Application Security Best Practices

Anthony Lim *MBA FCITIL CISSP CSSLP*

Director, Asia Pacific, Security

Rational Software

CSSLP

Certified Secure Software Lifecycle Professional

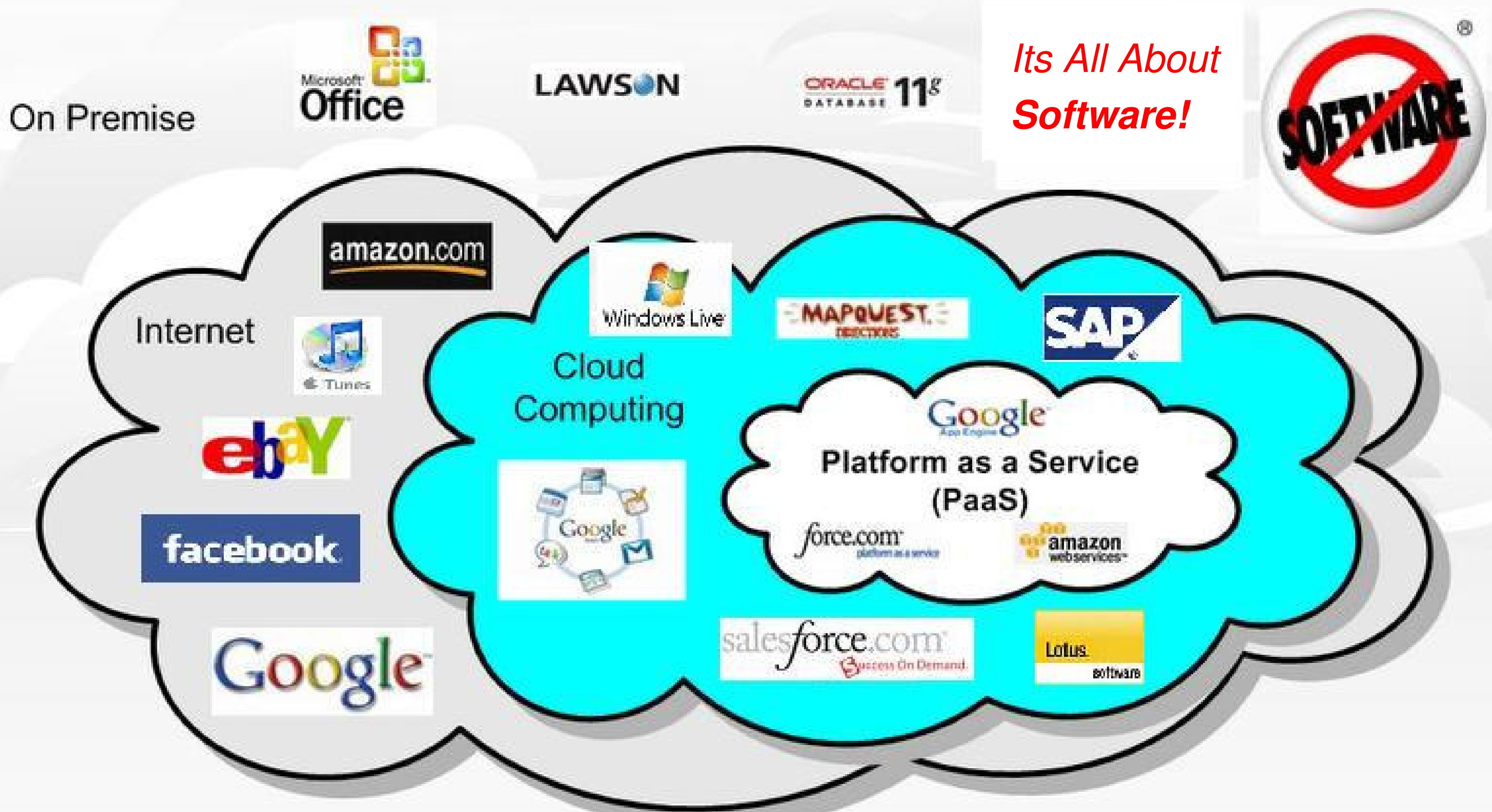
Let's build a smarter planet.

Hong Kong

20 Jan 2011

The Wonders of Cloud Computing

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



On Premise

Its All About

Software!

Internet

Cloud Computing

Platform as a Service (PaaS)

PC Laptop / Netbook Thin Client Mobile Device

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

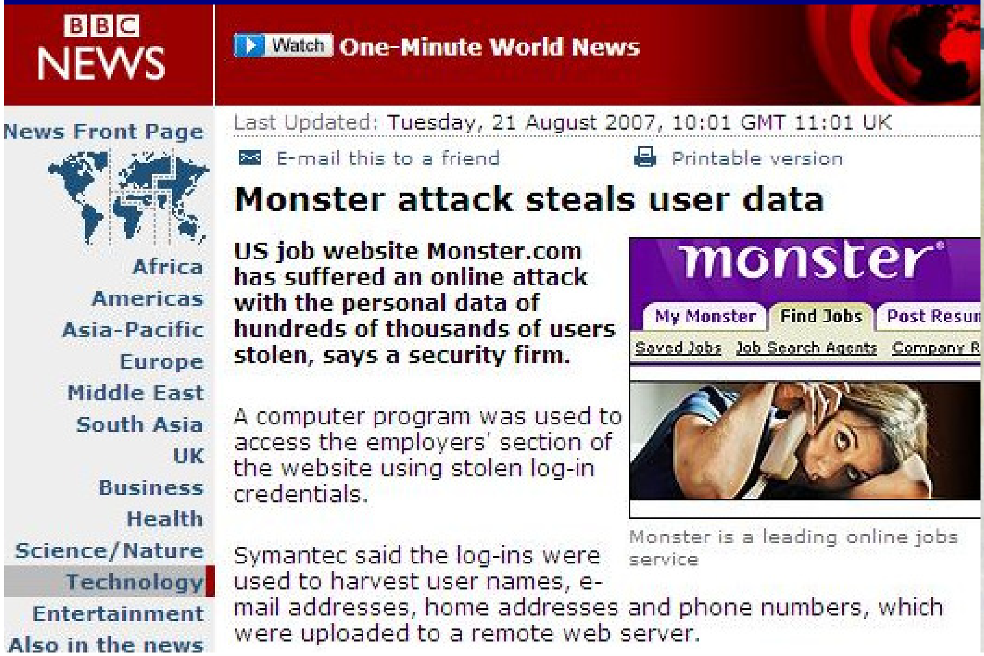
We Use Network Vulnerability Scanners

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
Also in the news

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

E-mail this to a friend   Printable version

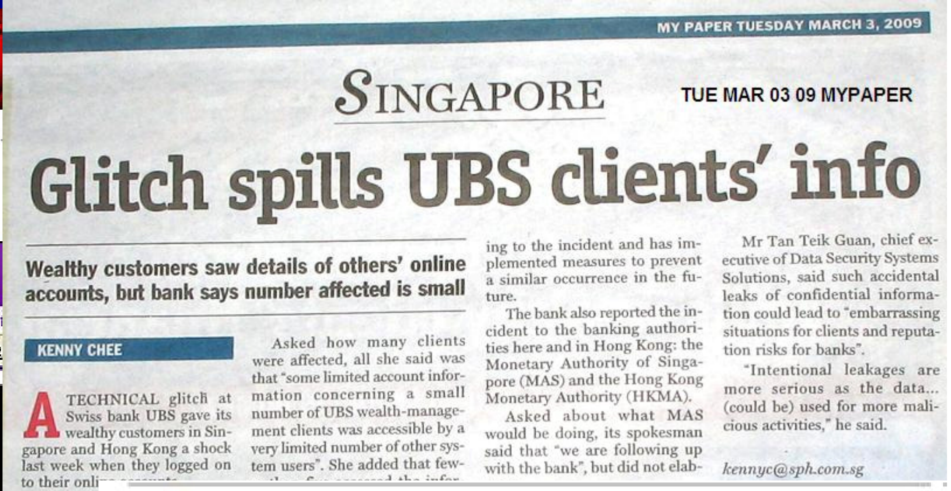
Monster attack steals user data

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

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

Monster is a leading online jobs service

Symantec said the log-ins were used to harvest user names, e-mail addresses, home addresses and phone numbers, which were uploaded to a remote web server.



MY PAPER TUESDAY MARCH 3, 2009

SINGAPORE   TUE MAR 03 09 MYPAPER

Glitch spills UBS clients' info

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

KENNY CHEE

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

The priv found confi er clients' b account inf their own. counts, thou their names.

When c spokesman dent and sai

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 few-

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

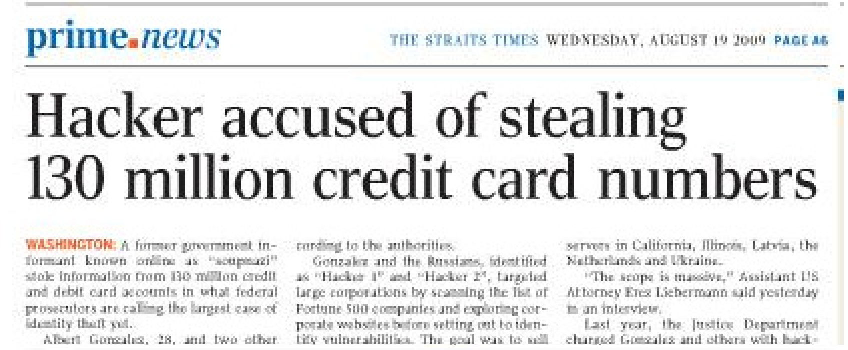
The bank also reported the incident to the banking authorities here and in Hong Kong: the Monetary Authority of Singapore (MAS) and the Hong Kong Monetary Authority (HKMA).

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



prime.news   THE STRAITS TIMES WEDNESDAY, AUGUST 19 2009 PAGE A6

Hacker accused of stealing 130 million credit card numbers

WASHINGTON: A former government informant known online as "soupnazi" stole information from 130 million credit and debit card accounts in what federal prosecutors are calling the largest case of identity theft yet.

Albert Gonzalez, 28, and two other

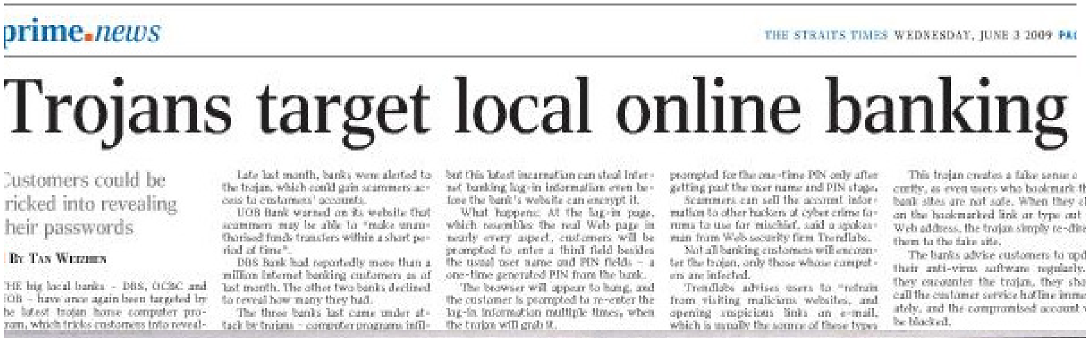
cording to the authorities.

