



THE HACKER'S NEW TARGET – SOFTWARE APPLICATIONS

IBM Software

PCTY2010 

Pulse Comes to You

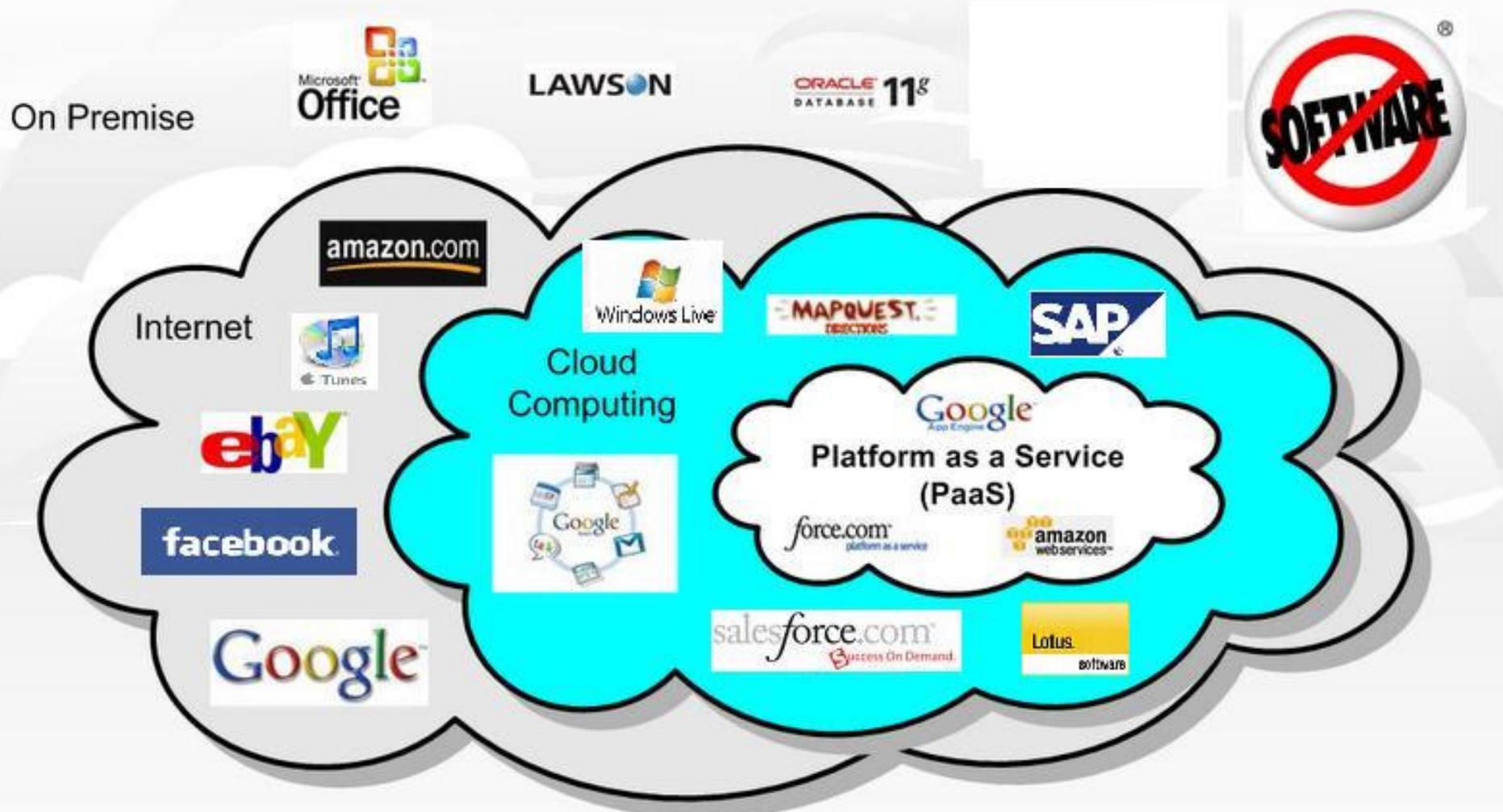
Anthony Lim

MBA CISSP CSSLP FCITIL

Director Asia Pacific, Software Security Solutions, IBM

Singapore Tue 13 Apr 2010

The Wonders of Cloud Computing



PC

Laptop / Netbook

Thin Client

Mobile Device

Welcome to THE SMARTER PLANET



Globalization and Globally Available Resources

Billions of mobile devices accessing the Web



* Web 2.0

• SOA

• CLOUD

Access to streams of information in the Real Time



New Possibilities..

