The Hacker's New Target

- Software Applications on the Internet

Adrian Lim

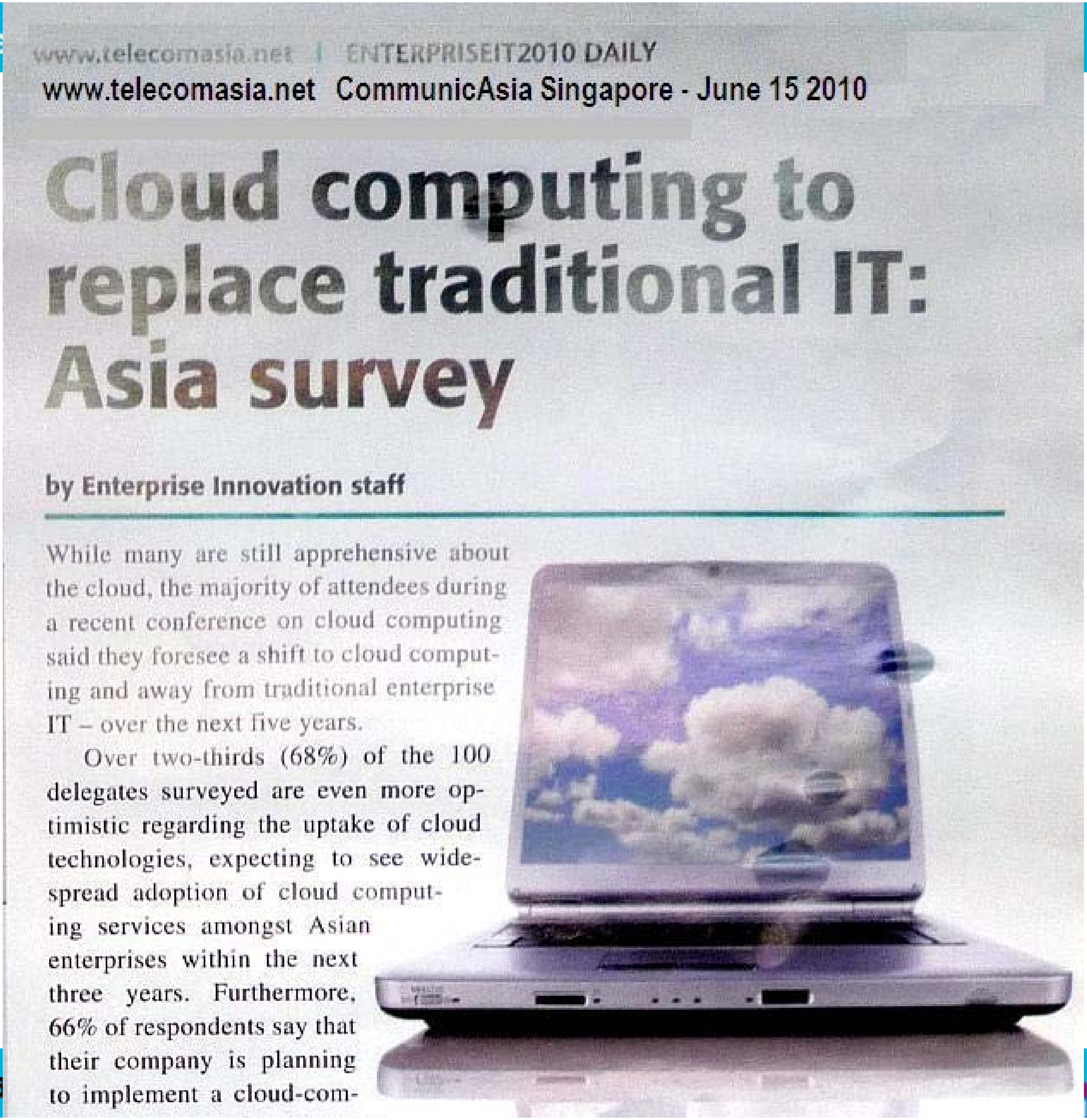
Rational Software

IBM Singapore

Let's build a smarter planet

The premiere software and product delivery event.

THAILAND IBM SECURITY CONFERENCE, SEP 15 2010



www.telecomasia.net | ENTERPRISEIT2010 DAILY

www.telecomasia.net CommunicAsia Singapore - June 15 2010

Cloud computing to replace traditional IT: Asia survey

by Enterprise Innovation staff

While many are still apprehensive about the cloud, the majority of attendees during a recent conference on cloud computing said they foresee a shift to cloud computing and away from traditional enterprise IT – over the next five years.

Over two-thirds (68%) of the 100 delegates surveyed are even more optimistic regarding the uptake of cloud technologies, expecting to see widespread adoption of cloud computing services amongst Asian enterprises within the next three years. Furthermore, 66% of respondents say that their company is planning to implement a cloud-com-

Platform as a service?

Infra as a service?

Appication as a service?

Service as a Service?!