Gonzalez and the Russians, identified as "Hacker 1" and "Hacker 2", targeted large corporations by scanning the list of Fortune 500 companies and exploring corporate websites before setting out to identify vulnerabilities. The goal was to sell

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 hack-



prime.news   THE STRAITS TIMES WEDNESDAY, JUNE 3 2009 PA

Trojans target local online banking

ustomers could be ricked into revealing heir passwords

By Tan Weizhen

HE big local banks – DBS, OCBC and OB – have once again been targeted by he latest trojan horse computer pro- ram, which tricks customers into reveal-

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

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

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

The three banks last came under attack by trojans – computer programs infil-

But this latest incarnation can steal Internet banking log-in information even before the bank's website can encrypt it.

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

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

prompted for the one-time PIN only after getting past the user name and PIN stage.

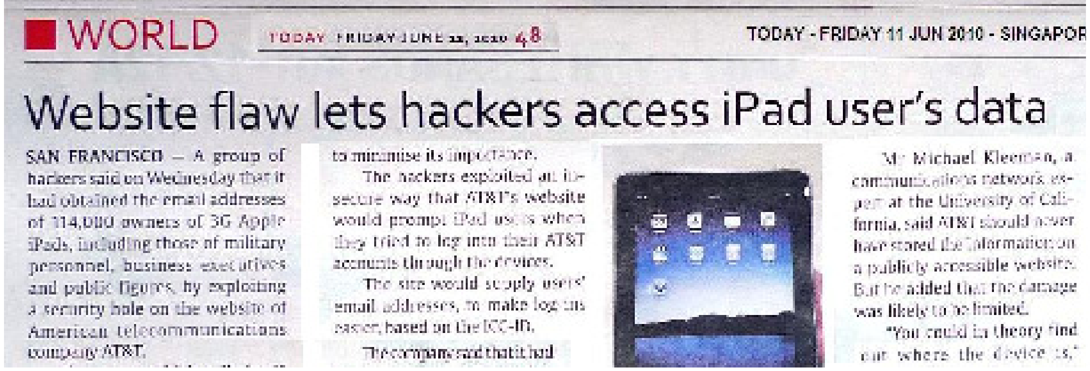
Scammers can sell the account information to other hackers or cyber crime forums to use for mischief, said a spokesman from Web security firm Trendlabs.

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

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

This trojan creates a false sense o curity, as even users who bookmark th bank sites are not safe. When they cl on the bookmarked link or type out Web address, the trojan simply re-dire them to the fake site.

The banks advise customers to upd their anti-virus software regularly. they encounter the trojan, they sho call the customer service hotline imme ately, and the compromised account be blocked.



WORLD   TODAY FRIDAY JUNE 11, 2010 48

TODAY - FRIDAY 11 JUN 2010 - SINGAPOR

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.

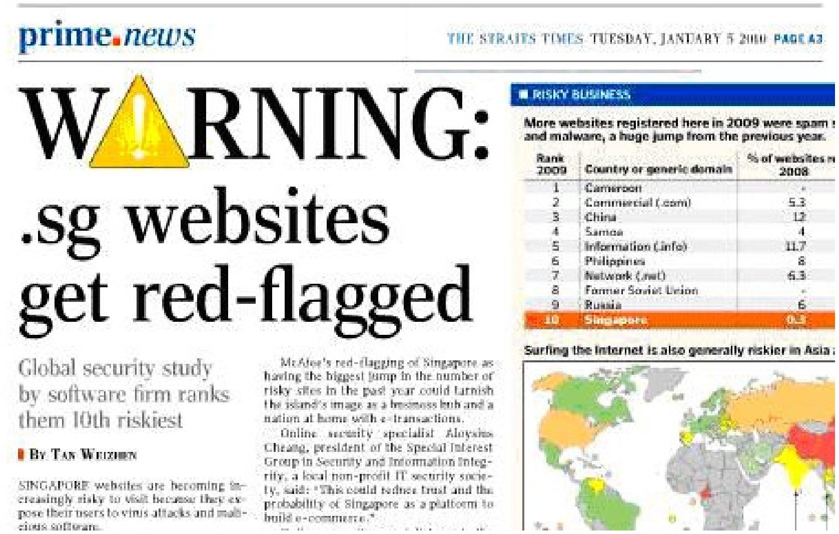
The hackers exploited an insecure way that AT&T's website would prompt iPad users when they tried to log into their AT&T accounts through the devices.

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 networks 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,"



prime.news   THE STRAITS TIMES TUESDAY, JANUARY 5 2010 PAGE A3

W⚠RNING: .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.

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.

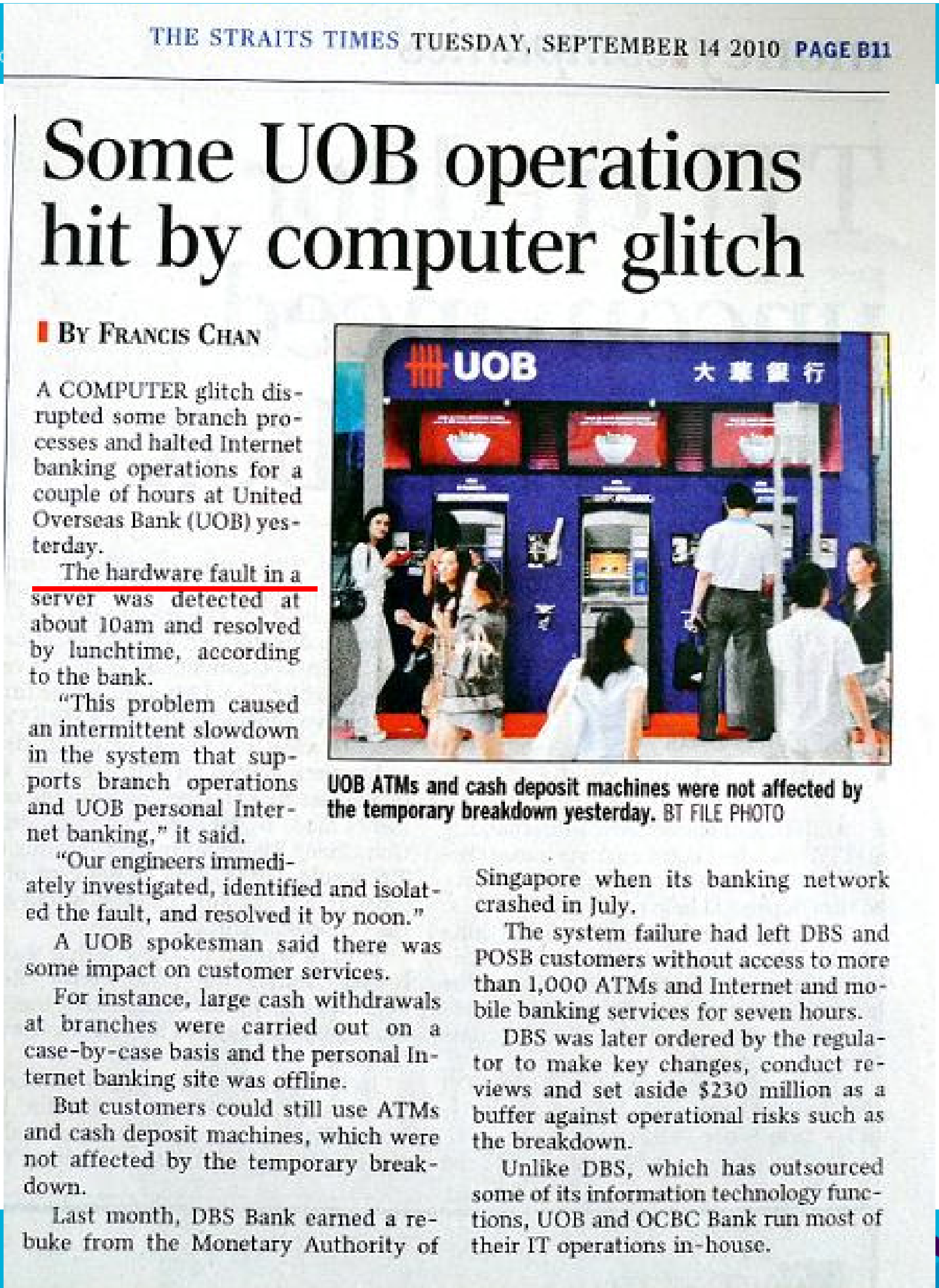
Online security specialist Aloysius Cheang, president of the Special Interest Group in Security and Information Integrity, a local non-profit IT security society, said: "This could reduce trust and the probability of Singapore as a platform to build e-commerce."

RISKY BUSINESS

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

Rank 2009	Country or generic domain	% of websites r 2008
1	Cameroon	-
2	Commercial (.com)	5.3
3	China	12
4	Samoa	4
5	Information (.info)	11.7
6	Philippines	8
7	Network (.net)	6.3
8	Former Soviet Union	-
9	Russia	6
10	Singapore	0.3

Surfing the Internet is also generally riskier in Asia



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 supports branch operations and UOB personal Internet banking," it said.

"Our engineers immediately investigated, identified and isolated the fault, and resolved it by noon."

A UOB spokesman said there was some impact on customer services.

For instance, large cash withdrawals at branches were carried out on a case-by-case basis and the personal Internet banking site was offline.

But customers could still use ATMs and cash deposit machines, which were not affected by the temporary breakdown.

Last month, DBS Bank earned a rebuke from the Monetary Authority of Singapore when its banking network crashed in July.

The system failure had left DBS and POSB customers without access to more than 1,000 ATMs and Internet and mobile banking services for seven hours.

DBS was later ordered by the regulator to make key changes, conduct reviews and set aside $230 million as a buffer against operational risks such as the breakdown.

Unlike DBS, which has outsourced some of its information technology functions, UOB and OCBC Bank run most of their IT operations in-house.

UOB ATMs and cash deposit machines were not affected by the temporary breakdown yesterday. BT FILE PHOTO

Its always the hardware?!

Maybe the network?!

Never the software?!

Cloud Computing Security – The Soft Spot - Application Security Issues

Applications can be CRASHED to reveal source, logic, script or infrastructure information that can give a hacker intelligence

Applications can be COMPROMISED to make it provide unauthorised entry access or unauthorised access to read, copy or manipulate data stores, or reveal information that it otherwise would not.

- Eg. Parameter tampering, cookie poisoning

Applications can be HIJACKED to make it perform its tasks but for an authorised user, or send data to an unauthorised recipient, etc.

