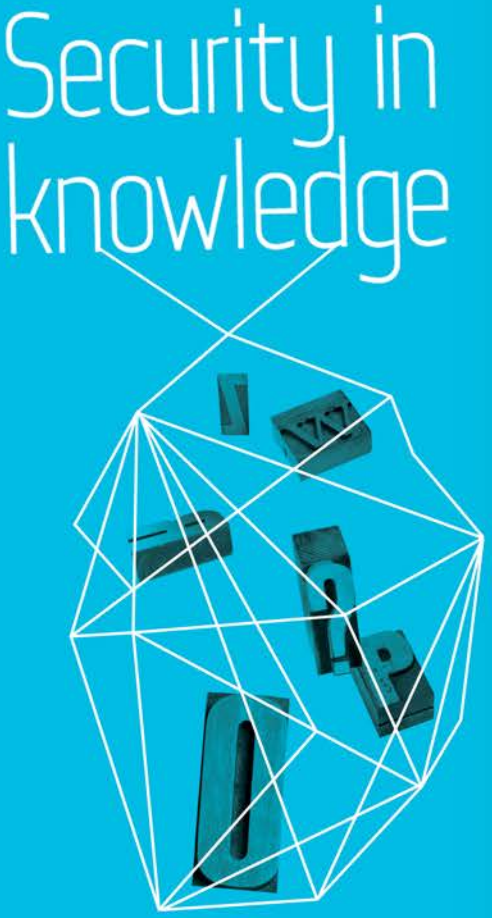
RSA CONFERENCE
ASIA PACIFIC 2013



# CLOUD COMPUTING SECURITY – ARE YOU FORGETTING SOMETHING?

Anthony Lim
MBA CISSP FCITIL CSSLP

Application Security Advisory Board

(ISC)2 www.isc2.org

*Session ID:* DAS-T04

*Session Classification:* General Interest

CSSLP
Certified Secure Software Lifecycle Professional

(ISC)2™
International Standard
for Information Security

# Prolog: The Security Journey Continues

- New, More, Bigger, Better …
  - SYSTEMS
  - APPLICATIONS
  - SERVICES
    - -> *New Risks*
    - -> *New Vulnerabilities*
    - -> *New Hacking methods*
      - *Viruses, Worms, RATS, Bots …*

*(Remote Access TROJANS = Spyware)*

*-> GOVERNANCE & COMPLIANCE!*

*-> CLOUD*

*-> MOBILE & APPS*

- **Data Privacy**
- **Data Leakage**

# Some 2013 Cyber-Security Predictions

CNET

1 The internet as government tool

2 More mobile devices, bigger targets

3 Desktop threat, still a threat

4 Privacy & Data Breaches

FORBES

Biggest CyberSecurity Threats

1 Social Engineering

2 APT's

3 Internal Threats

4 BYOD

5 Cloud

6 HTML5

NETWORK WORLD

1 Hactivism gets worse

2 Continued Cyber-waffling on Capitol Hill

3 Mobile malware whopper

4 Boom Year for Security Services

INTEL

1 Real target are BANKS

2 Legislation remains inconsistent across geographies

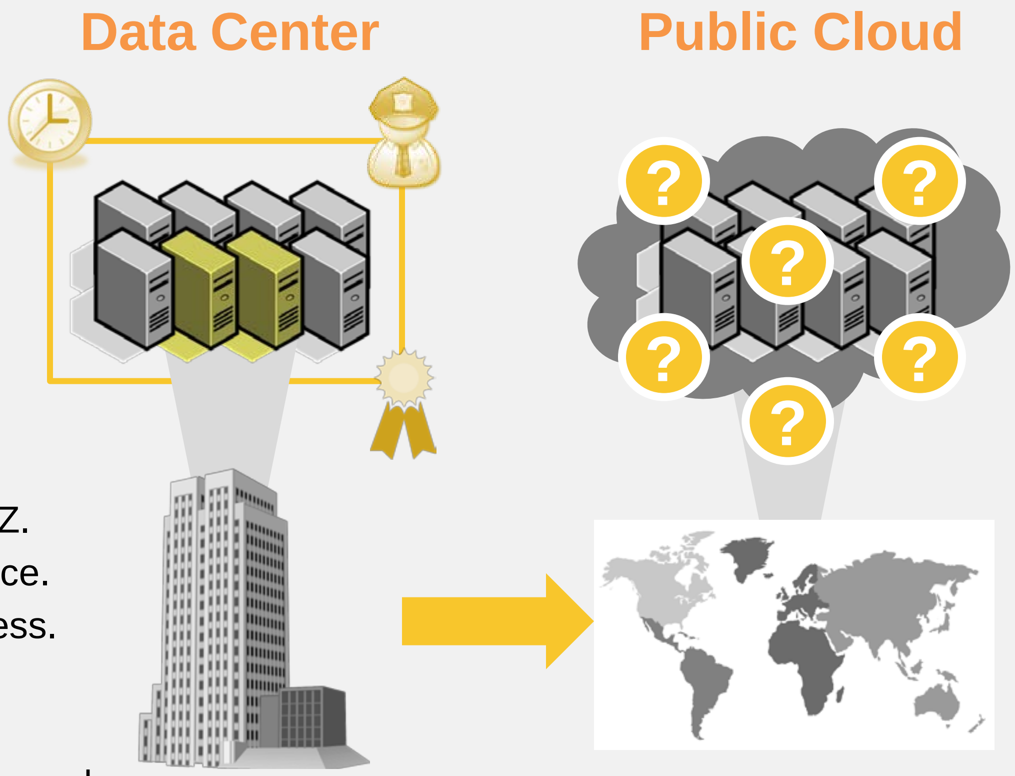
3 Government invests heavily in Cyber

4 More regulations

5 Mobile malware and attacks increase

6 Covert attacks get better /worse

# Cloud Computing – Security Considerations



**We Have Control**

It's located at X.

It's stored in server's Y, Z.

We have backups in place.

Our admins control access.

Our uptime is sufficient.

The auditors are happy.

Our security team is engaged.

**Who Has Control?**

Where is it located?

Where is it stored?

Who backs it up?

Who has access?

How resilient is it?

How do auditors observe?

How does our security team engage?

# Top Threats to Cloud Computing

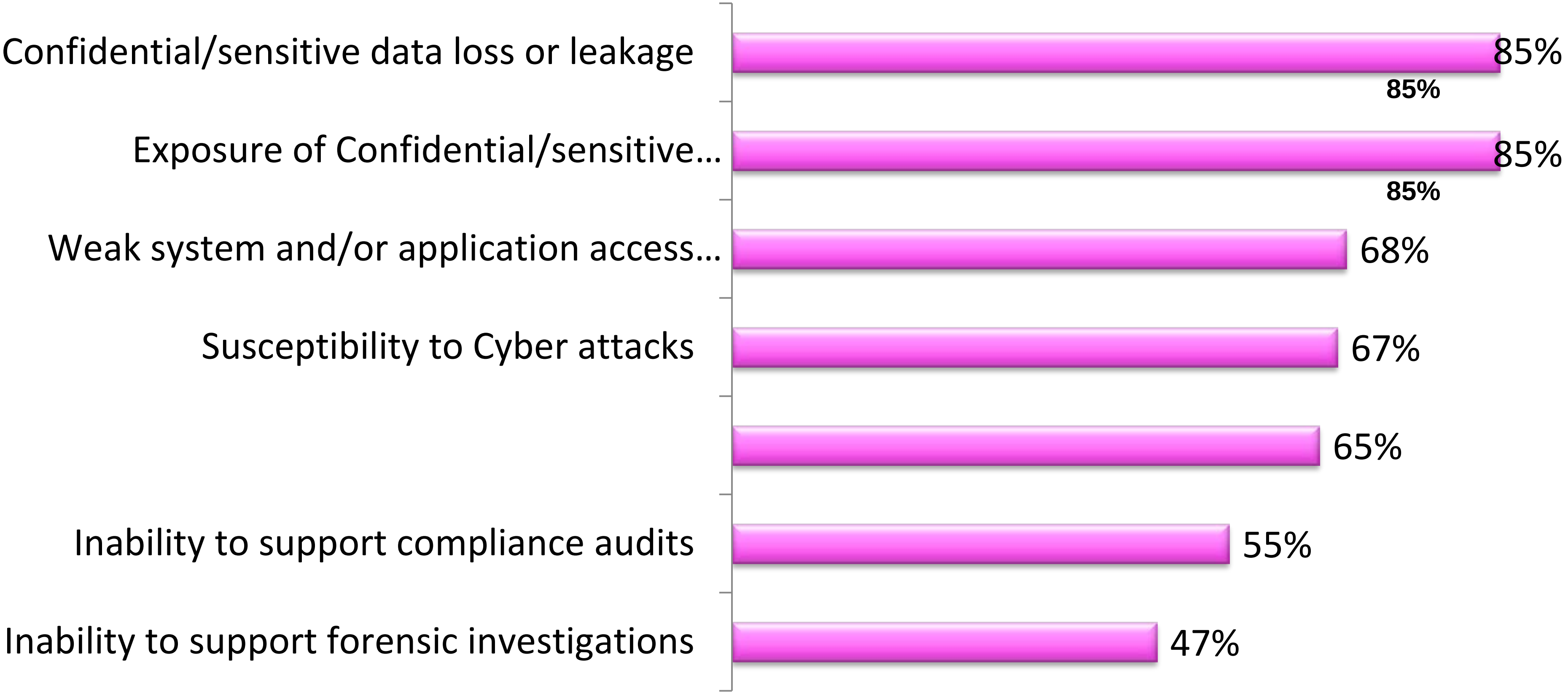
## Cloud Security Risks / Threats

- Shared Technology Vulnerabilities
- Data Loss/Data Leakage
- Malicious Insiders
- Account Service or Hijacking of Traffic
- Insecure APIs
- Nefarious Use of Service
- Unknown Risk Profile

*ISC2 Global Workforce Security Study 2011-12*

# Changing Landscape - Cloud Computing

- Cloud computing illustrates a serious gap between technology implementation and the skills necessary to provide security. 74% said new skills were necessary to help alleviate concerns.



# 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

BUSINESS TIMES SINGAPORE 04 AUG 2010

# Cloud attracting hackers, warns security body

It says fog in the cloud can be cloak for criminals to hide

Reports by RAJU CHELLAM

BEWARE of the fogs that the clouds conceal. Since

have overridden security concerns. In some cases, the business has bypassed internal functions altogether and contracted directly with cloud suppliers."

The result? Corporate security functions are battling

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.

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

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,"

a security strated computing.

world.international

# Hackers break into Nasdaq Web service

'Suspicious files' detected on exchange's Directors Desk, where 300 firms share info with directors

NEW YORK: Hackers broke into a Nasdaq service that handles confidential communications for some 300 corporations, the company said – the latest vulnerability exposed in the computer systems that Wall Street depends on.

## 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.

SINGAPORE TUE MAR 03 09 MYPAPER

# Glitch spills UBS clients' info

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

KENNY CHEE

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

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 infor-

ing to the incident and has implemented measures to prevent a similar occurrence in the future.

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

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

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

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

kennyc@sph.com.sg

TODAY @ PCWORLD

# IMF Hacked; No End in Sight to Security Horror Shows

By Ian Paul, PCWorld Jun 12, 2011 2:22 PM

Graphic: Diego Aguirre

The recent online intrusion into International Monetary Fund servers may have been the work of malicious hackers working for a foreign government, according to online reports.

The IMF is reportedly reluctant to disclose where it believes the attacks came from since 187 of the world's 194 nations (as recognized by the U.S. Department of State) are members of the fund. The hack's perpetrators obtained a "large quantity of data," including e-mail and other documents during the intrusion, according to Bloomberg.

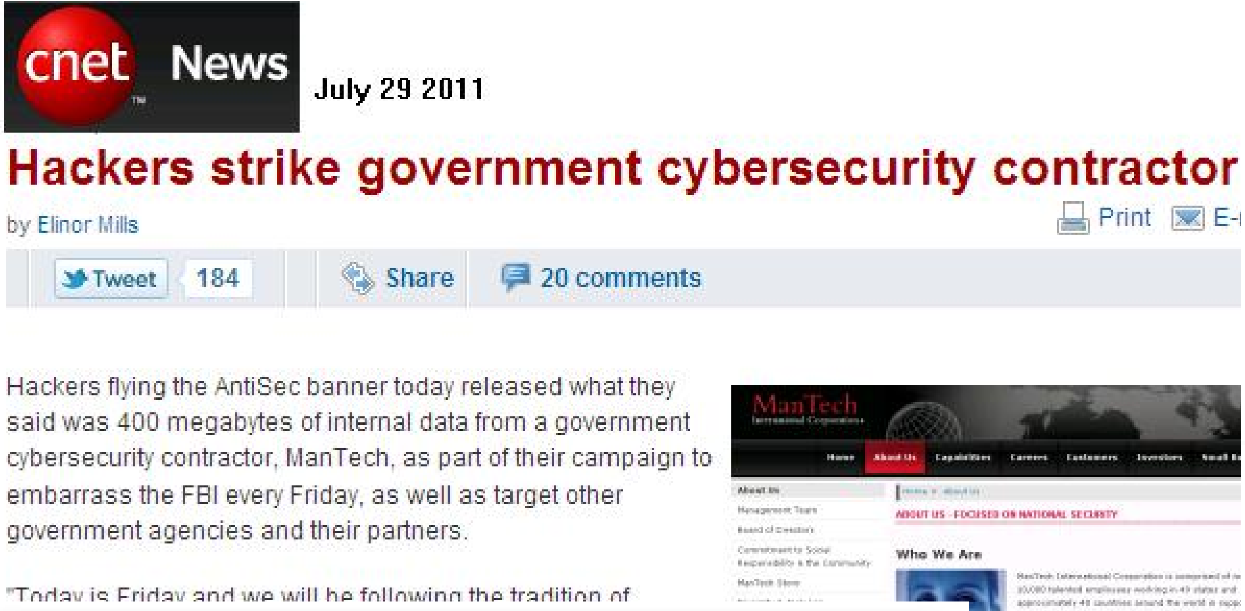
# PLAYSTATION NETWORK, HACKER USING A SIMPLE SQL INJECTION VULNERABILITY FOR ATTACK SONY

June 2, 2011 | Filed under: GAMES NEWS | Posted by: adel

Playstation Network, The hacker organisation which took over a website of PBS NewsHour final week end has returned to a initial adore — hacking Sony.

LulzSec voiced Thursday it hacked servers during **Sony Pictures** as well as **Sony BMG**. The organisation posted what crop up to be a stolen e-mail addresses as well as passwords of about 50,000 consumers who'd purebred for a single of 3 Sony promotional sweepstakes: final year's Seinfeld — We're Going to Del Boca Vista! giveaway, a Jun competition Sony conducted with AutoTrader, as well as a Sony competition to foster a movie Green Hornet.

Something is still out there …



cnet News July 29 2011

# Hackers strike government cybersecurity contractor

by Elinor Mills

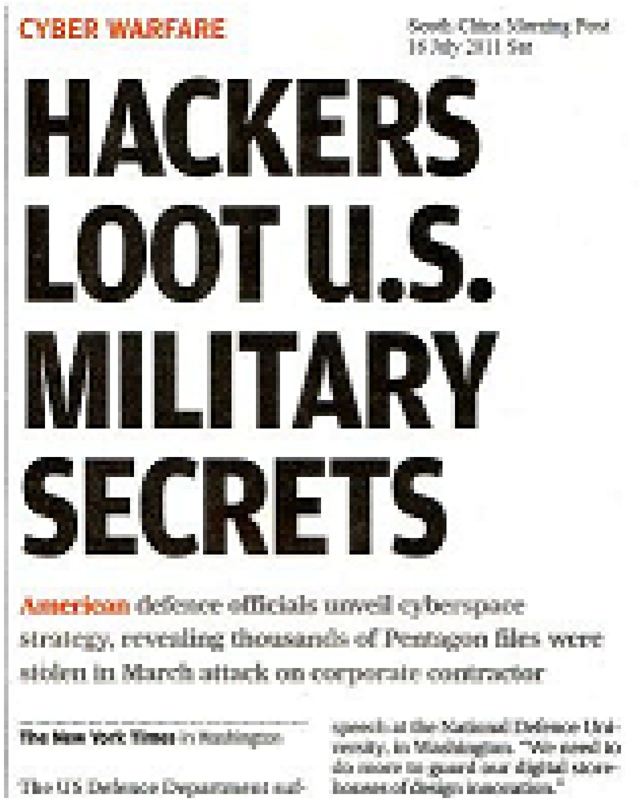
Print E-

Tweet 184 Share 20 comments

Hackers flying the AntiSec banner today released what they said was 400 megabytes of internal data from a government cybersecurity contractor, ManTech, as part of their campaign to embarrass the FBI every Friday, as well as target other government agencies and their partners.

