Is Your Web App-solutely Secure?

Anthony Lim

MBA FCITIL CISSP CSSLP

Asia Pacific Business Unit Executive

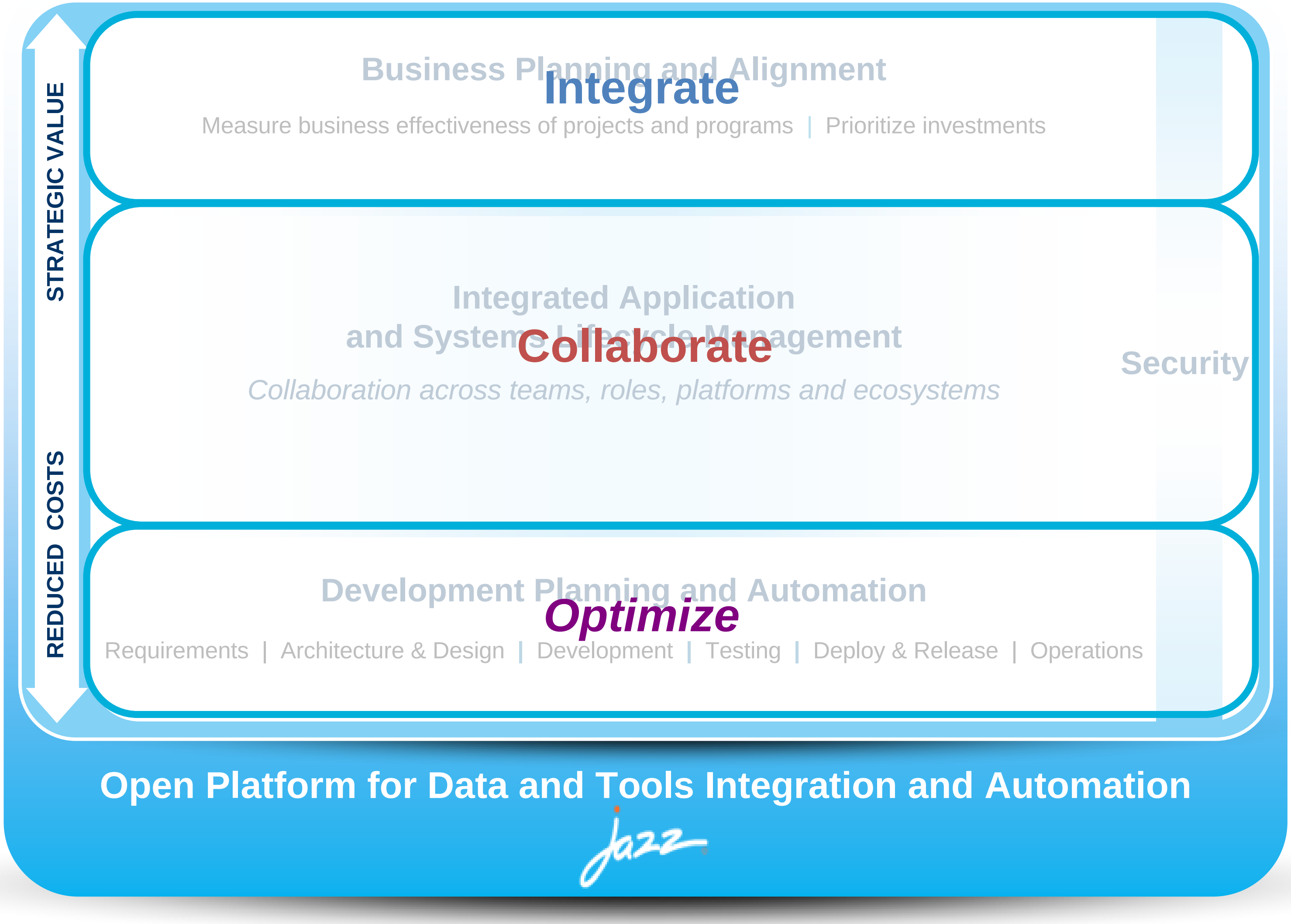
Security

Rational Software

02 Aug 2011

Bangkok, Thailand

Our Capabilities to Help You Achieve Breakthrough Benefits



STRATEGIC VALUE

REDUCED COSTS

Business Planning and Alignment

Integrate

Measure business effectiveness of projects and programs | Prioritize investments

Integrated Application and Systems Lifecycle Management

Collaborate

Collaboration across teams, roles, platforms and ecosystems

Security

Development Planning and Automation

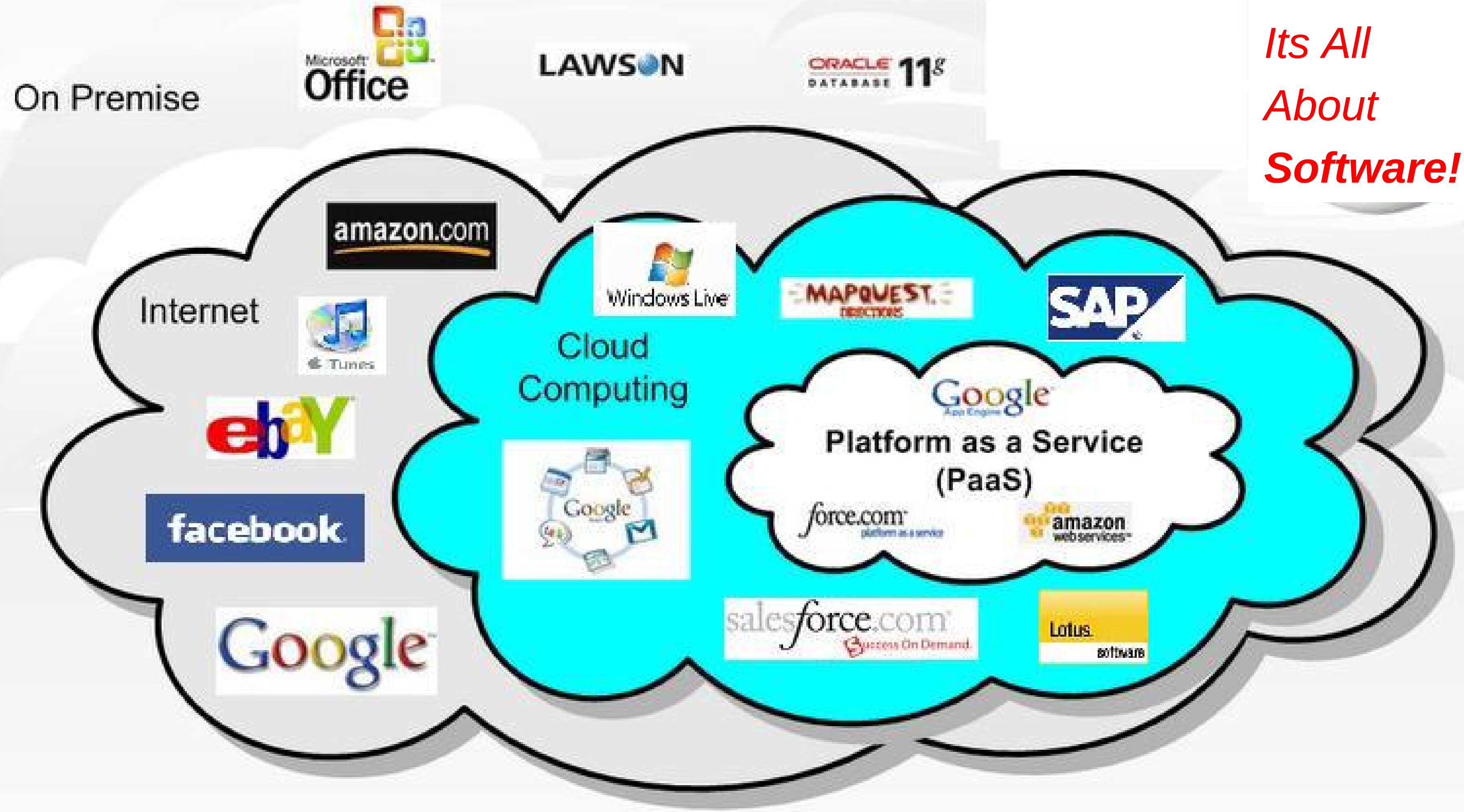
Optimize

Requirements | Architecture & Design | Development | Testing | Deploy & Release | Operations