- Eg. ***Cross-site Scripting, SQL Injection***

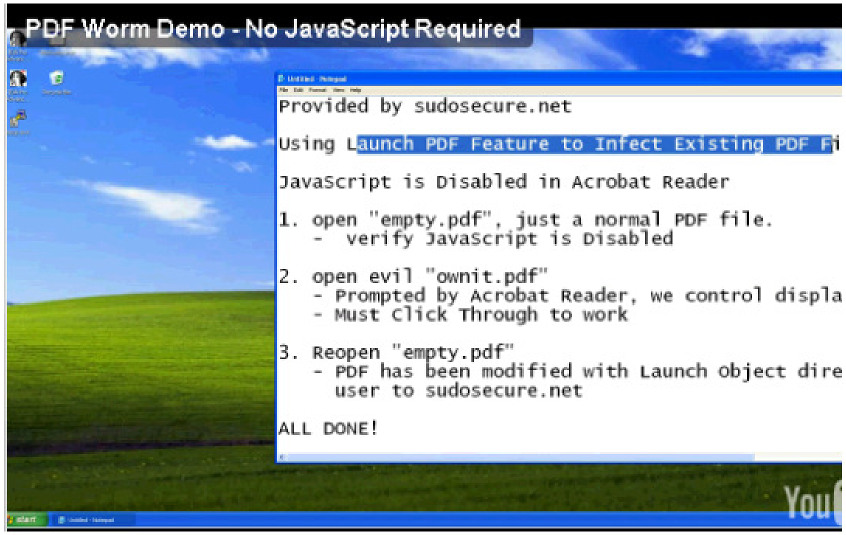
April 5, 2010 3:32 PM PDT

Exploits not needed to attack via PDF files

by Elinor Mills

9 con

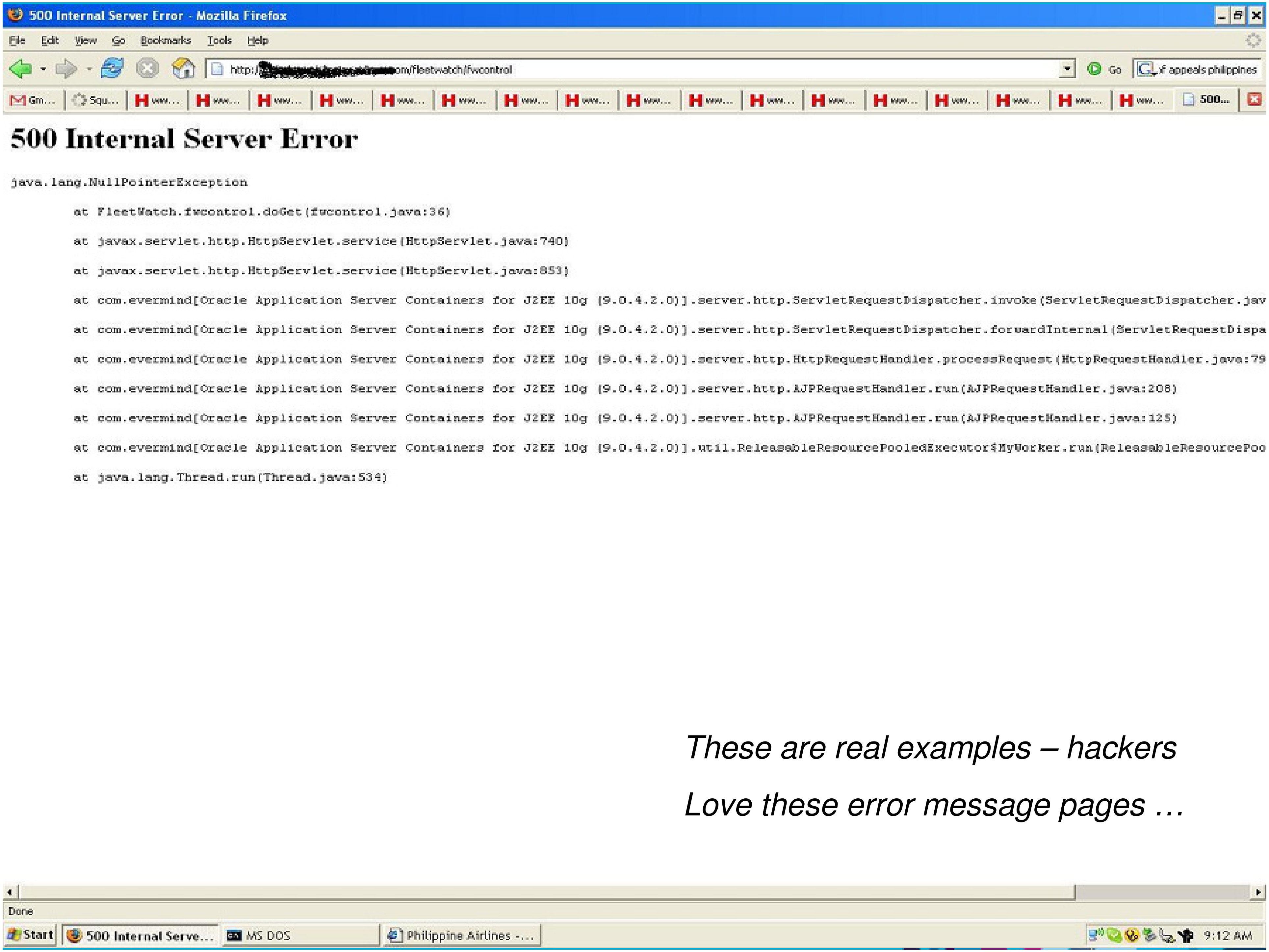
77 retweet Share 23



PDF Worm Demo - No JavaScript Required

```
Provided by sudosecure.net

Using Launch PDF Feature to Infect Existing PDF Fi

JavaScript is Disabled in Acrobat Reader

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

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

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

ALL DONE!
```

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

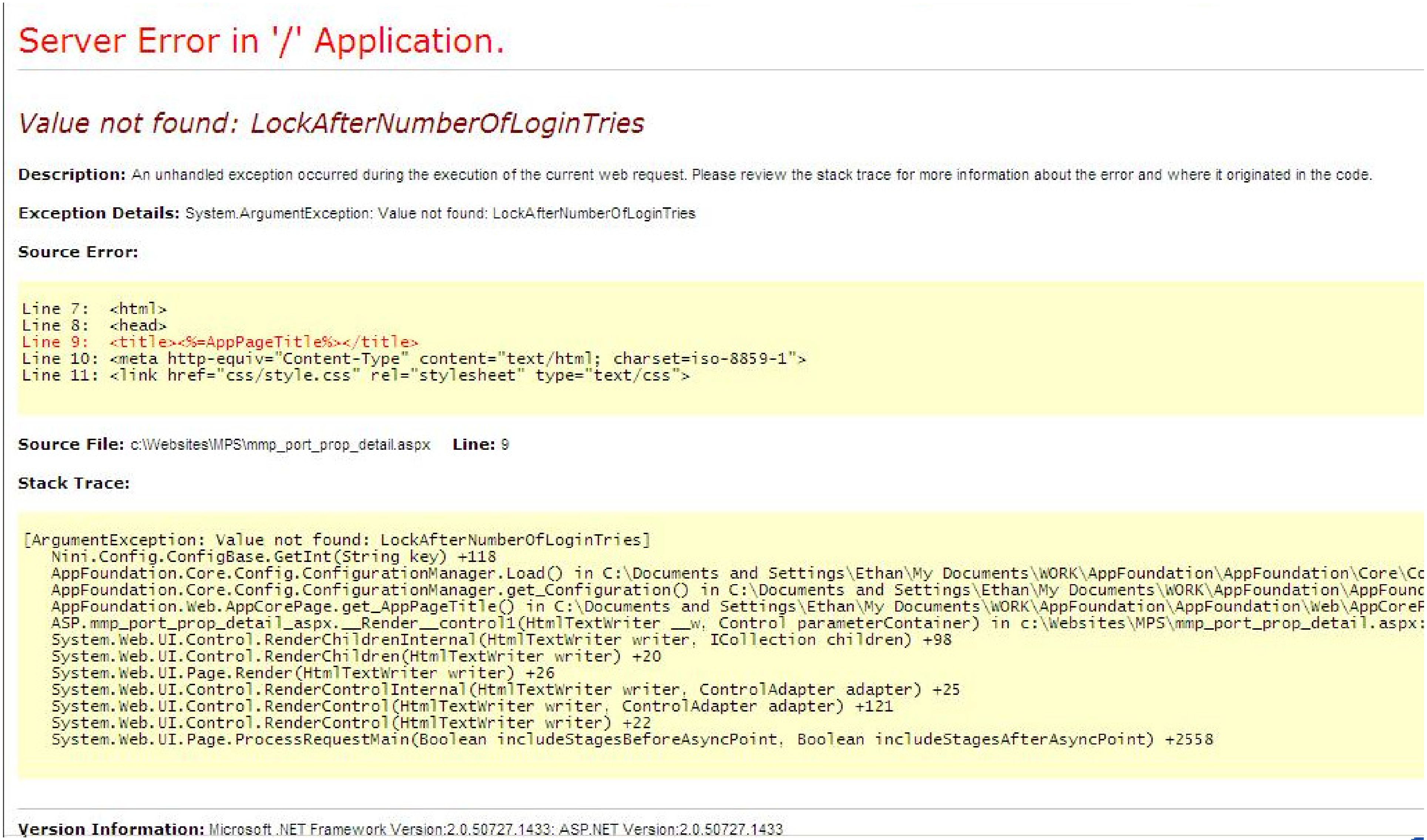

500 Internal Server Error - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://[redacted]om/fleetwatch/fwcontrol
Go
if appeals philippines
Gm... Squ... ww... ww... ww... ww... ww... ww... ww... ww... ww... ww... ww... ww... ww... ww... ww... ww... ww... 500...
Done
Start
500 Internal Serve...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

500 Internal Server Error

```
java.lang.NullPointerException

	at FleetWatch.fwcontrol.doGet(fwcontrol.java:36)

	at javax.servlet.http.HttpServlet.service(HttpServlet.java:740)

	at javax.servlet.http.HttpServlet.service(HttpServlet.java:853)

	at com.evermind[Oracle Application Server Containers for J2EE 10g (9.0.4.2.0)].server.http.ServletRequestDispatcher.invoke(ServletRequestDispatcher.jav

	at com.evermind[Oracle Application Server Containers for J2EE 10g (9.0.4.2.0)].server.http.ServletRequestDispatcher.forwardInternal(ServletRequestDispa

	at com.evermind[Oracle Application Server Containers for J2EE 10g (9.0.4.2.0)].server.http.HttpRequestHandler.processRequest(HttpRequestHandler.java:79

	at com.evermind[Oracle Application Server Containers for J2EE 10g (9.0.4.2.0)].server.http.AJPRequestHandler.run(AJPRequestHandler.java:208)

	at com.evermind[Oracle Application Server Containers for J2EE 10g (9.0.4.2.0)].server.http.AJPRequestHandler.run(AJPRequestHandler.java:125)

	at com.evermind[Oracle Application Server Containers for J2EE 10g (9.0.4.2.0)].util.ReleasableResourcePooledExecutor$MyWorker.run(ReleasableResourcePoo

	at java.lang.Thread.run(Thread.java:534)
```

These are real examples – hackers

Love these error message pages …



Server Error in '/' Application.