"Today is Friday and we will be following the tradition of

ManTech
International Corporation
Home
About Us
Capabilities
Careers
Customers
Investors
About Us
Management Team
Board of Directors
ManTech Store
ABOUT US - FOCUSED ON NATIONAL SECURITY
Who We Are



CYBER WARFARE

South China Morning Post
18 July 2011 Sat

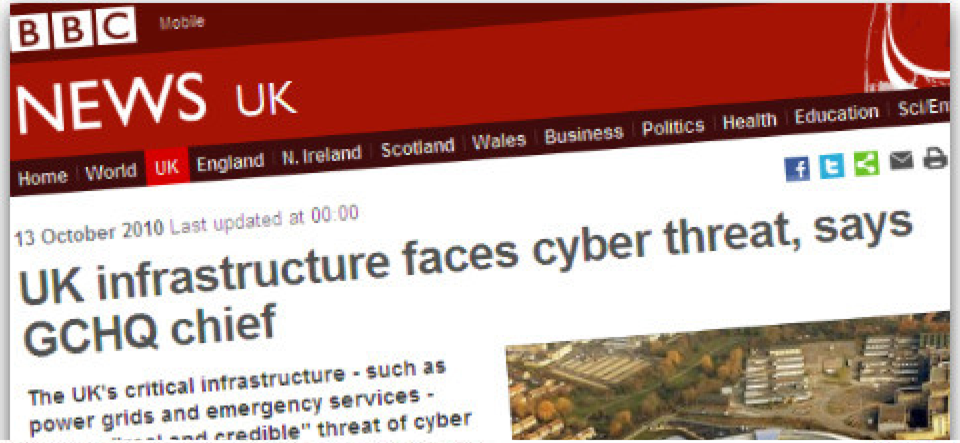
# HACKERS LOOT U.S. MILITARY SECRETS

American defence officials unveil cyberspace strategy, revealing thousands of Pentagon files were stolen in March attack on corporate contractor

The New York Times in Washington

The US Defence Department sub-

speech at the National Defence University, in Washington. "We need to do more to guard our digital storehouses of design innovation."



BBC Mobile

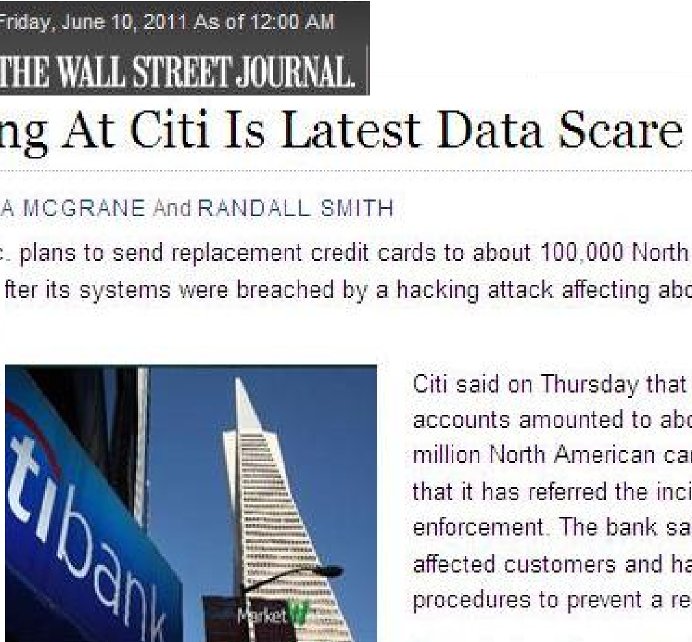
NEWS UK

Home World UK England N. Ireland Scotland Wales Business Politics Health Education Sci/En

13 October 2010 Last updated at 00:00

# UK infrastructure faces cyber threat, says GCHQ chief

The UK's critical infrastructure - such as power grids and emergency services - faced a "real and credible" threat of cyber



Friday, June 10, 2011 As of 12:00 AM

THE WALL STREET JOURNAL.

BUSINESS

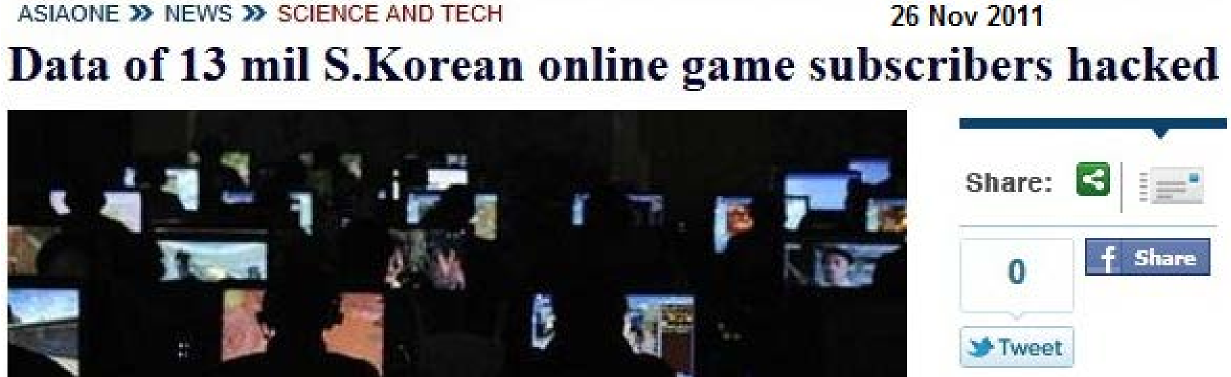
# Hacking At Citi Is Latest Data Scare

By VICTORIA MCGRANE And RANDALL SMITH

Citigroup Inc. plans to send replacement credit cards to about 100,000 North

fter its systems were breached by a hacking attack affecting abo

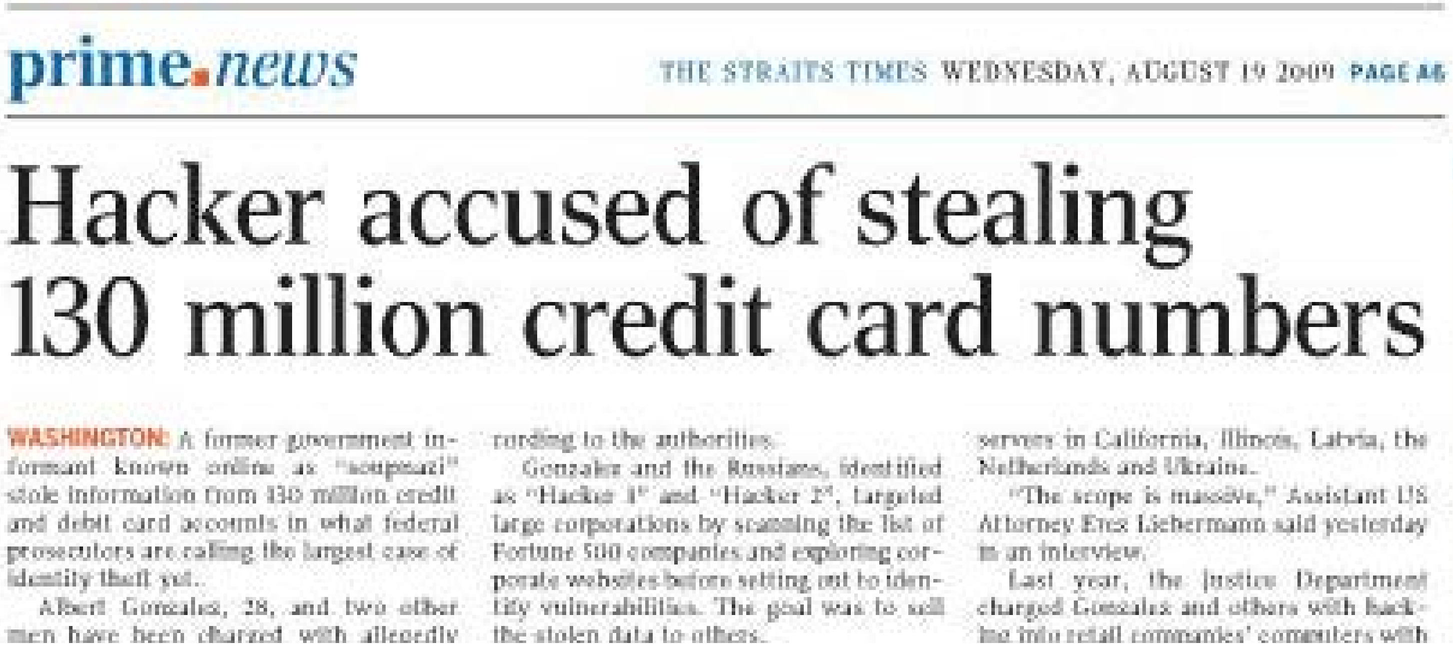
Citi said on Thursday that accounts amounted to abo million North American ca that it has referred the inci enforcement. The bank sa affected customers and ha procedures to prevent a re



ASIAONE » NEWS » SCIENCE AND TECH 26 Nov 2011

# Data of 13 mil S.Korean online game subscribers hacked

**2009:**



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 Gonzales, 28, and two other men have been charged with allegedly

cording to the authorities.

Gonzales 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.

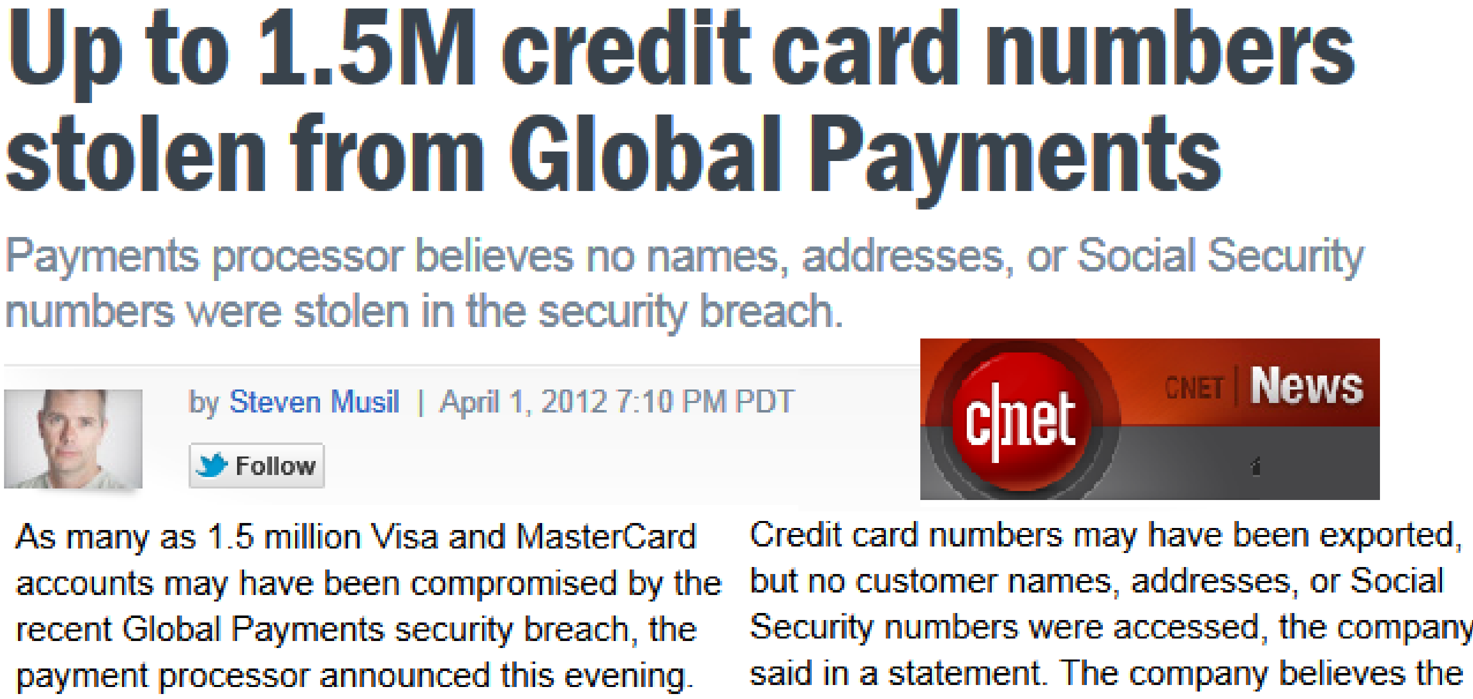
servers in California, Illinois, Latvia, the Netherlands and Ukraine.

"The scope is massive," Assistant US Attorney Erez Liebermann said yesterday in an interview.

Last year, the Justice Department charged Gonzales and others with hacking into retail companies' computers with

***WE NEVER LEARN?***

**2012:**



# Up to 1.5M credit card numbers stolen from Global Payments

Payments processor believes no names, addresses, or Social Security numbers were stolen in the security breach.

by Steven Musil | April 1, 2012 7:10 PM PDT

As many as 1.5 million Visa and MasterCard accounts may have been compromised by the recent Global Payments security breach, the payment processor announced this evening.

Credit card numbers may have been exported, but no customer names, addresses, or Social Security numbers were accessed, the company said in a statement. The company believes the

YOU HAVE BEEN HACKED !

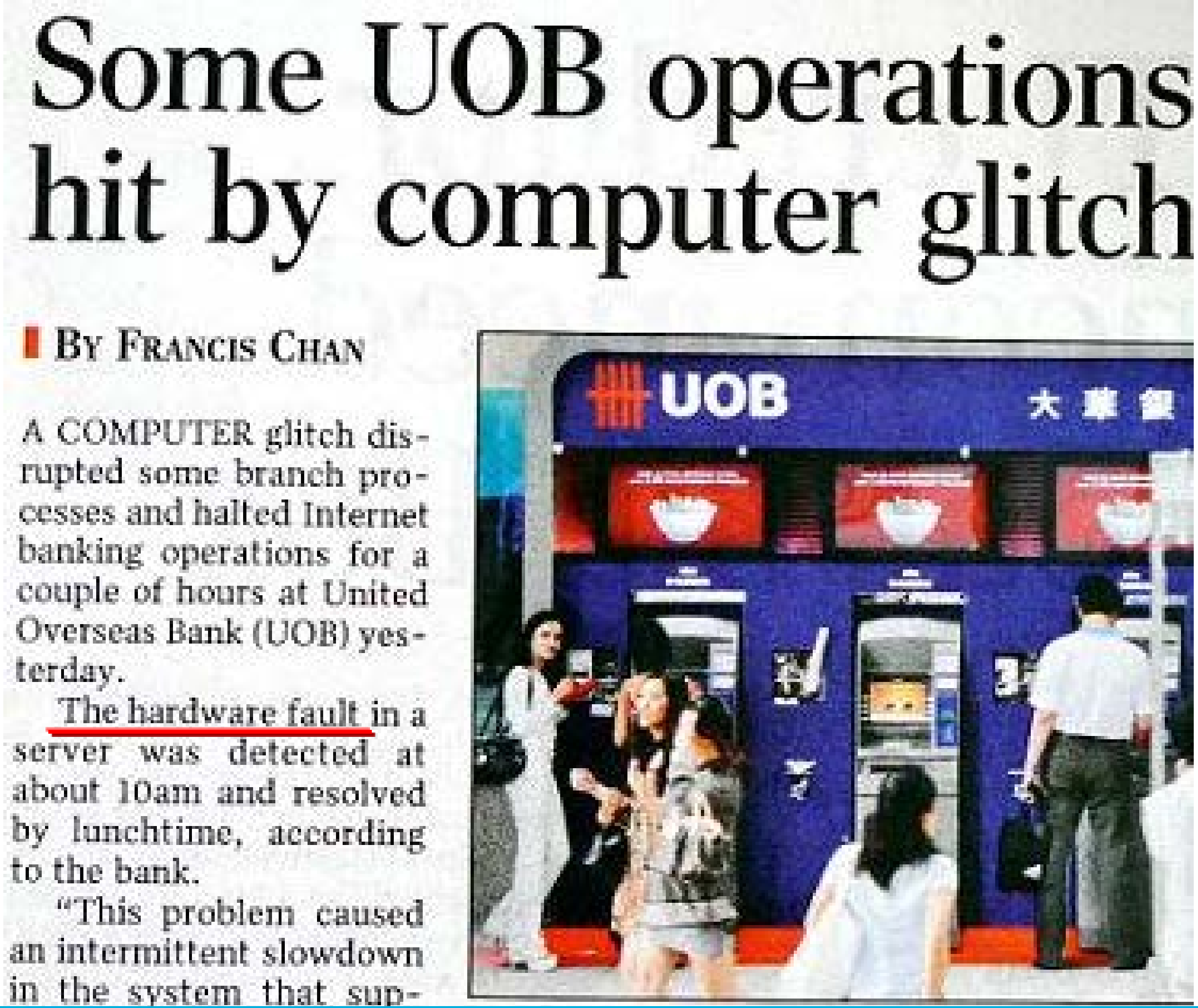
# Some recent cyber-attacks 2013

- Middle-East Debit Card Cyber-Hacking $$$ Theft
- The US-China govt “steath cyber-war” debacle
- Apple Mac users (via Facebook)
- Yahoo Mail Service (back-scatter spam)
- IOS6 Flaw allow access to phone contacts
- Twitter – hacked for spam; FIFA Twitter
- Korea online banking digital cert theft scam
- Korea broadcasting & banking systems down
- **ANONYMOUS WIKI-LEAKS**

# Main reasons for Cyber attacks and Hacking

- **Mischief (make trouble)**
  - ***Hacktivism (political messages)***
    - ***eg Anonymous, WikiLeaks***
- **Disrupt Systems and Services**
  - ***Damage / alter data***
- **Steal money electronically**
- **STEAL DATA**
  - *For use, abuse, sell, threat …*

# “Its never the software?!”



## Some UOB operations hit by computer glitch

By Francis Chan

A COMPUTER glitch disrupted some branch processes and halted Internet banking operations for a couple of hours at United Overseas Bank (UOB) yesterday.