Open Platform for Data and Tools Integration and Automation

Jazz

The Wonders of Cloud Computing



Its All About ***Software!***

Application Security 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

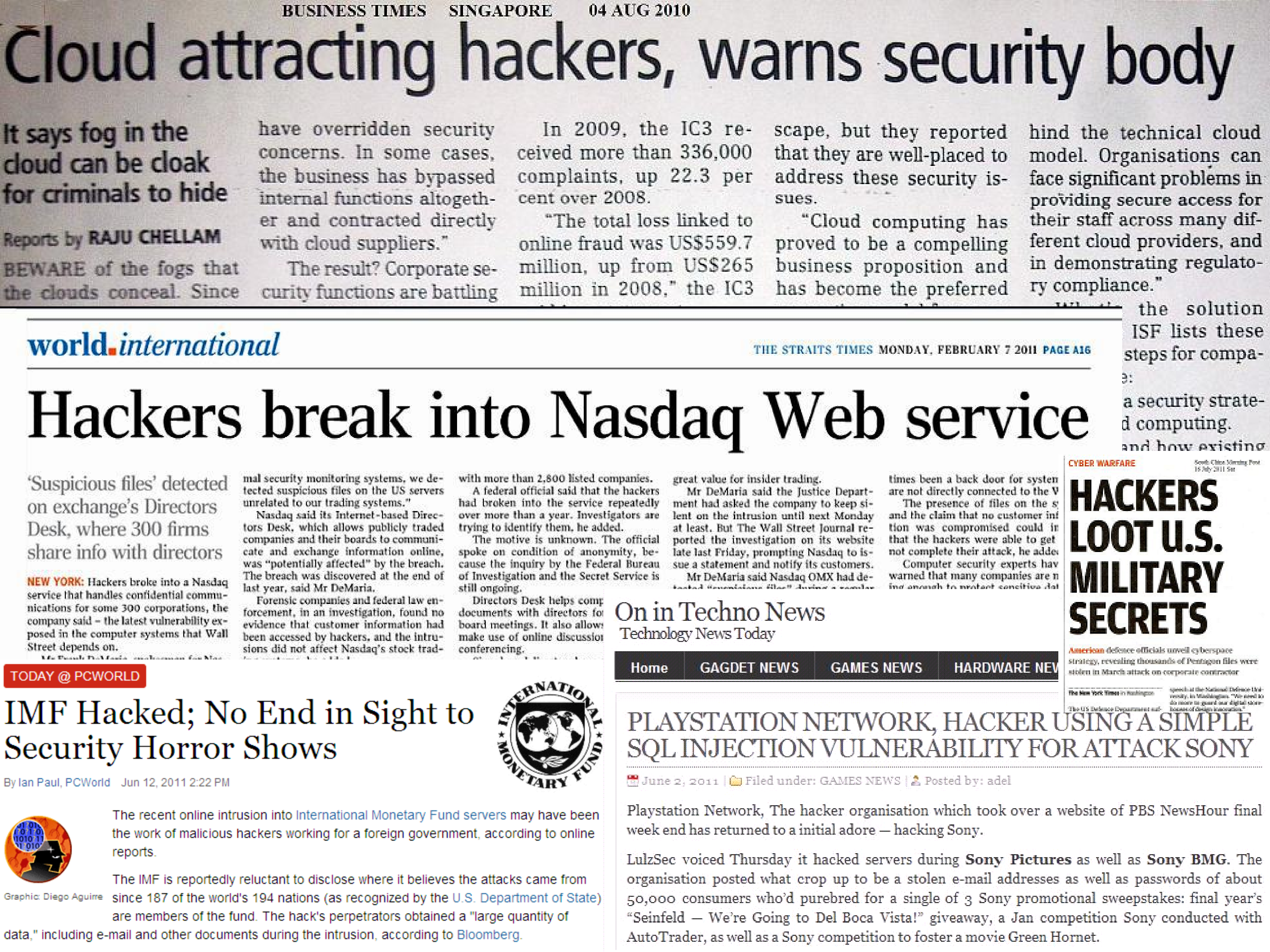
Applications are constantly changing

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

In 2009, the IC3 received more than 336,000 complaints, up 22.3 per cent over 2008.

"The total loss linked to online fraud was US$559.7 million, up from US$265 million in 2008," the IC3

scape, but they reported that they are well-placed to address these security issues.

"Cloud computing has proved to be a compelling business proposition and has become the preferred

hind the technical cloud model. Organisations can face significant problems in providing secure access for their staff across many different cloud providers, and in demonstrating regulatory compliance."

the solution ISF lists these steps for compa-

e:

a security strate-

d computing.

and how existing

world.international

THE STRAITS TIMES MONDAY, FEBRUARY 7 2011 PAGE A16

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.

mal security monitoring systems, we detected suspicious files on the US servers unrelated to our trading systems."

Nasdaq said its Internet-based Directors Desk, which allows publicly traded companies and their boards to communicate and exchange information online, was "potentially affected" by the breach. The breach was discovered at the end of last year, said Mr DeMaria.

Forensic companies and federal law enforcement, in an investigation, found no evidence that customer information had been accessed by hackers, and the intrusions did not affect Nasdaq's stock trad-

with more than 2,800 listed companies.

A federal official said that the hackers had broken into the service repeatedly over more than a year. Investigators are trying to identify them, he added.

The motive is unknown. The official spoke on condition of anonymity, because the inquiry by the Federal Bureau of Investigation and the Secret Service is still ongoing.

Directors Desk helps comp documents with directors fo board meetings. It also allow make use of online discussio conferencing.

great value for insider trading.

Mr DeMaria said the Justice Department had asked the company to keep silent on the intrusion until next Monday at least. But The Wall Street Journal reported the investigation on its website late last Friday, prompting Nasdaq to issue a statement and notify its customers.

Mr DeMaria said Nasdaq OMX had de-

times been a back door for systen are not directly connected to the V

The presence of files on the s and the claim that no customer inf tion was compromised could in that the hackers were able to get not complete their attack, he adde

Computer security experts hav warned that many companies are n

CYBER WARFARE

South China Morning Post
16 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."

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.

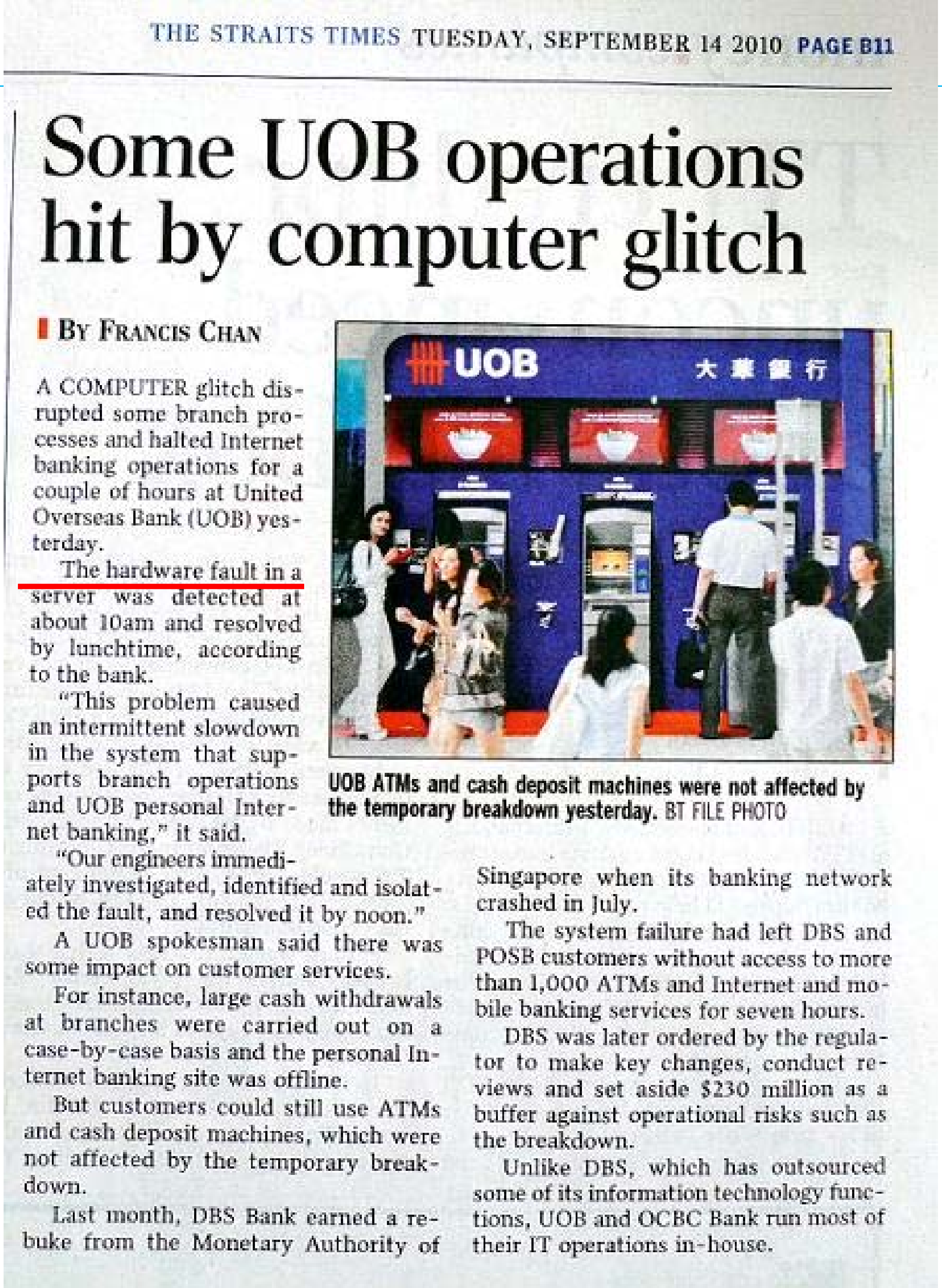
On in Techno News
Technology News Today

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 Jan competition Sony conducted with AutoTrader, as well as a Sony competition to foster a movie Green Hornet.



THE STRAITS TIMES TUESDAY, SEPTEMBER 14 2010 PAGE B11

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.

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

"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.

Its always the hardware?!

Maybe the network?!

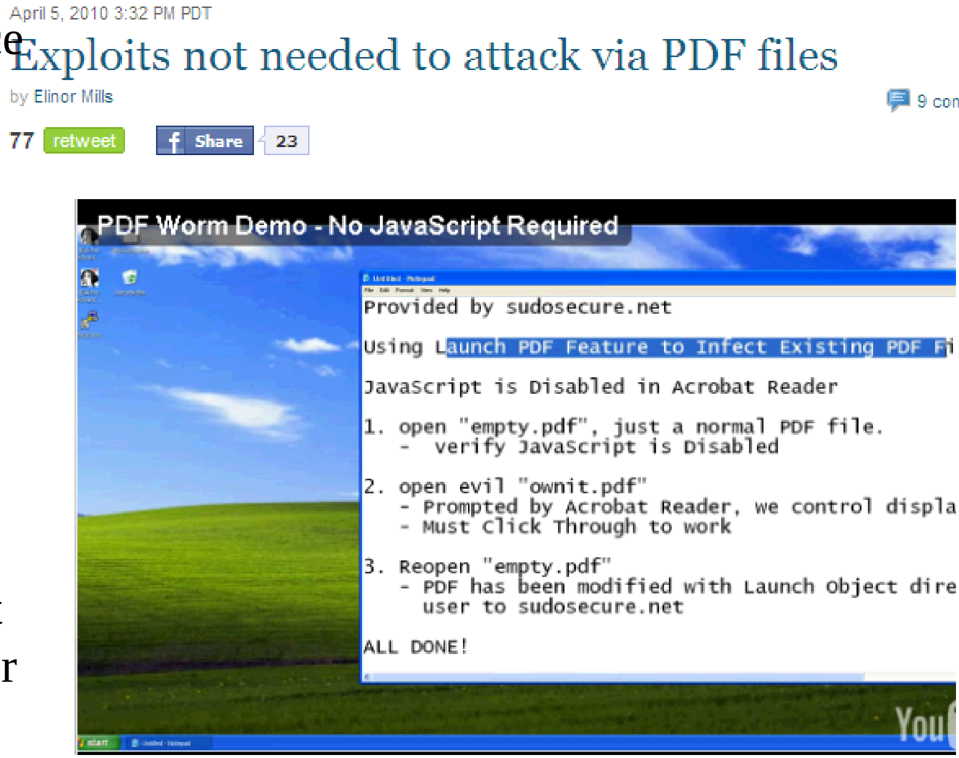
Its never the software?!