PWC 2010 CIO-CSO INFOSEC SURVEY



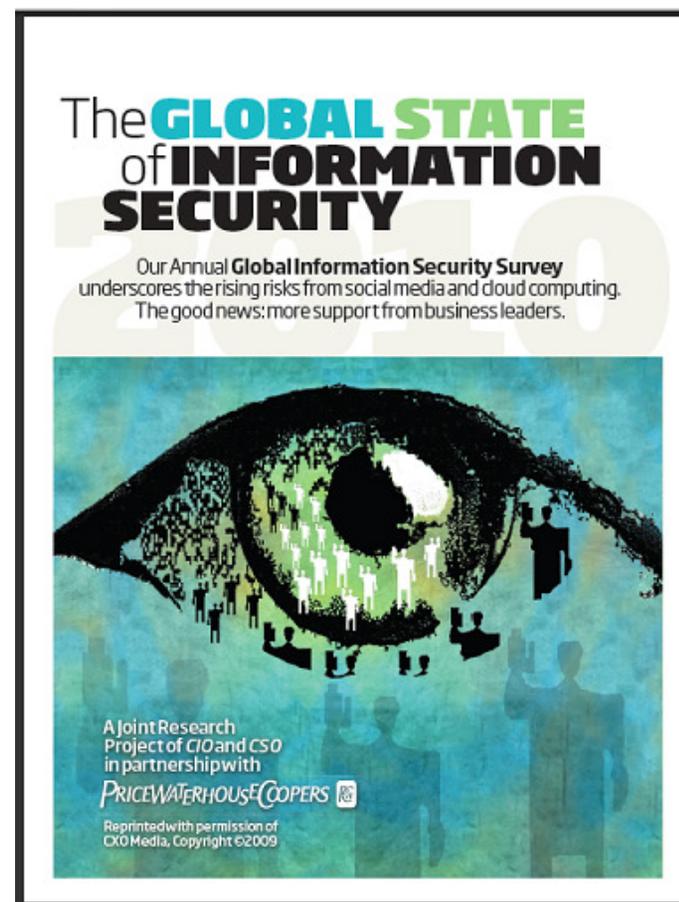
– Some Highlights

Some 2010 CIO-CSO IT Security Priorities

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

Trends:

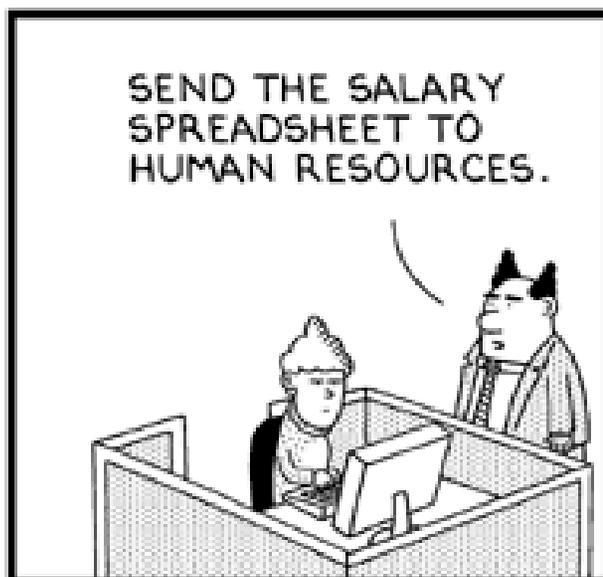
- (1) **Promise and Peril of SOCIAL NETWORKING**
- (2) **Jumping into the CLOUD (w/o parachute)**
- (3) **INSOURCING Security Management**
- (4) **NEW CORPORATE COMMITMENT**
- (5) **ATTACKS ON DATABASES**



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

- It is part of doing business
- Business Continuity
- An environment of TRUST
 - For doing business
 - Ensure Orderliness in Internet world
 - Promote Economic growth
- More than just Confidentiality, Integrity and Availability
- Privacy

3rd Party Customer Data



www.dilbert.com scottadams@aol.com



9-11-04 © 2004 Scott Adams, Inc./Dist. by 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 ...



BBC NEWS

▶ Watch **One-Minute World News**

News Front Page

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

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

E-mail this to a friend Printable version

Monster attack steals user data

US job website Monster.com has suffered an online attack with the personal data of hundreds of thousands of users stolen, says a security firm.

A computer program was used to access the employers' section of the website using stolen log-in credentials.

Symantec said the log-ins were used to harvest user names, e-mail addresses, home addresses and phone numbers, which



Monster is a leading online jobs service

c|net NEWS.com

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

April 6, 2007 4:39 PM PDT

Asus Web site harbors threat

Posted by Joris Evers

It is not such a Good Friday for ASUSTek Computer.