The hardware fault in a server was detected at about 10am and resolved by lunchtime, according to the bank.

“This problem caused an intermittent slowdown in the system that sup-

- Hardware

- Network

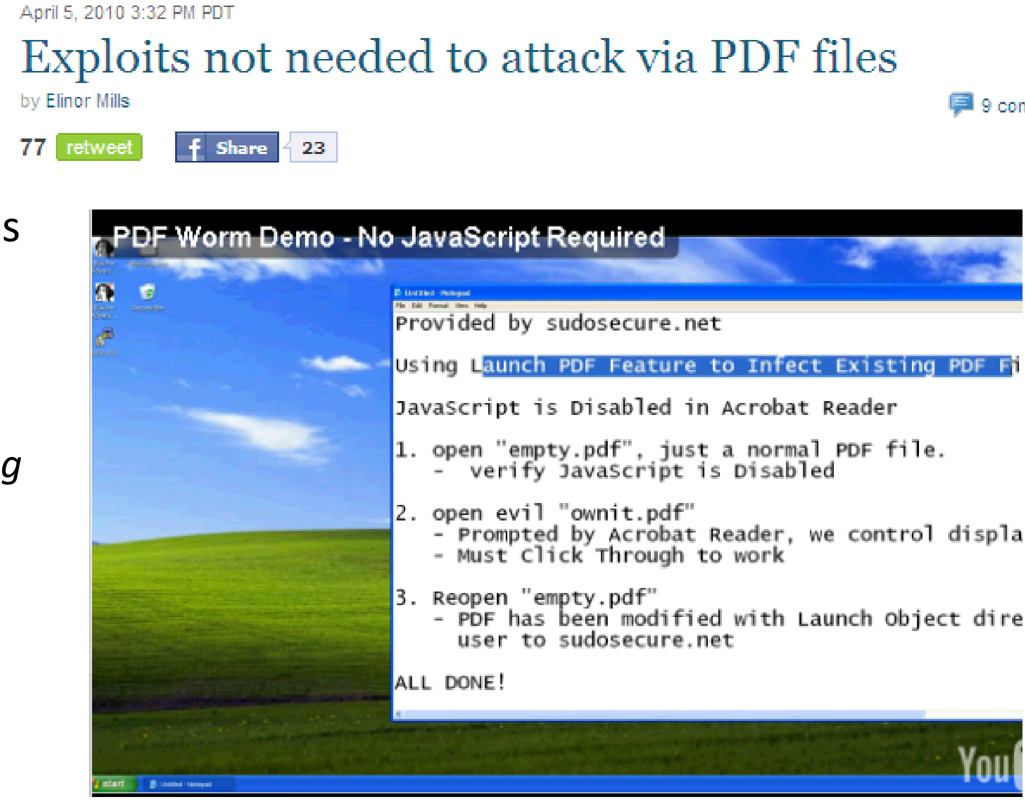
- Bandwidth, provider …

# Hackers Now Attack Web Applications

- 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 unauthorized entry access or unauthorized 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 authorized user, or send data to an unauthorized recipient, etc.
  - Eg. *Cross-site Scripting, SQL Injection*



April 5, 2010 3:32 PM PDT

## Exploits not needed to attack via PDF files

by Elinor Mills

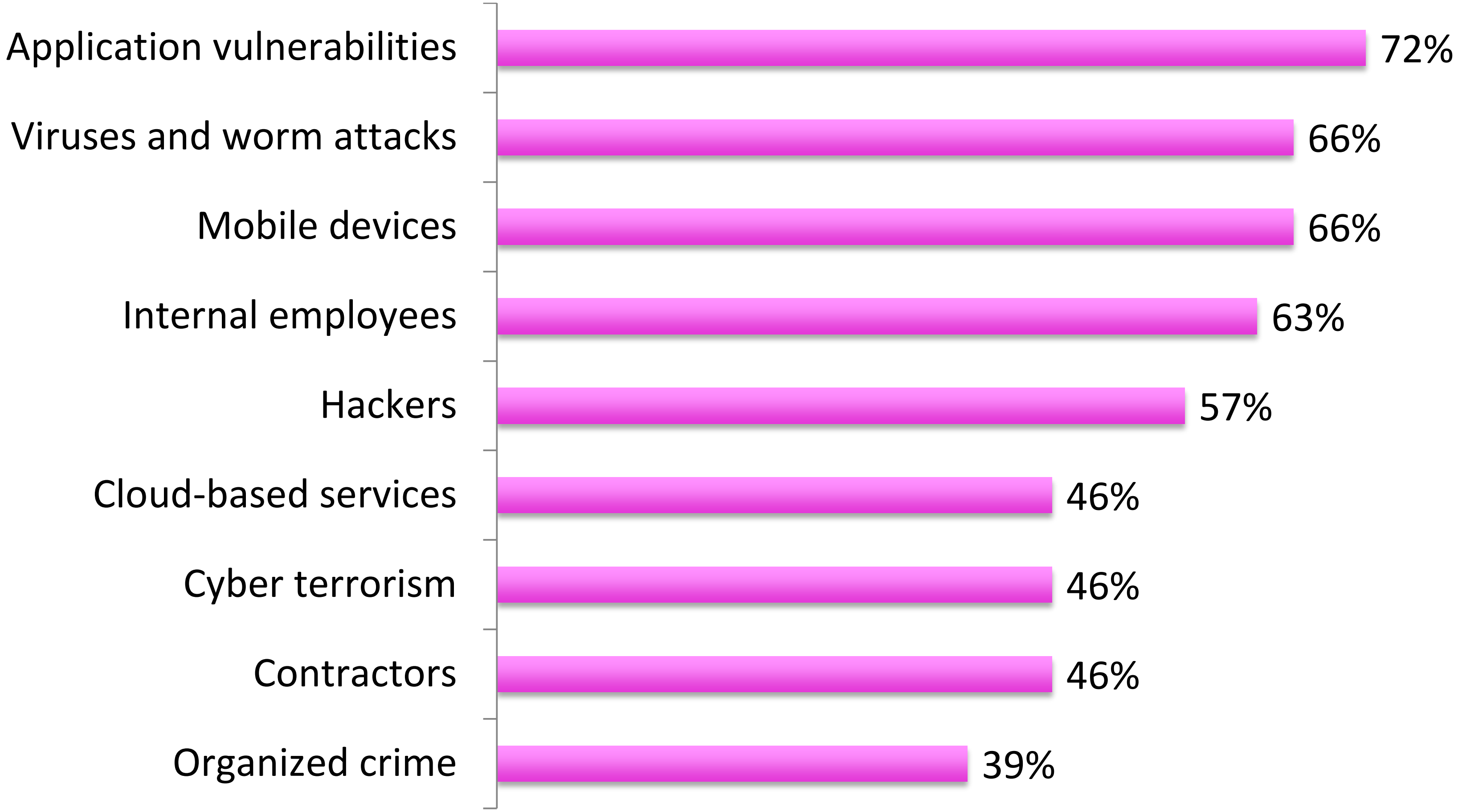
```
Provided by sudosecure.net

Using Launch PDF Feature to Infect Existing PDF Fi

JavaScript is Disabled in Acrobat Reader

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

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

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

ALL DONE!
```

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

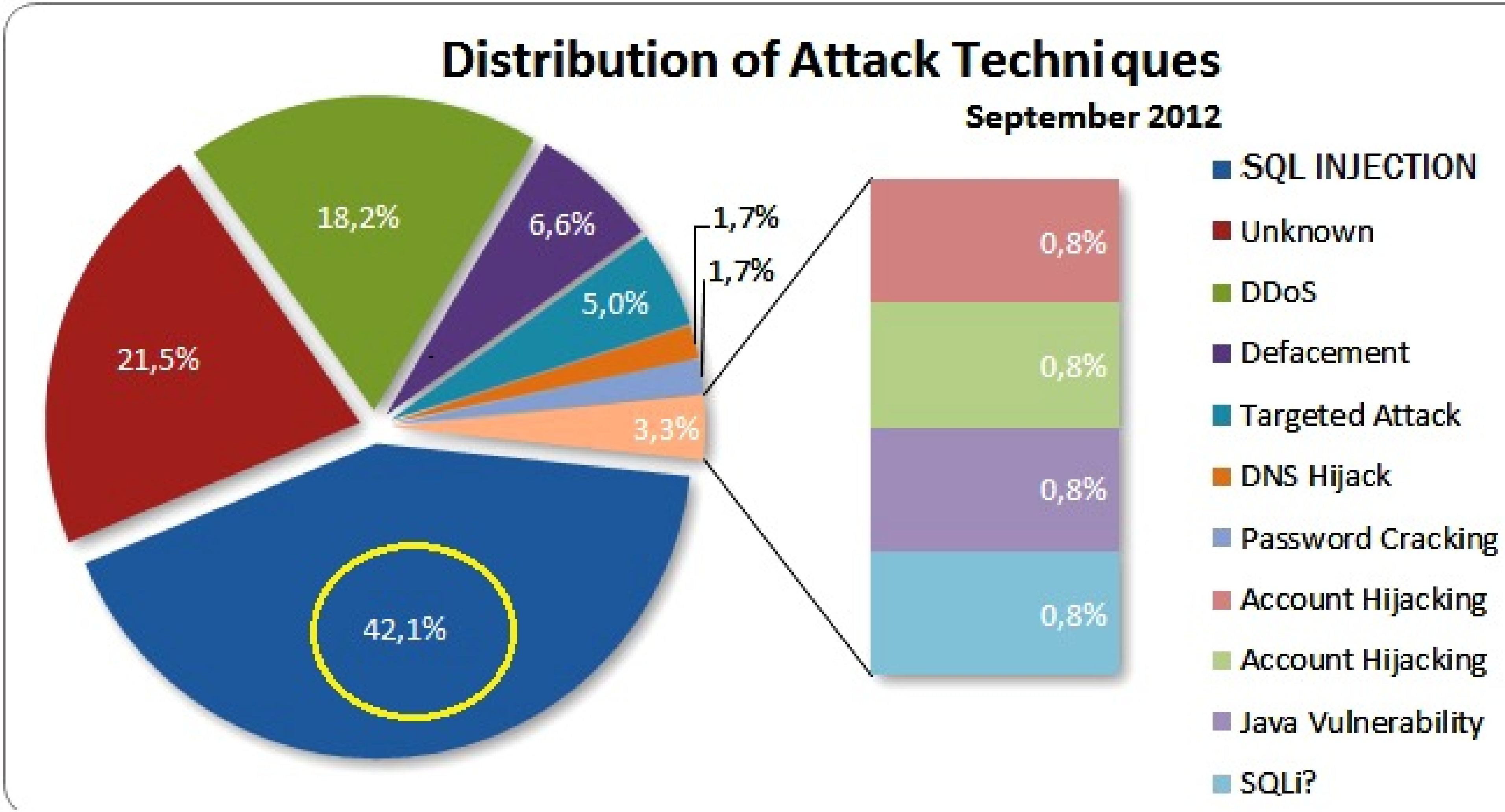
# ISC2 Global Workforce Security Survey 2012

- Application vulnerabilities is Top of the list

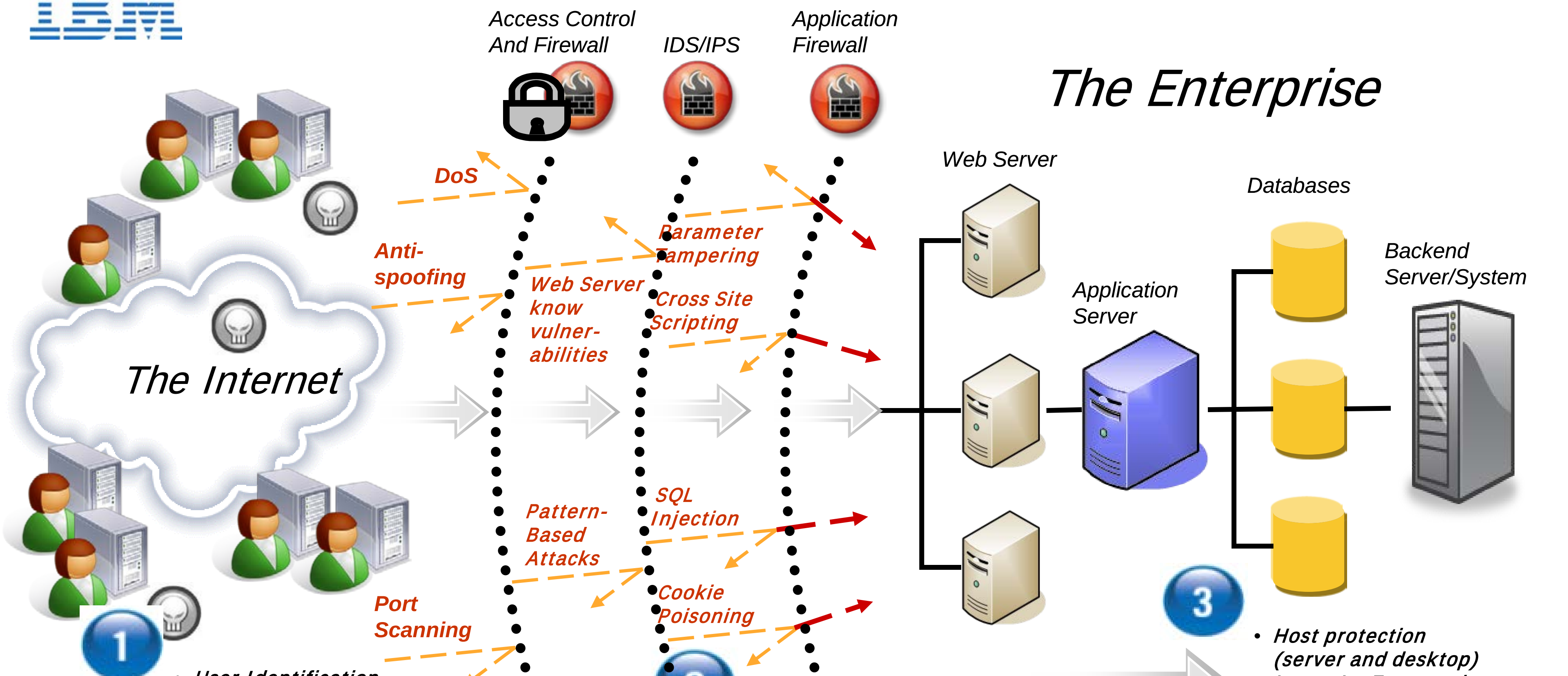
*- in 2008, it was not even on the list*



