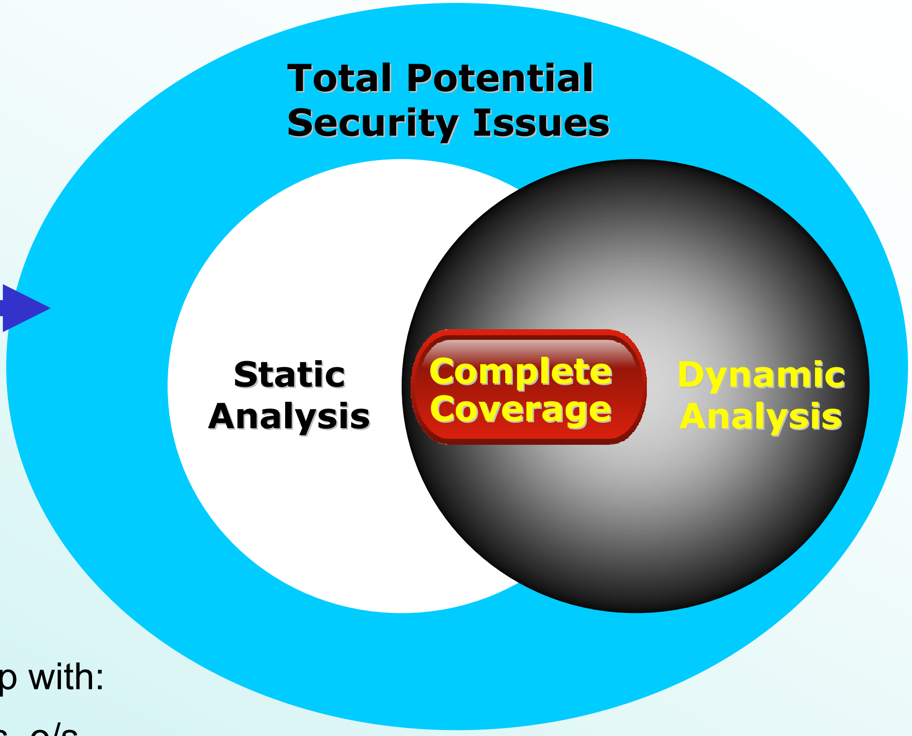
```
{
*************************** TnxCSSFontStyle ****************************
}
constructor TnxCSSFontStyle.Create(aFontStyle: TnxCSSFontStyleEnum);
begin
  inherited Create(sFontStyle);
  FFontStyle := aFontStyle;
end;

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


IBM Canada - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://www.ibm.com/ca/en/
Go
IBM
Canada | change | English Français
Search
Home
Business solutions
IT services
Products
Support & downloads
My IBM
You've been waiting for a break like this
New lower prices on IBM Intel-powered servers—starting at just $869
Learn about
Shop for
Get support
My IBM links
About IBM
Customer support links
My links
My company links
Create an ibm.com that reflects you
Internet



Relationship with:

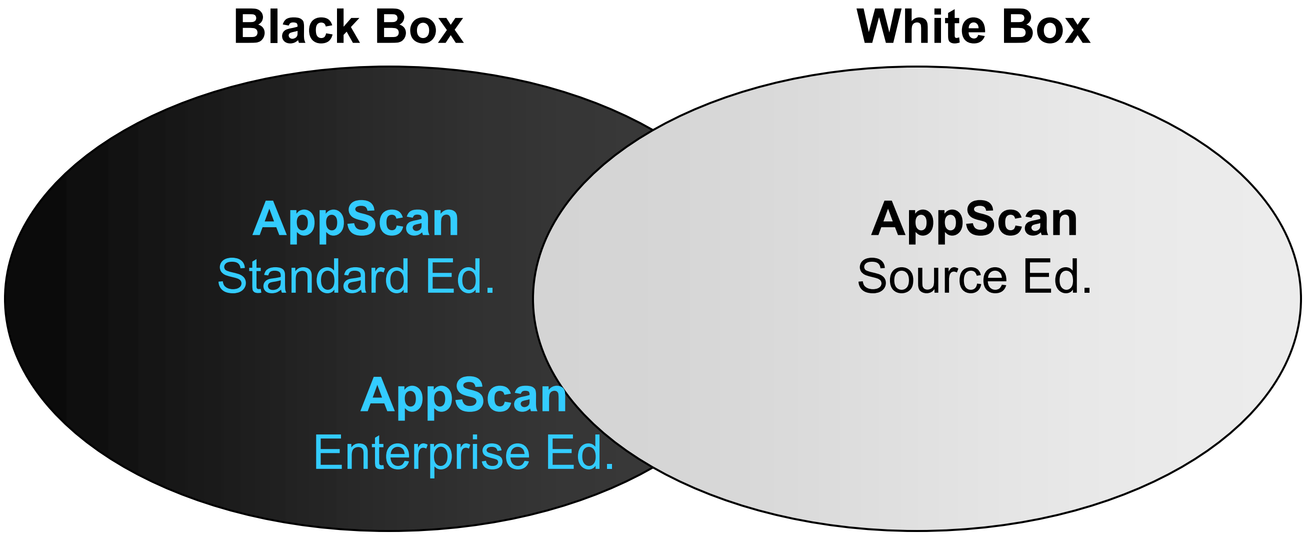
-Other apps, o/s

-Middleware, infra

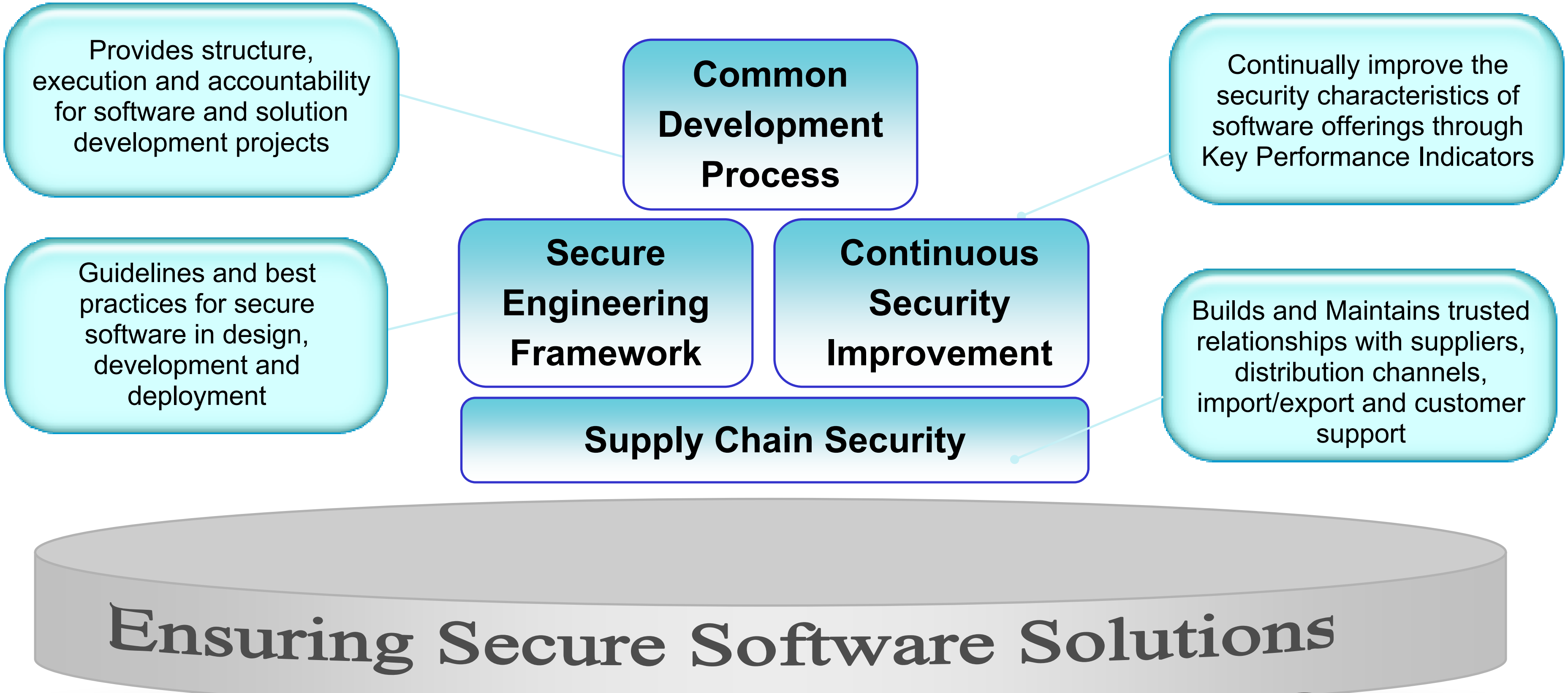
Application Development Security Testing Domains

BLACK BOX 黑箱 *IBM Rational Appscan Standard Edition*	WHITE BOX 白箱 *IBM Rational Appscan Source Edition*