How Do Hackers 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 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*


77
retweet
Share
23
9 con
PDF Worm Demo - No JavaScript Required
Untitled - Notepad
File Edit Format View Help

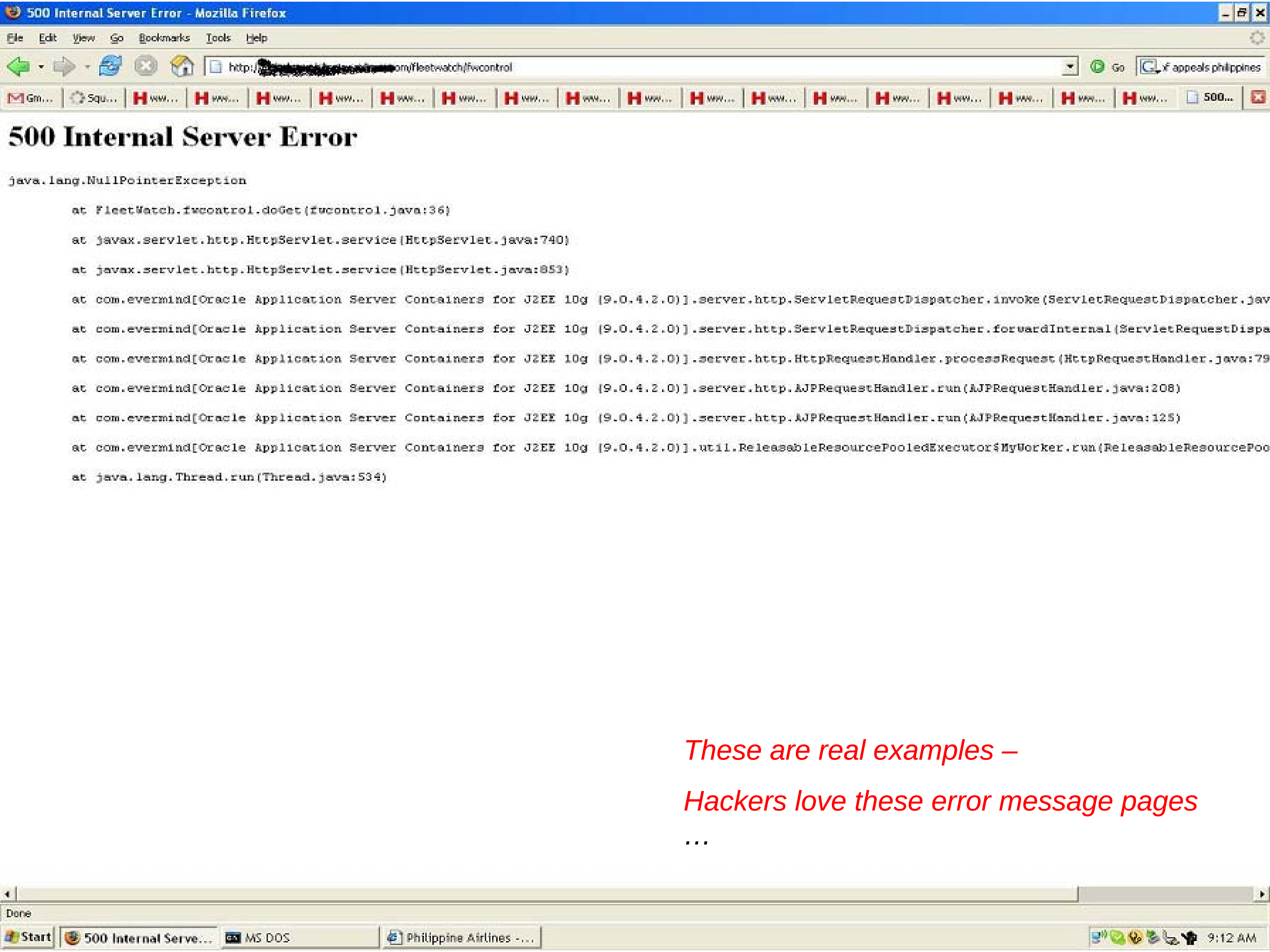
April 5, 2010 3:32 PM PDT

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.


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

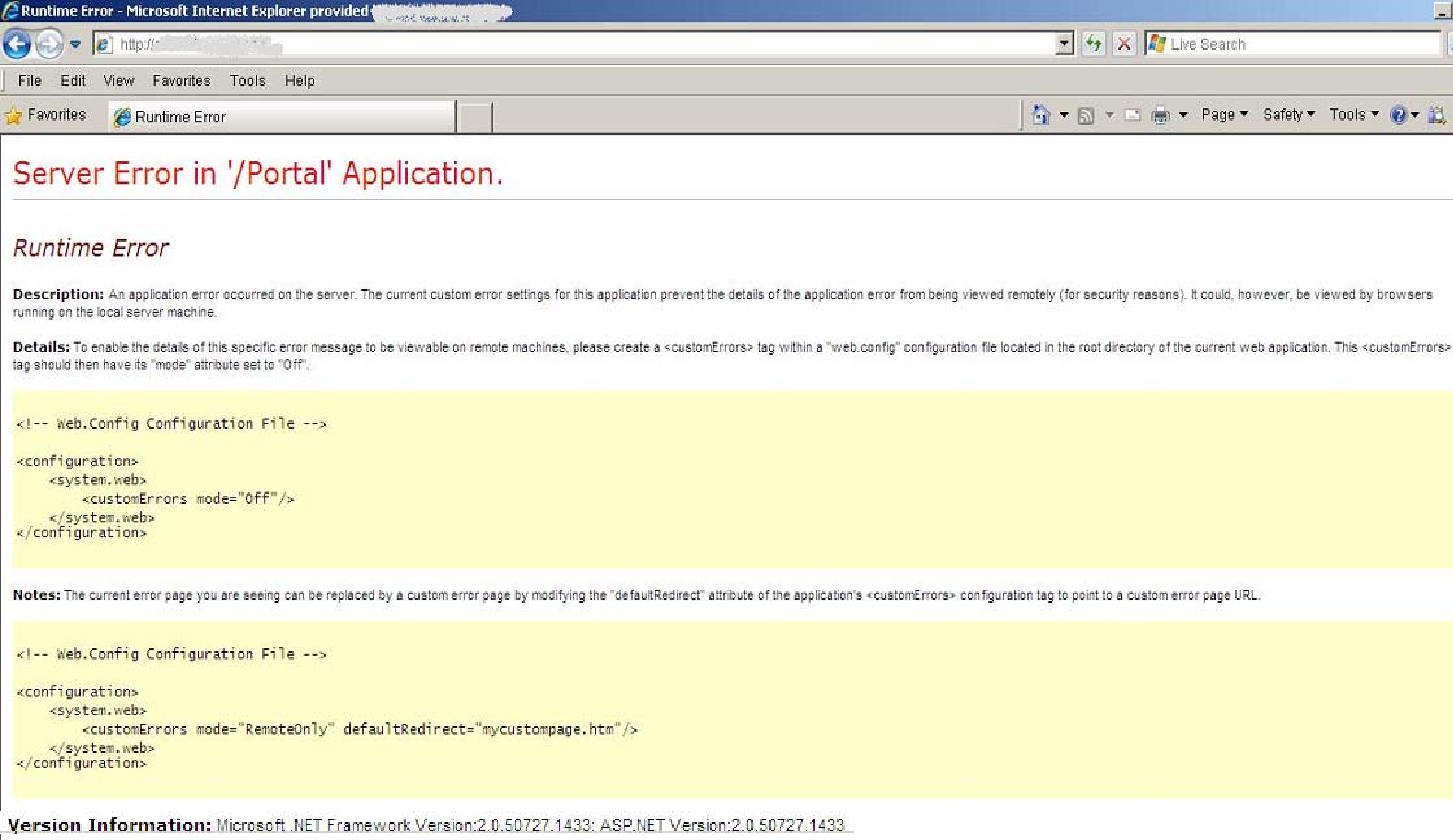
500 Internal Server Error

```
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 '/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>
```

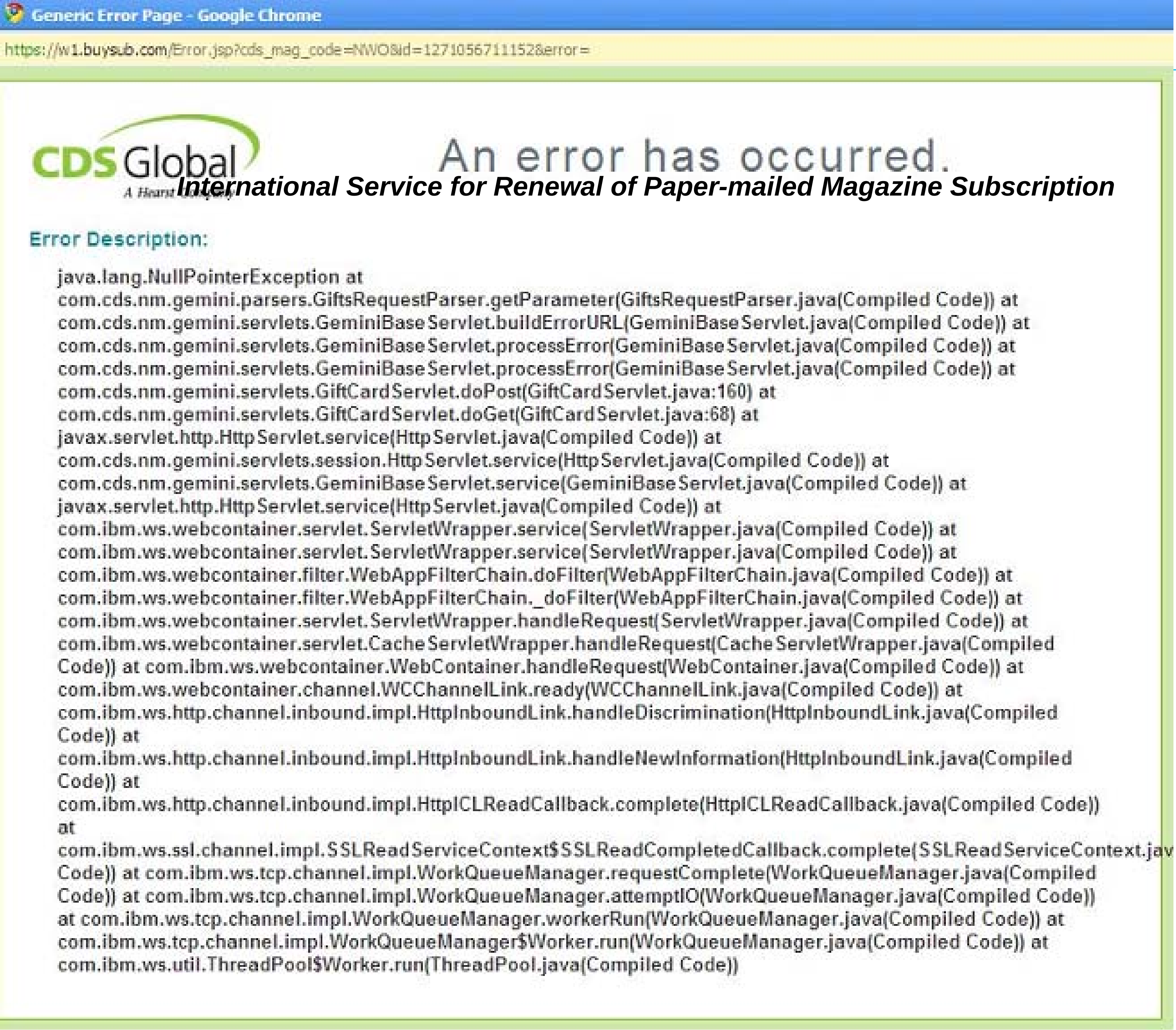
Notes: The current error page you are seeing can be replaced by a custom error page by modifying the "defaultRedirect" attribute of the application's <customErrors> configuration tag to point to a custom error page URL.