Value not found: LockAfterNumberOfLoginTries

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.ArgumentException: Value not found: LockAfterNumberOfLoginTries

Source Error:

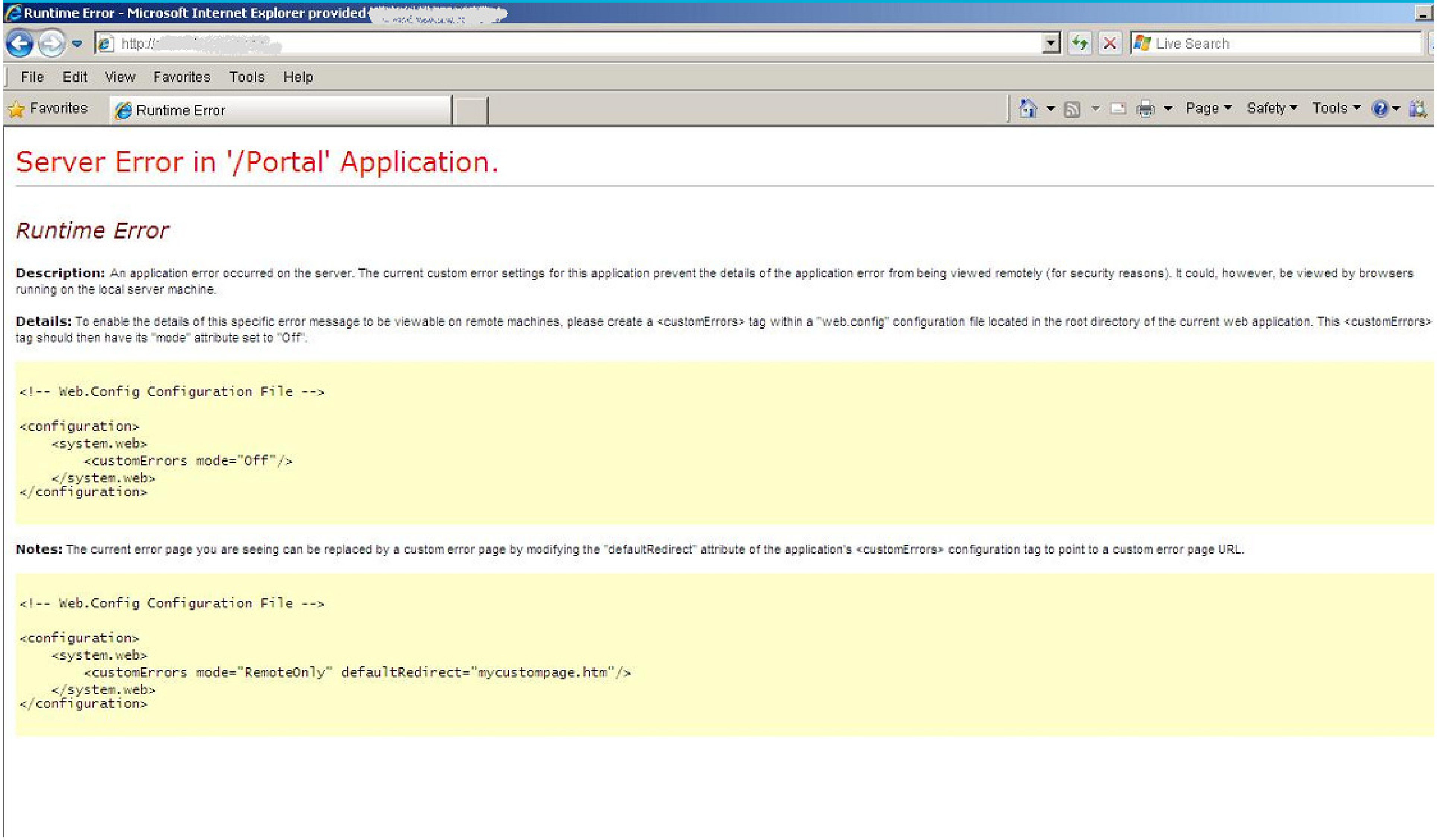
```
Line 7:  <html>
Line 8:  <head>
Line 9:  <title><%=AppPageTitle%></title>
Line 10: <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
Line 11: <link href="css/style.css" rel="stylesheet" type="text/css">
```

Source File: c:\Websites\MPS\mmp_port_prop_detail.aspx   **Line:** 9

Stack Trace:

```
[ArgumentException: Value not found: LockAfterNumberOfLoginTries]
   Nini.Config.ConfigBase.GetInt(String key) +118
   AppFoundation.Core.Config.ConfigurationManager.Load() in C:\Documents and Settings\Ethan\My Documents\WORK\AppFoundation\AppFoundation\Core\Cc
   AppFoundation.Core.Config.ConfigurationManager.get_Configuration() in C:\Documents and Settings\Ethan\My Documents\WORK\AppFoundation\AppFounc
   AppFoundation.Web.AppCorePage.get_AppPageTitle() in C:\Documents and Settings\Ethan\My Documents\WORK\AppFoundation\AppFoundation\Web\AppCoreF
   ASP.mmp_port_prop_detail_aspx.__Render__control1(HtmlTextWriter __w, Control parameterContainer) in c:\Websites\MPS\mmp_port_prop_detail.aspx:
   System.Web.UI.Control.RenderChildrenInternal(HtmlTextWriter writer, ICollection children) +98
   System.Web.UI.Control.RenderChildren(HtmlTextWriter writer) +20
   System.Web.UI.Page.Render(HtmlTextWriter writer) +26
   System.Web.UI.Control.RenderControlInternal(HtmlTextWriter writer, ControlAdapter adapter) +25
   System.Web.UI.Control.RenderControl(HtmlTextWriter writer, ControlAdapter adapter) +121
   System.Web.UI.Control.RenderControl(HtmlTextWriter writer) +22
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +2558
```

Version Information: Microsoft .NET Framework Version:2.0.50727.1433; ASP.NET Version:2.0.50727.1433


Runtime Error - Microsoft Internet Explorer provided [redacted]
http://[redacted]
Live Search
File Edit View Favorites Tools Help
Favorites
Runtime Error
Page Safety Tools

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".

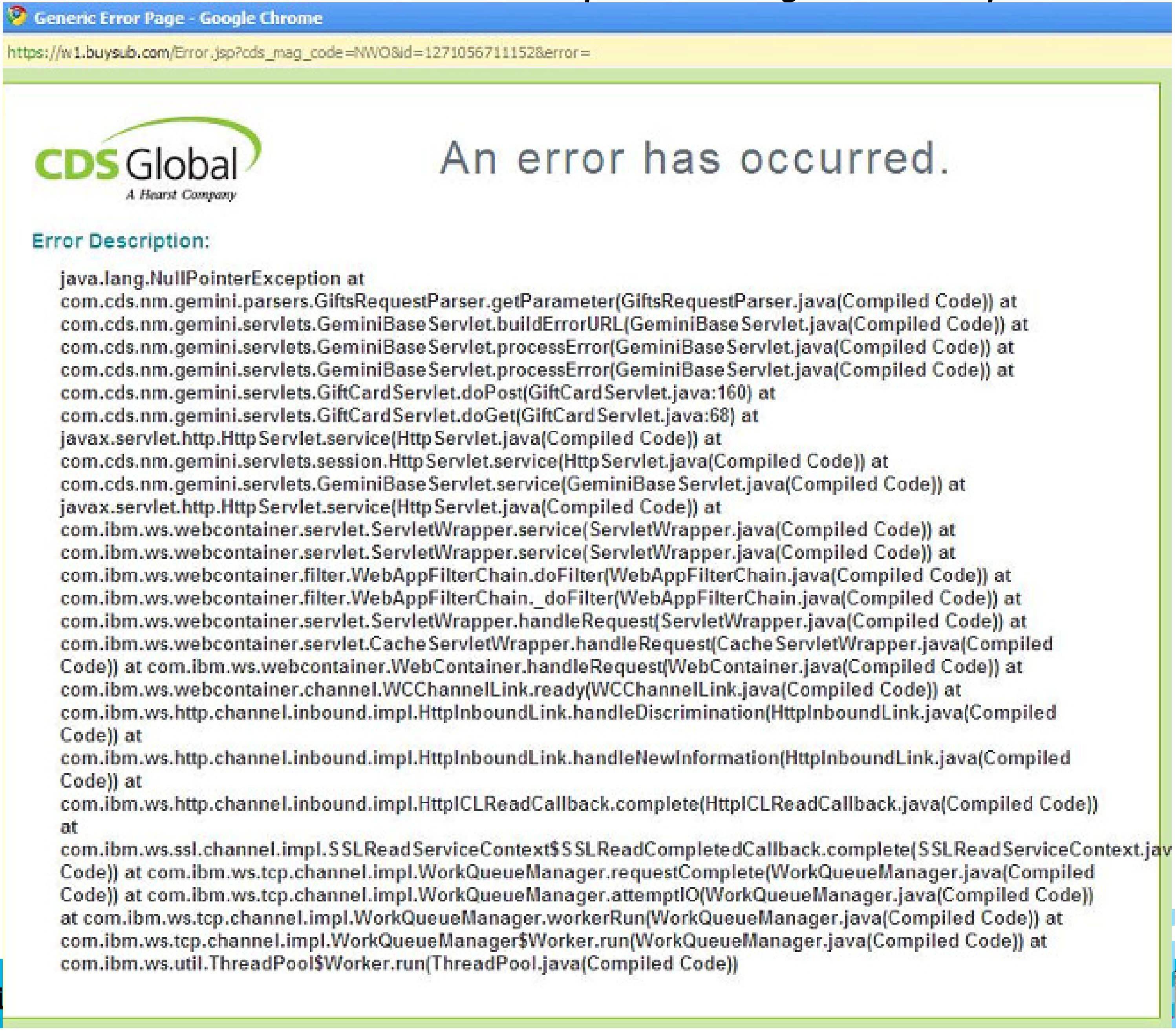
```
<!-- Web.Config Configuration File -->

<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>
```

“Self-inflicted” Social Engineering?!