Dynamic APPLICATION Analysis	**Static 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

- **Two approaches to web application security scanning**
  - Black-box - Automates attacker actions
  - White-box - Automates code auditing
- Challenges and issue coverage are different
- Complete solution – ***involve more people in the organization***
- Objective – ***build the knowledge, minimize future errors & risks***



IBM Secure Engineering Initiative



Provides structure, execution and accountability for software and solution development projects

Common Development Process

Continually improve the security characteristics of software offerings through Key Performance Indicators

Guidelines and best practices for secure software in design, development and deployment

Secure Engineering Framework

Continuous Security Improvement

Builds and Maintains trusted relationships with suppliers, distribution channels, import/export and customer support

Supply Chain Security

Ensuring Secure Software Solutions

Link to Security Engineering Framework: http://www.redbooks.ibm.com/redpieces/abstracts/redp4641.html?Open

- IBM develops products and solutions for sale.
- IBM develops and operates solutions and services for its own internal use.
- IBM develops and operates solutions and services on behalf of customers.

NEW

IBM

for Review February 24, 2010 3:41 pm REDP-4641-00

Security in Development: The IBM Secure Engineering Framework

Redguides for Business Leaders

Danny Allan
Tim Hahn
Andras Szakal
Jim Whitmore
Axel Buecker

- Investigating common development processes and the IBM Integrated Product Development process
- Emphasizing security awareness and requirements in the software development process
- Discussing test and vulnerability assessments

Redbooks

Introducing IBM Secure by Design

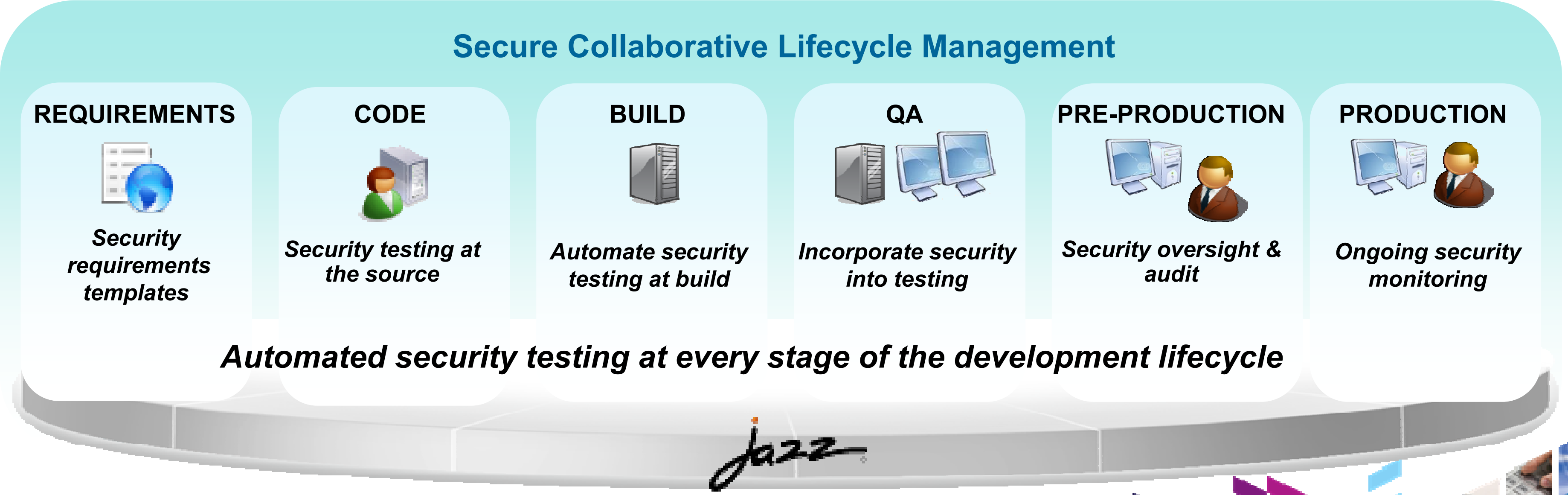
Automate security testing early & often throughout the development lifecycle

- Identify and remediating vulnerabilities throughout the application and/or product lifecycle
- Experience a 70% reduction in remediation costs by implementing a pro-active, automated approach
- Avoid repercussions from failed compliance audits

Deliver New Services Faster