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

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

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

MY PAPER TUESDAY MARCH 3, 2009

SINGAPORE TUE MAR 03 09 MYPAPER PAGE H2

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 Solutions, said such accidental leaks of confidential information could lead to "embarrassing situations for clients and reputation risks for banks".

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

kennyc@sph.com.sg

HBLPDESK 我的字

Glitch: 小故障
xiǎo gù zhàng

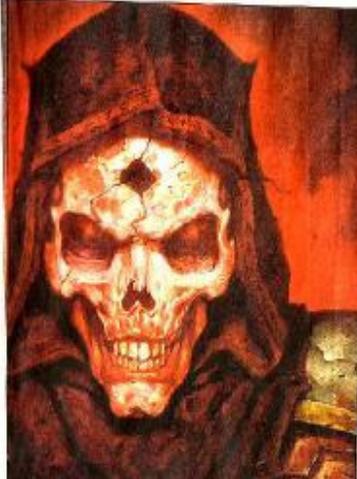
Confidential: 私人的 sī rén de

Rectify: 矫正 jiǎo zhèng

TRAITS TIMES FRIDAY FEBRUARY 11, 2005

GAME OVER

Four friends spent two years amassing \$15,000 worth of riches in an online game — only to lose it all to a hacker. In a new series on digital crime in Singapore, Chua Hian Hou looks at how the victims and the police learned to crack the first such case here



Two years, over 100,000 hours, and a fortune in virtual gold. For four friends, the online game *Diablo II* was not just a pastime; it was a source of real-world wealth. They had spent two years amassing a fortune of \$15,000 worth of virtual gold. But then, one day, it was all gone. A hacker had stolen their accounts, leaving them with nothing but empty pockets.

Chua Hian Hou, a reporter for *Traits Times*, looks at how the victims and the police learned to crack the first such case here.

The story begins with a group of four friends who had spent two years amassing a fortune of \$15,000 worth of virtual gold in the online game *Diablo II*. They had spent two years amassing a fortune of \$15,000 worth of virtual gold. But then, one day, it was all gone. A hacker had stolen their accounts, leaving them with nothing but empty pockets.

The story begins with a group of four friends who had spent two years amassing a fortune of \$15,000 worth of virtual gold in the online game *Diablo II*. They had spent two years amassing a fortune of \$15,000 worth of virtual gold. But then, one day, it was all gone. A hacker had stolen their accounts, leaving them with nothing but empty pockets.

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 con

77 retweet

Share 23



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

Cloud Computing - Dangers and Vulnerabilities



- The Soft Spot

Security is to save data and program from

Dangers -

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

Vulnerabilities -

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



Fri, Mar 19, 2010
Reuters

New password-stealing virus targets Facebook

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

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

WORST CREDIT CARD IDENTITY THEFT CASE



- DONE BY A SOFTWARE ATTACK! (“SQL Injection”)

STRAITS TIMES SINGAPORE 19AUG09

prime.news

THE STRAITS TIMES WEDNESDAY, AUGUST 19 2009 PAGE A6

Hacker accused of stealing 130 million credit card numbers

WASHINGTON: A former government informant known online as “acpuenzi” 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, ac-

ording 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 steal 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 ring-leader 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 “wanddriving”.

This involved cruising through different areas with a laptop computer and

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 alert its presence, prosecutors said.

THE NEW YORK TIMES, BLOOMBERG

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

School website tests show up security lapses

Personal data of staff and students easily, says

popped up. With these, a hacker could use the server at the secondary school to send spam messages or even host an Inter-

SSMG's findings confirm this view. The issue of data privacy had been raised in Parliament in January by Ms Lee

Teachers have also been reminded that it is against school policy to include IC numbers in online documents, he added.

One document on the website of the National University of Singapore (NUS) had the personal particulars of a research fellow, including his address in China.

An NUS spokesman said its users were advised not to divulge personal information in data stored for public access and they need to take personal responsibility for any disclosure.

Republic Polytechnic spokesman Kheng Eu Meng blamed its leak of names, IC numbers and e-mail addresses of 300 students on "human error", and said steps

Why leaks occur

THERE are four main reasons why data leaks occur, says Mr Wong Chee Choo.

- These are:
1. Web servers that are infected with malware, or malicious software, that siphons off information from the server.
 2. Vulnerabilities in Web applications, such as poorly

By KRISHNANT

FOR a week, membership known as the Mashup Group (SMG) sites of various schools with plenty of personal addresses and telephone numbers of staff.