International Service for Renewal of Paper-mailed Magazine Subscription



Generic Error Page - Google Chrome

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

CDS Global

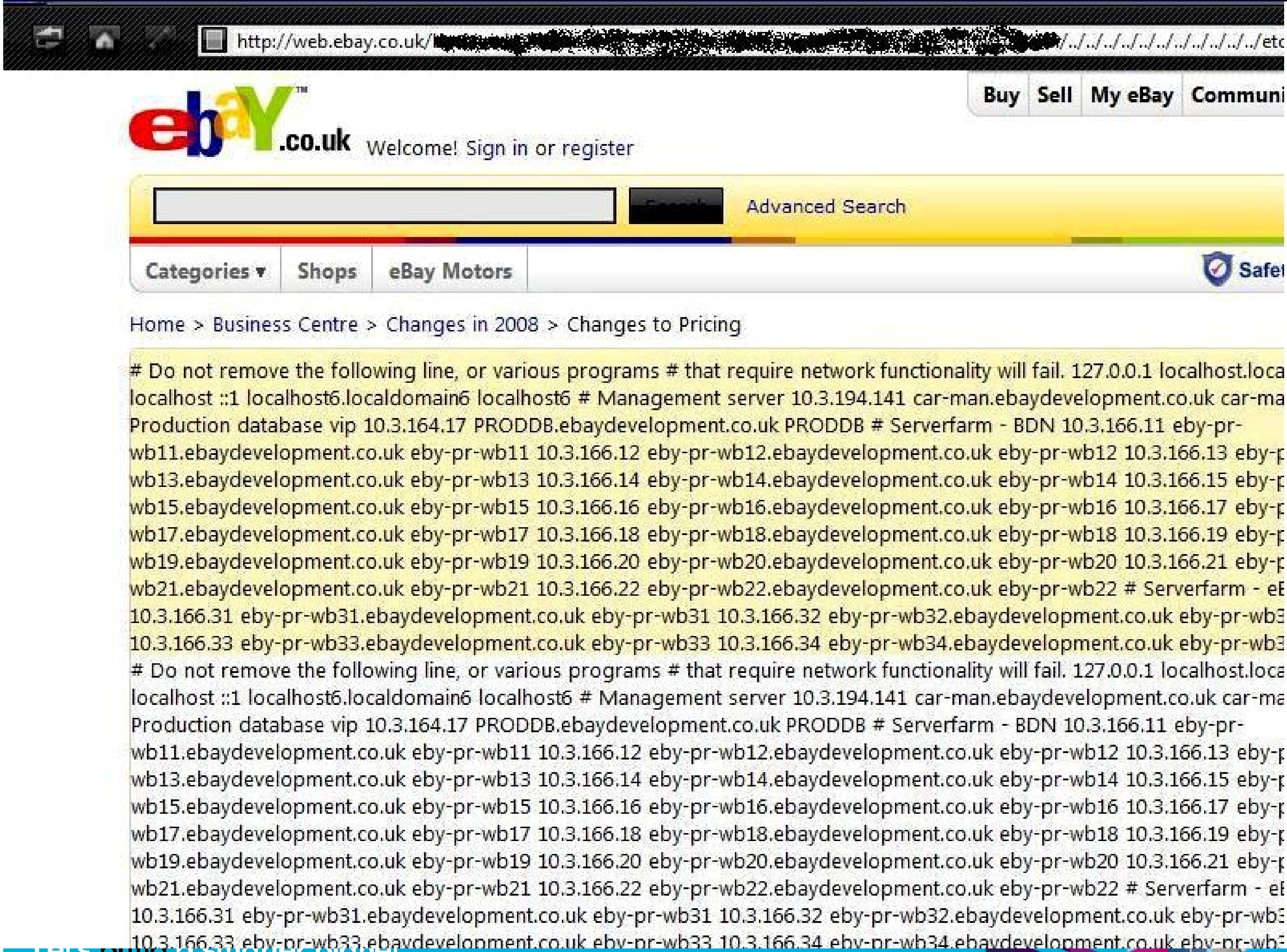
A Hearst Company

An error has occurred.

Error Description:

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



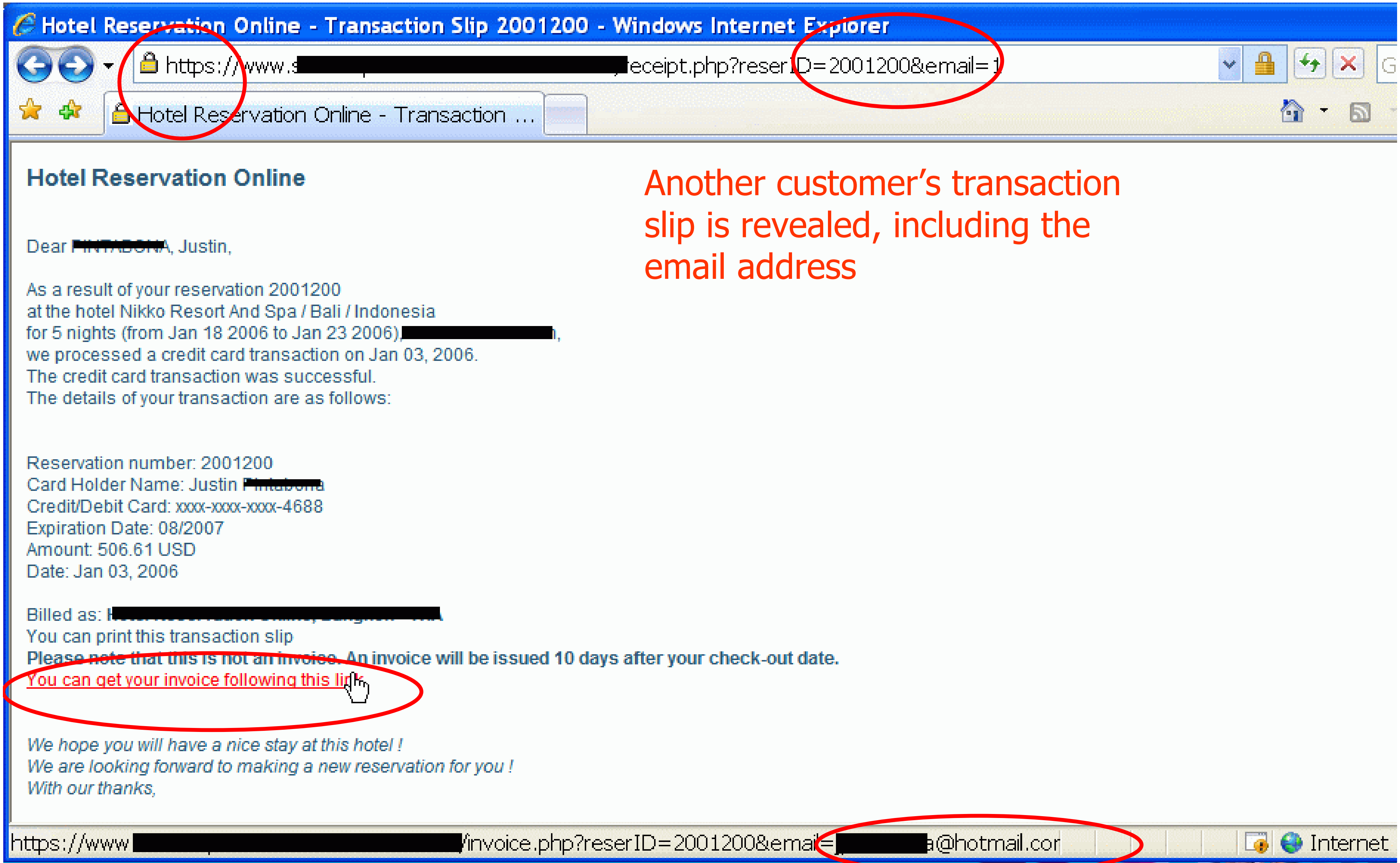
http://web.ebay.co.uk/[redacted]/../../../../../../../../../../../etc
Buy
Sell
My eBay
Communi
ebY .co.uk
Welcome! Sign in or register
Advanced Search
Categories ▾
Shops
eBay Motors
Safet
Home > Business Centre > Changes in 2008 > Changes to Pricing

```
# 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 – insufficient authorization



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

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

Hotel Reservation Online

Dear [redacted], Justin,

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

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

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

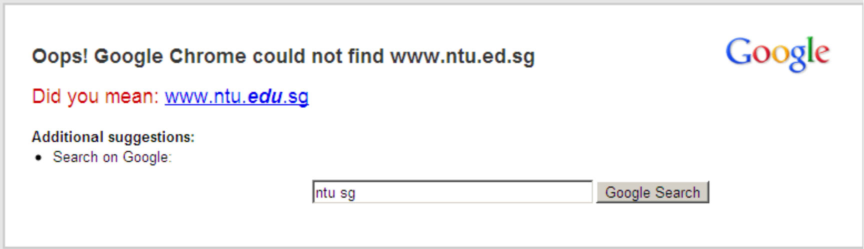
We hope you will have a nice stay at this hotel !
We are looking forward to making a new reservation for you !
With our thanks,

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

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

WHY DO HACKERS TODAY ATTACK 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**



Oops! Google Chrome could not find www.ntu.ed.sg

Did you mean: www.ntu.*edu*.sg

Additional suggestions:

- Search on Google:

ntu sg | Google Search

- **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**

Issues Affecting Application Development

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 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 ….***

Developers are hired faster than they can be trained properly

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

-> Choose 2!

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

E-mail: SCOTTADAMS@AOL.COM

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

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

1 Unvalidated Input

2 Broken Access Control

3 Broken Authentication and Session Management

4 Cross Site Scripting Flaws

5 Buffer Overflows

6 Injection Flaws

7 Improper Error Handling

8 Insecure Storage

9 *Denial of Service*

10 Insecure Configuration Management

2010

1 Injection

2 Cross-Site Scripting (XSS)

3 Broken Authentication and Session Management

4 Insecure Direct Object References

5 Cross-Site Request Forgery (CSRF)

6 Security Misconfiguration

7 Insecure Cryptographic Storage

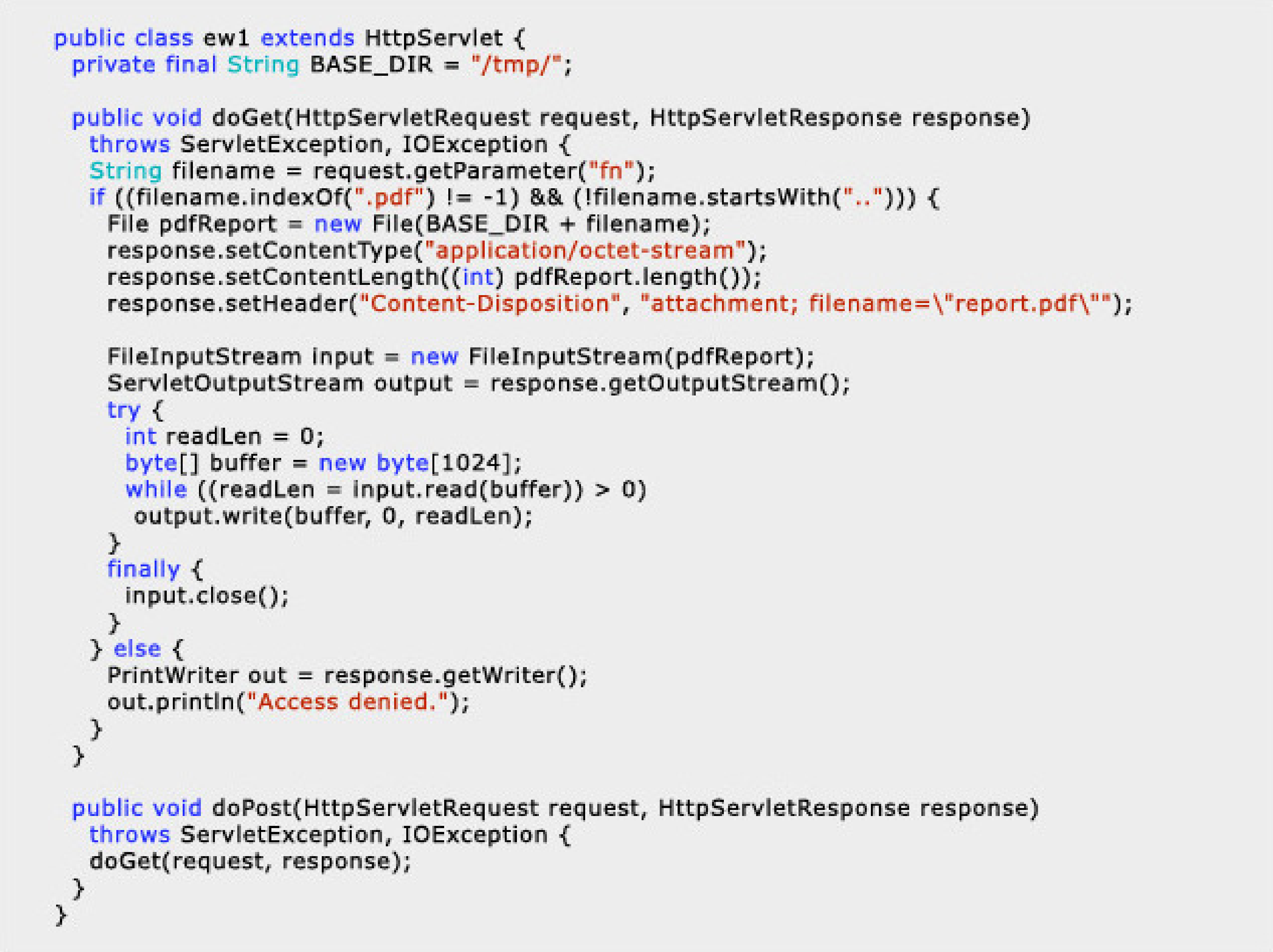
8 Failure to Restrict URL Access

9 Insufficient Transport Layer Protection

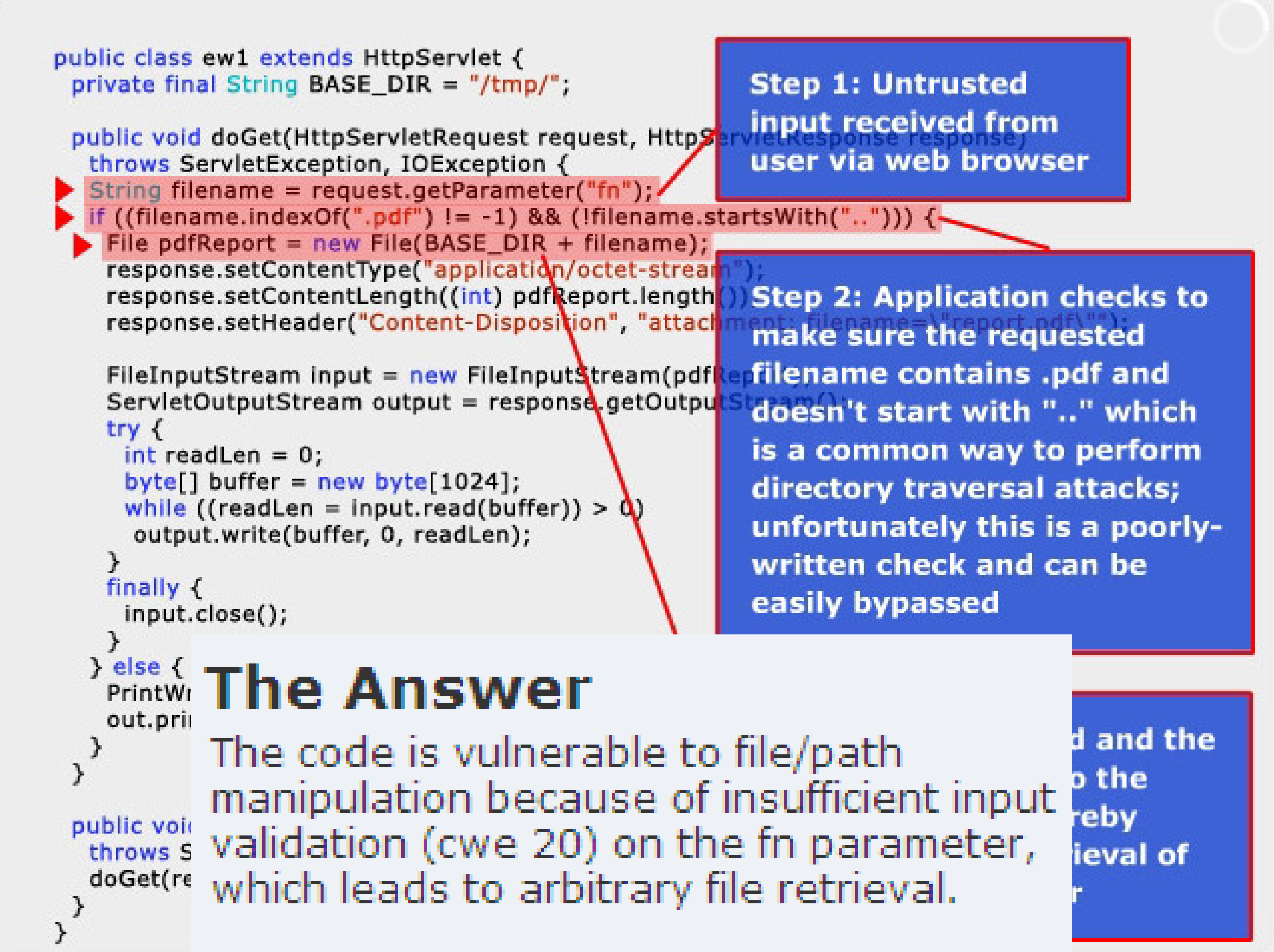
10 Unvalidated Redirects and Forwards

BUSINESS MOTIVATIONS FOR APPLICATION SECURITY

- Reduce the risk of outage, defacement or data theft associated with Web applications
- Improve your ability to meet compliance requirements
- Protect your brand and reputation
- Improve your ability to integrate business-critical applications
- Reduce long-term security costs by focusing on building security into application development and delivery, instead of retrofitting it after the fact