# IBM X-Force Report Sep 2012



# Simple Application Security Landscape

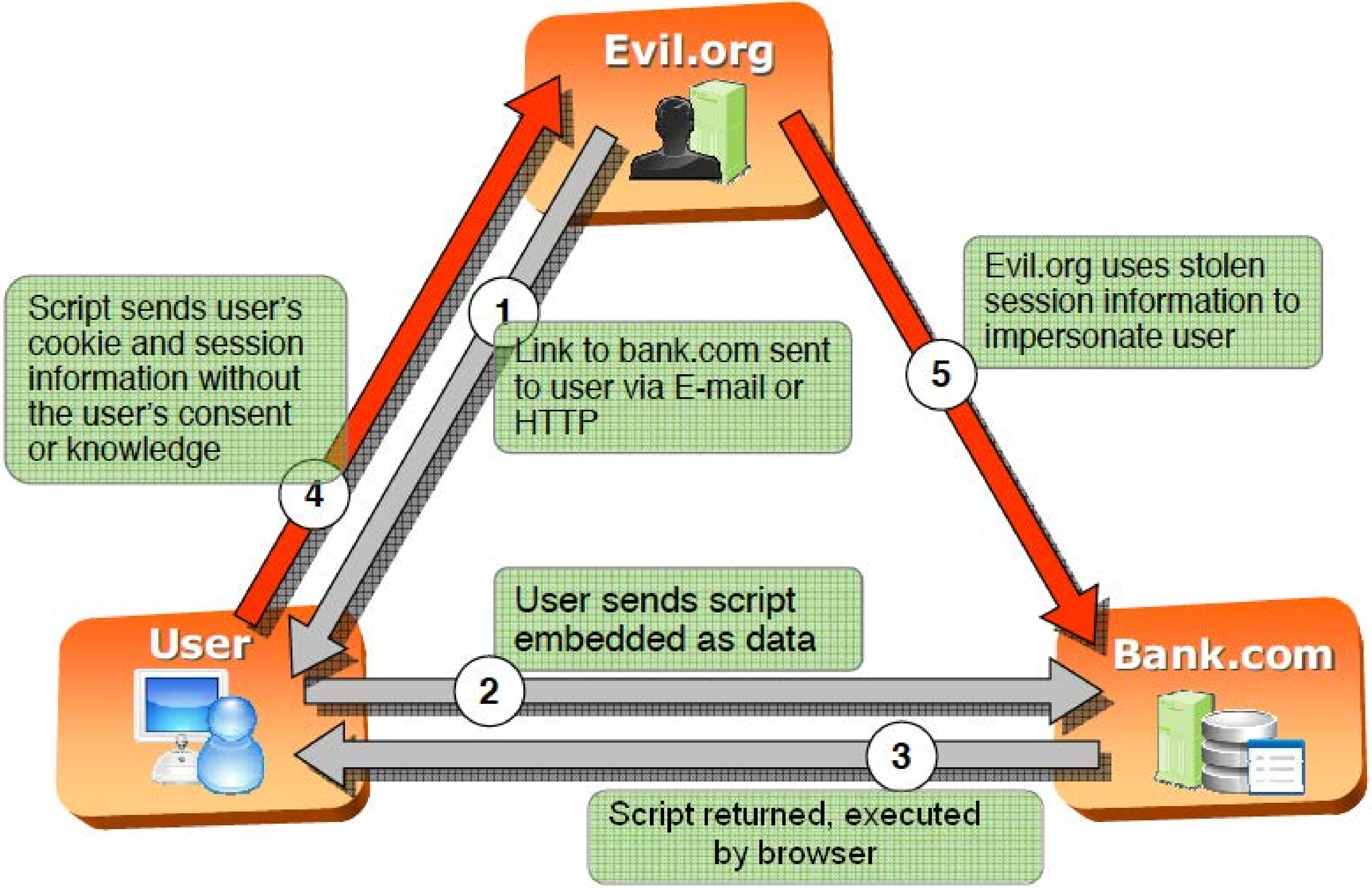


- User Identification
- Access Control
- Encrypted transport of data
- Firewall
- Universal threat management

- Anomaly detection
- Intrusion prevention
- Vulnerability management
- Remediation/Patching
- Compliance and risk management

- Host protection (server and desktop)
- Layer 4 – 7 protection (content, URL, Web)
- Content Control
- Data Leakage management

# Cross Site Scripting (XSS)



Link to bank.com sent to user via E-mail or HTTP

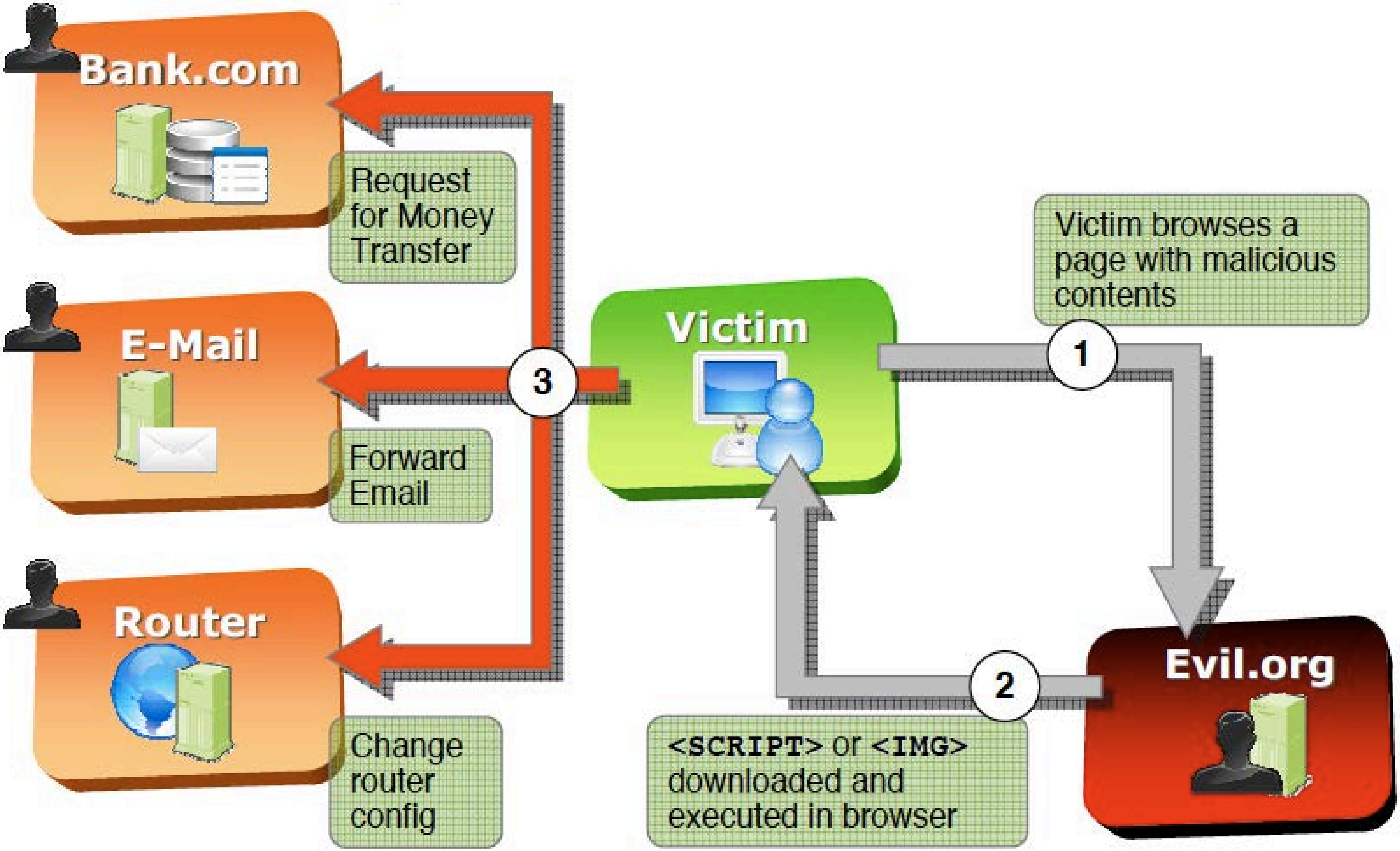
User sends script embedded as data

Script returned, executed by browser

Script sends user's cookie and session information without the user's consent or knowledge

Evil.org uses stolen session information to impersonate user

# Cross-Site Request Forgery (CRSF)



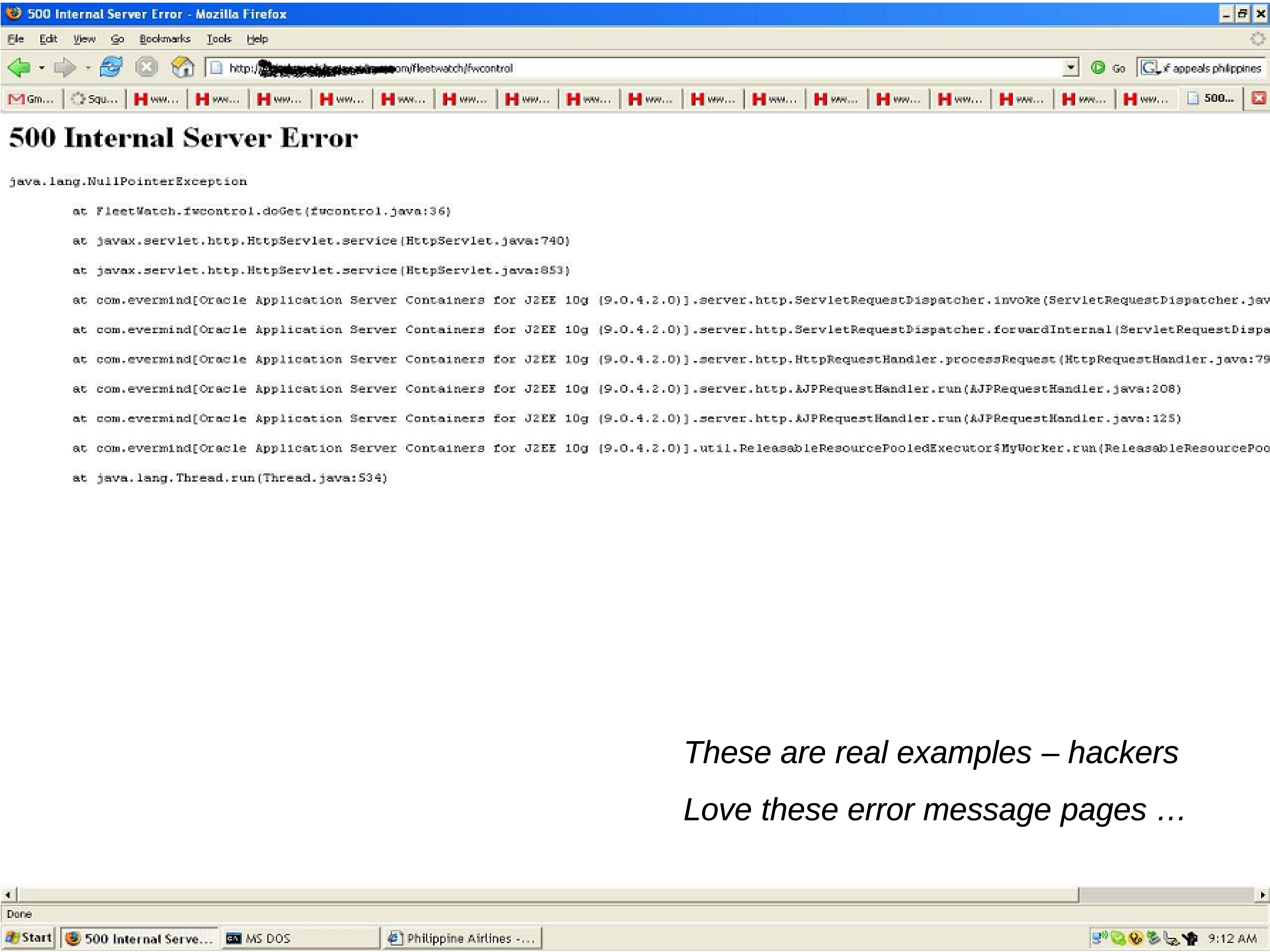
Request for Money Transfer

Forward Email

Change router config

Victim browses a page with malicious contents

<SCRIPT> or <IMG> downloaded and executed in browser



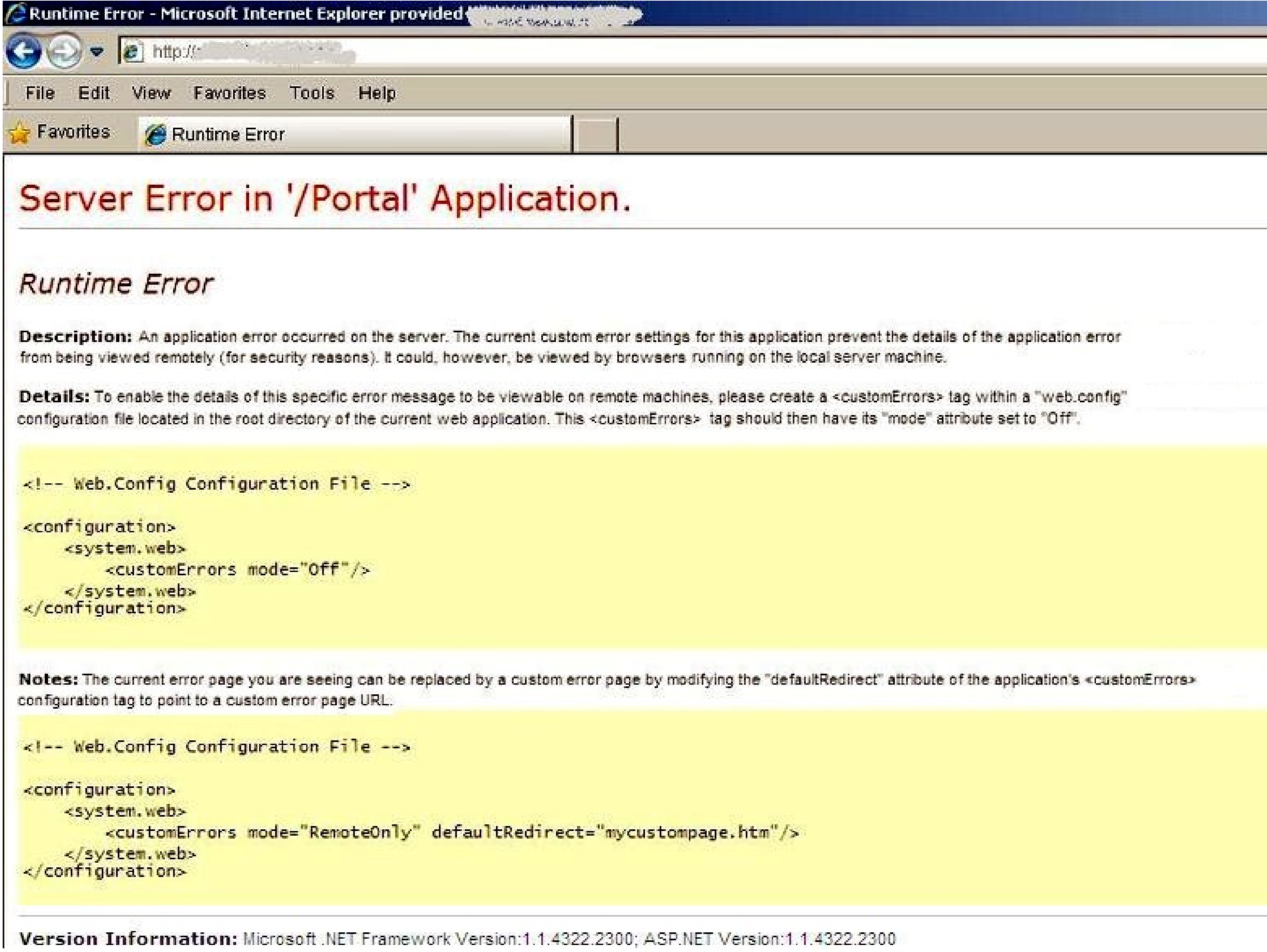
500 Internal Server Error - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://[redacted]om/fleetwatch/fwcontrol
Go
if appeals philippines
Gm... Squ... ww... 500...
Done
Start
500 Internal Serve...
MS DOS
Philippine Airlines -...
9:12 AM

# 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 '/Portal' 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 remotely (for security reasons). It could, however, be viewed by browsers running on the local server machine.