No hacking, spyware needed. All they did was to use Google to find out who they are. In one case, the word of a system

prime.news

THE STRAITS TIMES

THE STRAITS TIMES TUESDAY, JANUARY 5 2010 PAGE A3

WARNING: .sg websites get red-flagged

Global security study by software firm ranks them 10th riskiest

By TAN WEIZHEN

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

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

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

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

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

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

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

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

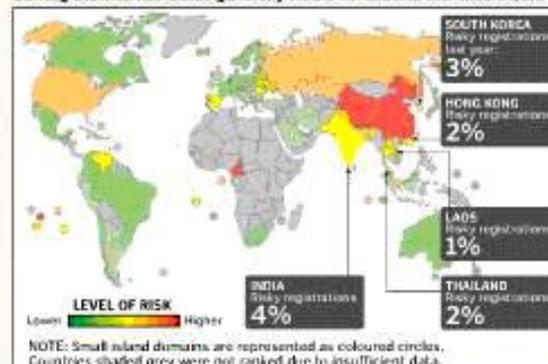
In 2008, just 0.3 per cent of these sites were malicious - that is, they could spread viruses or malware or secretly

RISKY BUSINESS

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

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

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



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

Source: McAfee

ST STRAITS

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

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

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

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

Mr Cheang said the high computer and Internet penetration rate here had created a large pool of potential victims for scammers. As of last October, each household here had 1.3 broadband lines, an increase on a year ago, when it was under one per household.

He noted that the situation here mirrored that of Hong Kong a few years ago. Public education drives for Internet users there have since fixed the problem: Only 2.1 per cent of Hong Kong sites were deemed risky last year, down from 19.2 per cent in 2008, said the McAfee study.

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

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

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



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.java:
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.HttpServletRequestHandler.processRequest(HttpServletRequestHandler.java:79
at com.evermind[Oracle Application Server Containers for J2EE 10g (9.0.4.2.0)].server.http.AJPRequestHandler.run(AJPRequestHandler.java:208)
at com.evermind[Oracle Application Server Containers for J2EE 10g (9.0.4.2.0)].server.http.AJPRequestHandler.run(AJPRequestHandler.java:125)
at com.evermind[Oracle Application Server Containers for J2EE 10g (9.0.4.2.0)].util.ReleasableResourcePooledExecutor$MyWorker.run(ReleasableResourcePoo
at java.lang.Thread.run(Thread.java:534)
```

*These are real examples – hackers
Love these error message pages ...*



Runtime Error - Windows Internet Explorer

http://www.██████████.com/errors/404.aspx?aspxerrorpath=/Default.aspx

File Edit View Favorites Tools Help 9.0 minutes saved

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>
```

Done Internet 100%

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.██████████.com/career/career_job_opening.aspx

File Edit View Favorites Tools Help

Procedure 'car_Get_JobOpeningsKeyword' expects p...

Server Error in '/care

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

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

Internet 100%

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

File Edit View Favorites Tools Help

Favorites Asia...



WIN ONE ARENA PHONE a DAY!

ARENA
KM900



ABN AMRO Bank N.V.
Sign up for RBS
Platinum Card

TERMS AND CONDITIONS APPLY

asiaone news

[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

OK

Index of /

File Edit

Up Back

Go

Print Save As Find Search the web:

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	-	
BIBI_200609.html	02-Oct-2006 16:18	1.0K	
EBALL/	25-Sep-2006 09:37	-	
EIBALL/	19-Sep-2006 14:44	-	
EIBALL/	26-Sep-2006 15:16	-	
EIBALL/	26-Sep-2006 15:21	-	
EIBALL/	21-Sep-2006 17:31	-	
LONY/	02-Oct-2006 05:17	-	
MAKKYO6050/	14-Sep-2006 22:18	-	
RBSANAGUST/	27-Sep-2006 08:36	-	
SDBBP/	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	-	
dfn/	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	-	
eiball/	22-Sep-2006 09:59	-	
eiball/	14-Sep-2006 16:49	-	
eibab/	29-Sep-2006 09:49	-	
eibac/	02-Oct-2006 08:55	-	
eibab/	22-Sep-2006 16:38	-	
eibac/	28-Sep-2006 10:55	-	

A File List in HTML session?!

[Gmail - Label: Bankers] Index of / drexx@LOADSERVER:~ 100% 31 °C Mon Oct 2, 16:18

Real Example: Online Travel Reservation Portal

Hotel Reservation Online - Transaction Slip 20031959 - Windows Internet Explorer

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

Hotel Reservation Online - Transaction ...