```
public class ew1 extends HttpServlet {
  private final String BASE_DIR = "/tmp/";

  public void doGet(HttpServletRequest request, HttpServletResponse response)
    throws ServletException, IOException {
    String filename = request.getParameter("fn");
    if ((filename.indexOf(".pdf") != -1) && (!filename.startsWith(".."))) {
      File pdfReport = new File(BASE_DIR + filename);
      response.setContentType("application/octet-stream");
      response.setContentLength((int) pdfReport.length());
      response.setHeader("Content-Disposition", "attachment; filename=\"report.pdf\"");

      FileInputStream input = new FileInputStream(pdfReport);
      ServletOutputStream output = response.getOutputStream();
      try {
        int readLen = 0;
        byte[] buffer = new byte[1024];
        while ((readLen = input.read(buffer)) > 0)
         output.write(buffer, 0, readLen);
      }
      finally {
        input.close();
      }
    } else {
      PrintWriter out = response.getWriter();
      out.println("Access denied.");
    }
  }

  public void doPost(HttpServletRequest request, HttpServletResponse response)
    throws ServletException, IOException {
    doGet(request, response);
  }
}
```



```
public class ew1 extends HttpServlet {
  private final String BASE_DIR = "/tmp/";

  public void doGet(HttpServletRequest request, HttpServletResponse response)
    throws ServletException, IOException {
    String filename = request.getParameter("fn");
    if ((filename.indexOf(".pdf") != -1) && (!filename.startsWith(".."))) {
      File pdfReport = new File(BASE_DIR + filename);
      response.setContentType("application/octet-stream");
      response.setContentLength((int) pdfReport.length());
      response.setHeader("Content-Disposition", "attachment; filename=\"report.pdf\"");

      FileInputStream input = new FileInputStream(pdfRep
      ServletOutputStream output = response.getOutputStream();
      try {
        int readLen = 0;
        byte[] buffer = new byte[1024];
        while ((readLen = input.read(buffer)) > 0)
         output.write(buffer, 0, readLen);
      }
      finally {
        input.close();
      }
    } else {
      PrintWr
      out.pri
    }
  }