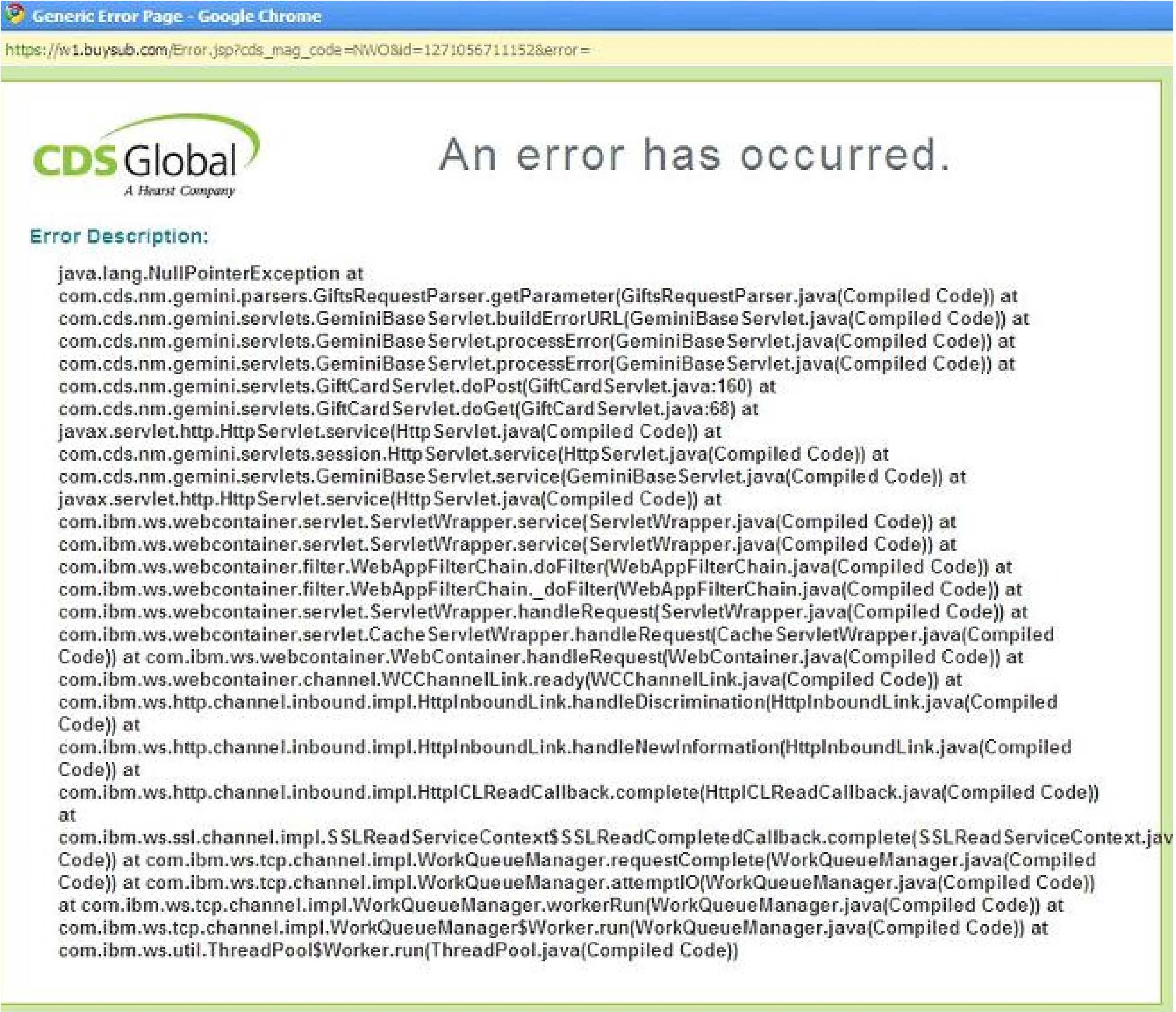
**Details:** To enable the details of this specific error message to be viewable on remote machines, please create a <customErrors> tag within a "web.config" configuration file located in the root directory of the current web application. This <customErrors> tag should then have its "mode" attribute set to "Off".

```
<!-- Web.Config Configuration File -->

<configuration>
    <system.web>
        <customErrors mode="Off"/>
    </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="RemoteOnly" defaultRedirect="mycustompage.htm"/>
    </system.web>
</configuration>
```

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

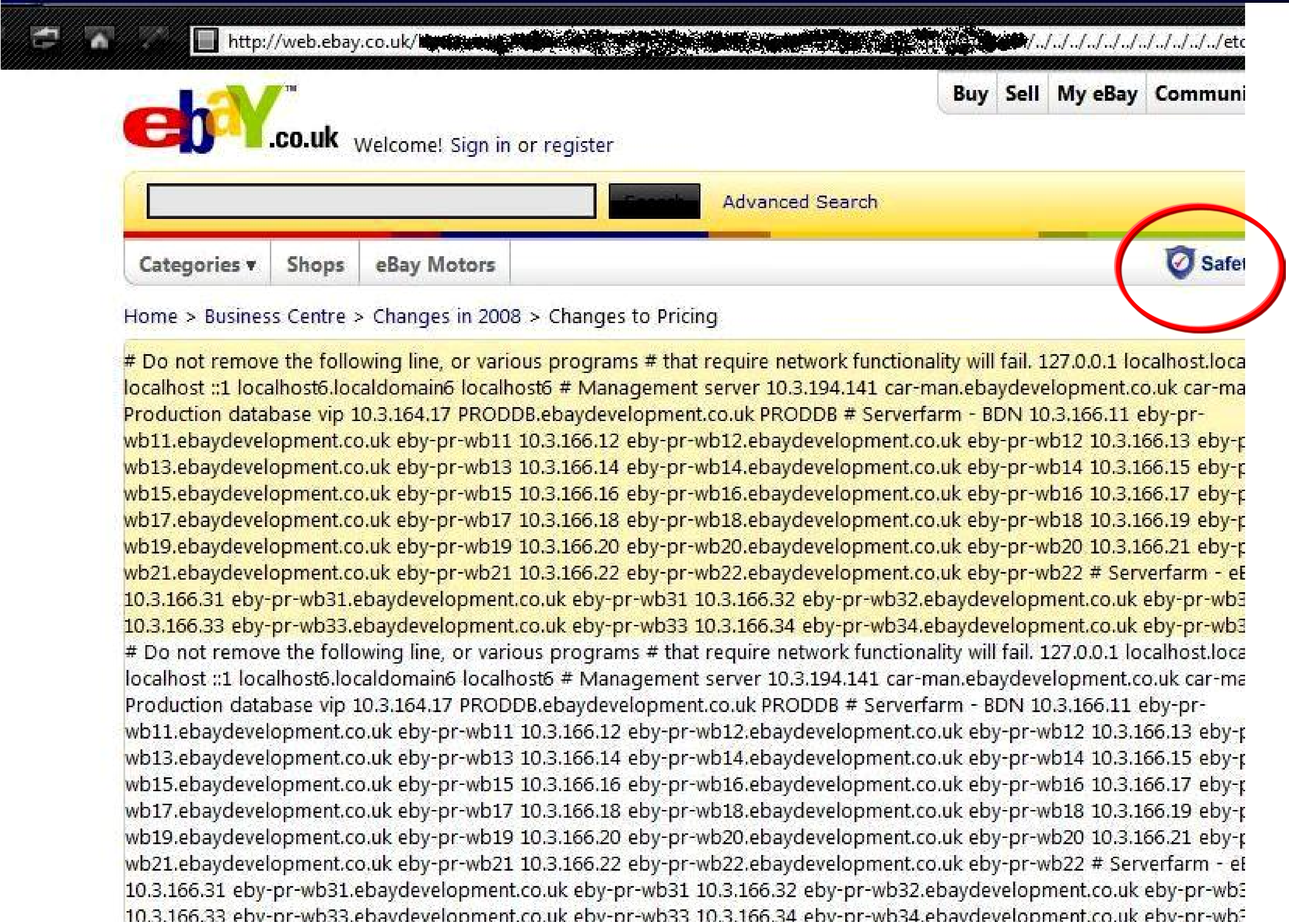

Generic Error Page - Google Chrome
https://w1.buysub.com/Error.jsp?cds_mag_code=NWO&id=1271056711152&error=
CDS Global
A Hearst Company

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$SSLReadCompletedCallback.complete(SSLReadServiceContext.jav
Code)) at com.ibm.ws.tcp.channel.impl.WorkQueueManager.requestComplete(WorkQueueManager.java(Compiled
Code)) at com.ibm.ws.tcp.channel.impl.WorkQueueManager.attemptIO(WorkQueueManager.java(Compiled Code))
at com.ibm.ws.tcp.channel.impl.WorkQueueManager.workerRun(WorkQueueManager.java(Compiled Code)) at
com.ibm.ws.tcp.channel.impl.WorkQueueManager$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

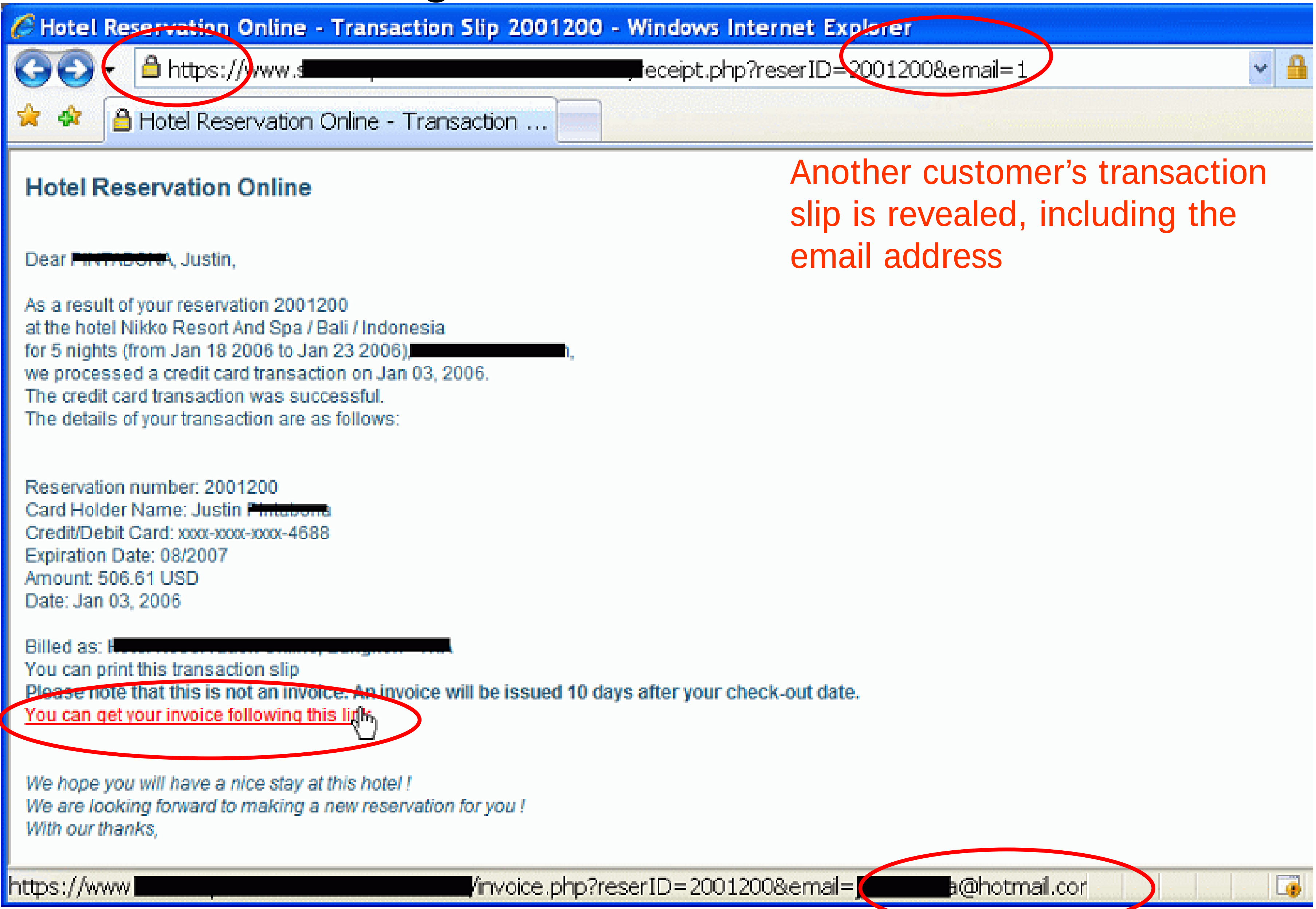
# Do not remove the following line, or various programs # that require network functionality will fail. 127.0.0.1 localhost.loca
localhost ::1 localhost6.localdomain6 localhost6 # Management server 10.3.194.141 car-man.ebaydevelopment.co.uk car-ma
Production database vip 10.3.164.17 PRODDB.ebaydevelopment.co.uk 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 : Parameter Tampering

## Reading another user's transaction

▶ URL Rotation


Hotel Reservation Online - Transaction Slip 2001200 - Windows Internet Explorer
Hotel Reservation Online - Transaction ...

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

Hotel Reservation Online

Dear [redacted], Justin,

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

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

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

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

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

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

# Software Attacks – Low Hanging Fruits

Shell Command Execution

HTTP PUT Defacement

Backup Files

Blind SQL Injection

Debug files and Test pages

Directory Listing

Insecure HTTP Methods

HTTP Response Splitting

SOAP Web Services Issues

XPath Injection

Path Traversal in Parameters

Server Side Includes

File Upload

Phishing Through URL redirection

Poison Null Byte

Buffer Overflows

Administration Pages

SQL Injection

LDAP Injection

MS FrontPage Issues

Email Spoofing

Cross Site Scripting

Path Traversal in URL

BEA WebLogic Issues

SUN iPlanet Issues

Oracle iAS Issues

Format Strings

VALIDATE INPUT

PHP Issues

Apache HTTPd Issues

ColdFusion Issues

Microsoft IIS Issues

Credentials Enumeration

Tomcat Issues

Cookie Poisoning SQL Injection

Privacy Issues

# Some Critical Software Development Security Issues

(ISC)²™
International Standard for Information Security

CSSLP
Certified Secure Software Lifecycle Professional

**www.OWASP.org**

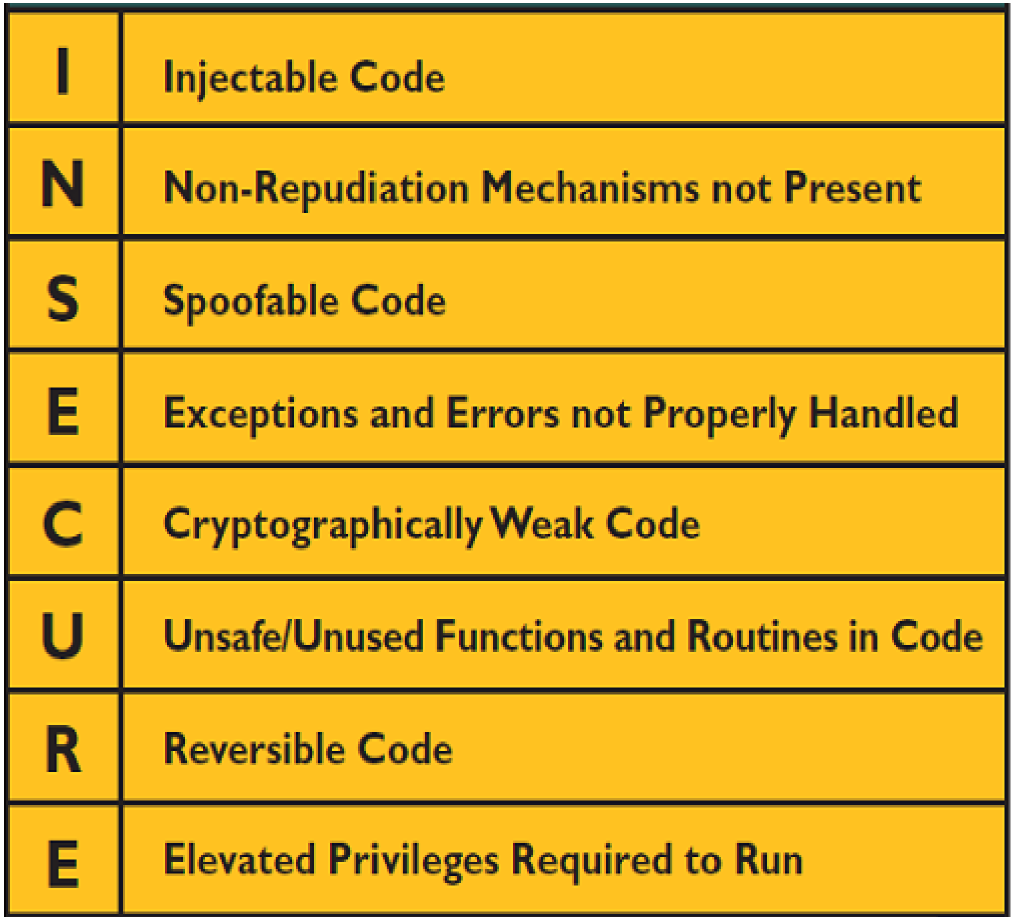
1. Unvalidated Input
2. Broken Access Control
3. Broken Authentication & Session Management
4. Cross Site Scripting Flaws
5. Buffer Overflows
6. Injection Flaws
7. Improper Error Handling
8. Insecure Storage
9. Denial of Service
10. Insecure Configuration Management