Hotel Reservation Online

Change the reserID to 2001200

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,

Done

Internet 100%

Real Example : Parameter Tampering

Reading another user's transaction – insufficient authorization

Hotel Reservation Online - Transaction Slip 2001200 - Windows Internet Explorer

https://www.██████████.com/receipt.php?reserID=2001200&email=1

Hotel Reservation Online

Dear ██████████, 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) ██████████, 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 ██████████
Credit/Debit Card: xxxx-xxxx-xxxx-4688
Expiration Date: 08/2007
Amount: 506.61 USD
Date: Jan 03, 2006

Billed as: ██████████

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.██████████.com/invoice.php?reserID=2001200&email=██████████@hotmail.com

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

invoice.php?reserID=2001200&email=[REDACTED]@hotmail.com

Hotel Reservation Online - Invoice 200...

[REDACTED]

The same customer invoice that reveals the address and contact number

To [REDACTED], Justin
Company
Address 23 [REDACTED] St, Melbourne, VIC 3000, 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

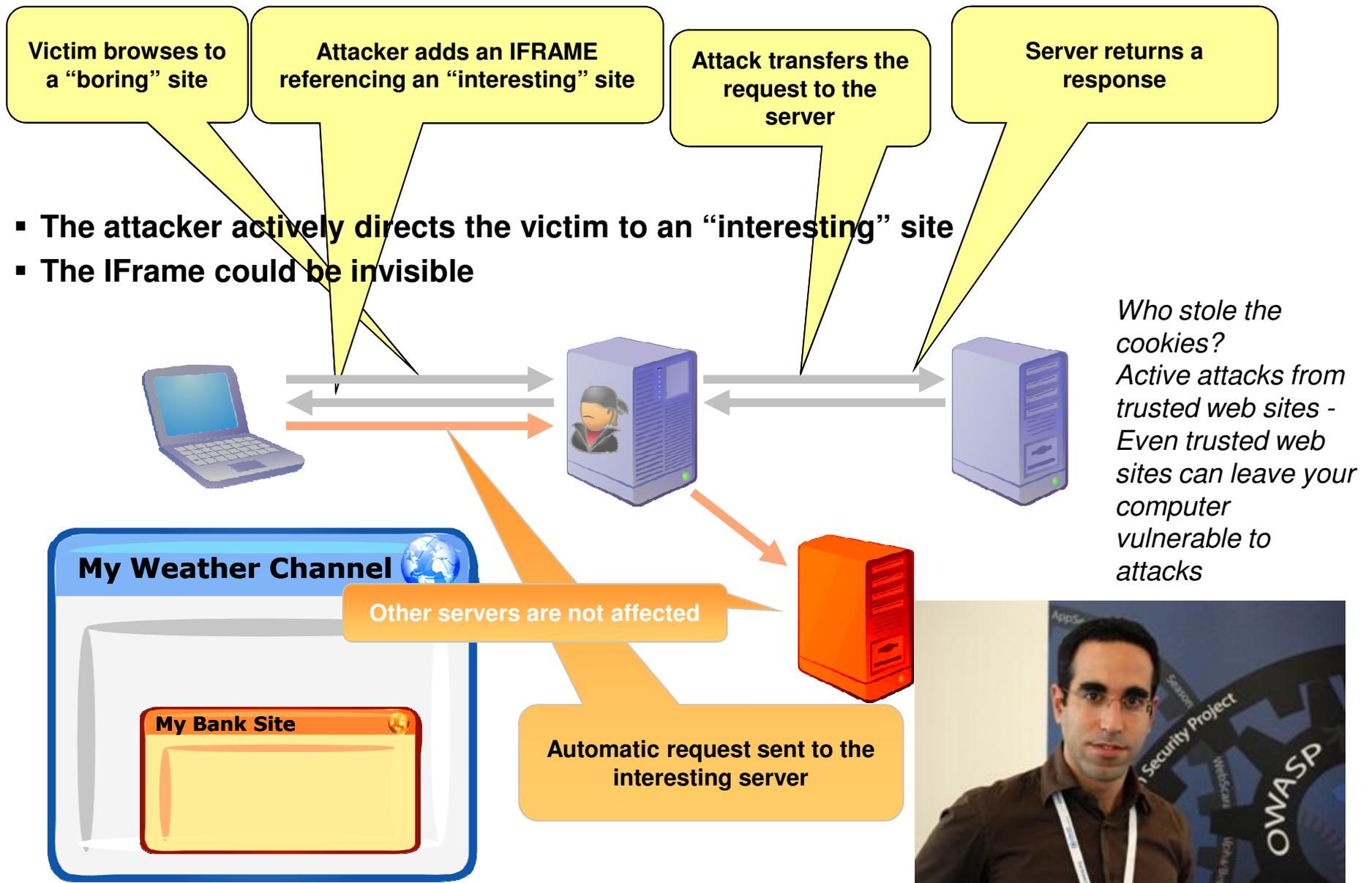
The Payment, billed as [REDACTED], was received by credit card, on Jan 03, 2006, to our account from [REDACTED]:

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,

Done Internet 100%

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



Adi Sharabani at OWASP

Since 2008 - Web Threats Take Center Stage



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

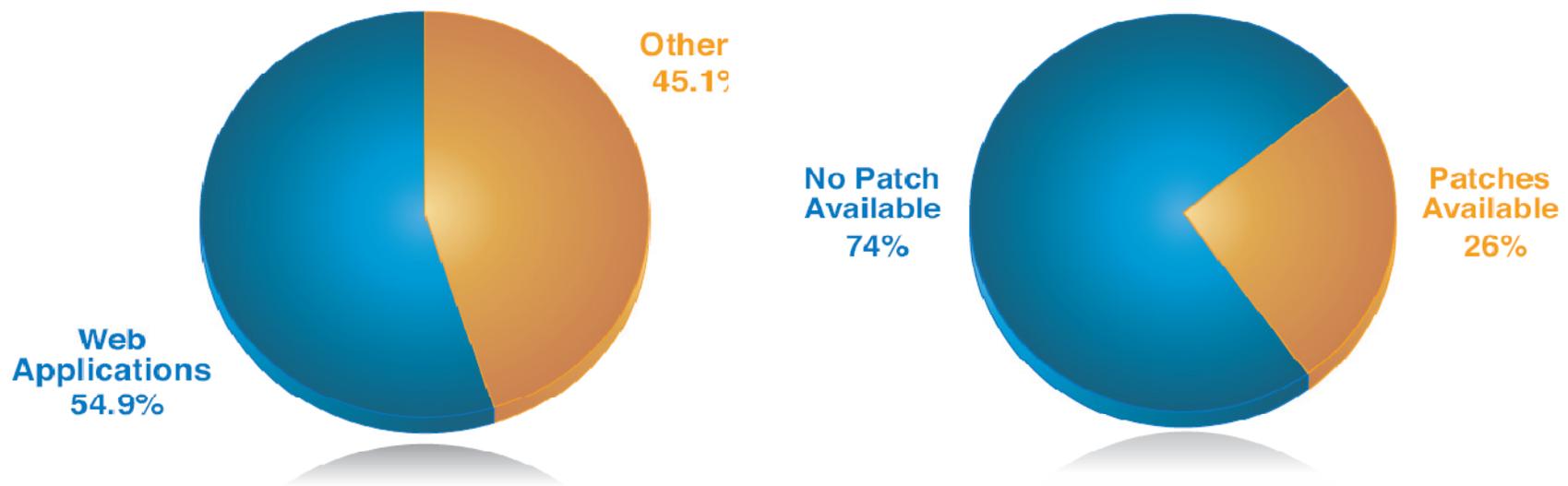


Figure 22: Percent of 2008 Web Application Vulnerabilities with No Vendor-Supplied Patch Available at the End of 2008

WHY DO HACKERS TODAY TARGET APPLICATIONS?



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

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

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

- **Because they can!**
 - **It is difficult or impossible to write a comprehensively robust application**
 - Developers are yet to have secure coding as second nature
 - Developers think differently from hackers
 - **Cheap, Fast, Good – choose two, you can't have it all**
 - **It is a nightmare to manually QA the application**
 - **Many companies today still do not have a software security QA policy or resource**

Software Application Development Pressures

Today I'm being asked to:

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

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



Top 10 OWASP Critical Web Application Security Issues '09

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

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

www.owasp.org

WHY DO APPLICATION SECURITY PROBLEMS EXIST?



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

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

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

Back then coding was done by engineers ...

*Then came Y2K ...
Dotcom boom ... etc*

DON'T TRY THIS AT HOME!