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

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

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

"Self-inflicted" Social Engineering?!

International Service for Renewal of Paper-mailed Magazine Subscription

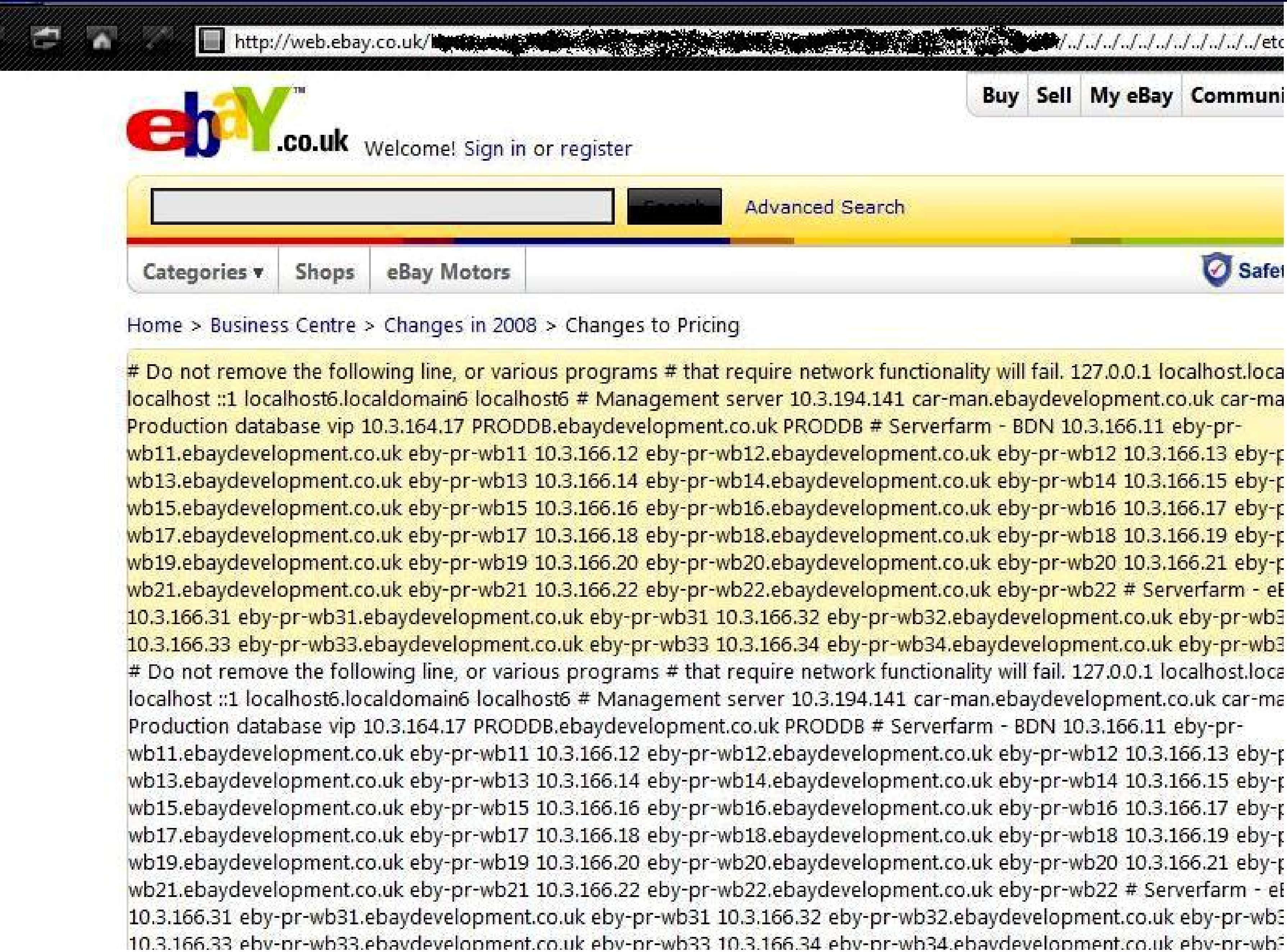

Generic Error Page - Google Chrome
https://w1.buysub.com/Error.jsp?cds_mag_code=NWO&id=1271056711152&error=
CDS Global
A Hearst Company

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
ebay.co.uk
Welcome! Sign in or register
Advanced Search
Categories ▾
Shops
eBay Motors
Safe