Java

**ISC2 :**

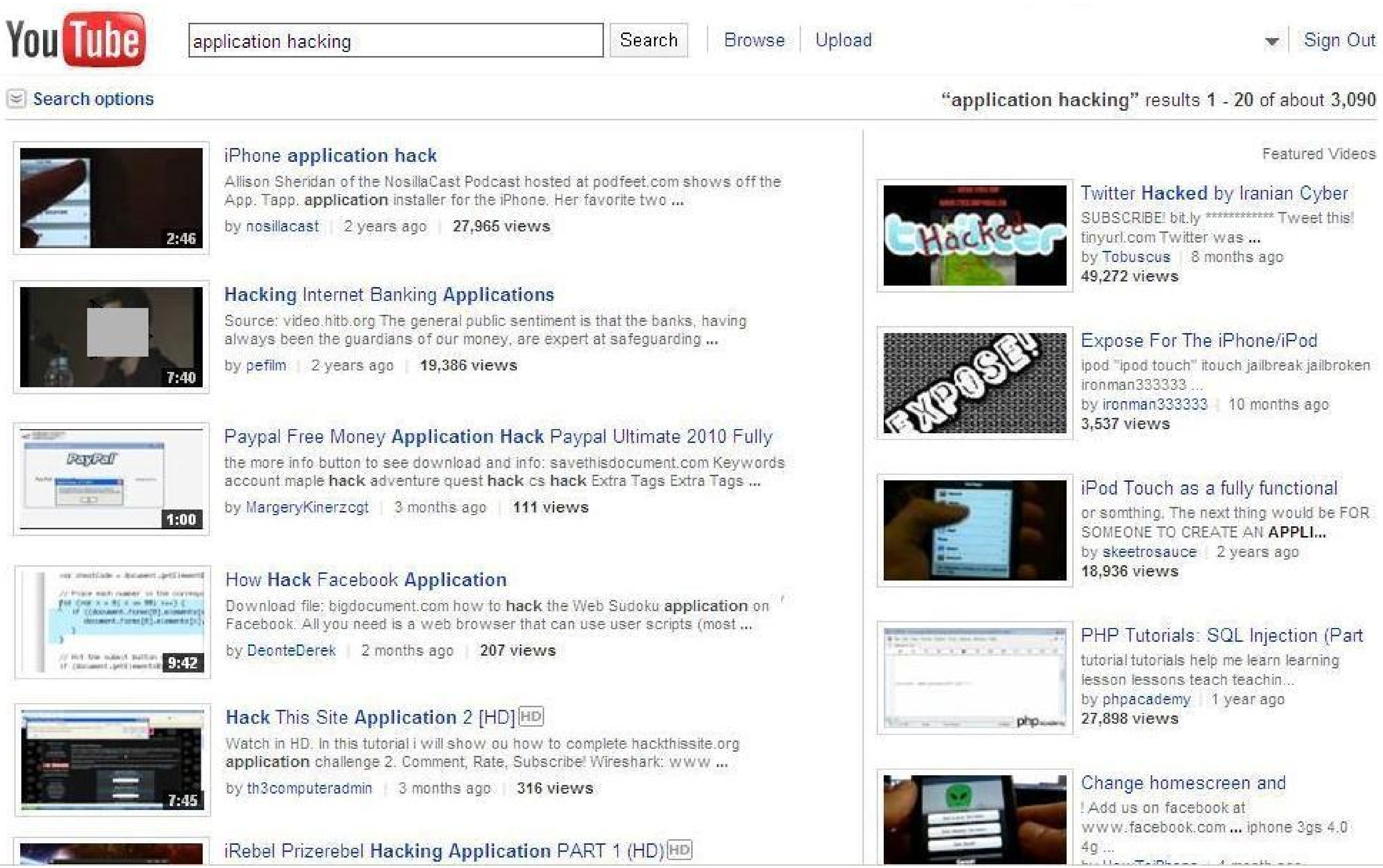
2010
1 Injection
2 Cross-Site Scripting (XSS)
Broken Authentication and Session Management
4 Insecure Direct Object References
5 Cross-Site Request Forgery (CSRF)
6 Security Misconfiguration
7 Insecure Cryptographic Storage
8 Failure to Restrict URL Access
9 Insufficient Transport Layer Protection
10 Unvalidated Redirects and Forwards

## Characteristics of Insecure Code



| | |
|---|---|
| I | Injectable Code |
| N | Non-Repudiation Mechanisms not Present |
| S | Spoofable Code |
| E | Exceptions and Errors not Properly Handled |
| C | Cryptographically Weak Code |
| U | Unsafe/Unused Functions and Routines in Code |
| R | Reversible Code |
| E | Elevated Privileges Required to Run |

# Don’t Try This At Home



“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 ...

# Why Do Hackers Attack Web Applications?

- **Because they know you have firewalls**
- So they need to find a new weak spot to hack through and steal or compromise your data

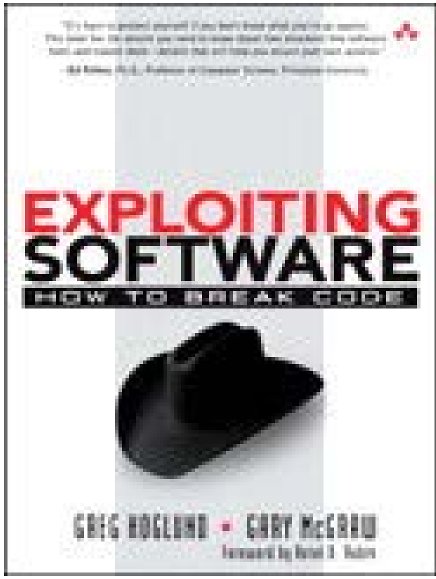
- **Because firewalls do not protect against app attacks!**
  - Very few people are actively aware of application security issues
  - **Most IT security professionals, from network & sys-admin side, have little experience or interest in software development. Programmers have little experience or interest in security or infrastructure.**
    - IT security staff are also often overworked and are focusing on other issues

- Because web sites have a large footprint; cloud makes it even bigger.

- **Because they can!**
  - **Many organizations today still lack a software development security policy!**
    - Many applications especially legacy ones still in use, were not built defensively
    - **Applications today are hundreds of thousands of lines long**
    - **It is a nightmare to QA the application, and requires discipline**
      - **So many people, even if aware, will skip or procrastinate this tedious process**
    - **Additional loss of control when outsourcing development work**

*IP vs HTTP*

*Gartner: ITSec Spend*
*HW/NW 80%*
*App Sec 20%*



# Software Development Security Issues

***No developer goes to work with the intention of writing bad code.***

- Developers are often not trained or experienced in secure coding techniques, and have never needed to worry about this before

*Developers are hired faster than they can be trained properly*

- Developers face pressures of demands for quality and functionality, and are often short on timeline, resources, information, budget, quality assurance tools investment.

- ***Plus heavy demands on outsourcing parties ….***

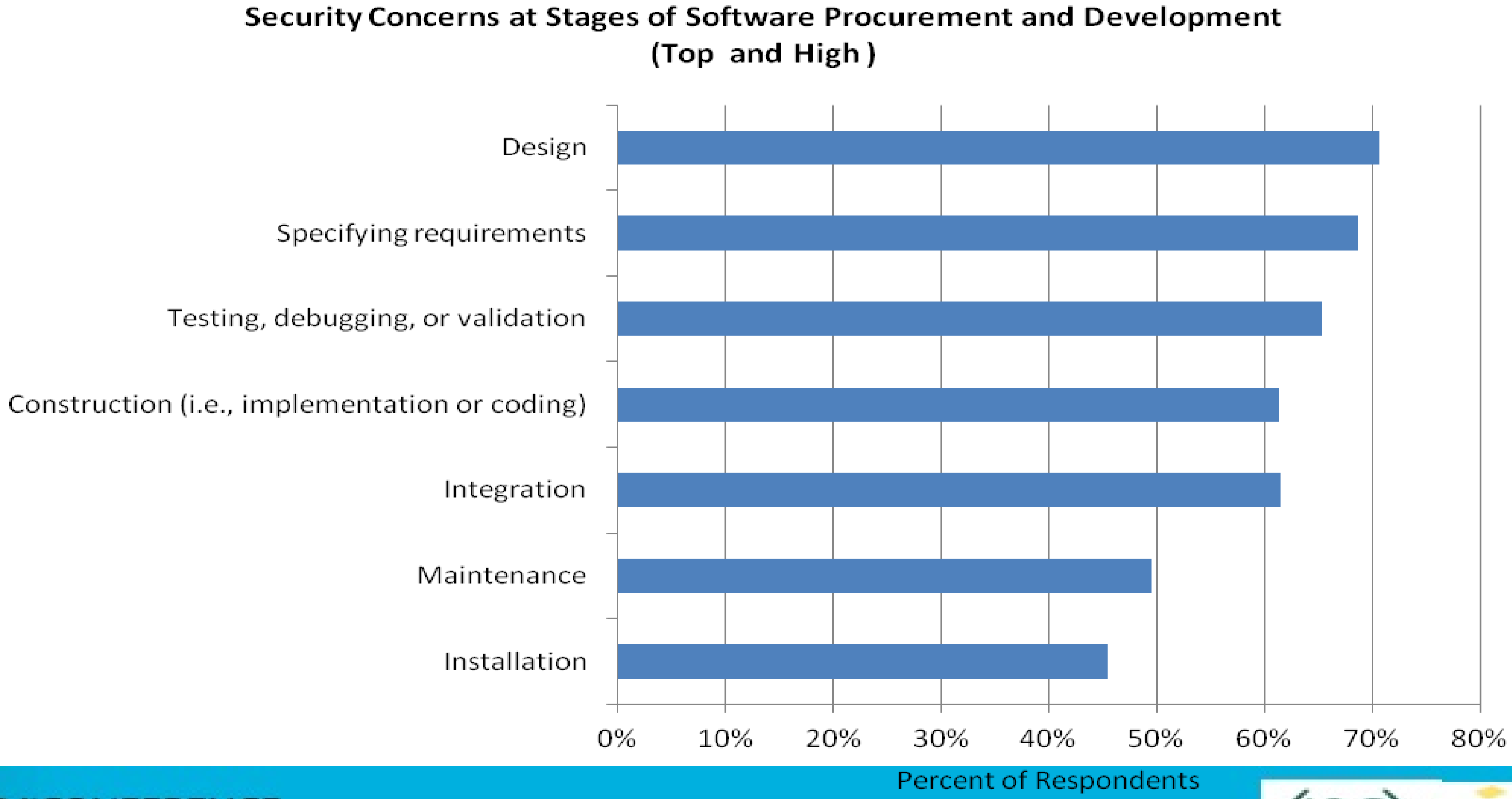
- **Cheap**
- **Fast**
- **Good**

**-> Choose 2**

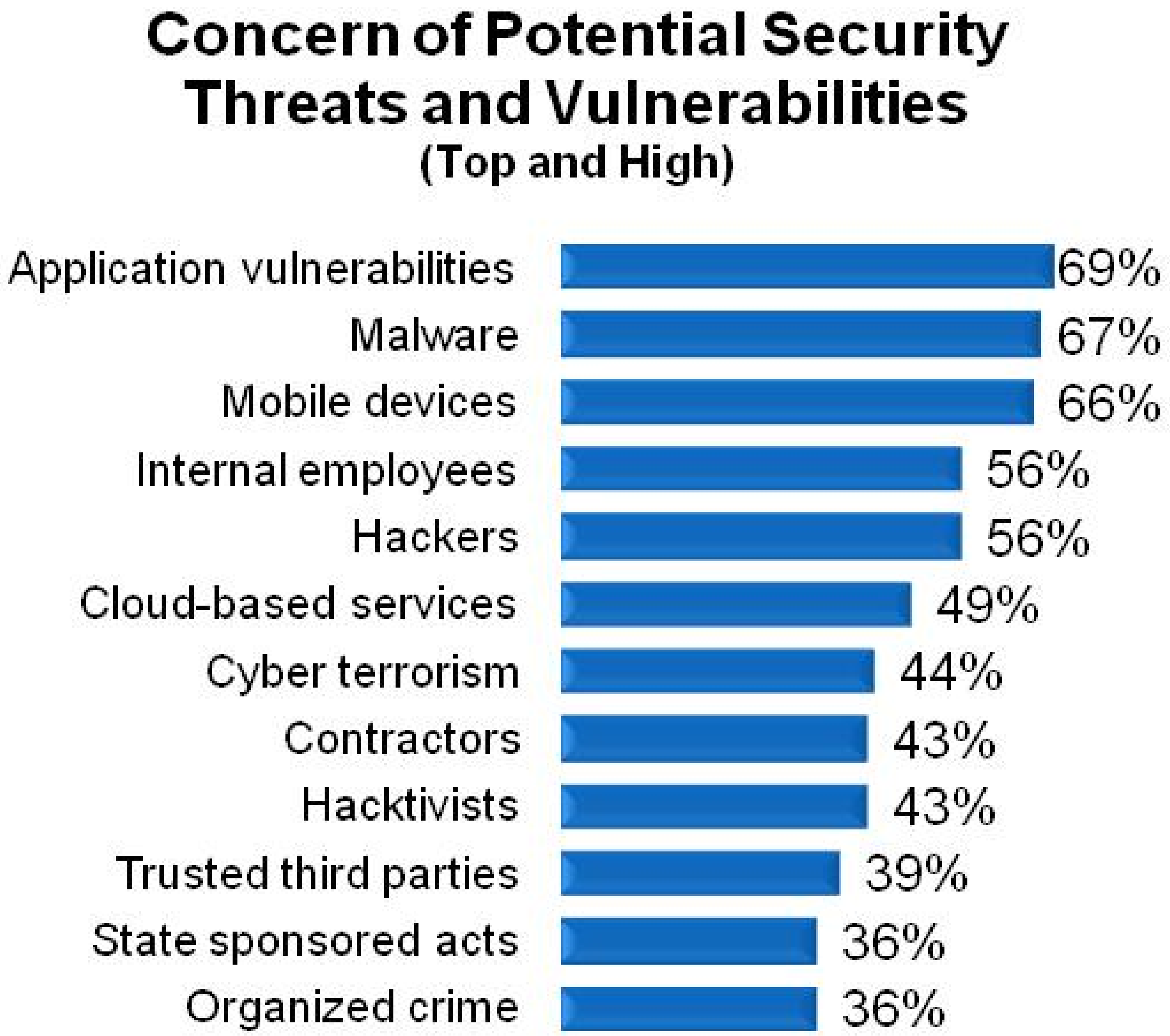
OUR GOAL IS TO WRITE BUG-FREE SOFTWARE. I'LL PAY A TEN-DOLLAR BONUS FOR EVERY BUG YOU FIND AND FIX.
S. Adams E-mail: SCOTTADAMS@AOL.COM
YAHOO!
WE'RE RICH
YES!!! YES!!! YES!!!
© 1995 United Feature Syndicate, Inc.(NYC)
I HOPE THIS DRIVES THE RIGHT BEHAVIOR.
I'M GONNA WRITE ME A NEW SUV THIS AFTER-NOON!

# Secure Software Development: Important but Under-supported

As previously reported, 69% of survey respondents rate application vulnerabilities as a top or high concern and separately respondents voice security concerns along the entire software development lifecycle



# ISC2 Global Workforce Study 2012-3



Concern of Potential Security Threats and Vulnerabilities (Top and High)

*Top Concerns:*

*-App Sec*

*-Malware*

*-Mobile Devices*

# What is needed
# to address application security issues?

Deep security expertise

Continuous assessment

Verified vulnerabilities

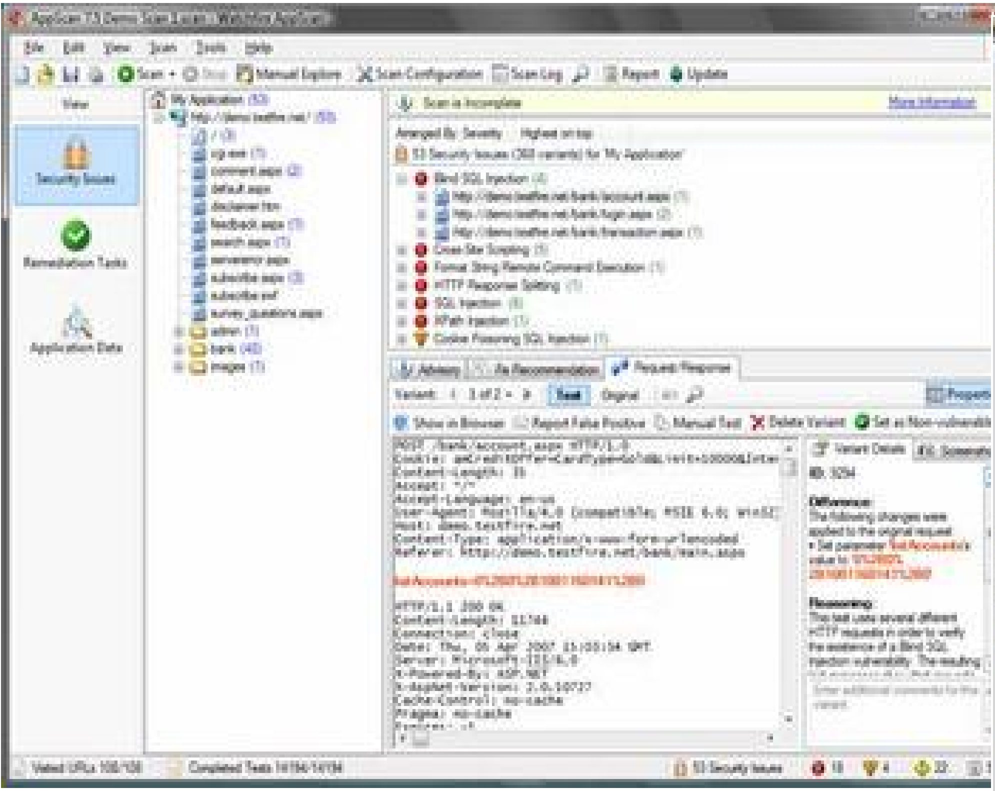
Easy-to-use solutions

# PROFESSIONAL SOFTWARE QA TOOLS

“WHITE BOX” (static code analyzer) and “BLACK BOX” (dynamic application analyzer)

- automate application-development testing, Q.A. and vulnerability management process

- providing comprehensive reports of security issues with remediation guidance.