  public voi
    throws S
    doGet(re
  }
}
```

Step 1: Untrusted input received from user via web browser

Step 2: Application checks to make sure the requested filename contains .pdf and doesn't start with ".." which is a common way to perform directory traversal attacks; unfortunately this is a poorly-written check and can be easily bypassed

d and the
o the
reby
ieval of
r

The Answer

The code is vulnerable to file/path manipulation because of insufficient input validation (cwe 20) on the fn parameter, which leads to arbitrary file retrieval.

Vulnerarbility Issues With Java Code – some examples

Note: the language itself is quite secure, its how people use it to write code that is an issue

- 244986: The Java Runtime Environment Creates Temporary Files That Have “Guessable” File Names
- 244987: Java Runtime Environment (JRE) Buffer Overflow Vulnerabilities in Processing Image Files and Fonts May Allow Applets or Java Web Start Applications to Elevate Their Privileges
- 244988: Multiple Security Vulnerabilities in Java Web Start and Java Plug-in May Allow Privilege Escalation
- 244989: The Java Runtime Environment (JRE) “Java Update” Mechanism Does Not Check the Digital Signature of the JRE that it Downloads
- 244990: A Buffer Overflow Vulnerability in the Java Runtime Environment (JRE) May Allow Privileges to be Escalated
- 244991: A Security Vulnerability in the Java Runtime Environment (JRE) Related to Deserializing Calendar Objects May Allow Privileges to be Escalated

- **Java Web Start Sandbox Security Bypass Vulnerability**
- A vulnerability has been reported in Java Web Start, which potentially can be exploited by malicious people to compromise a user's system.

  The vulnerability is caused due to an unspecified error, which may be exploited by a malicious, untrusted application to read and write local files.
- **Solution**
  The vulnerability has been fixed in J2SE releases 5.0 Update 6 and later for Windows, Solaris, and Linux.

“INSECURE CODE” per ISC2.org

I : Injectable Code

N :Non-Repudiation Mechanisms not Present

S : Spoofable Code

E : Exceptions and Errors not Properly Handled

C : Cryptographically Weak Code

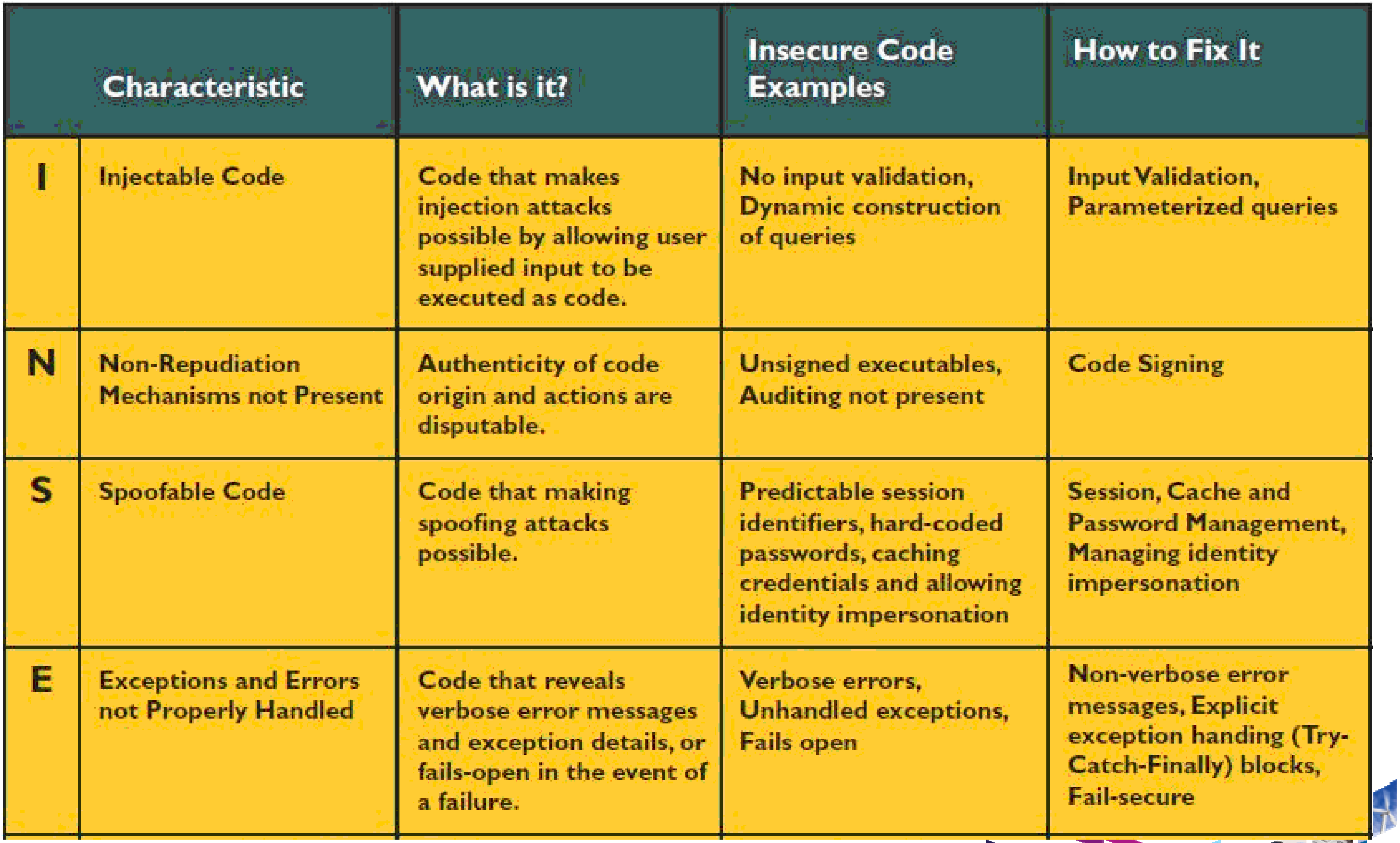
U : Unsafe/Unused Functions and Routines in Code

R : Reversible Code

E : Elevated Privileges Required to Run

INSECURE CODE

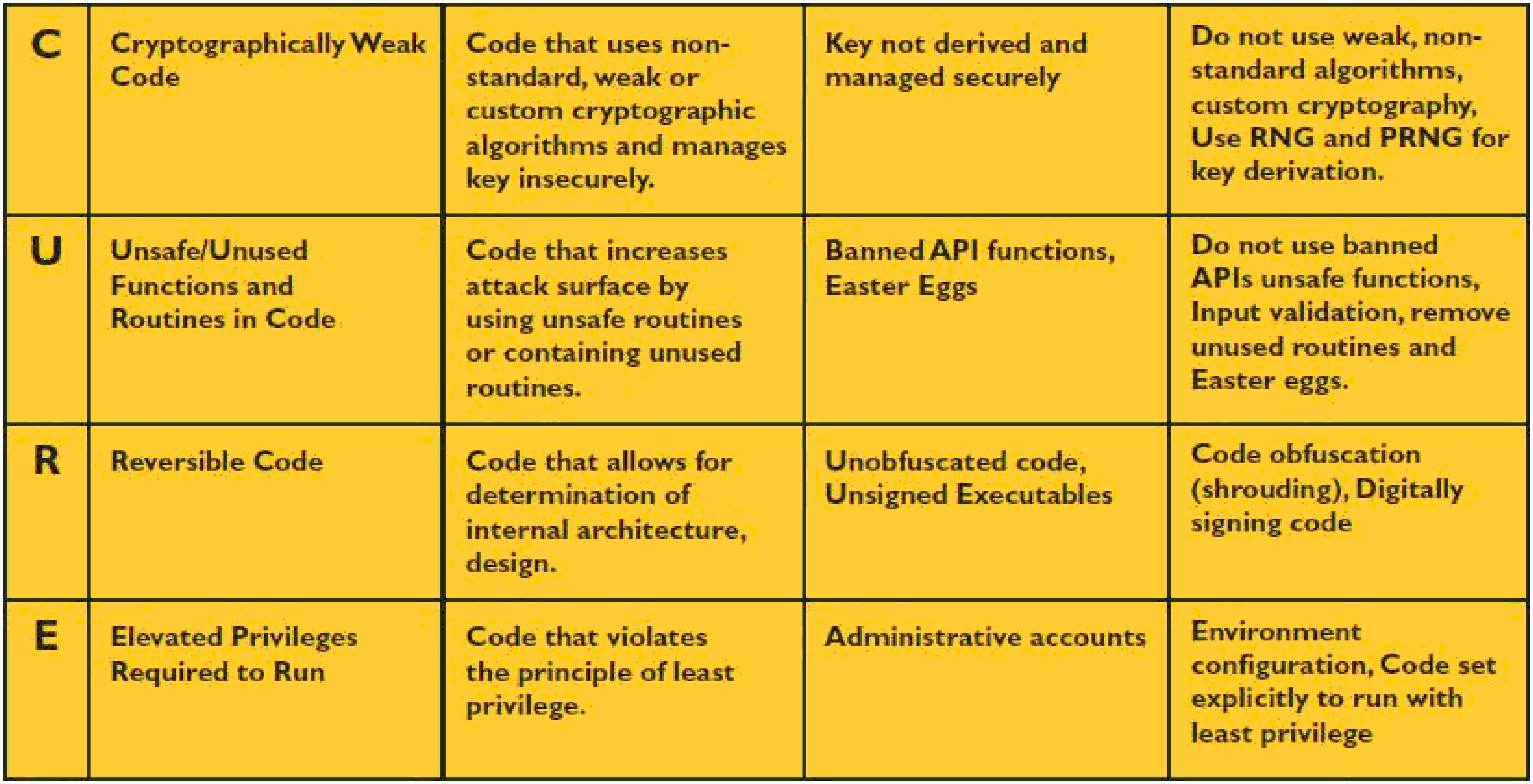
ISC2.org



Characteristic		What is it?	Insecure Code Examples	How to Fix It
I	Injectable Code	Code that makes injection attacks possible by allowing user supplied input to be executed as code.	No input validation, Dynamic construction of queries	Input Validation, Parameterized queries
N	Non-Repudiation Mechanisms not Present	Authenticity of code origin and actions are disputable.	Unsigned executables, Auditing not present	Code Signing
S	Spoofable Code	Code that making spoofing attacks possible.	Predictable session identifiers, hard-coded passwords, caching credentials and allowing identity impersonation	Session, Cache and Password Management, Managing identity impersonation
E	Exceptions and Errors not Properly Handled	Code that reveals verbose error messages and exception details, or fails-open in the event of a failure.	Verbose errors, Unhandled exceptions, Fails open	Non-verbose error messages, Explicit exception handing (Try-Catch-Finally) blocks, Fail-secure

INSECURE CODE (cont'd)

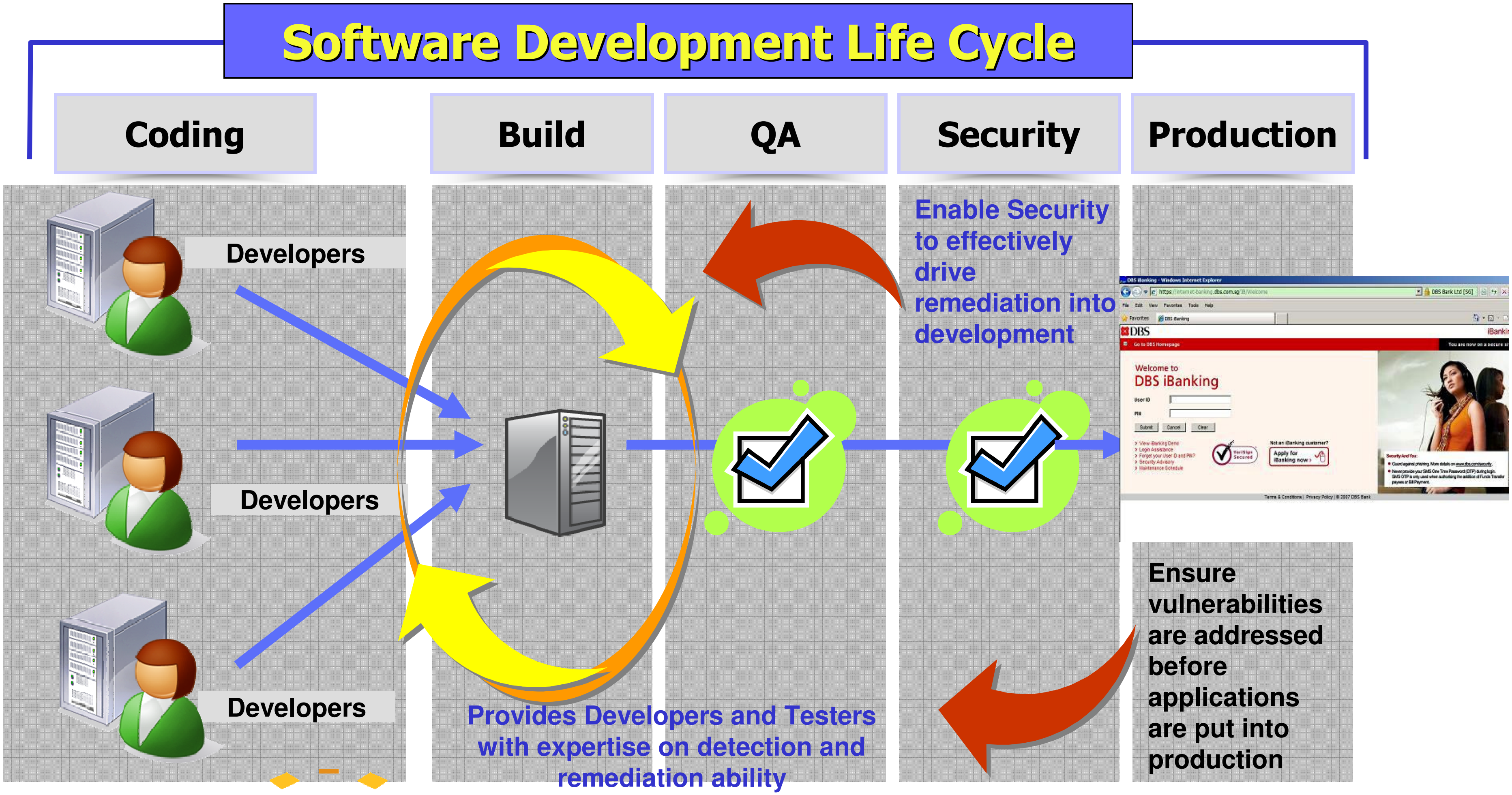
ISC2.org



C	Cryptographically Weak Code	Code that uses non-standard, weak or custom cryptographic algorithms and manages key insecurely.	Key not derived and managed securely	Do not use weak, non-standard algorithms, custom cryptography, Use RNG and PRNG for key derivation.
U	Unsafe/Unused Functions and Routines in Code	Code that increases attack surface by using unsafe routines or containing unused routines.	Banned API functions, Easter Eggs	Do not use banned APIs unsafe functions, Input validation, remove unused routines and Easter eggs.