Innovate Securely

Reduce Costs



Secure Collaborative Lifecycle Management

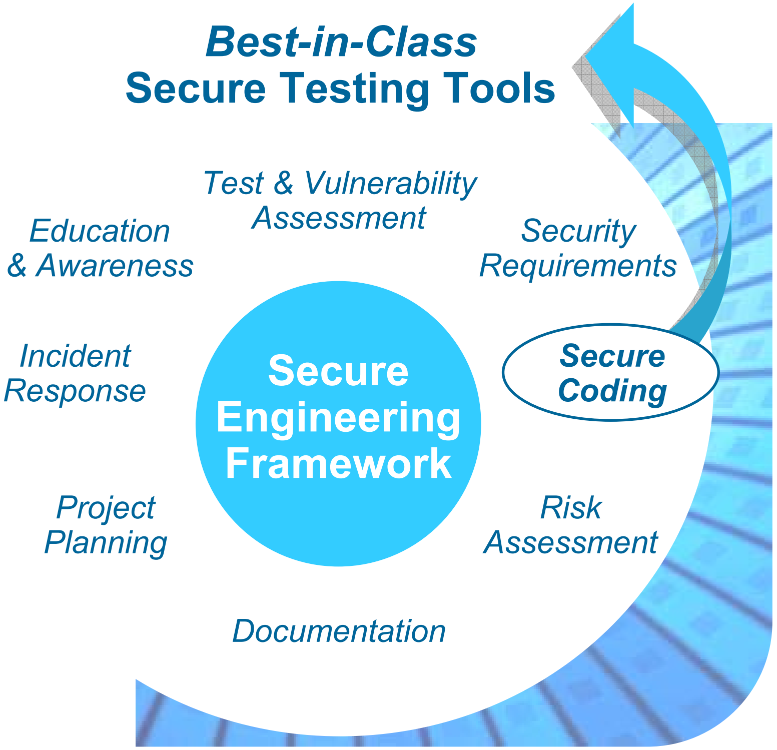
REQUIREMENTS	CODE	BUILD	QA	PRE-PRODUCTION	PRODUCTION
Security requirements templates	*Security testing at the source*	*Automate security testing at build*	*Incorporate security into testing*	*Security oversight & audit*	*Ongoing security monitoring*

Automated security testing at every stage of the development lifecycle

Delivering new Secure by Design tools and frameworks

Implement security best practices and tools into each phase of the lifecycle

- A proven security blueprint for building and deploying secure software in both application and manufactured product scenarios
- Enables on time, on budget delivery of secure software via automated source code testing
- Manage the proliferation of portal and Web applications with more scalable, high performance identity and access management



"Utilizing IBM's leading AppScan family of application security solutions has proven to be of significant value to our customers in reducing their overall risk and demonstrating compliance."

