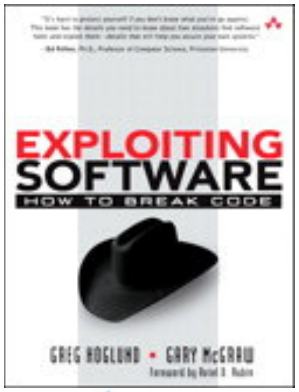
IBM SOFTWARE CONFERENCE 2011
Powered by Impact & Innovate 2011


# Is Your Web App-soultely Secure?





## *Anthony Lim*

***MBA FCITIL CISSP CSSLP***

*Asia Pacific Business Unit Executive*

*Security*

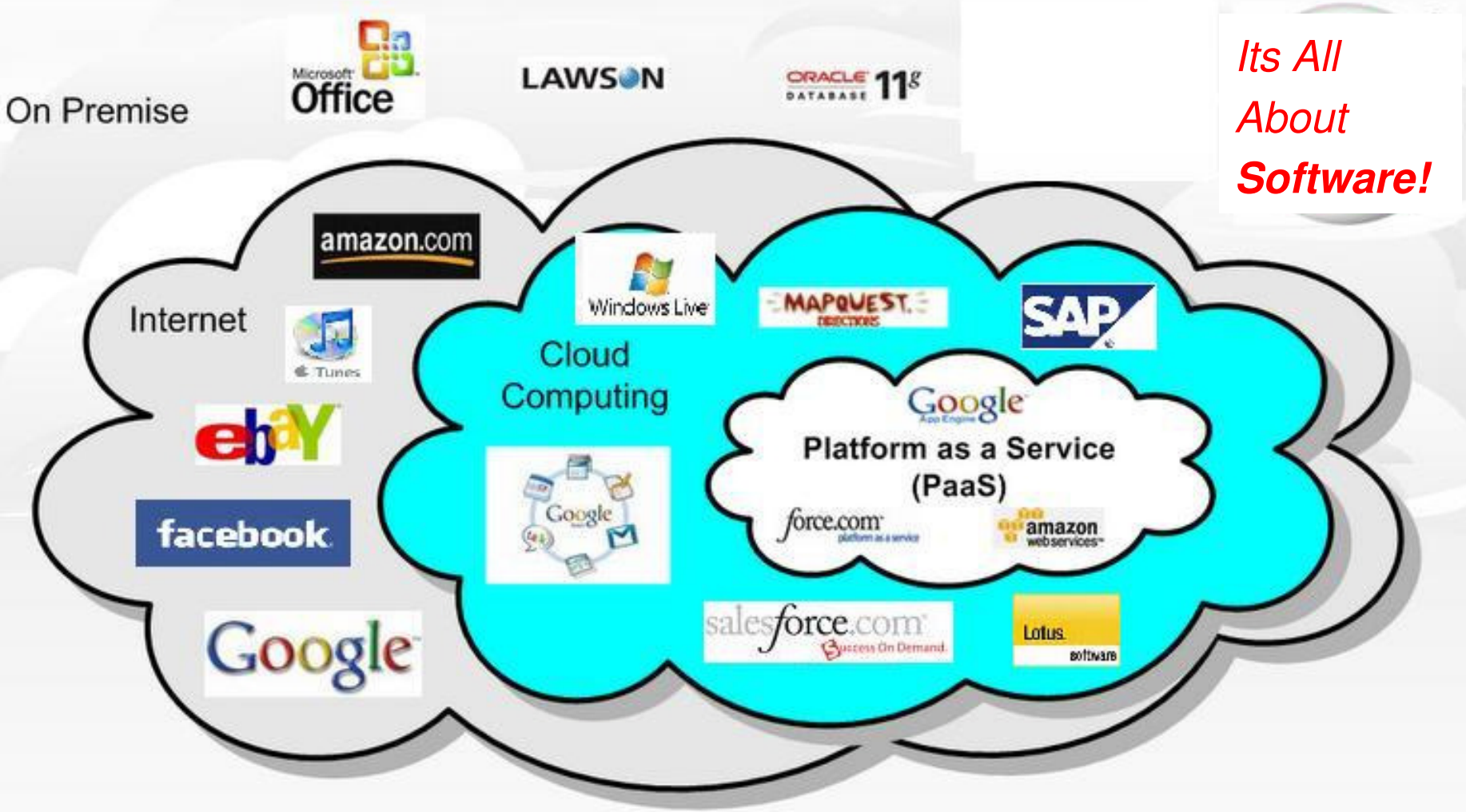
*Rational Software*


**27July 2011**

**Kuala Lumpur**

CSSLP
Certified Secure Software Lifecycle Professional

# The Wonders of Cloud Computing



IBM SOFTWARE CONFERENCE 2011
Powered by Impact & Innovate 2011

# Welcome to THE SMARTER PLANET

IBM

## Globalization and Globally Available Resources

**- Instrumented, Interconnected, Intelligent**

**Billions of mobile devices accessing the Web**



**Access to streams of information in the Real Time**

## CLOUD COMPUTING

***CUSTOMER ACCESSING PORTAL SERVICES FROM SMARTPHONES – EG IPHONES, ANDROID DEVICES***

***ITS ALL ABOUT SOFTWARE!***

# Customer Concerns with Cloud Computing

- LOSS OF GOVERNANCE
  - TRUST in the provider is paramount.
- COMPLIANCE RISKS
- ISOLATION FAILURE
- Hard to have "Personalized" Security Features
- DATA HANDLING
  - DATA PROTECTION
  - INSECURE or INCOMPLETE DATA DELETION:
- MANAGEMENT INTERFACE COMPROMISE
  - Monitoring & reporting difficulties
- MALICIOUS INSIDER
  - Or incompetent / careless insider / operator

* 2009 European Network and Information Security Agency (ENISA)
Cloud Computing: Benefits, risks and recommendations for information security

Gartner

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

# 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-

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 allows make use of online discussion 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 systems that are not directly connected to the Web.

The presence of files on the system, and the claim that no customer information was compromised could indicate that the hackers were able to get in but not complete their attack, he added.