R	Reversible Code	Code that allows for determination of internal architecture, design.	Unobfuscated code, Unsigned Executables	Code obfuscation (shrouding), Digitally signing code
E	Elevated Privileges Required to Run	Code that violates the principle of least privilege.	Administrative accounts	Environment configuration, Code set explicitly to run with least privilege

Building security & compliance into the SDLC

- ensure programs are tested for security resilience; ensure developers get Q.A. tools and training



Enable Security to effectively drive remediation into development

Provides Developers and Testers with expertise on detection and remediation ability

Ensure vulnerabilities are addressed before applications are put into production

DBS iBanking - Windows Internet Explorer

https://internet-banking.dbs.com.sg/IB/Welcome

DBS Bank Ltd [SG]

File Edit View Favorites Tools Help
Favorites
DBS iBanking
DBS
iBanki
Go to DBS Homepage
You are now on a secure si

Welcome to DBS iBanking

User ID

PIN

Submit Cancel Clear

- View iBanking Demo
- Login Assistance
- Forgot your User ID and PIN?
- Security Advisory
- Maintenance Schedule

VeriSign Secured

Not an iBanking customer?

Apply for iBanking now >

Security And You:

- Guard against phishing. More details on www.dbs.com/security.
- Never provide your SMS One Time Password (OTP) during login. SMS OTP is only used when authorising the addition of Funds Transfer payees or Bill Payment.

Terms & Conditions | Privacy Policy | © 2007 DBS Bank

CSSLP CM

Certified Secure Software Lifecycle Professional

Introducing IBM Secure by Design

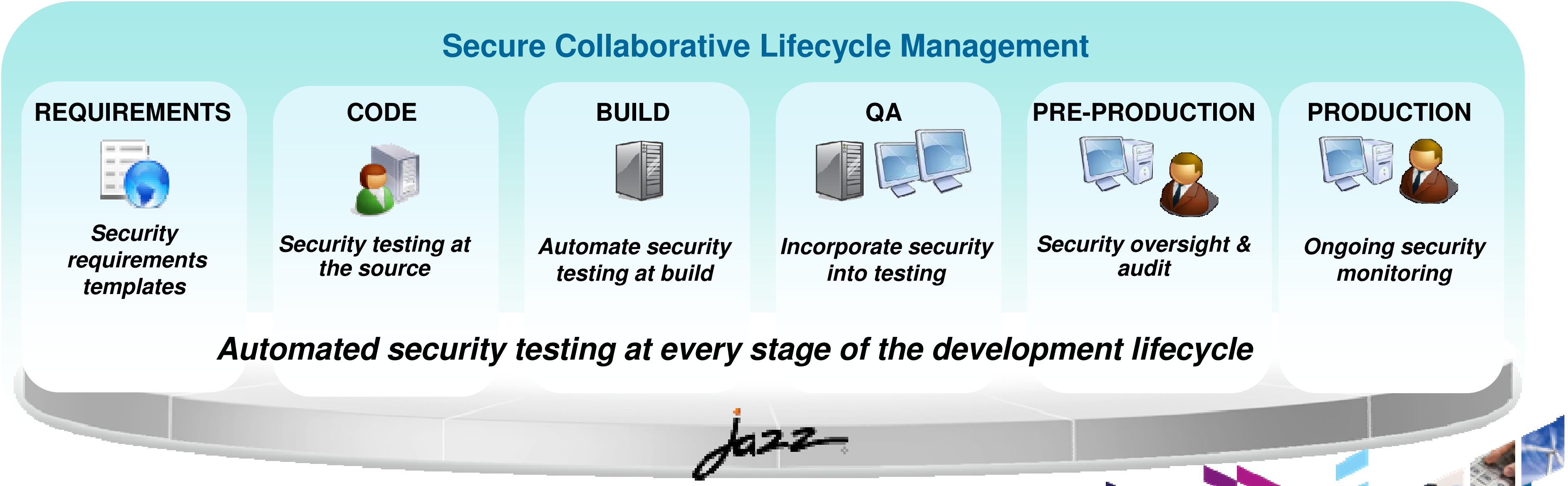
Automate security testing early & often throughout the development lifecycle from the beginning (User Requirements Phase)

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

Deliver New Services Faster

Innovate Securely

Reduce Costs

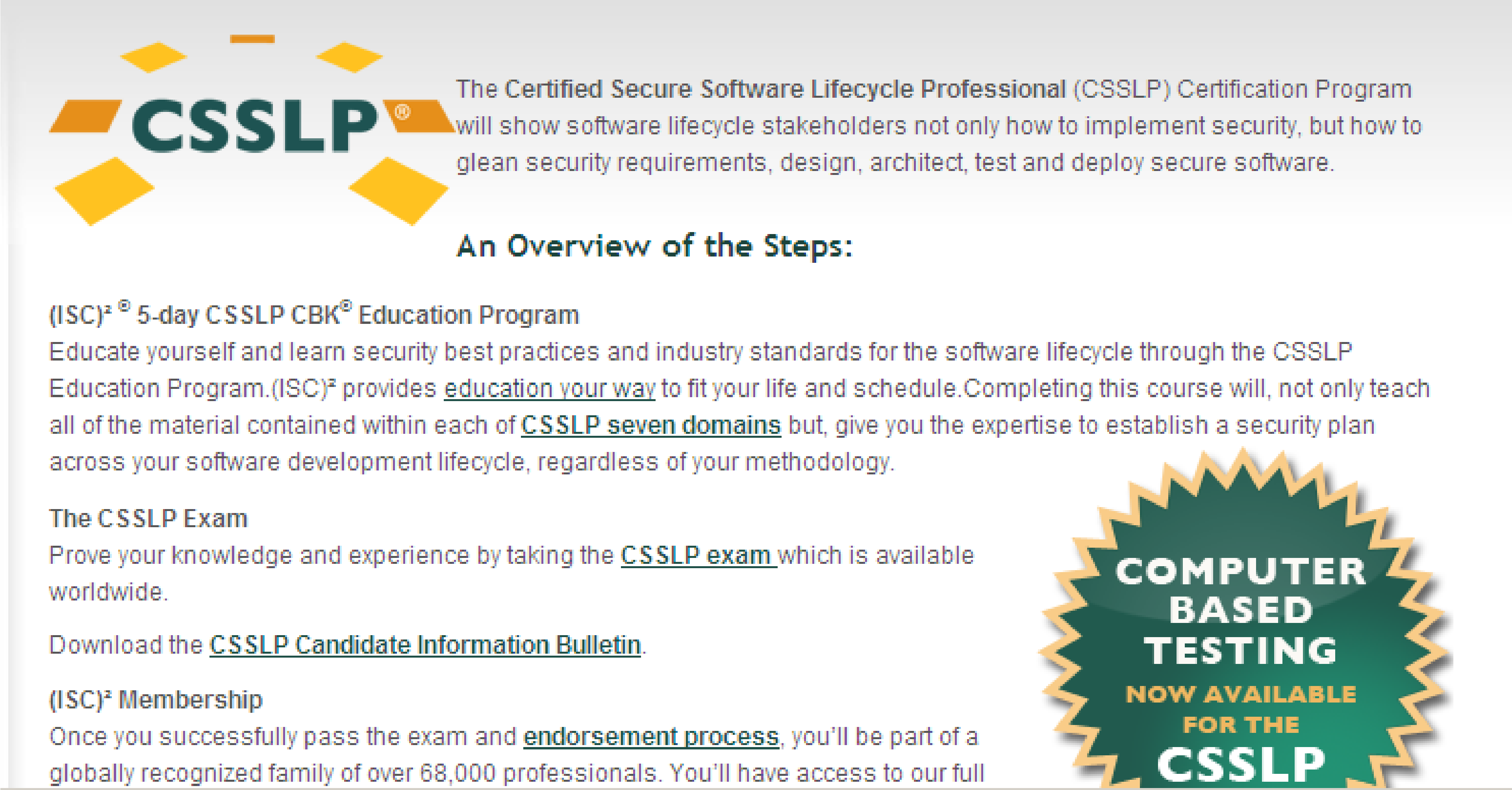

Secure Collaborative Lifecycle Management
REQUIREMENTS
Security requirements templates
CODE
Security testing at the source
BUILD
Automate security testing at build
QA
Incorporate security into testing
PRE-PRODUCTION
Security oversight & audit
PRODUCTION
Ongoing security monitoring
Automated security testing at every stage of the development lifecycle
Jazz

NEED FOR CONTINUING DEVELOPER EDUCATION

AND Security CERTIFICATION for Application Development Team

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

www.isc2.org **CISSP**



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

APPLICATION SECURITY BEST PRACTICES - SUMMARY

1. Security must be included at the beginning of the SLDC, not a bolted-on after-thought at the end, or left to the end

   EG: India software project : Jan – Dec, Oct for security audit becomes Dec 15, yet Jan 01 still must go live …

2. More people must be involved in the whole security process and workflow – especially business line managers, not just a limited few
3. Training and Education; appropriate incentives for appropriate behavior.
4. Pay attention to the OWASP.org Top Ten and other such lists
5. Do not try to save money on security tools, practices, service providers and resources! Don't just check-mark for Audit's Sake (A.U.D.I.T.) *eg. Fire Drill, SGP Merc*
6. You can outsource work but you cannot outsource the trust – don't just assign out the security quality testing, not even thru an SLA. Even if you do this you must test in house after delivery.
7. Have at least one clearly-defined and appropriately-equipped application security specialist on the team.

CSSLP CM

Certified Secure Software Lifecycle Professional

Conclusion:
APPLICATION DEVELOPMENT BEST PRACTICES

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

APPLICATION SECURITY BEST PRACTICES

http://www-01.ibm.com/software/rational/offerings/websecurity/

http://www-01.ibm.com/software/tivoli/governance/security/application-security.html

www.isc2.org **www.owasp.org**