You Tube [India](#) | [English](#)
Broadcast Yourself™

[Home](#) [Videos](#) [Channels](#)

application hacking Videos Search

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

Videos Channels Playlists Sort by: Relevance Uploaded: Anytime Type: All

	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 Original video, (much clearer and sounds normal) Easy ... (more)	Added: 1 year ago From: lvlmeupto100 Views: 24,283 ★★★★★ 01:46
	How to download Hacking Application This video is a part of http://www.youtube.com/watch?v=_cl-zZKxkIo 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 ★★★★★ 04:28

Playlist Results for **application hacking**

[frienster.myspace.facebook.hackers](#) (15 Videos)

			Play all videos	Updated: 3 days ago From: kisszha
hacking friendster #PART 1	hacking friendster #PART 2	Myspace Account Hacking		

	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 ★★★★★ 09:53
--	---	---

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

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

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

Lower Compliance & Security Costs by:

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

You need a professional solution to
Identify Vulnerabilities

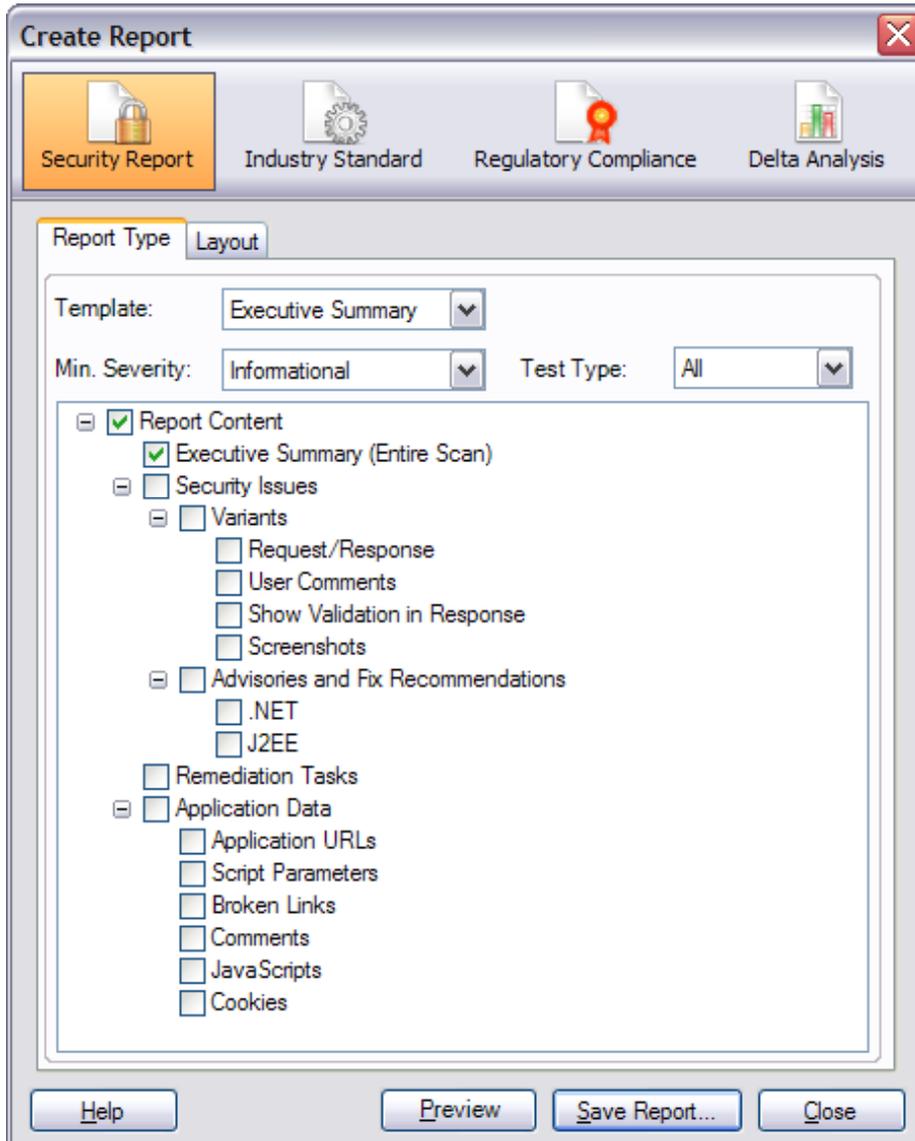
The screenshot displays the Watchfire AppScan interface. The main window shows a scan of 'My Application' with 53 security issues identified. The issues are categorized by severity, with the highest on top. The top categories include Blind SQL Injection (4), Cross-Site Scripting (5), Format String Remote Command Execution (1), HTTP Response Splitting (1), SQL Injection (6), XPath Injection (1), and Cookie Poisoning SQL Injection (1).

The detailed view of a Blind SQL Injection variant (ID: 9294) is shown. The original request is a POST to /bank/account.aspx with a cookie: amCreditOffer=CardType=Gold&Limit=10000&Inter. The difference between the original and the test request is the addition of the parameter listAccounts=0%2B0%2B1001160141%2B0. The reasoning states that this test uses several different HTTP requests to verify the existence of a Blind SQL Injection vulnerability.