Computer security experts have long warned that many companies are not do-

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

Home | GAGDET NEWS | GAMES NEWS | HARDWARE NEWS | INTERNET NEWS | SCI

# 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.

"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?!*

# How Do Hackers Attack Web Applications

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


April 5, 2010 3:32 PM PDT

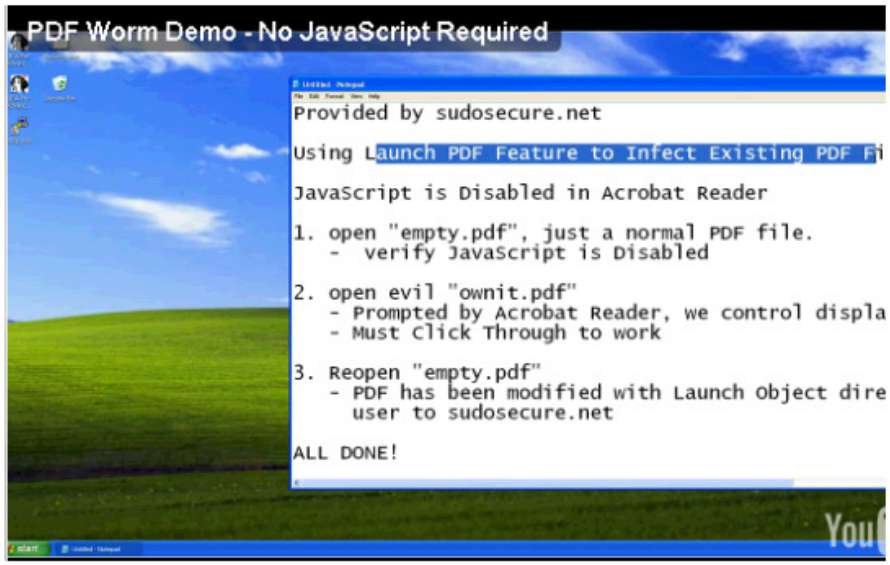
Exploits not needed to attack via PDF files

by Elinor Mills

9 con

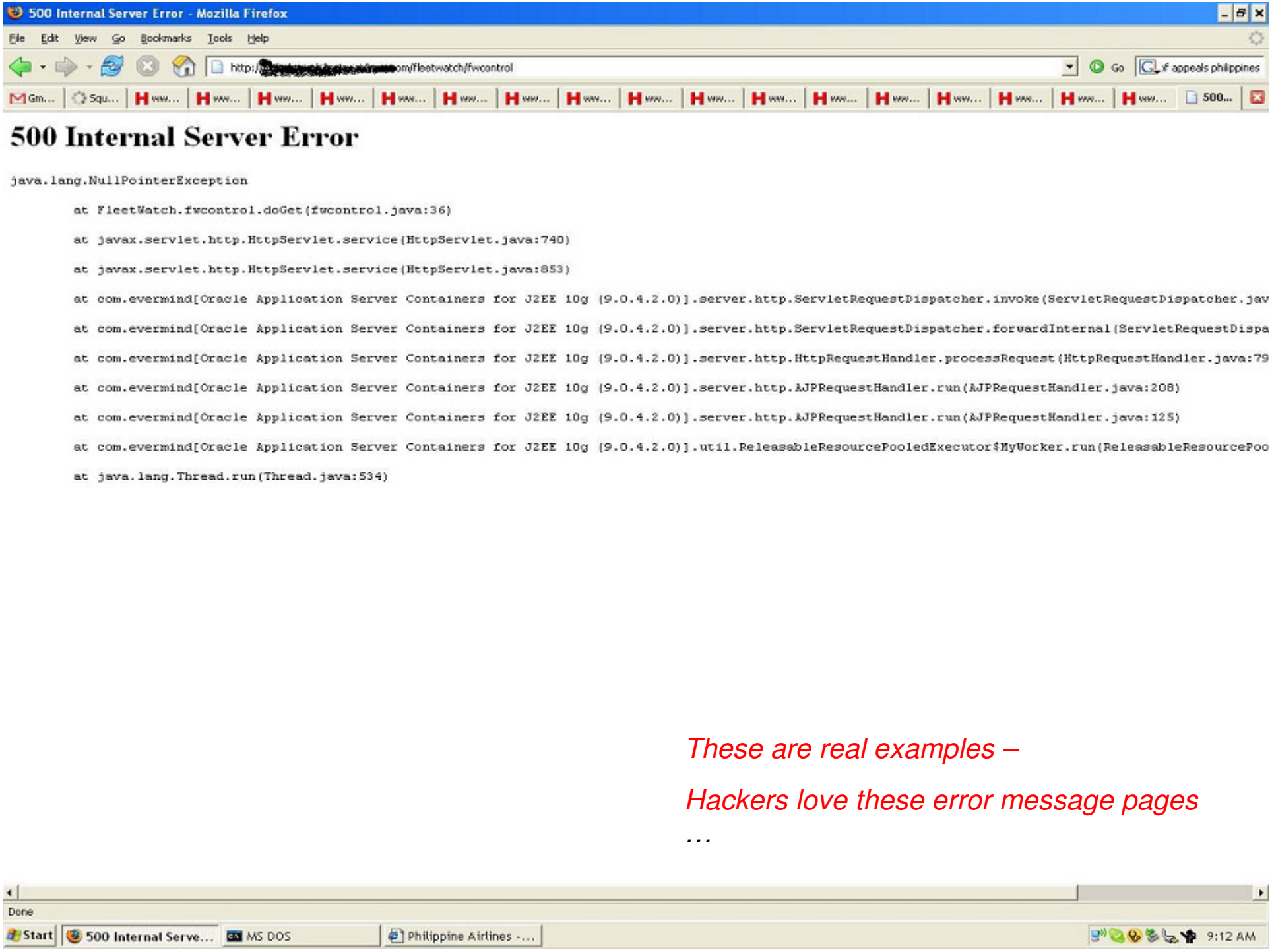
77 retweet Share 23

- **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*



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

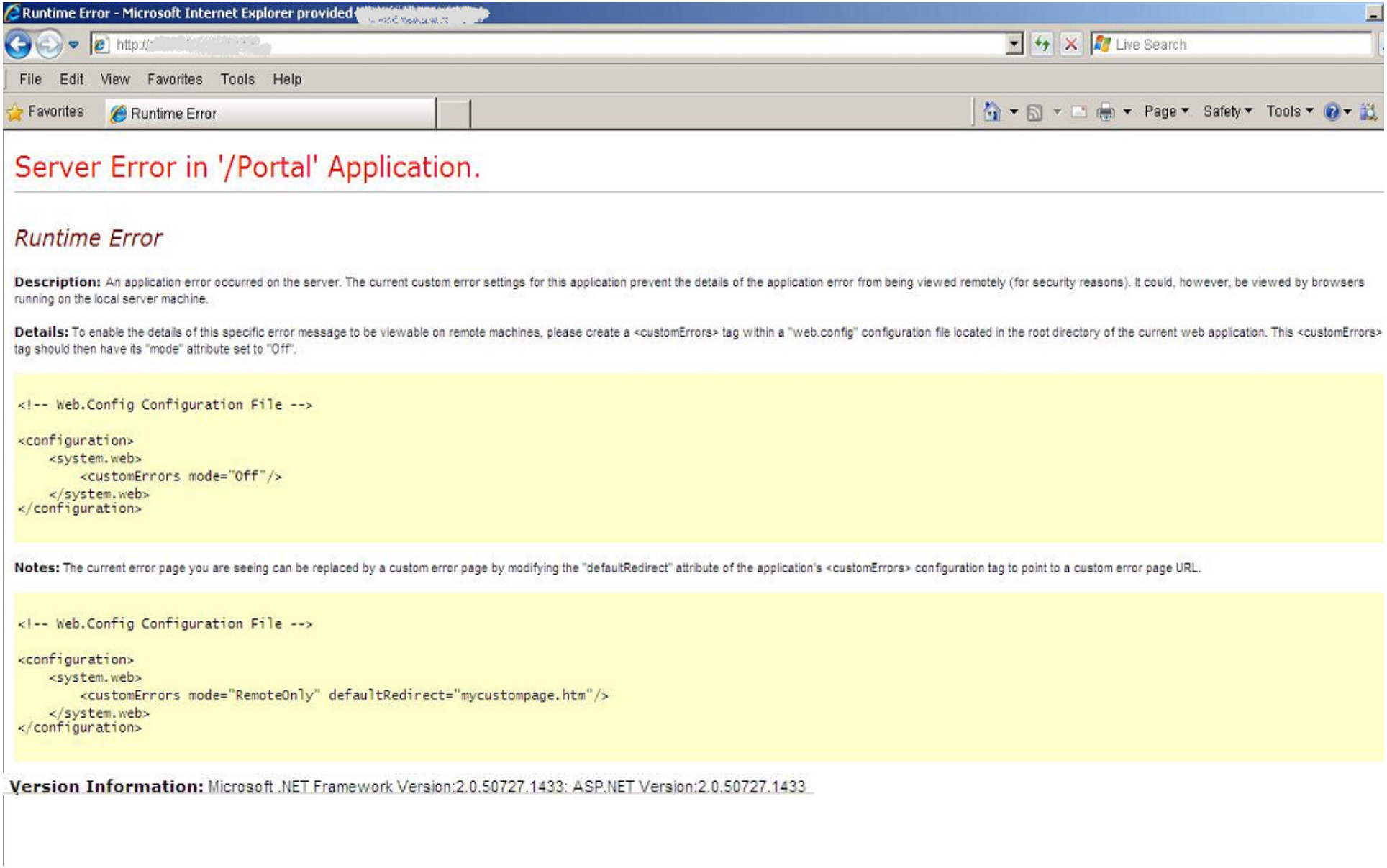
- **Applications can be HIJACKED** to make it perform its tasks but for an authorised user, or send data to an unauthorised recipient, etc.
  - Eg. *Cross-site Scripting, SQL Injection*