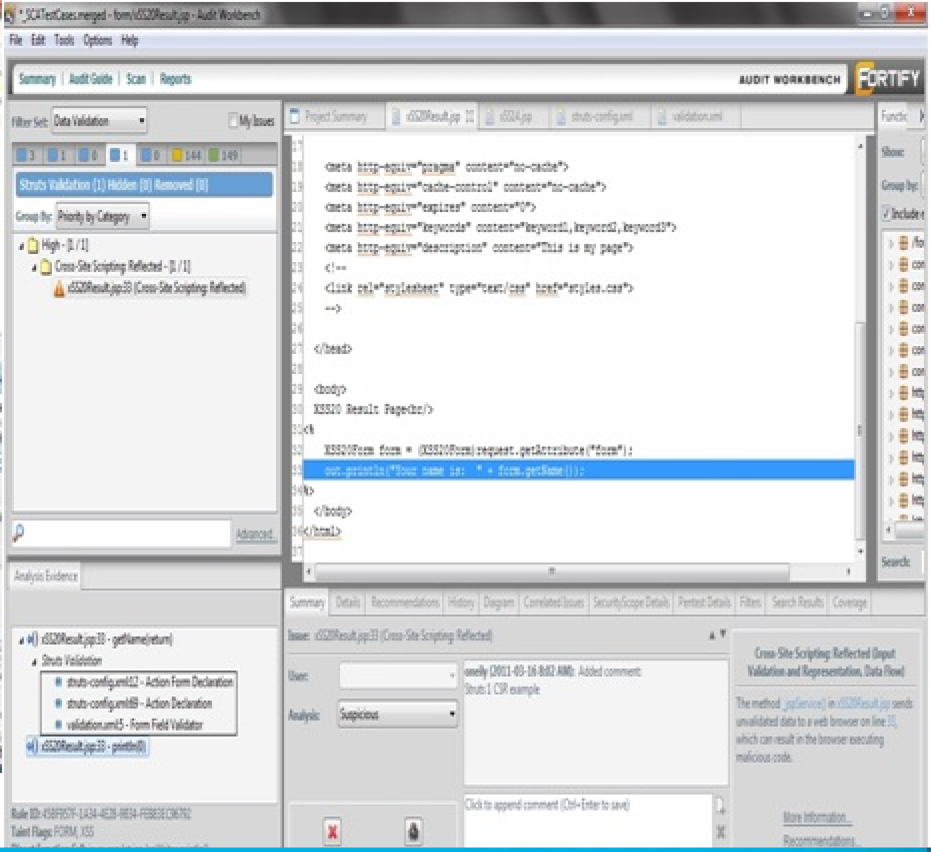

AppScan 7.5 Demo Scan Layout - Watchfire AppScan
File Edit View Scan Tools Help
Scan Stop Manual Explore Scan Configuration Scan Log Report Update
View
Security Issues
Remediation Tasks
Application Data
My Application (53)
http://demo.testfire.net/ (53)
Scan is Incomplete
More Information
Arranged By: Severity Highest on top
53 Security Issues (368 variants) for 'My Application'
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)
Advisory Fix Recommendation Request/Response
Variant: 1 of 2 Test Original
Show in Browser Report False Positive Manual Test Delete Variant Set as Non-vulnerable
Variant Details
Difference:
Reasoning:
Visited URLs: 108/108 Completed Tests: 14194/14194 53 Security Issues

```
POST /bank/account.aspx HTTP/1.0
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Inter
Content-Length: 31
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: demo.testfire.net
Content-Type: application/x-www-form-urlencoded
Referer: http://demo.testfire.net/bank/main.aspx

listAccounts=[illegible]

HTTP/1.1 200 OK
Content-Length: 11744
Connection: close
Date: Thu, 05 Apr 2007 11:03:34 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
Pragma: no-cache
```

The following changes were applied to the original request:

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

**IBM Appscan**


*SCATestCases.merged - form/xss20Result.jsp - Audit Workbench
File Edit Tools Options Help
Summary Audit Guide Scan Reports
AUDIT WORKBENCH FORTIFY
Filter Set: Data Validation
My Issues
Struts Validation (1) Hidden (0) Removed (0)
Group By: Priority by Category
High - [1/1]
Cross-Site Scripting: Reflected - [1/1]
xss20Result.jsp:33 (Cross-Site Scripting: Reflected)
Advanced...
Project Summary xss20Result.jsp xss24.jsp struts-config.xml validation.xml
Summary Details Recommendations History Diagram Correlated Issues SecurityScope Details Pentest Details Filters Search Results Coverage
Analysis Evidence
xss20Result.jsp:33 - getName(return)
Struts Validation
struts-config.xml:12 - Action Form Declaration
struts-config.xml:8 - Action Declaration
validation.xml:5 - Form Field Validator
xss20Result.jsp:33 - println(0)
User:
Analysis: Suspicious
Click to append comment (Ctrl-Enter to save)
More information...
Recommendations...

```
<meta http-equiv="pragma" content="no-cache">
<meta http-equiv="cache-control" content="no-cache">
<meta http-equiv="expires" content="0">
<meta http-equiv="keywords" content="keyword1,keyword2,keyword3">
<meta http-equiv="description" content="This is my page">
<!--
<link rel="stylesheet" type="text/css" href="styles.css">
-->

</head>

<body>
XSS20 Result Page<br/>
<%
  XSS20Form form = (XSS20Form)request.getAttribute("form");
  out.println("Your name is: " + form.getName());
%>
</body>
</html>
```

Issue: xss20Result.jsp:33 (Cross-Site Scripting: Reflected)

Cross-Site Scripting: Reflected (Input Validation and Representation, Data Flow)

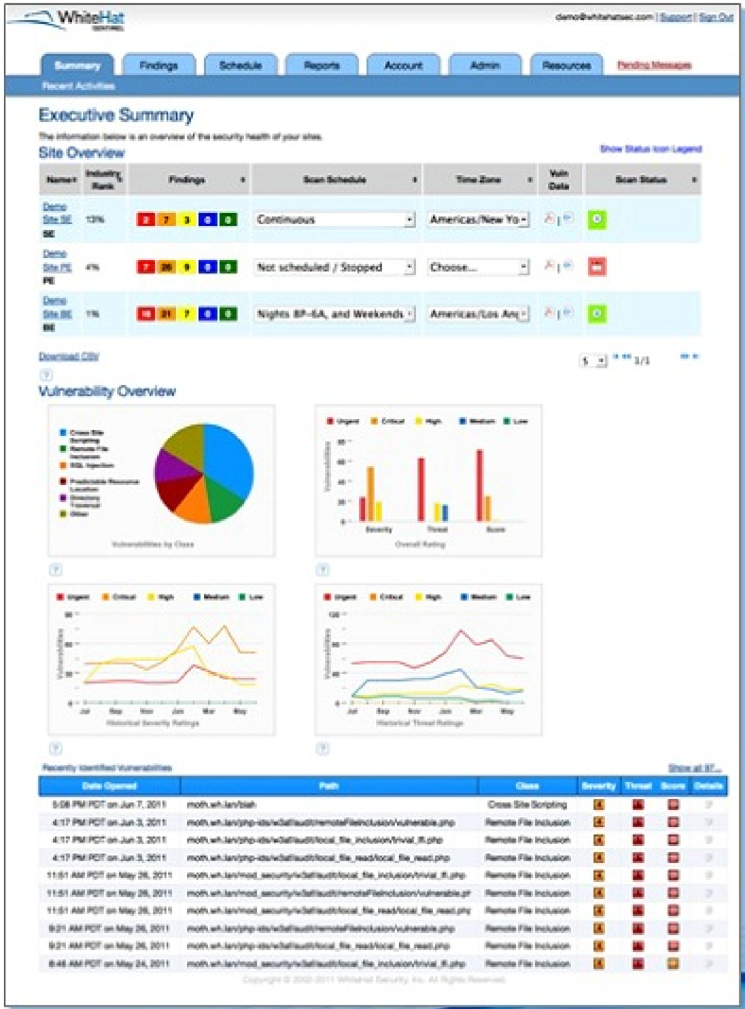
The method _jspService() in xss20Result.jsp sends unvalidated data to a web browser on line 33, which can result in the browser executing malicious code.

**HP Fortify**

EXAMPLE

# WhiteHat Sentinel – Assessment Service

- **SaaS (Annual Subscription)**
  - *Unlimited Assessments / Users*
  - *Fixed Flat Rate per Website*
- **Assessment Methodology**
  - *Proprietary scanning technology*
  - *Direct access to Security Experts*
  - *Continuous Monitoring*
- **100% Vulnerability Verification** – eliminating false positives, prioritizing enterprise risk
- **XML API** leverages other security investments
- **Easy to get started –**
  - *Need URL and Credentials*
  - *No Management of Hardware or Software*
  - *No Additional Training*



Executive Summary

The information below is an overview of the security health of your sites.

Site Overview

Show Status Icon Legend

| Name | Industry Rank | Findings | Scan Schedule | Time Zone | Vuln Data | Scan Status |
|---|---|---|---|---|---|---|
| Demo Site SE<br>SE | 13% | 2 7 3 0 0 | Continuous | Americas/New Yo | | |
| Demo Site PE<br>PE | 4% | 7 26 9 0 0 | Not scheduled / Stopped | Choose... | | |
| Demo Site BE<br>BE | 1% | 10 21 7 0 0 | Nights 8P-6A, and Weekends | Americas/Los An | | |

Download CSV

1/1

Vulnerability Overview

Recently Identified Vulnerabilities

Show all 37...

| Date Opened | Path | Class | Severity | Threat | Score | Details |
|---|---|---|---|---|---|---|
| 5:08 PM PDT on Jun 7, 2011 | moth.wh.lan/blah | Cross Site Scripting | | | | |
| 4:17 PM PDT on Jun 3, 2011 | moth.wh.lan/php-ids/w3afaudit/remoteFileInclusion/vulnerable.php | Remote File Inclusion | | | | |
| 4:17 PM PDT on Jun 3, 2011 | moth.wh.lan/php-ids/w3afaudit/local_file_inclusion/trivial_lfi.php | Remote File Inclusion | | | | |
| 4:17 PM PDT on Jun 3, 2011 | moth.wh.lan/php-ids/w3afaudit/local_file_read/local_file_read.php | Remote File Inclusion | | | | |
| 11:51 AM PDT on May 26, 2011 | moth.wh.lan/mod_security/w3afaudit/local_file_inclusion/trivial_lfi.php | Remote File Inclusion | | | | |
| 11:51 AM PDT on May 26, 2011 | moth.wh.lan/mod_security/w3afaudit/remoteFileInclusion/vulnerable.pl | Remote File Inclusion | | | | |
| 11:51 AM PDT on May 26, 2011 | moth.wh.lan/mod_security/w3afaudit/local_file_read/local_file_read.php | Remote File Inclusion | | | | |
| 9:21 AM PDT on May 26, 2011 | moth.wh.lan/php-ids/w3afaudit/remoteFileInclusion/vulnerable.php | Remote File Inclusion | | | | |
| 9:21 AM PDT on May 26, 2011 | moth.wh.lan/php-ids/w3afaudit/local_file_read/local_file_read.php | Remote File Inclusion | | | | |
| 8:46 AM PDT on May 24, 2011 | moth.wh.lan/mod_security/w3afaudit/local_file_inclusion/trivial_lfi.php | Remote File Inclusion | | | | |

# Web Application Firewalls (WAF)

## *Advantages*

- Convenient; easy to install and run
- Immediately stops 70% of common web attacks

## *Issues to consider*

- Difficult to configure, and need to configure often
  - *The web application is updated and changed often*
- Does not fix the problem; issues still in the software;
  *(staff not learning the issues)*

# Cloud-hosted Virtual Desktops

## – eliminate the endpoint?!

*Eg. An Asian Govt – policy – no data resides on client machine*

*Desktone*
*Example*

***TODAY***

- IT Consumerization (iPad, Macs)
- Windows 7 (8) migrations began
- Mobile employees becomes norm
- Costs out of alignment
- Security/IP concerns

## Cloud Came Along

- ✓ Leverage "as a Service"
- ✓ Lower Cost, no Cap-Ex
- ✓ Centralized Management
- ✓ Turn-key Services
- ✓ Datacenter proximity
- ✓ Elastic, scalable

DaaS = "Desktop as a Service"

Windows 7, 8

**1990** Desktop in PC

**2008** Desktop in Datacenter

**2011** Desktops in cloud

Desktop goes virtual

Virtual Desktop goes Cloud

**1990s: Thick Client PC**

LAN

*Install software from CD*

WAN

… Server Farm …

**2008: Datacenters**

Virtual Desktop

Financial Crash

*Download software from vendor website*

**User PC/ notebook as thin client**

**2011: Cloud Services**

*Download software from cloud service*

**PC/NB, Thin Client, Mobile smart devices, IPADS, remote desk**

# Application Vulnerabilities can start in Development

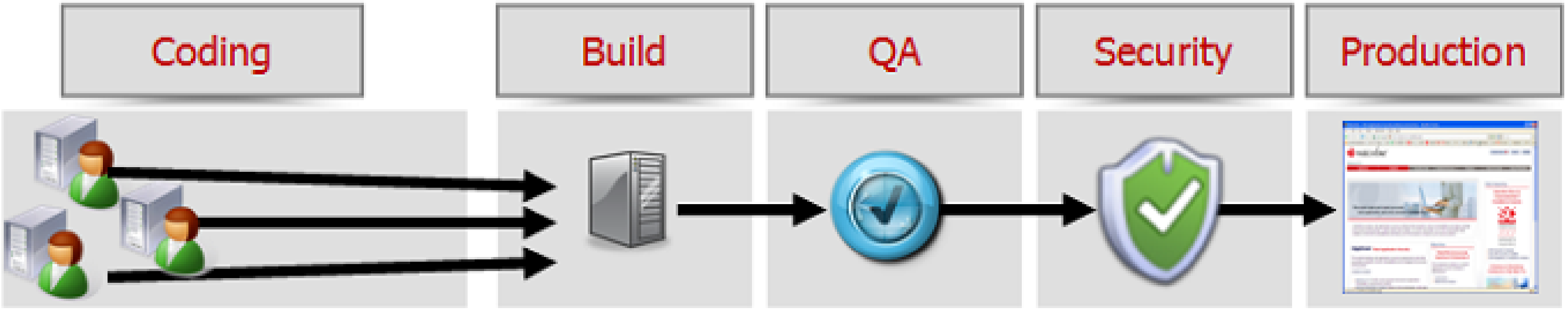
## Developers Lack Security Insights

*(or Incentives to Address Security)*

- Mandate to deliver functionality on-time and on-budget – but not to develop secure applications
- Developers rarely educated in secure code practices
- Product innovation drives development of increasingly complicated applications

## Security Team = SDLC Bottleneck

- Security tests executed just before launch
  - Adds time and cost to fix vulnerabilities late in the process
- Growing number of web applications but small security staff
  - Most enterprises scan ~10% of all web apps
- Continuous monitoring of production apps limited or non-existent
  - Unidentified vulnerabilities & risk