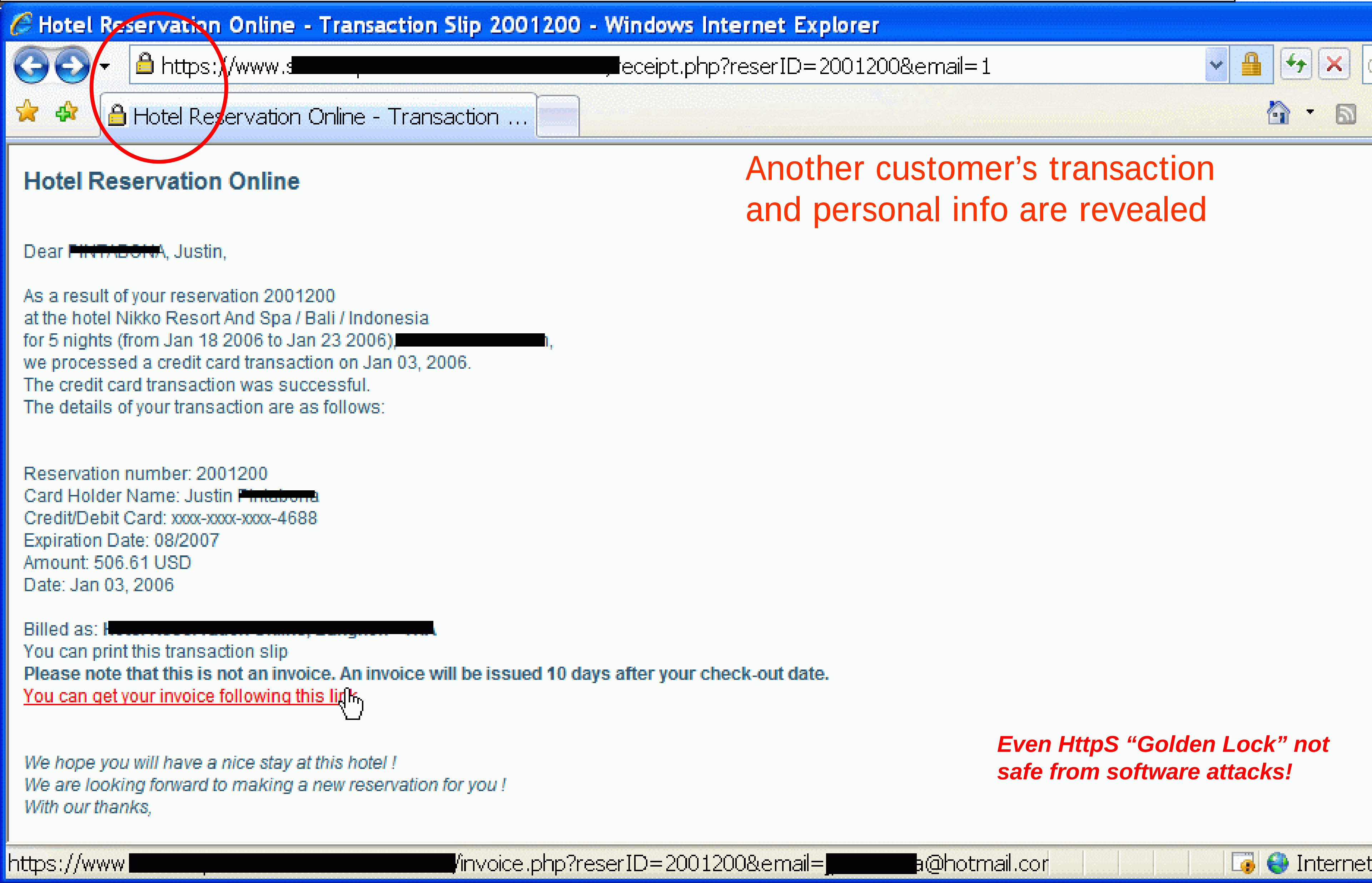
Home > Business Centre > Changes in 2008 > Changes to Pricing

```
# 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 - eB
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 - eB
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 : Travel & Hotel Reservation Site

Reading another user’s transaction – insufficient authorization



Hotel Reservation Online - Transaction Slip 2001200 - Windows Internet Explorer

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

Another customer’s transaction and personal info are revealed

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,

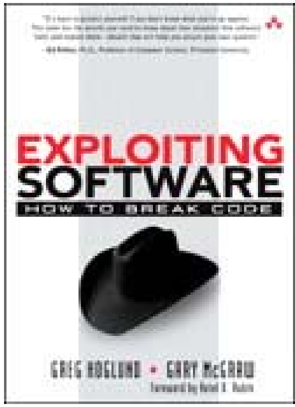
Even HttpS “Golden Lock” not safe from software attacks!

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

Web Application Attacks are a Business Issue

Application Threat	Negative Impact	Potential Business Impact
Buffer overflow	Denial of Service (DoS)	Site Unavailable; Customers Gone
Cookie poisoning	Session Hijacking	Larceny, theft
Hidden fields	Site Alteration	Illegal transactions
Debug options	Admin Access	Unauthorized access, privacy liability, site compromised
Cross Site scripting	Identity Theft	Larceny, theft, customer mistrust
Stealth Commanding	Access O/S and Application	Access to non-public personal information, fraud, etc.
Parameter Tampering	Fraud, Data Theft	Alter distributions and transfer accounts
Forceful Browsing / SQL Injection	Unauthorized Site/Data Access	Read/write access to customer databases

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



2009

1 Unvalidated Input

2 Broken Access Control

3 Broken Authentication and Session Management

4 Cross Site Scripting Flaws

5 Buffer Overflows

6 Injection Flaws

7 Improper Error Handling

8 Insecure Storage

9 *Denial of Service*

10 Insecure Configuration Management

2010

1 Injection

2 Cross-Site Scripting (XSS)

3 Broken Authentication and Session Management

4 Insecure Direct Object References

5 Cross-Site Request Forgery (CSRF)

6 Security Misconfiguration

7 Insecure Cryptographic Storage

8 Failure to Restrict URL Access

9 Insufficient Transport Layer Protection

10 Unvalidated Redirects and Forwards

WHY CAN HACKERS ATTACK WEB APPLICATIONS?

- **Developers are mandated to deliver functionality on-time and on-budget - but not to develop secure applications**
  - **Developers often short on training, budget, resources, timeline, companies do not have secure software policy**
- **IT Security professionals usually from network/infra side**
  - **They are usually not knowledgeable or interested in programming**
  - **Network scanners won't find application vulnerabilities**
  - **Developers are usually not interested in network or security**
- **Product innovation is driving development of increasingly complicated software for a Smarter Planet *(apps >200,000 lines)***

Volumes of applications continue to be deployed that are riddled with security flaws…

…and are non compliant with industry regulations

OUR GOAL IS TO WRITE BUG-FREE SOFTWARE. I'LL PAY A TEN-DOLLAR BONUS FOR EVERY BUG YOU FIND AND FIX.
S. Adams E-mail: SCOTTADAMS@AOL.COM
YAHOO!
WE'RE RICH
YES!!! YES!!! YES!!!
11/3 © 1995 United Feature Syndicate, Inc.(NYC)
I HOPE THIS DRIVES THE RIGHT BEHAVIOR.