- Joey Peloquin, Director, Application Security, Fishnet Security

Conclusion:

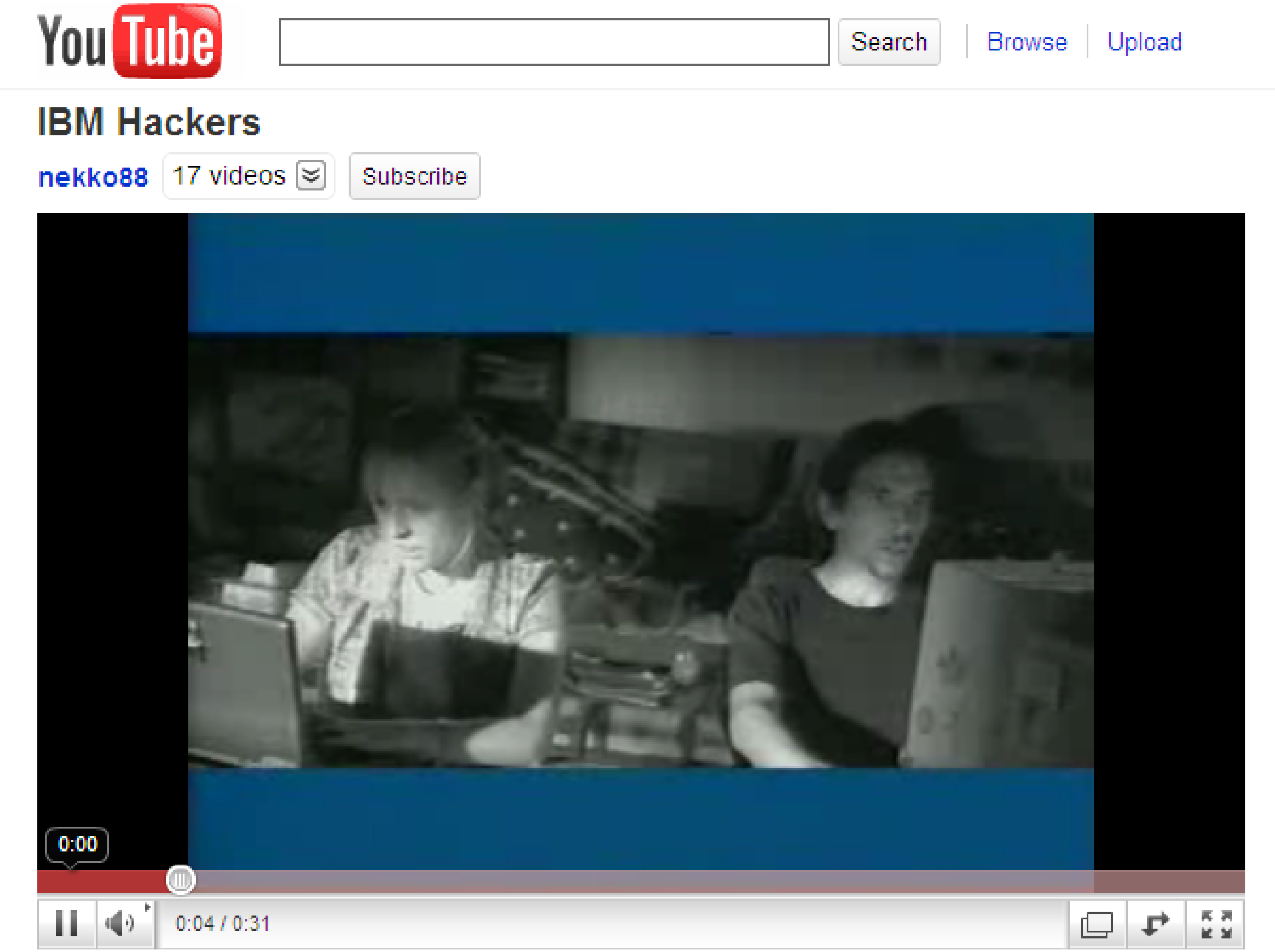
SECURITY BY APPLICATION DEVELOPMENT QUALITY

- **The Application Must Defend Itself**
  - Firewalls & IPS etc cannot stop an application attack
- **Application Security must be strategic, not ad hoc or afterthought**
- **Both security and development teams need to be in harmony**
- **Need to move application security testing back into development (code & build) stages of cycle**
- **Need professional, world-class automated scanning, reporting & remediation tools, backed by comprehensive top R&D.**
- **Future integration with other security solutions eg requirements, network**

Lower Compliance & Security Costs by:

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

http://www.youtube.com/watch?v=LbKaJz_TaLY



IBM Hackers

nekko88 17 videos Subscribe

多 謝 大 家

www.ibm.com/software/rational

ww.ibm.com/security

www.isc2.org CSSLP

www.owasp.org