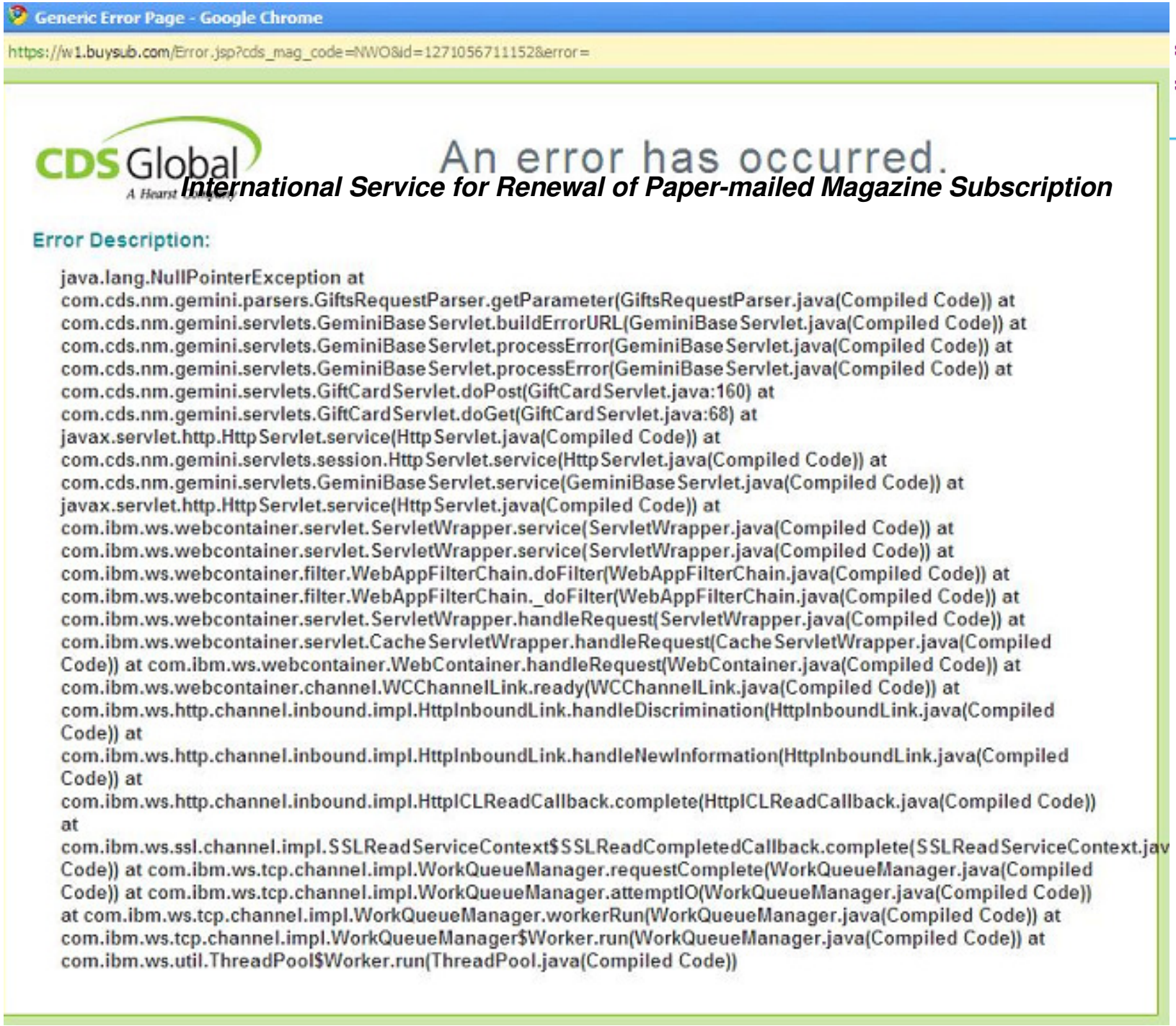

*These are real examples –*

*Hackers love these error message pages*

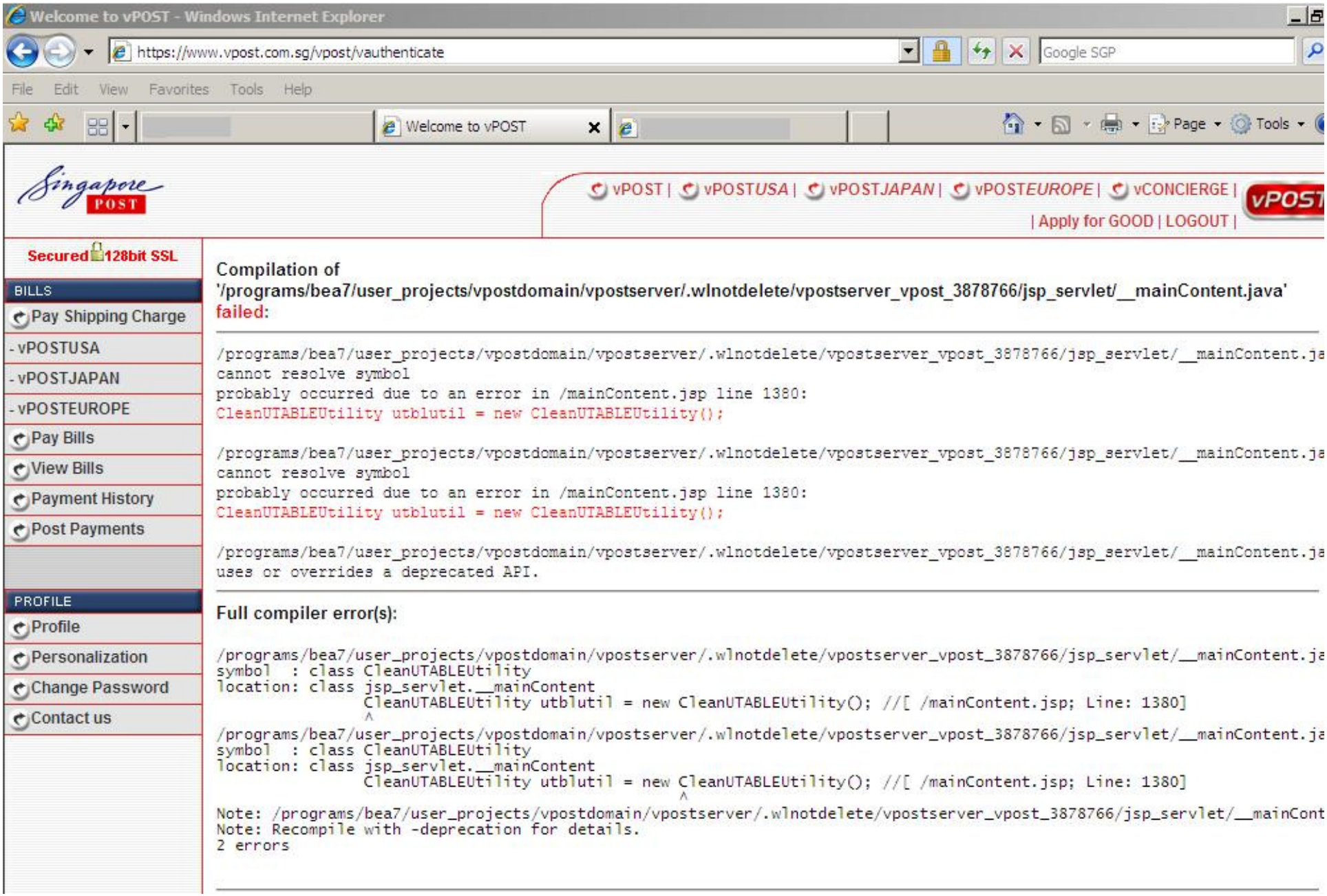
*…*

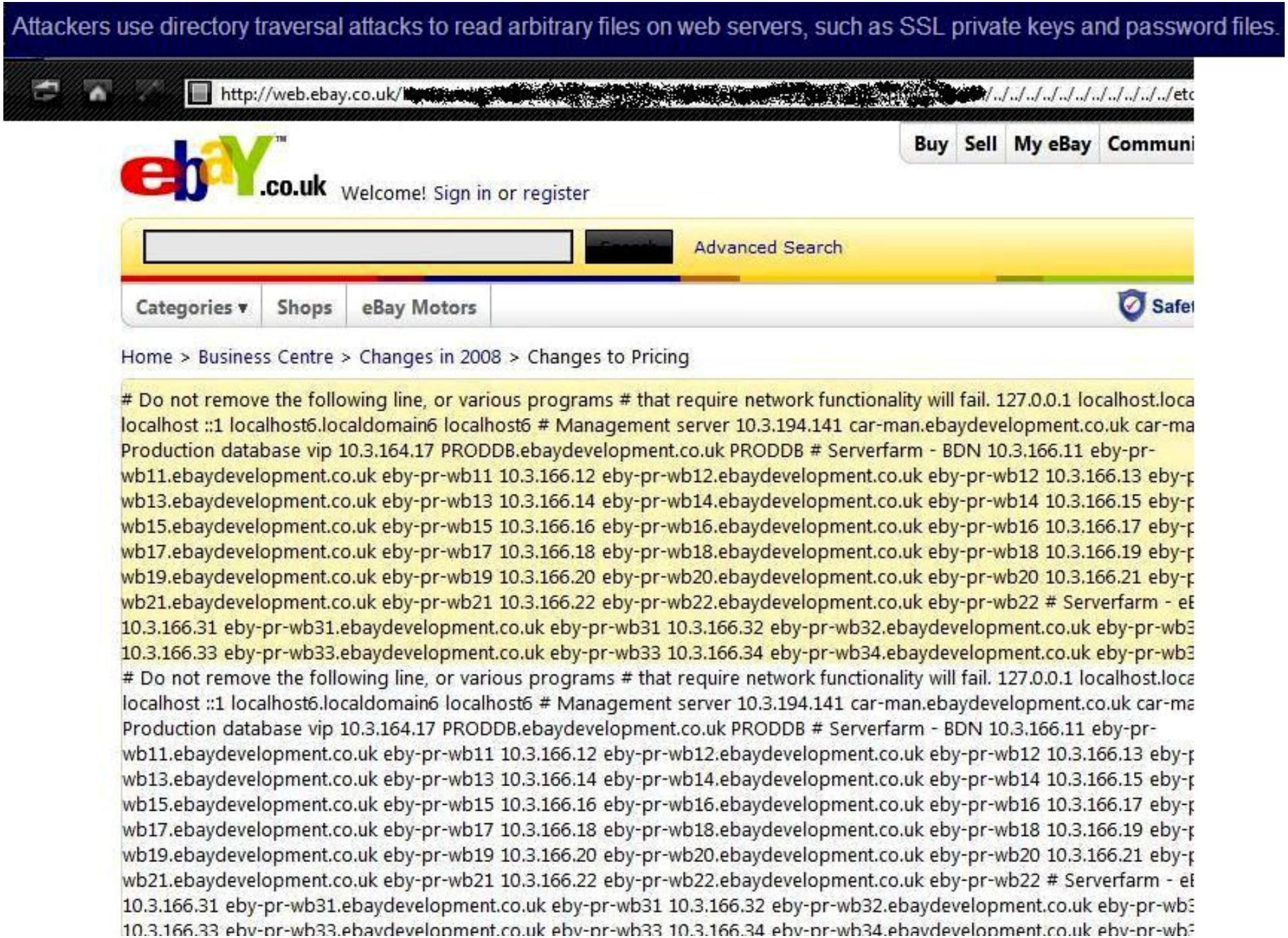



*"Self-inflicted" Social Engineering?!*



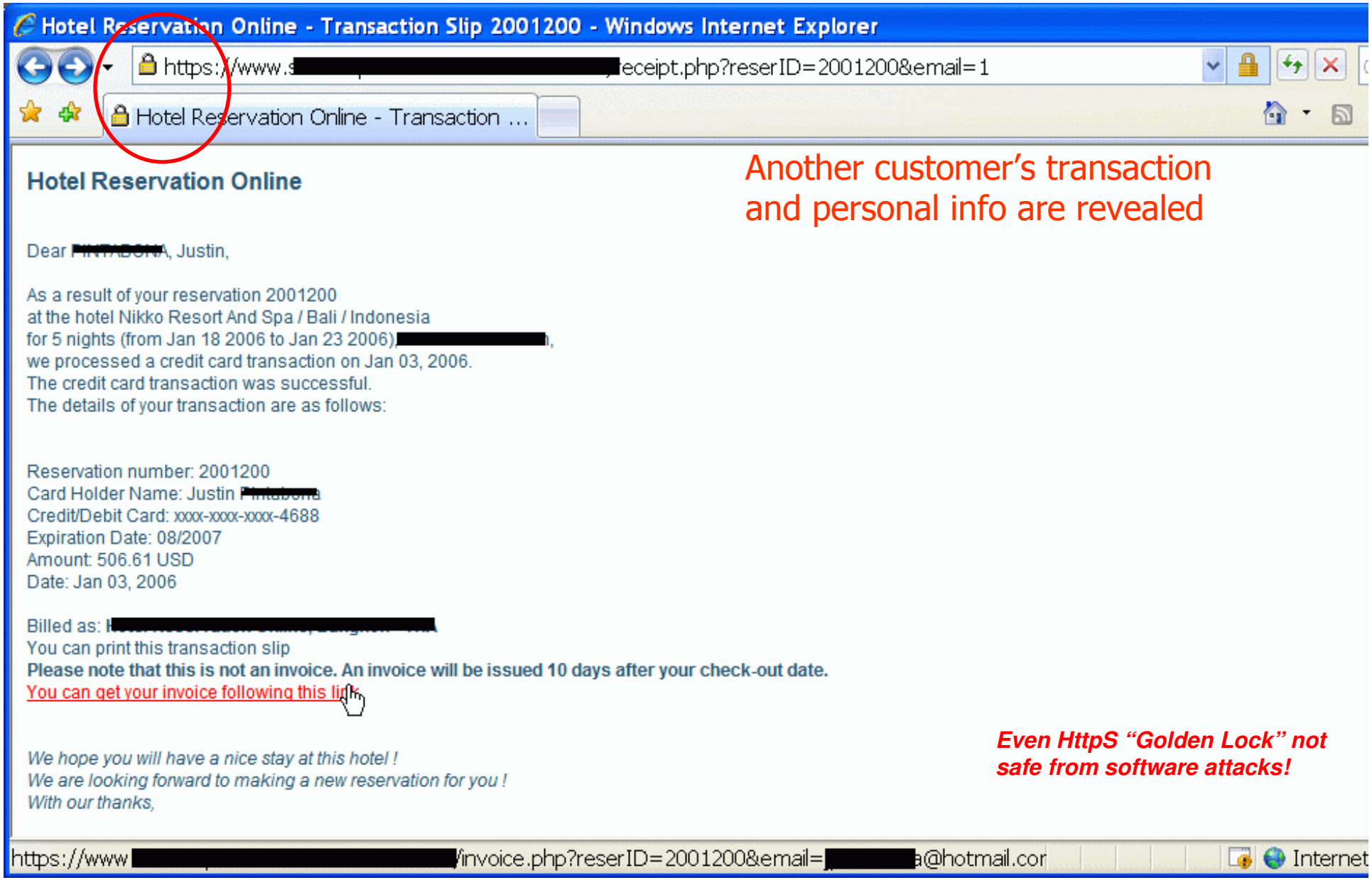

***International Service for Renewal of Paper-mailed Magazine Subscription***


Welcome to vPOST - Windows Internet Explorer
https://www.vpost.com.sg/vpost/vauthenticate
Google SGP
File Edit View Favorites Tools Help
Welcome to vPOST
Page Tools
Singapore POST
vPOST | vPOSTUSA | vPOSTJAPAN | vPOSTEUROPE | vCONCIERGE |
| Apply for GOOD | LOGOUT |
Secured 128bit SSL
BILLS
Pay Shipping Charge
- vPOSTUSA
- vPOSTJAPAN
- vPOSTEUROPE
Pay Bills
View Bills
Payment History
Post Payments
PROFILE
Profile
Personalization
Change Password
Contact us
Compilation of