I'M GONNA WRITE ME A NEW SUV THIS AFTER-NOON!

CHEAP
FAST
GOOD

Make Applications Secure, by Design

Security as an Intrinsic Property of the Development Process

Design Phase

- Consideration is given to security requirements of the application
- Issues such as required controls and best practices are documented on par with functional requirements

Development Phase

- Software is checked during coding for:
  - Implementation error vulnerabilities
  - Compliance with security requirements

Build & Test Phase

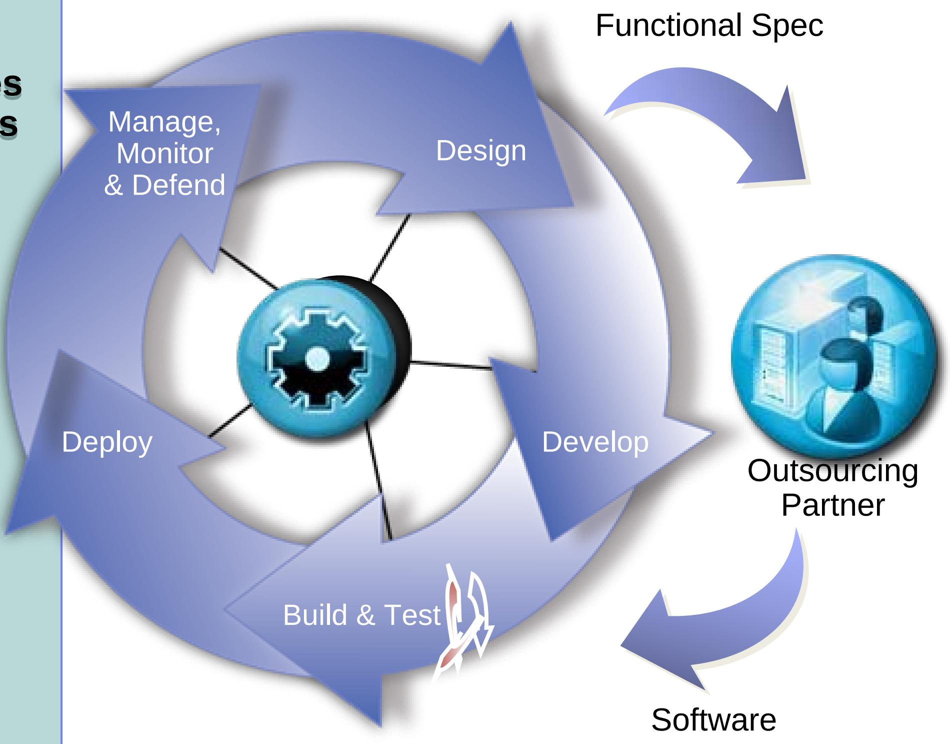
- Testing begins for errors and compliance with security requirements across the entire application
- Applications are also tested for exploitability in deployment scenario

Deployment Phase

- Configure infrastructure for application policies
- Deploy applications into production

Operational Phase

- Continuously monitor applications for appropriate application usage, vulnerabilities and defend against attacks



Web Application Security - Solution Strategy

- **Objective - Reduce Remediation Work, Cost and Time to Market**
  - Find the issues earlier in the Software Development Life Cycle
  - **Automate the process**
  - Use less security-savvy employees by using **Professional TOOLS (train the users!)**

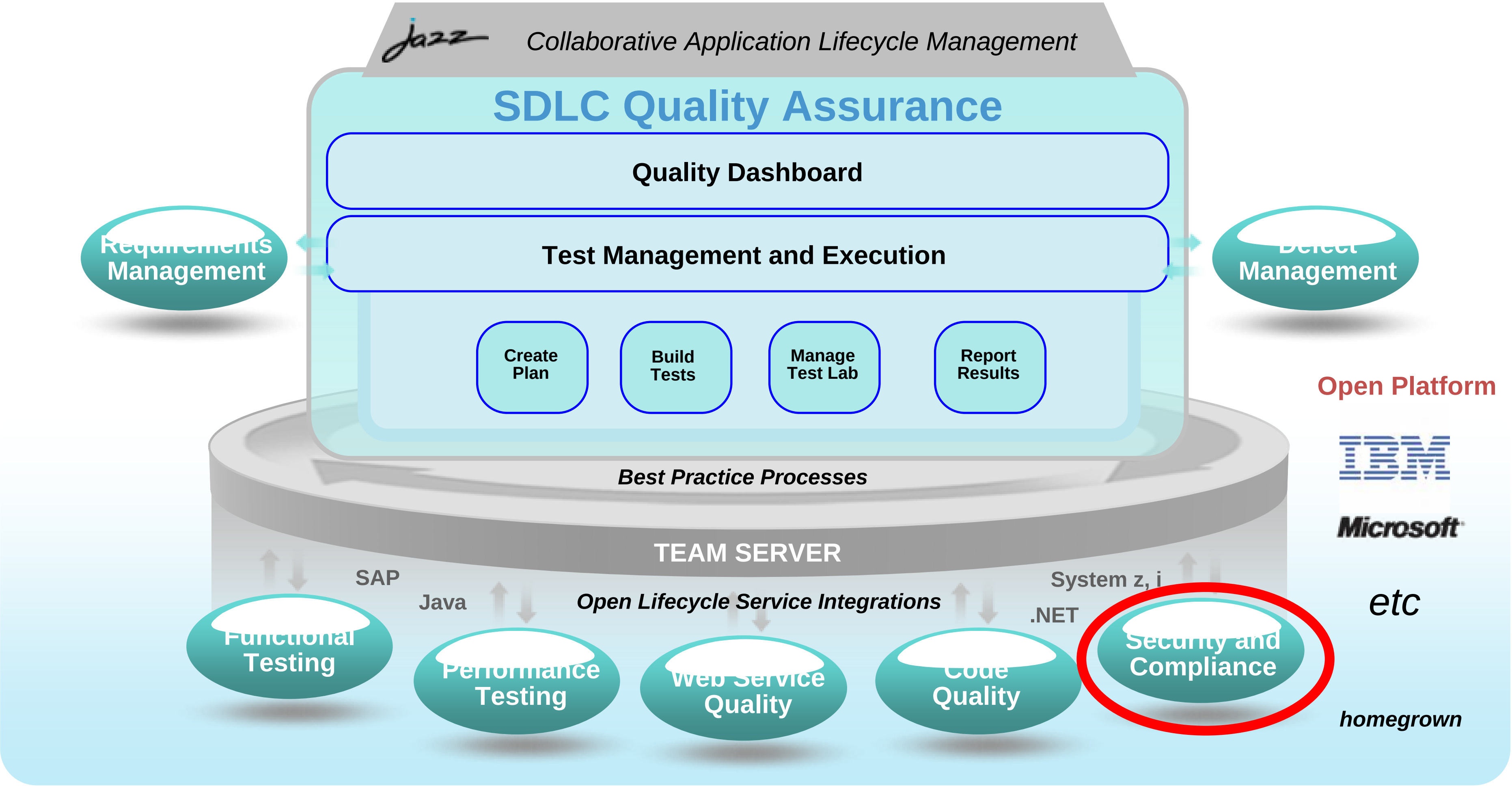
- **Mitigate Risk and increase quality**
  - Increase coverage
  - **Involve more people in the process of Software Security QA – not just development team**
    - **Need executive sponsor - business dept owner, project owner, etc.**

- **Increase Visibility Of The Security Issue**
  - Distribute reports to different levels
  - Management Dashboards (from the Professional TOOLS)

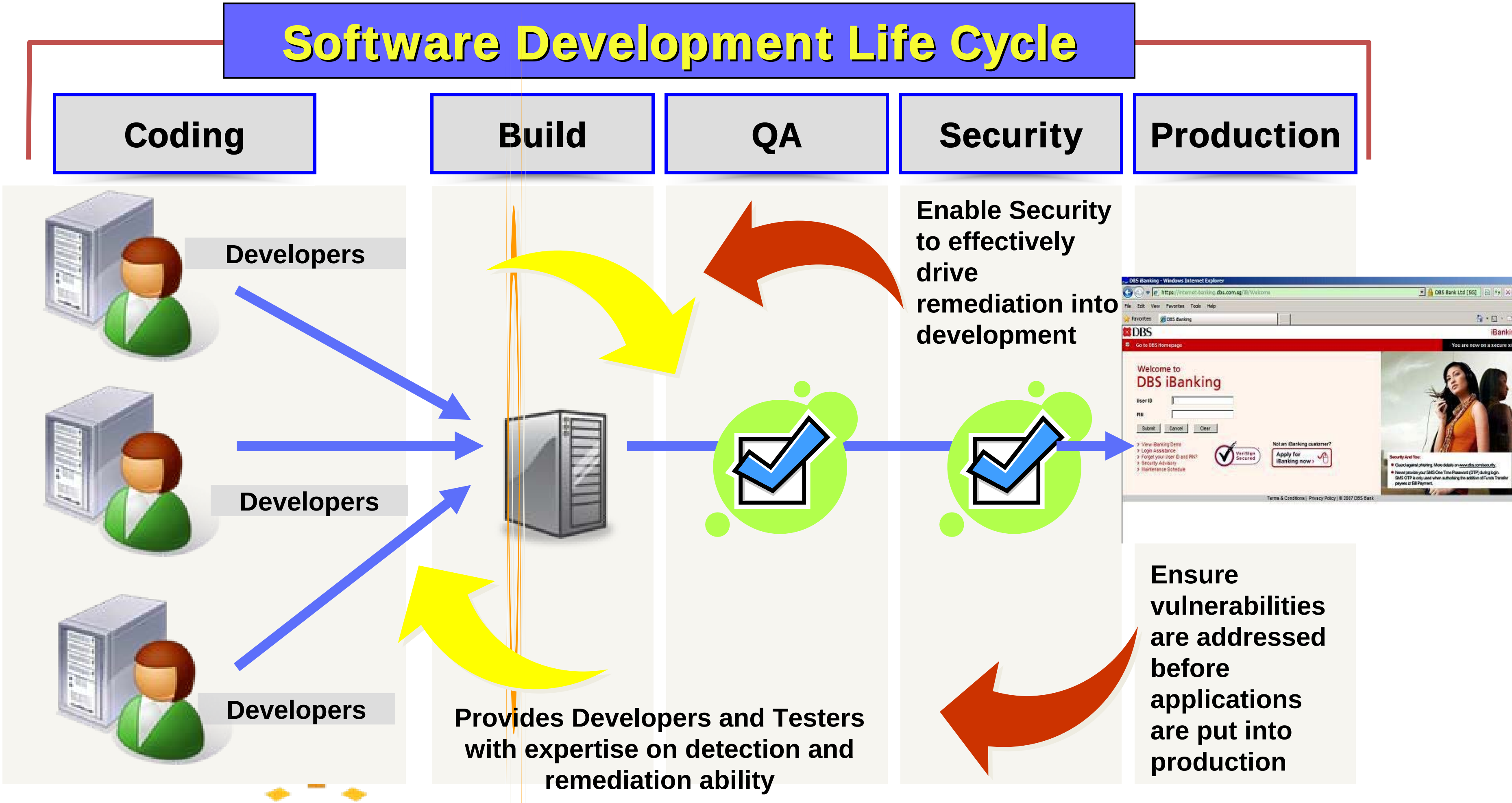
- **Increase Productivity**
  - **Build the knowledge among the team – HAVE A SECURE CODING TRAINING PROGRAM**
  - Prevent making the same mistakes

SECURITY TESTING IS PART OF SDLC QUALITY TESTING

Software Development Life Cycle



Building security & compliance into the SDLC itself



Enable Security to effectively drive remediation into development

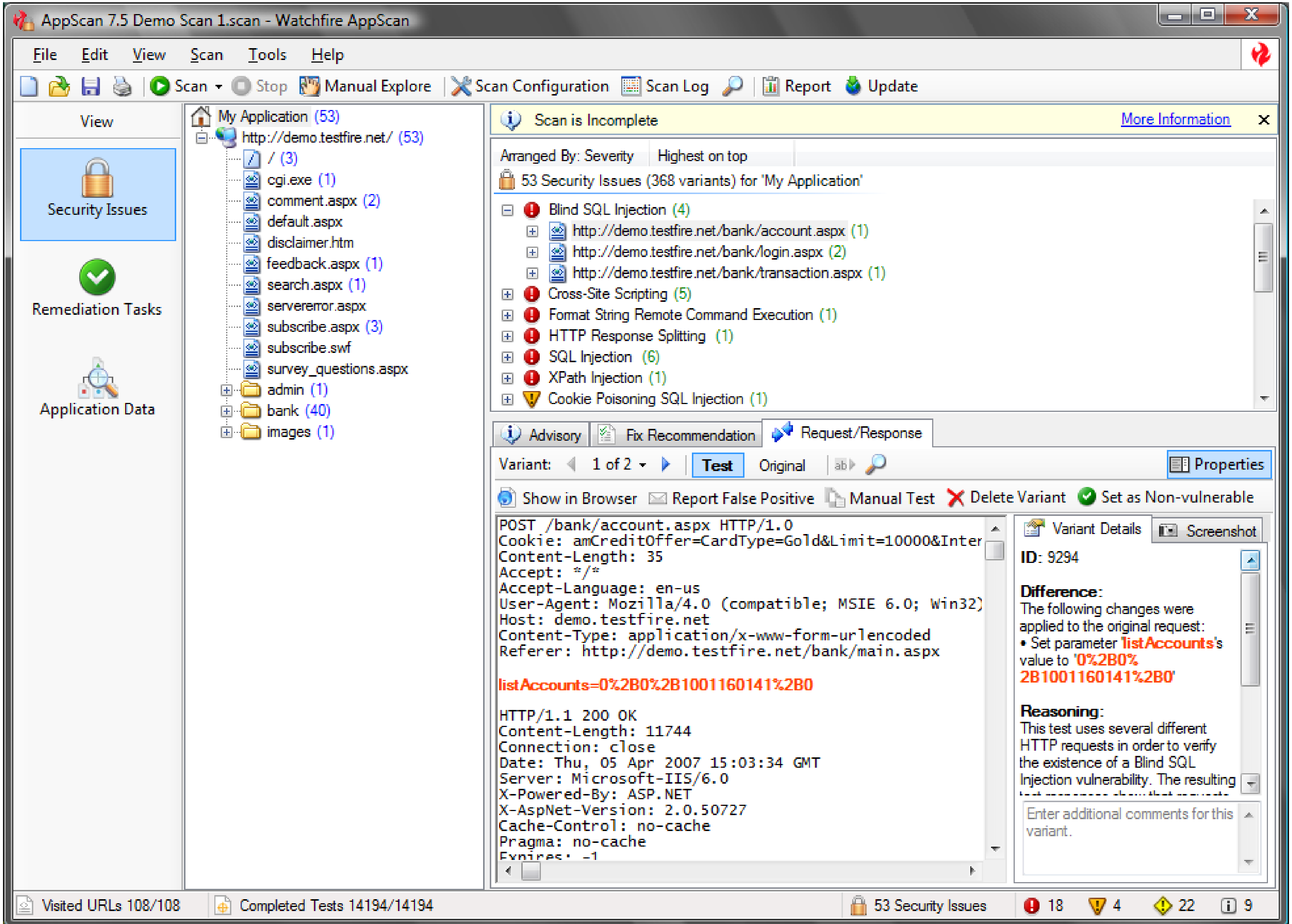
Provides Developers and Testers with expertise on detection and remediation ability

Ensure vulnerabilities are addressed before applications are put into production

CSSLP
Certified Secure Software Lifecycle Professional

APPSCAN – A professional software solution that SCAN THE APPLICATION to

Identify Vulnerabilities



AppScan 7.5 Demo Scan 1.scan - 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)
    - / (3)
    - cgi.exe (1)
    - comment.aspx (2)
    - default.aspx
    - disclaimer.htm
    - feedback.aspx (1)
    - search.aspx (1)
    - servererror.aspx
    - subscribe.aspx (3)
    - subscribe.swf
    - survey_questions.aspx
    - admin (1)
    - bank (40)
    - images (1)

Scan is Incomplete — More Information

Arranged By: Severity — Highest on top

53 Security Issues (368 variants) for 'My Application'

- Blind SQL Injection (4)
  - http://demo.testfire.net/bank/account.aspx (1)
  - http://demo.testfire.net/bank/login.aspx (2)
  - http://demo.testfire.net/bank/transaction.aspx (1)
- 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 · Properties

Show in Browser · Report False Positive · Manual Test · Delete Variant · Set as Non-vulnerable