Coding

Build

QA

Security

Production

***Challenge to share test results and enable self-testing in the SDLC***

EMPOWERING THE HUMAN RESOURCE ELEMENT

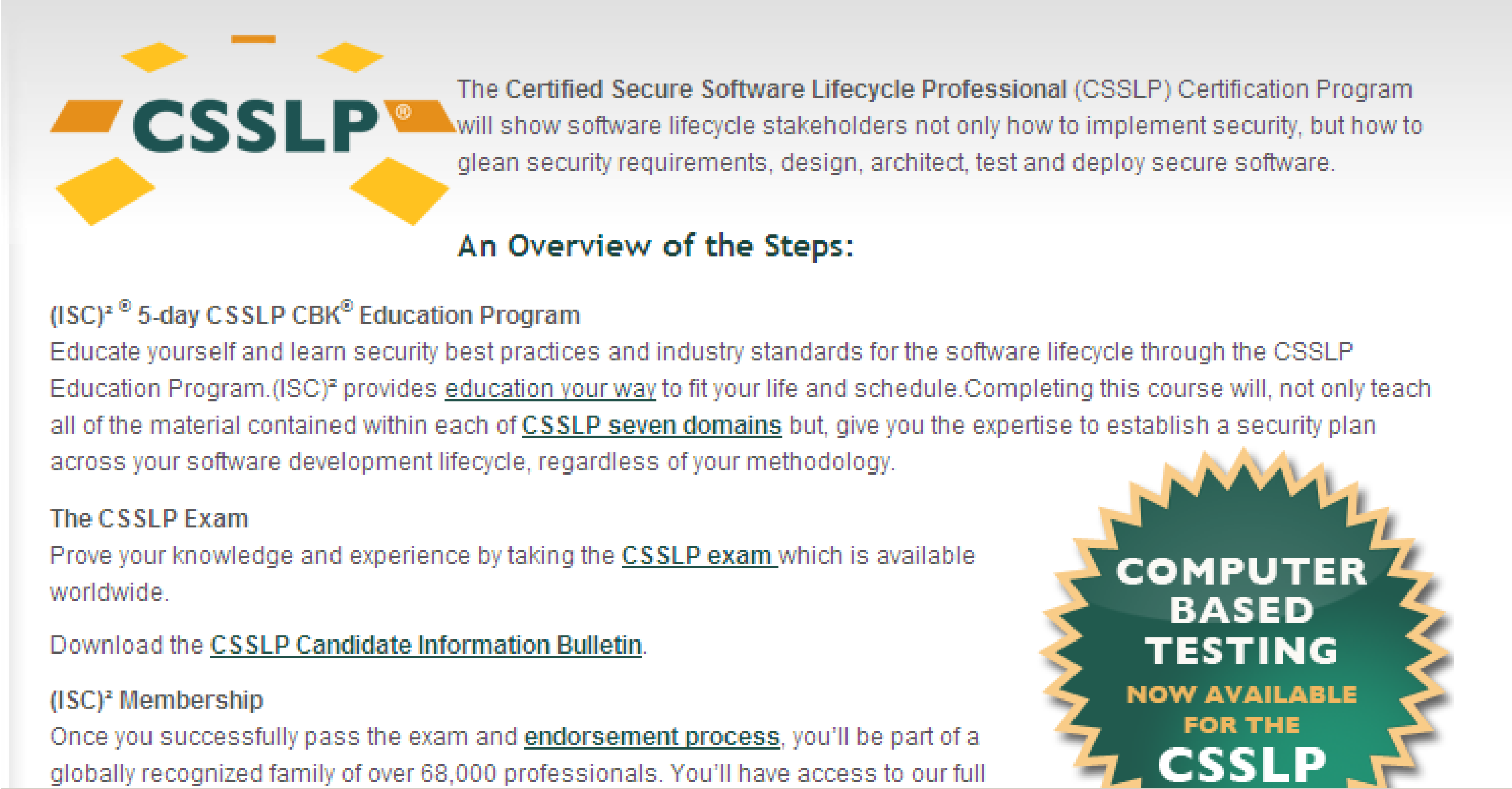
# Continuing Education and Certification

## Security CERTIFICATION for Application Development & Security Teams

**www.isc2.org**

**CISSP**

*'COS DEVELOPERS NEVER HAD TO WORRY ABOUT THIS BEFORE … UNTIL NOW*



The Certified Secure Software Lifecycle Professional (CSSLP) Certification Program will show software lifecycle stakeholders not only how to implement security, but how to glean security requirements, design, architect, test and deploy secure software.

### An Overview of the Steps:

(ISC)² ® 5-day CSSLP CBK® Education Program
Educate yourself and learn security best practices and industry standards for the software lifecycle through the CSSLP Education Program.(ISC)² provides education your way to fit your life and schedule.Completing this course will, not only teach all of the material contained within each of CSSLP seven domains but, give you the expertise to establish a security plan across your software development lifecycle, regardless of your methodology.

The CSSLP Exam
Prove your knowledge and experience by taking the CSSLP exam which is available worldwide.

Download the CSSLP Candidate Information Bulletin.

(ISC)² Membership
Once you successfully pass the exam and endorsement process, you'll be part of a globally recognized family of over 68,000 professionals. You'll have access to our full

# ISC2 Certified Secure Software Lifecycle Professional (CSSLP®) Domains

CSSLP
Certified Secure Software Lifecycle Professional

- Secure Software Concepts
- Secure Software Requirements
- Secure Software Design
- Secure Software Implementation/Coding
- Secure Software Testing
- Software Acceptance
- Software Deployment, Operations, Maintenance, and Disposal
- SUPPLY CHAIN & Software Acquisition

(ISC)²®

## Security in the Skies

*Cloud computing security concerns, threats, and controls*

Mano Paul, CSSLP, CISSP, AMBCI, MCAD, MCSD, Network+, ECSA

**Introduction**

The Internet, often represented as a cloud in architectural diagrams, has changed the way of life for both the individual and businesses. This whitepaper highlights the security concerns that are evident in cloud computing, with particular focus on information assurance, and provides strategies to adopt when evaluating cloud service providers and when designing, developing, and deploying applications that will operate in the cloud. It also gives guidance on what some of the next steps need to be for secure cloud computing.

**What is Cloud Computing?**

Cloud computing is one of the most highly discussed topics within the typical organization, according to the 2011 (ISC)² Global Information Security Workforce Study (GISWS) conducted by Frost and Sullivan. But what is cloud computing? Is it a silver lining in computing, or is it a harbinger of an impending perfect storm? Because the cloud computing paradigm is still evolving, a common

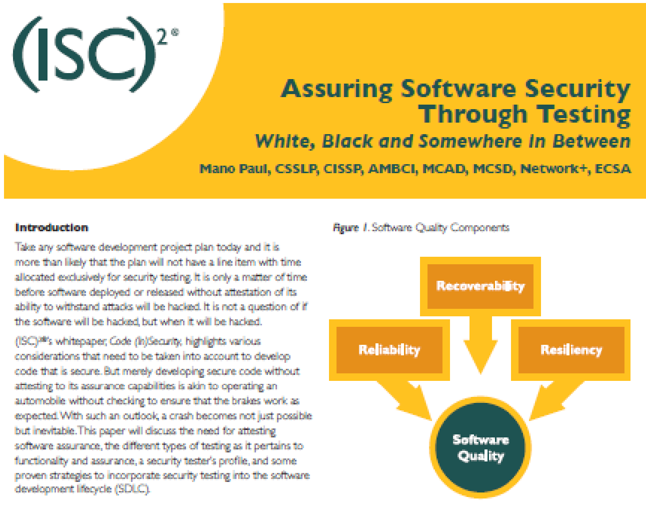
Institute of Standards and Technology (NIST) developed:
*Cloud Computing – A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*

**Architecture and Service Models**

The cloud computing architecture is primarily a multi-tenant, service based architecture. It has a distinct consumer front-end and the

*"The three primary service models in cloud computing are IaaS, PaaS and SaaS"*

provider cloud back-end which provides services to the multiple



(ISC)²®

## Assuring Software Security Through Testing

***White, Black and Somewhere In Between***

Mano Paul, CSSLP, CISSP, AMBCI, MCAD, MCSD, Network+, ECSA

**Introduction**

Take any software development project plan today and it is more than likely that the plan will not have a line item with time allocated exclusively for security testing. It is only a matter of time before software deployed or released without attestation of its ability to withstand attacks will be hacked. It is not a question of if the software will be hacked, but when it will be hacked.

(ISC)²®'s whitepaper, *Code (In)Security*, highlights various considerations that need to be taken into account to develop code that is secure. But merely developing secure code without attesting to its assurance capabilities is akin to operating an automobile without checking to ensure that the brakes work as expected. With such an outlook, a crash becomes not just possible but inevitable. This paper will discuss the need for attesting software assurance, the different types of testing as it pertains to functionality and assurance, a security tester's profile, and some proven strategies to incorporate security testing into the software development lifecycle (SDLC).

*Figure 1.* Software Quality Components

# CSSLP New Domain - Supply Chain and Software Acquisition

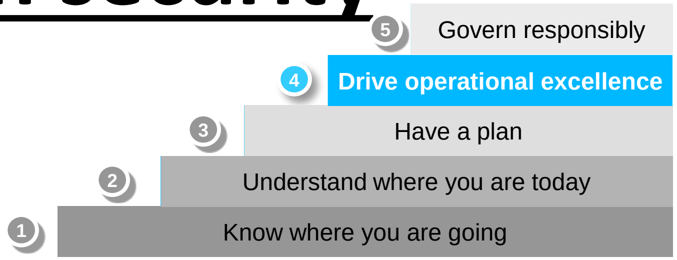
- Supplier Risk Assessment
- Supplier Sourcing
- Software Developement Test
- Software Delivery, Operations & Maintenance
- Supplier Transitioning

## ***Conclusion***

So, why do we still have Information Security issues today?

# Unplanned Proliferation of Data

# Things you can do to maintain security


5 Govern responsibly

4 **Drive operational excellence**

3 Have a plan

2 Understand where you are today

1 Know where you are going

- Measure the cost of being secure
  - As you scale out your security program, measure the cost per defect for fixing
- Educate your development teams
  - Developers do not need to be security experts or auditors
  - Developers do need to understand the implications of vulnerabilities
- Reduce the cost of being secure through early detection and remediation (better still, build in security from the start)
  - Develop a template of security requirements – don't reinvent the wheel each time!
  - Engage the architects to design for security, and the testers to build security into their test plans
- Build security into your procurement process
  - Your security requirements need to be part of specifications to third parties for development or delivery of software
- Update your sponsor – demonstrate value!

# (ISC)$^2$ Survey & Global Information Security Workforce Study -Stats

- **59% not following a rigorous Security process**
- 26% have no hint of Security within their development lifecycle
- **48% claim to audit procedures regularly**
- 69% Blame Culture as reason for current practices
- 57% blame lack of Education
- 70% claim to have insufficient guidance for key technology models

*59% of staff will try to bypass a security process*

A ☑
U ☑
D ☑
I ☑
T ☑

***The worst reason to have security is Governance & Regulation***

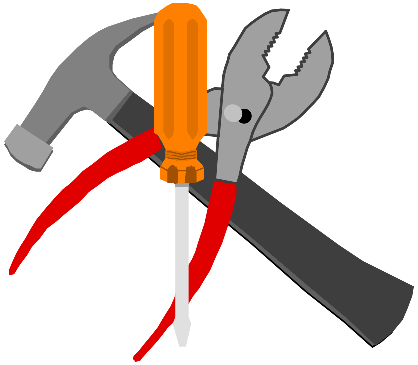
-***You must know why you want security, not because someone said so***

*- we end up trying all sorts of ways to get by or get past the feared (or hated) auditor …*

# Conclusion:  2 Components to I.T. Security

## Technical Component

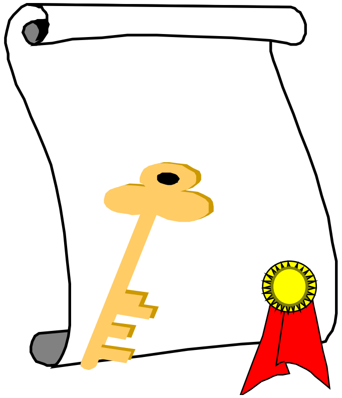
- Access Control
- Authenticated Access
- Encryption & Privacy
- Policy-based traffic filtering
- Enterprise Management etc



I.T. SECURITY TODAY IS NO LONGER A TECHNOLOGY THING – IT IS A HUMAN AND SOCIAL MATTER!

## Human & Policy Component

- Education
- Enforcement
- Reinforcement
- Diligence & Vigilance
- CLEAR OWNERSHIP



AS LONG AS HUMANS BEHAVE LIKE HUMANS WE WILL STILL HAVE A JOB IN I.T. SECURITY!

**Technologies today can provide the technical component.**

**Only commitment at the highest levels can the human factor be successful.**

# Cloud and Web Application Security : Conclusion – Security by Application Development Q.A

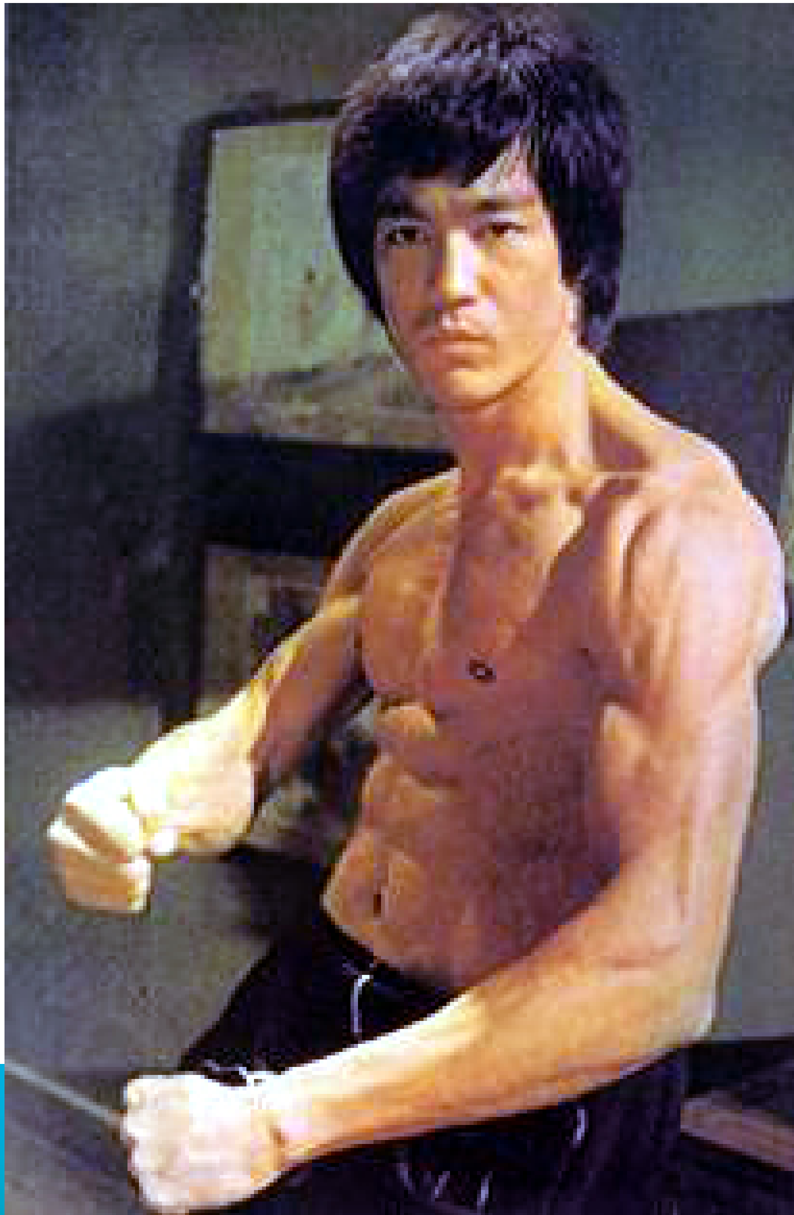
- **The Application Must Defend Itself**

  **(ie. Write the programs properly)**

  – Network security solutions do not stop application attacks

  – Existing network security solutions do not automatically work well in cloud environments

- **THIS IS THE BEST AND ONLY WAY TO MINIMISE SOFTWARE ATTACKS**
- Both security and development teams need to be in harmony
- **DEVELOPERS NEED TO BE TRAINED APPROPRIATELY IN SECURE CODING**
- **MANAGEMENT MUST ACTIVELY SUPPORT AND FINANCE A SOFTWARE SECURITY POLICY AND TEAM**



- *Cloud Security – Are You Forgetting Something?*

# THANK YOU

**Anthony Lim**

*MBA CISSP CSSLP FCITIL*

**Application Security**
**Advisory Board**
**ISC2.org**
**Singapore**

(ISC)$^2$™
International Standard
for Information Security

CSSLP®
Certified Secure Software Lifecycle Professional

# ▶ APPENDIX

# What Is Software Security?

- Security is a distinct property of a software system or application. It is composed of Confidentiality, Integrity, Availability, Authenticity, and other related attributes*.

- Software Security vs. Secure Software
  - Secure software can be delivered by rigorously applying all the techniques of a software security plan
- Software Security vs. Secure Coding
  - Secure coding is one aspect of an overall software security plan
- Software Security vs. Software Quality
  - High quality software can also be insecure
  - Security requires specialized skills

*Definition derived from description provided in Software Assurance BoK from DHS.

# Secure Coding Itself is Not Enough

- Common misconception that writing secure code is the only answer
- Many eyeballs won't solve the security problem. (e.g. recent DNS bug took 10 years to discover)

- Software security requires:
  1) Policy -- pertinent and enforceable
  2) Process -- formal and structured
  3) People -- trained and qualified (first line of defense and organization's most critical asset)

# Secure Software Concepts

- Confidentiality, Integrity, Availability Authentication, Authorization, and Auditing
- Security Design Principles
- Risk Management (e.g., vulnerabilities, threats and controls)
- Regulations, Privacy, and Compliance
- Software Architecture (e.g., layers)
- Software Development Methodologies
- Legal (e.g., Copyright, IP and trademark)
- Standards (e.g., ISO 2700x, OWASP, PCI-DSS, NIST)
- Security Models (e.g., Bell-LaPadula, Clark-Wilson & Brewer-Nash)
- Trusted Computing (e.g., TPM, TCB)
- Acquisition (e.g., contracts, SLAs and specifications)

# Software Security - Getting Started

- Training and Awareness
  - Start with basic concepts
  - Train developers and testers first

- Appoint or hire a Security Lead
  - Becomes local authority on software security
  - Coordinates security activities and drive SDL
  - Establishes risk management process