'/programs/bea7/user_projects/vpostdomain/vpostserver/.wlnotdelete/vpostserver_vpost_3878766/jsp_servlet/__mainContent.java'
failed:
/programs/bea7/user_projects/vpostdomain/vpostserver/.wlnotdelete/vpostserver_vpost_3878766/jsp_servlet/__mainContent.ja
cannot resolve symbol
probably occurred due to an error in /mainContent.jsp line 1380:
CleanUTABLEUtility utblutil = new CleanUTABLEUtility();
/programs/bea7/user_projects/vpostdomain/vpostserver/.wlnotdelete/vpostserver_vpost_3878766/jsp_servlet/__mainContent.ja
cannot resolve symbol
probably occurred due to an error in /mainContent.jsp line 1380:
CleanUTABLEUtility utblutil = new CleanUTABLEUtility();
/programs/bea7/user_projects/vpostdomain/vpostserver/.wlnotdelete/vpostserver_vpost_3878766/jsp_servlet/__mainContent.ja
uses or overrides a deprecated API.
Full compiler error(s):
/programs/bea7/user_projects/vpostdomain/vpostserver/.wlnotdelete/vpostserver_vpost_3878766/jsp_servlet/__mainContent.ja
symbol : class CleanUTABLEUtility
location: class jsp_servlet.__mainContent
CleanUTABLEUtility utblutil = new CleanUTABLEUtility(); //[ /mainContent.jsp; Line: 1380]
^
/programs/bea7/user_projects/vpostdomain/vpostserver/.wlnotdelete/vpostserver_vpost_3878766/jsp_servlet/__mainContent.ja
symbol : class CleanUTABLEUtility
location: class jsp_servlet.__mainContent
CleanUTABLEUtility utblutil = new CleanUTABLEUtility(); //[ /mainContent.jsp; Line: 1380]
^
Note: /programs/bea7/user_projects/vpostdomain/vpostserver/.wlnotdelete/vpostserver_vpost_3878766/jsp_servlet/__mainCont
Note: Recompile with -deprecation for details.
2 errors


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
.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 - 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