```
POST /bank/account.aspx HTTP/1.0
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Inter
Content-Length: 35
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=0%2B0%2B1001160141%2B0

HTTP/1.1 200 OK
Content-Length: 11744
Connection: close
Date: Thu, 05 Apr 2007 15:03:34 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
Pragma: no-cache
Expires: -1
```

Variant Details · Screenshot

ID: 9294

Difference:
The following changes were applied to the original request:
• Set parameter 'listAccounts's value to '0%2B0%2B1001160141%2B0'

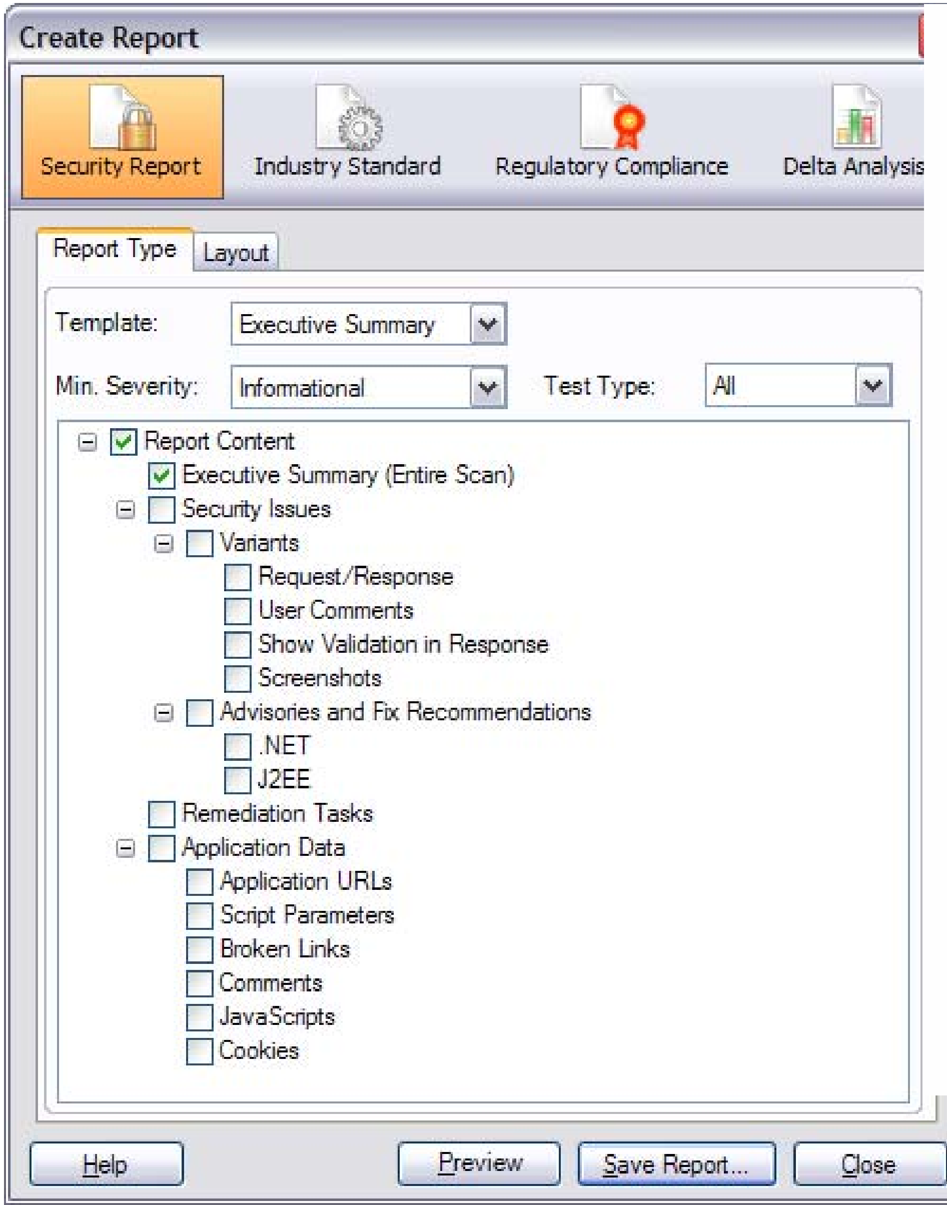
Reasoning:
This test uses several different HTTP requests in order to verify the existence of a Blind SQL Injection vulnerability. The resulting

Enter additional comments for this variant.

Visited URLs 108/108 · Completed Tests 14194/14194 · 53 Security Issues · 18 · 4 · 22 · 9

With Rich Report Options

44 Regulatory Compliance Standards, for Executive, Security, Developers, PLUS customizable test criteria.



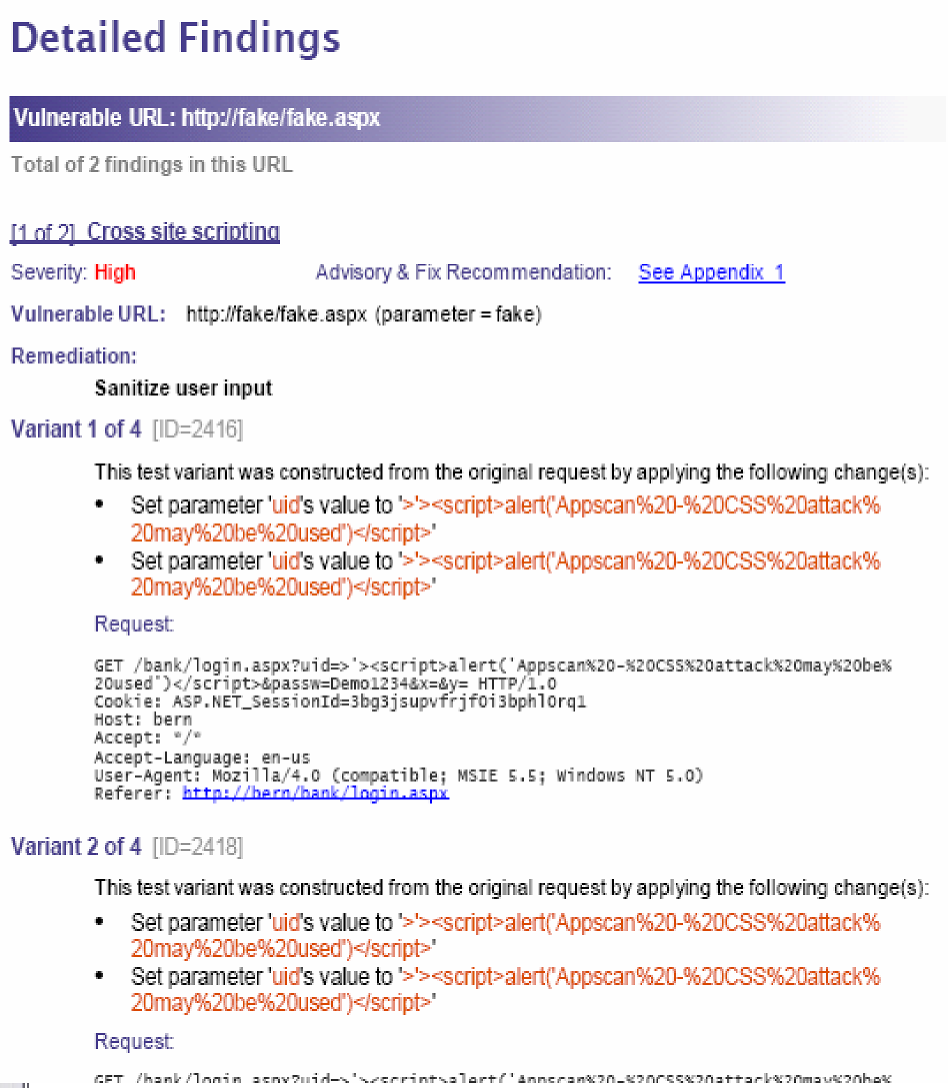
Create Report

Template: Executive Summary

Min. Severity: Informational

Test Type: All

- ☑ Report Content
  - ☑ Executive Summary (Entire Scan)
  - □ Security Issues
    - □ Variants
      - □ Request/Response
      - □ User Comments
      - □ Show Validation in Response
      - □ Screenshots
    - □ Advisories and Fix Recommendations
      - □ .NET
      - □ J2EE
  - □ Remediation Tasks
  - □ Application Data
    - □ Application URLs
    - □ Script Parameters
    - □ Broken Links
    - □ Comments
    - □ JavaScripts
    - □ Cookies



Detailed Findings

Vulnerable URL: http://fake/fake.aspx

Total of 2 findings in this URL

[1 of 2] Cross site scripting

Severity: High   Advisory & Fix Recommendation: See Appendix 1

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

Remediation:

Sanitize user input

Variant 1 of 4 [ID=2416]

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

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

Request:

```
GET /bank/login.aspx?uid=>'><script>alert('Appscan%20-%20CSS%20attack%20may%20be%
20used')</script>&passw=Demo1234&x=&y= HTTP/1.0
Cookie: ASP.NET_SessionId=3bg3jsupvfrjf0i3bphl0rq1
Host: bern
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
Referer: http://bern/bank/login.aspx
```

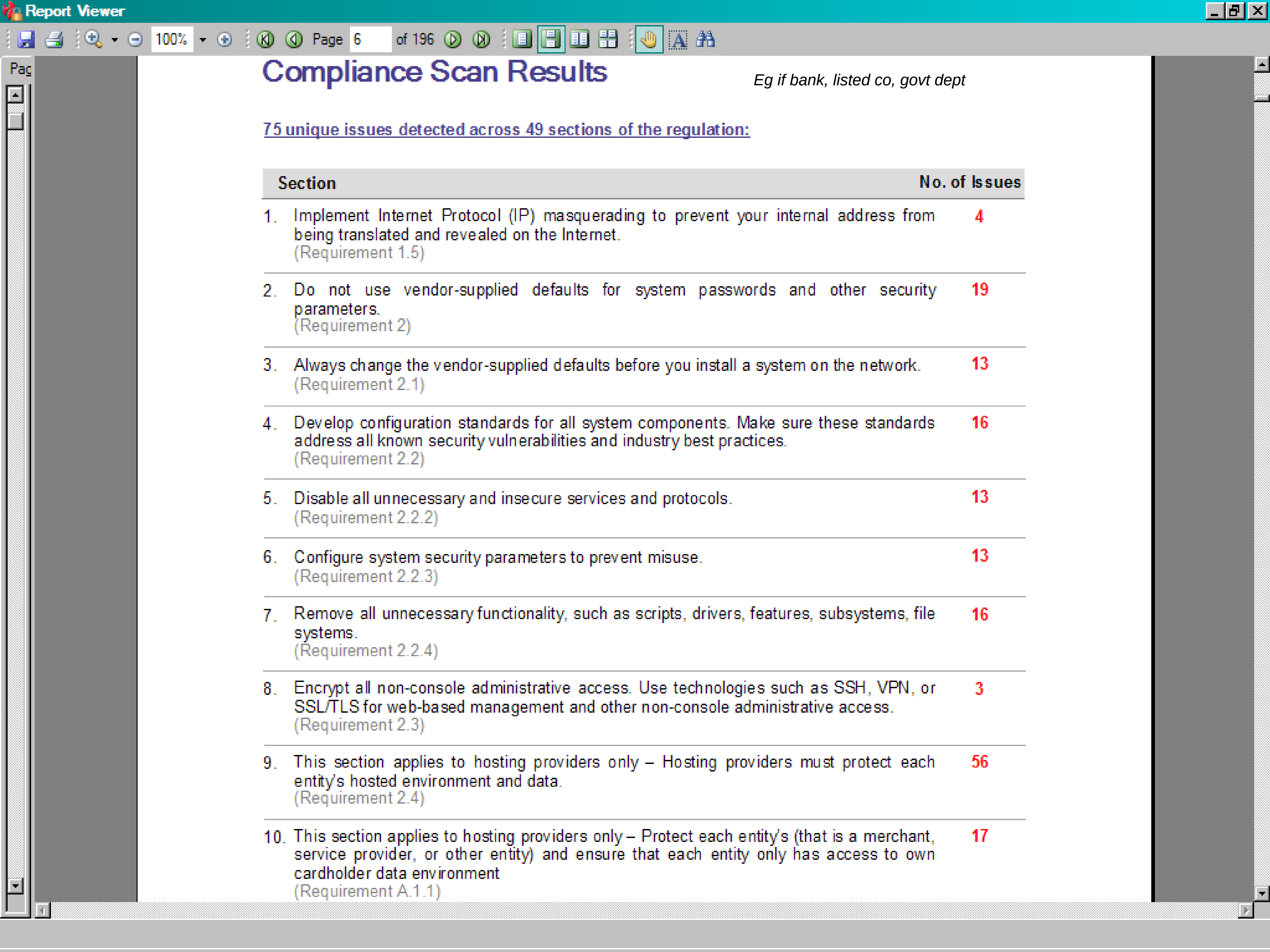
Variant 2 of 4 [ID=2418]

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

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

Request:

```
GET /bank/login.aspx?uid=>'><script>alert('Appscan%20-%20CSS%20attack%20may%20be%
```



Compliance Scan Results

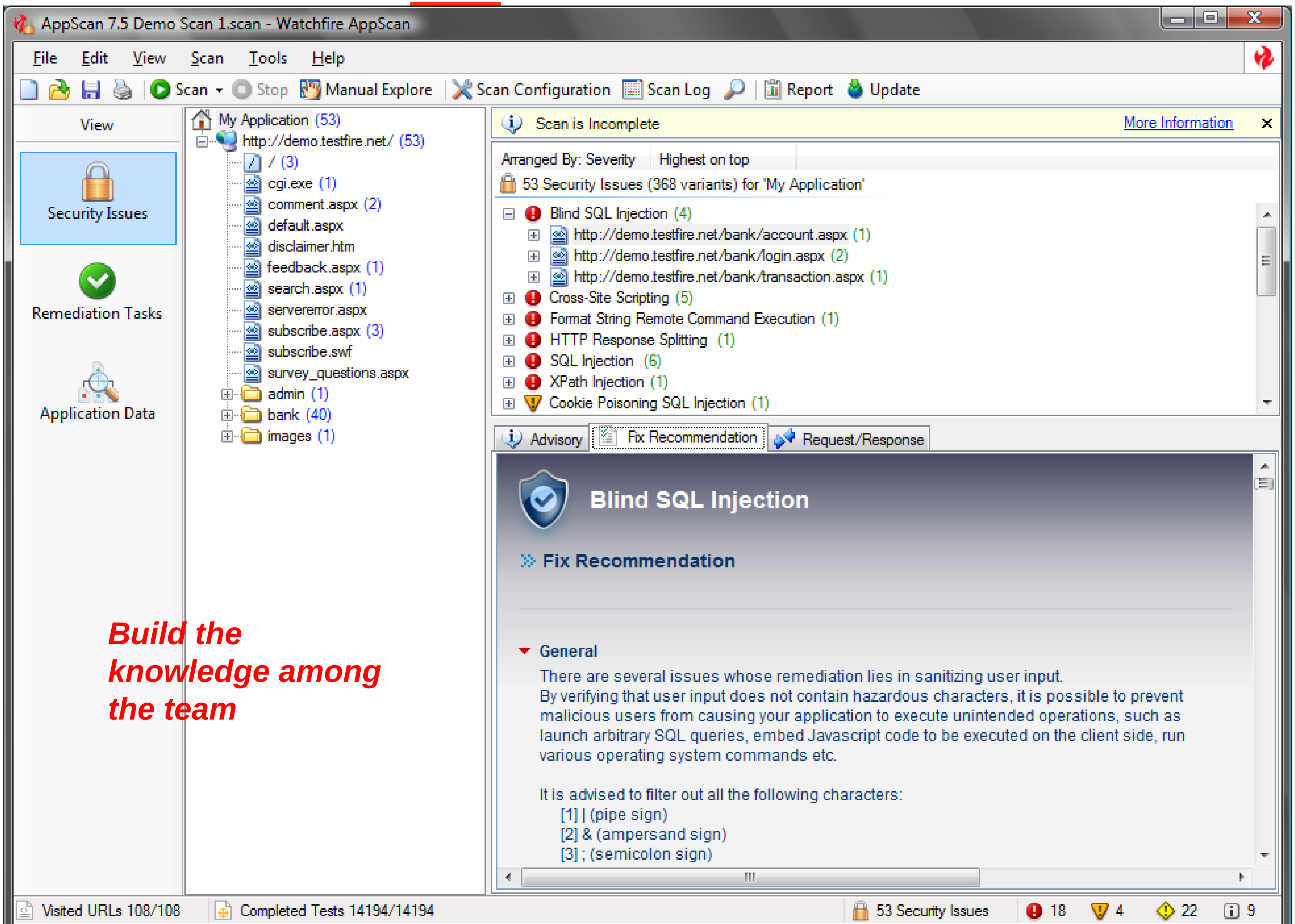
Eg if bank, listed co, govt dept

75 unique issues detected across 49 sections of the regulation:

	Section	No. of Issues
1.	Implement Internet Protocol (IP) masquerading to prevent your internal address from being translated and revealed on the Internet. (Requirement 1.5)	4
2.	Do not use vendor-supplied defaults for system passwords and other security parameters. (Requirement 2)	19
3.	Always change the vendor-supplied defaults before you install a system on the network. (Requirement 2.1)	13
4.	Develop configuration standards for all system components. Make sure these standards address all known security vulnerabilities and industry best practices. (Requirement 2.2)	16
5.	Disable all unnecessary and insecure services and protocols. (Requirement 2.2.2)	13
6.	Configure system security parameters to prevent misuse. (Requirement 2.2.3)	13
7.	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems. (Requirement 2.2.4)	16
8.	Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access. (Requirement 2.3)	3
9.	This section applies to hosting providers only – Hosting providers must protect each entity's hosted environment and data. (Requirement 2.4)	56
10.	This section applies to hosting providers only – Protect each entity's (that is a merchant, service provider, or other entity) and ensure that each entity only has access to own cardholder data environment (Requirement A.1.1)	17

And Most Important :

Actionable Fix Recommendations



My Application (53)
http://demo.testfire.net/ (53)
/ (3)
cgi.exe (1)
comment.aspx (2)
default.aspx
disclaimer.htm
feedback.aspx (1)
search.aspx (1)
servererror.aspx
subscribe.aspx (3)
subscribe.swf
survey_questions.aspx
admin (1)
bank (40)
images (1)

Scan is Incomplete

Arranged By: Severity | Highest on top

53 Security Issues (368 variants) for 'My Application'

- Blind SQL Injection (4)
  - http://demo.testfire.net/bank/account.aspx (1)
  - http://demo.testfire.net/bank/login.aspx (2)
  - http://demo.testfire.net/bank/transaction.aspx (1)
- 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)

Blind SQL Injection

Fix Recommendation

General

There are several issues whose remediation lies in sanitizing user input.
By verifying that user input does not contain hazardous characters, it is possible to prevent malicious users from causing your application to execute unintended operations, such as launch arbitrary SQL queries, embed Javascript code to be executed on the client side, run various operating system commands etc.

It is advised to filter out all the following characters:
[1] | (pipe sign)
[2] & (ampersand sign)
[3] ; (semicolon sign)

Visited URLs 108/108 | Completed Tests 14194/14194 | 53 Security Issues | 18 | 4 | 22 | 9

Build the knowledge among the team

Summary:
Rational Appscan - Web Application Security by QA

- Cloud services today are expected to have the usual security solutions: Firewall, IPS, authentication … etc
  - **Hackers know this too, so they need to find a new way to attack and steal data**
  - Hence they are attacking SOFTWARE APPLICATIONS today
- **Firewalls etc do not stop application attacks**
  - The cloud is one big rich software environment to attract hackers
  - in the cloud there is no way to monitor and stop hacker activities
  - **THE APPLICATION MUST DEFEND ITSELF**
- **APPSCAN VALUE PROPOSITION**
  - A professional software solution tool that
    - **SCANS THE APPLICATION TO FIND BUGS, FLAWS, CODING IMPERFECTIONS**
    - **Flags the errors – types, priorities, locations, quantities**
    - **Generate a variety of reports**
    - **Offers instruction to developers on how to fix the applications**
      - **Appscan "hardens" the application to make it resistant to hacker attacks.**
      - **This is the best and only way to stop an application attack**

Introducing IBM Secure by Design

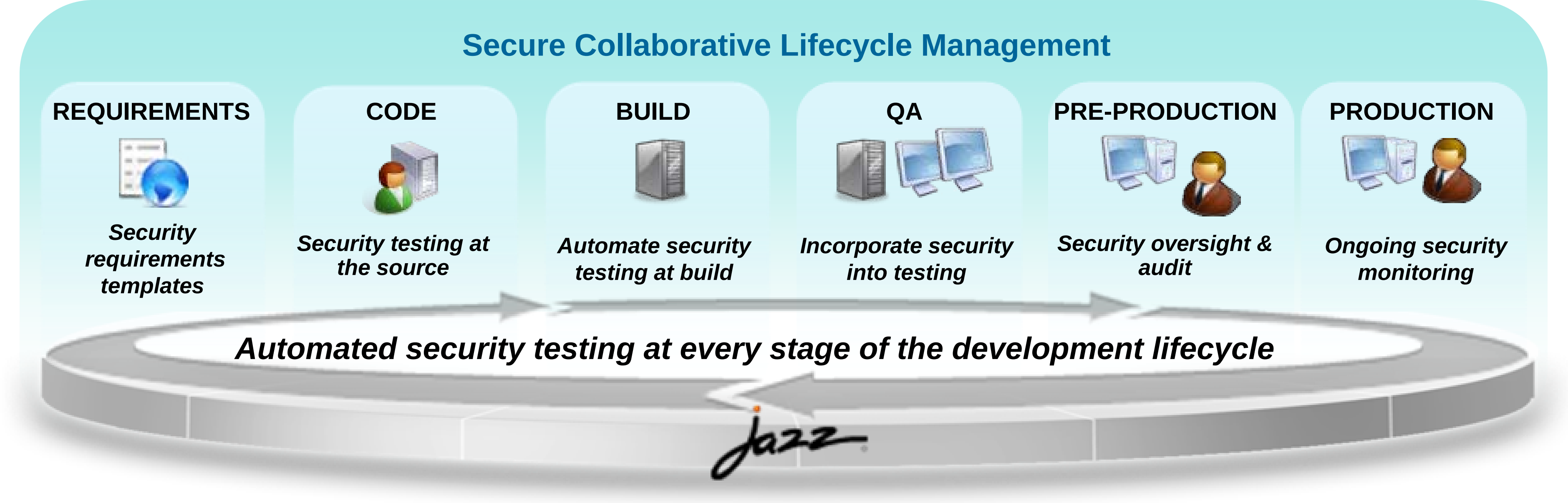
Automate security testing early & often throughout the development lifecycle

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

Deliver New Services Faster

Innovate Securely

Reduce Costs



Secure Collaborative Lifecycle Management

REQUIREMENTS
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
jazz

Automated security testing at every stage of the development lifecycle

Mobile App Question

Question: Which feature is not a key capability in Rational Appscan?

A. securing the endpoint
B. scanning applications for vulnerabilities
C. 44 regulatory compliance standards
D. actionable fix recommendations

Is Your Web App-solutely Secure?

02 Aug 2011
Bangkok

Anthony Lim

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

www.ibm.com/security