The status bar at the bottom indicates 53 Security Issues, 18 Critical, 4 High, 22 Medium, and 9 Low severity issues.

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 Recommendation: [See Appendix 1](#)

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

Remediation:

Sanitize user input

Variant 1 of 4 [ID=2416]

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

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

Request:

```
GET /bank/Login.aspx?uid=>><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>&passw=Demo1234&x=&y= HTTP/1.0
Cookie: ASP.NET_SessionId=3bg3jsupvfrjf0i3bph10rq1
Host: bern
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
Referer: http://bern/bank/Login.aspx
```

Variant 2 of 4 [ID=2418]

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

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

Request:

```
GET /bank/Login.aspx?uid=>><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>&passw=Demo1234&x=&y= HTTP/1.0
Cookie: ASP.NET_SessionId=3bg3jsupvfrjf0i3bph10rq1
Host: bern
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
Referer: http://bern/bank/Login.aspx
```

And Most Important :

Actionable Fix Recommendations

The screenshot displays the Watchfire AppScan 7.5 interface. The main window shows a scan of 'My Application' at 'http://demo.testfire.net/'. The scan is incomplete, and 53 security issues (368 variants) are listed. The issues are arranged by severity, with the highest on top. The top issues include:

- Blind SQL Injection (4)
- Cross-Site Scripting (5)
- Format String Remote Command Execution (1)
- HTTP Response Splitting (1)
- SQL Injection (6)
- XPath Injection (1)
- Cookie Poisoning SQL Injection (1)

The detailed view for 'Blind SQL Injection' is shown below, featuring a 'Fix Recommendation' section. The general advice is to sanitize user input to prevent malicious operations. The recommended characters to filter out are:

- [1] | (pipe sign)
- [2] & (ampersand sign)
- [3] ; (semicolon sign)

The status bar at the bottom indicates 53 Security Issues, 18 Critical, 4 High, 22 Medium, and 9 Low severity issues.

AppScan Enterprise – Dashboards and Metrics



Policies

Controls

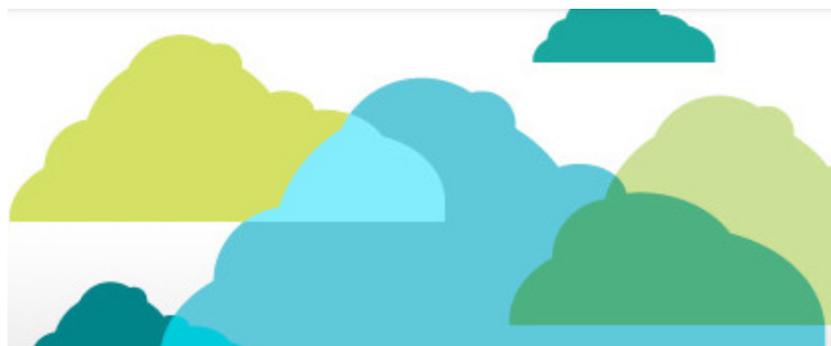
Compliance

AppScan - CQTM & RQM Integration *Protect Your Investment*

The screenshot displays the ClearQuest IDE interface with the following components:

- Test Manager - Planning:** A tree view showing the test hierarchy: Asset Registries > Asset1 > Test Plans > TP1 > TC1 > AppScanTest.
- Console:** Shows the execution progress of the AppScanTest, including scanning statistics and completion times.
- Test Log:**
 - Events:** A list of events including multiple 'message' events and one 'fail' event labeled 'Watchfire AppScan Event'.
 - Watchfire AppScan Regression Results:** Includes links for 'Show in AppScan', 'Update Baseline', and 'View Delta Analysis Report'.
 - Extended Properties:** A table with columns 'Name' and 'Value'. One entry is 'baseFileName' with the value '\\conboy-xpl2\...'.
 - Attachments:** A table with columns 'Name', 'Size', and 'Type', and an 'Open' button.
- Test Results Table:**

Result	Test Type	Verdict	Descri...	ID	Headline	Test Script File	Lo...
Uncommitted ...							
Configure...	AppScan	fail		SAMPL00000075	AppScanTest	\\conboy-xpl2\...	\\cc...
Recently Com...							
- Progress:** Shows 'Test Script Execution' with a progress bar and 'Executing Tests' with a green progress bar.
- Status Bar:** Displays 'Writable' and 'Test Script Execution: (0%)'.



Thank You

Anthony LIM

MBA CISSP CSSLP FCITIL

The Hacker's New Target – Software Applications

www.isc2.org

www.owasp.org

www.ibm.com/security