Another customer's transaction and personal info are revealed

***Even HttpS "Golden Lock" not safe from software attacks!***

# 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

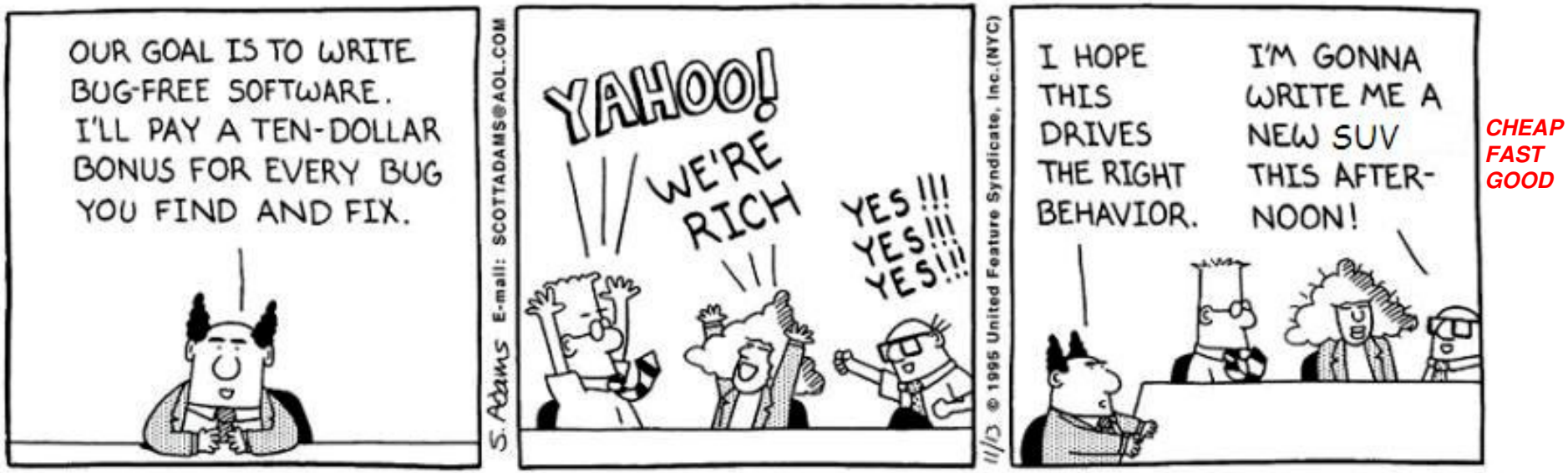
| 2009 | 2010 |
|---|---|
| **1** Unvalidated Input | 1 Injection |
| 2 Broken Access Control | 2 Cross-Site Scripting (XSS) |
| 3 Broken Authentication and Session Management | 3 Broken Authentication and Session Management |
| 4 Cross Site Scripting Flaws | 4 Insecure Direct Object References |
| 5 Buffer Overflows | 5 Cross-Site Request Forgery (CSRF) |
| 6 Injection Flaws | 6 Security Misconfiguration |
| 7 Improper Error Handling | 7 Insecure Cryptographic Storage |
| 8 Insecure Storage | 8 Failure to Restrict URL Access |
| 9 *Denial of Service* | 9 Insufficient Transport Layer Protection |
| 10 Insecure Configuration Management | 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**




*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

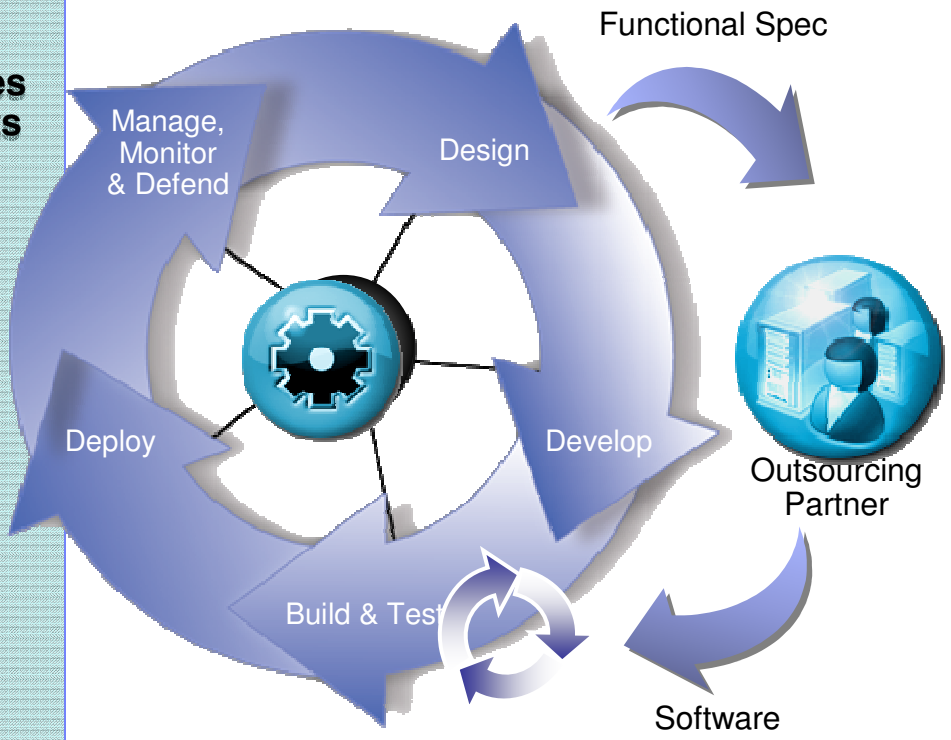
- Testing begins for errors and compliance with security requirements across the entire application
- Applications are also tested for exploitability in deployment scenario

## Deployment Phase

- Configure infrastructure for application policies
- Deploy applications into production

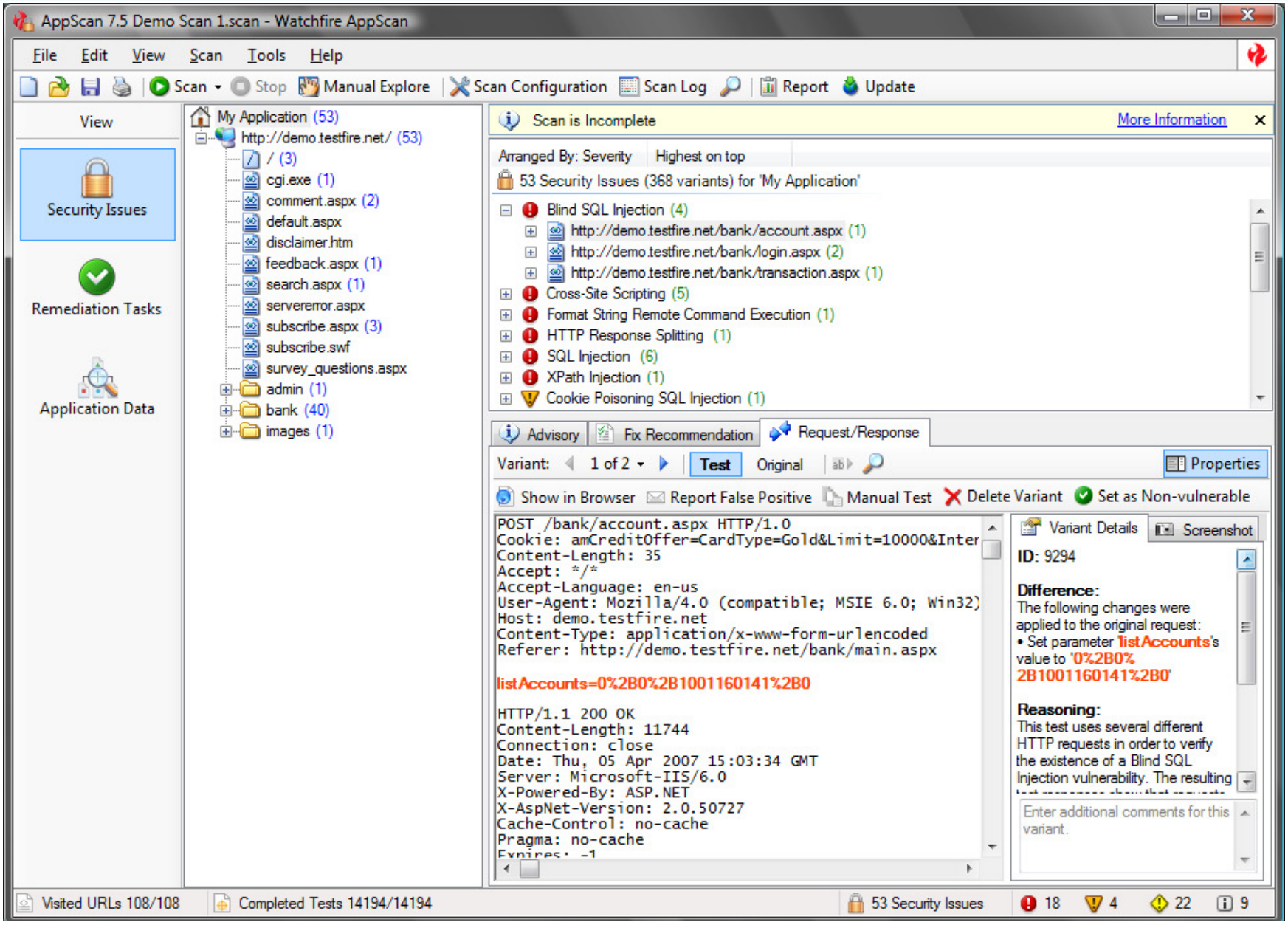
## Operational Phase

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



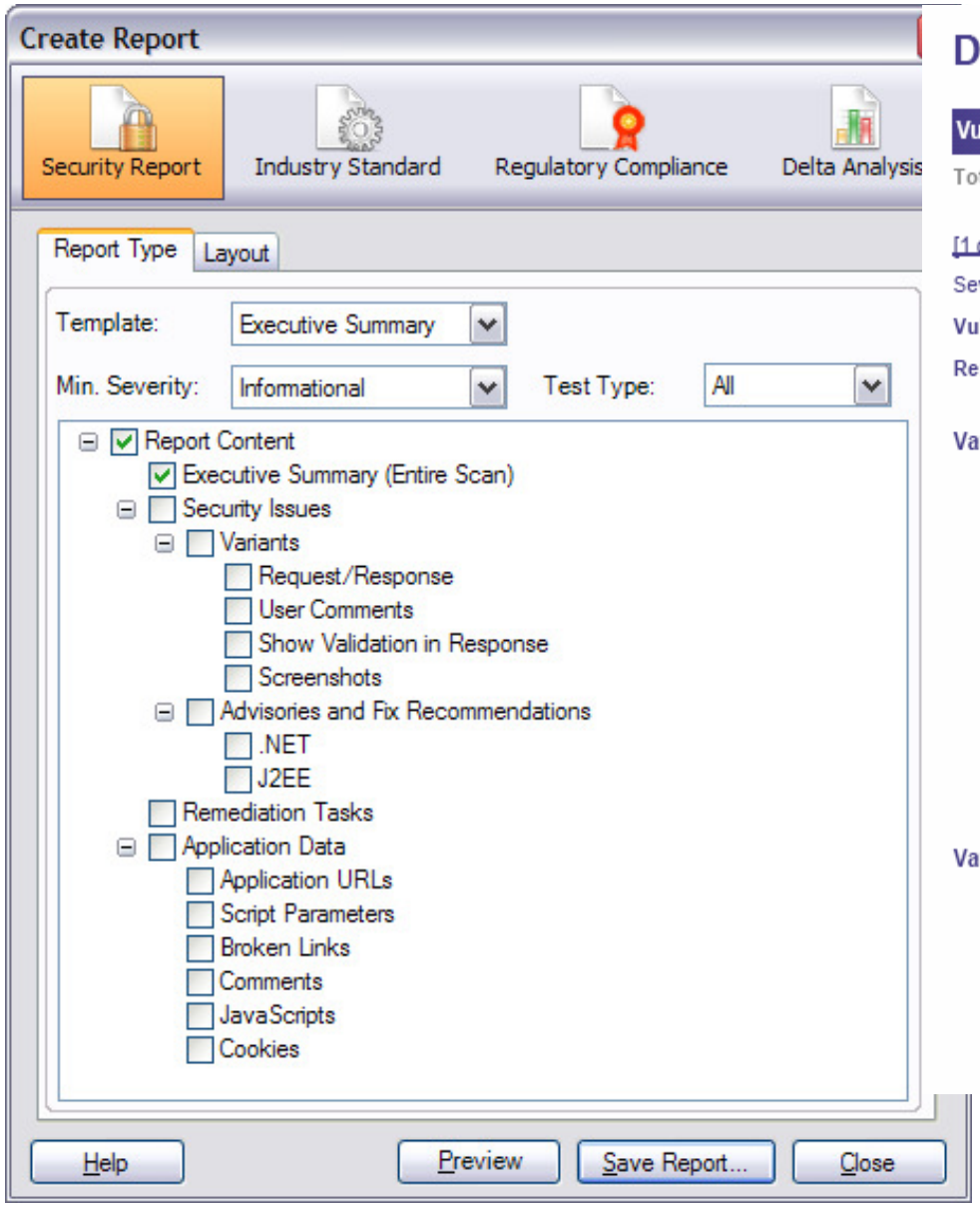
*APPSCAN – A professional software solution that SCAN THE APPLICATION to*

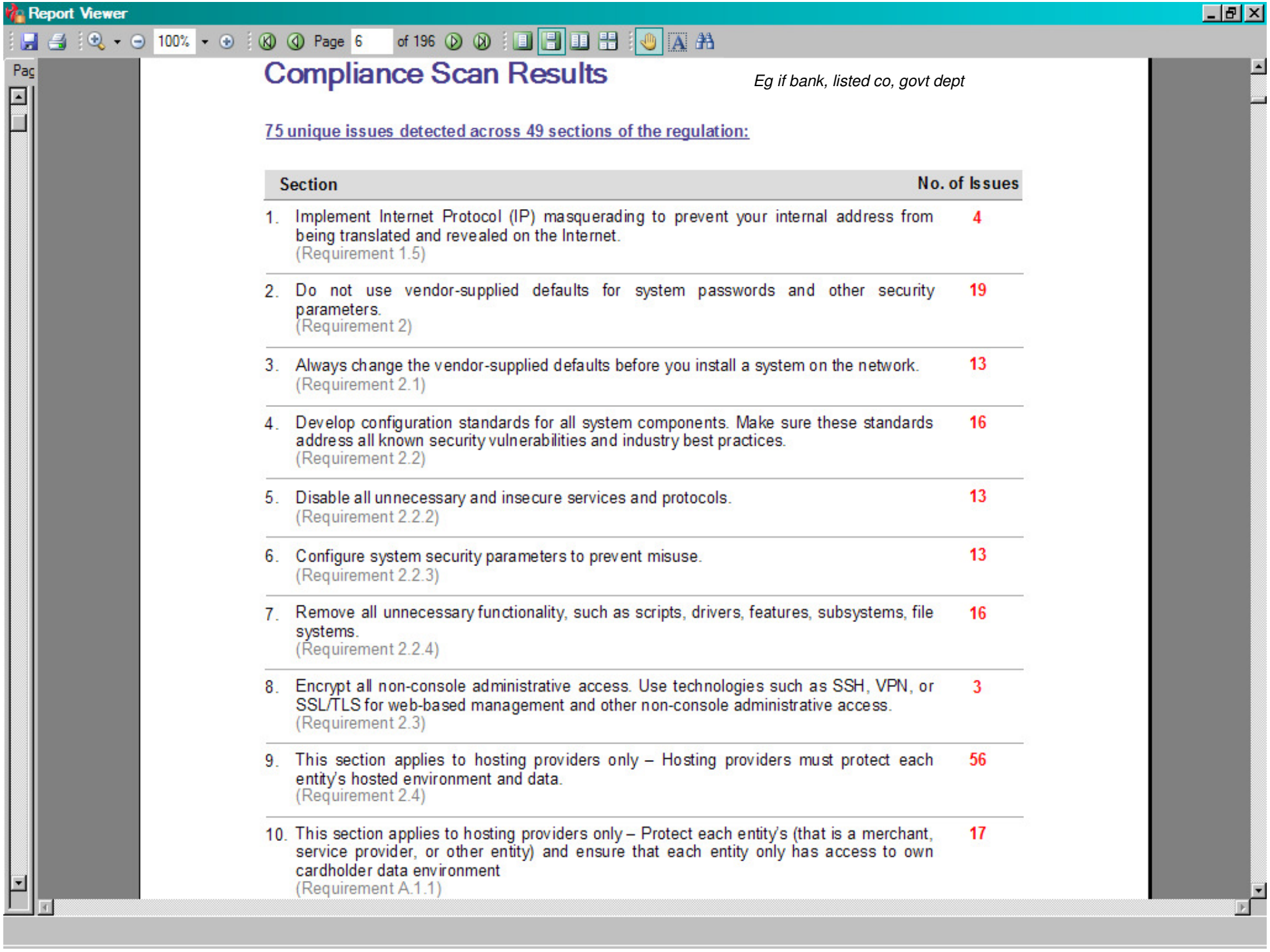
# Identify Vulnerabilities



# With Rich Report Options

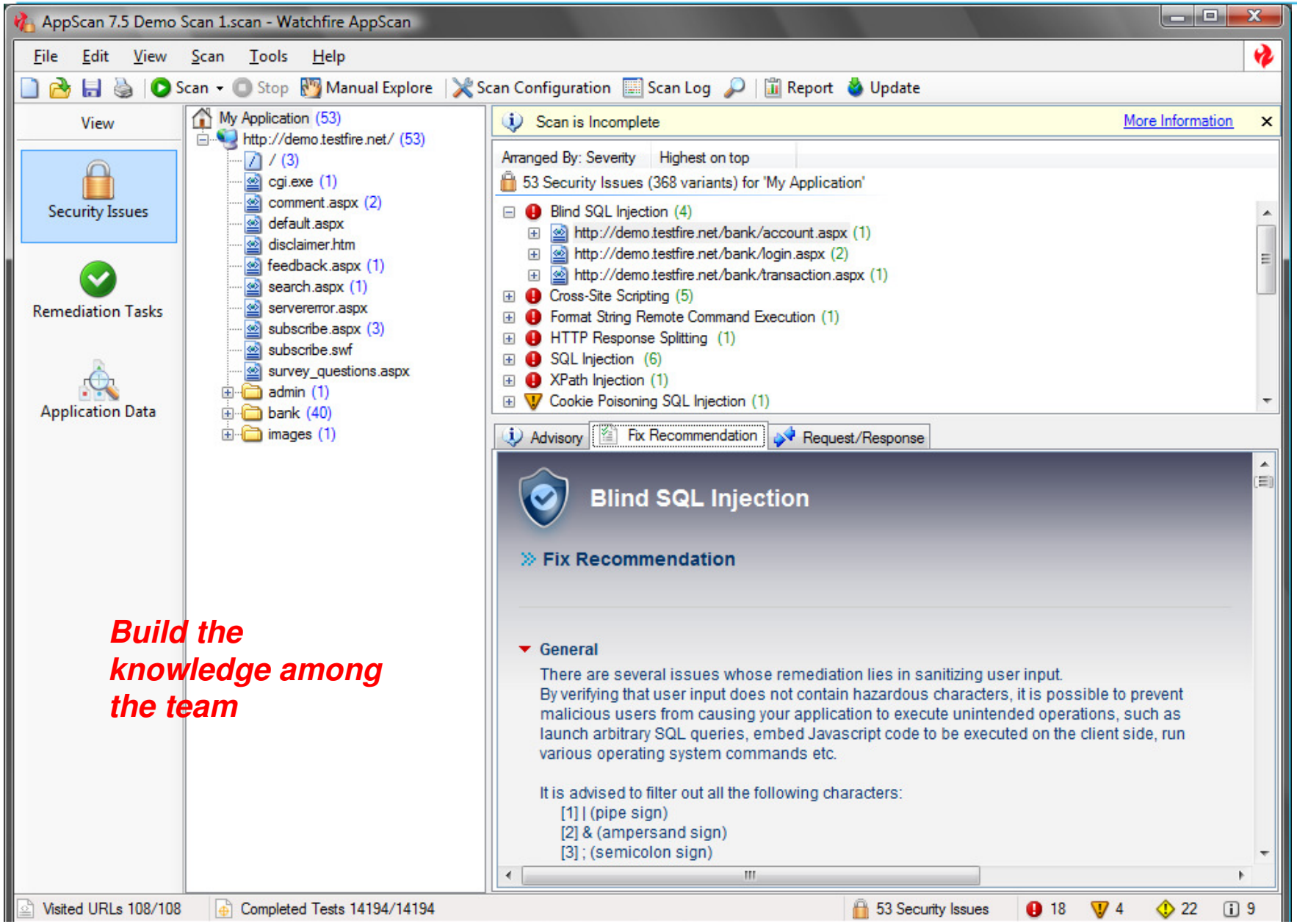
***44 Regulatory Compliance Standards, for Executive, Security, Developers, PLUS customizable test criteria.***





Report Viewer
100%
Page 6 of 196
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




***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.**

# Is Your Web App-solutely Secure?

## TERIMA KASIH


*27-7-2011*

*Anthony Lim*


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

**www.ibm.com/security**

CSSLP
Certified Secure Software Lifecycle Professional

**© Copyright IBM Corporation 2010. All rights reserved.** The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, Rational, the Rational logo, Telelogic, the Telelogic logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.