Welcome to THE SMARTER PLANET

Globalization and Globally Available Resources

- Instrumented, Interconnected, Intelligent

*** Web 2.0**

• SOA

• CLOUD

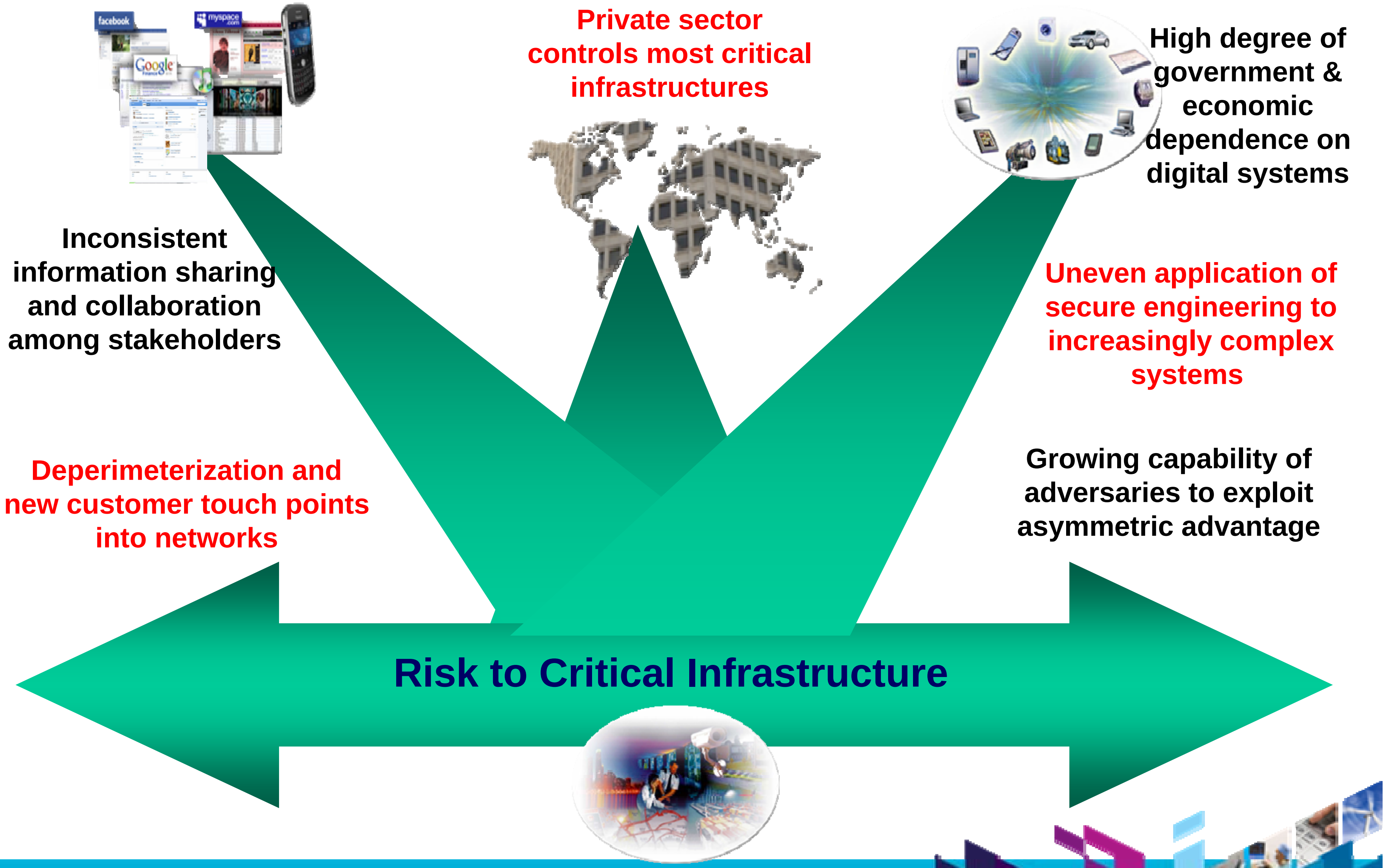
Billions of mobile devices accessing the Web

Access to streams of information in the Real Time

New Possibilities..

ITS ALL ABOUT SOFTWARE!

The challenge of cyber security in cloud computing



Private sector controls most critical infrastructures

High degree of government & economic dependence on digital systems

Inconsistent information sharing and collaboration among stakeholders

Uneven application of secure engineering to increasingly complex systems

Deperimeterization and new customer touch points into networks

Growing capability of adversaries to exploit asymmetric advantage

Risk to Critical Infrastructure

CLOUD COMPUTING SECURITY CONSIDERATIONS

- **Confidentiality: Data exposure & leakage**
- **Integrity: Data compromise**
- **Availability: Reliability of service, business continuity**

- **Reduced Ability to Demonstrate Compliance:**
- **Reduced Ability to Manage the Security Environment:**
- **Storage and Backup, disaster recover**

Can the provider segregate and protect individual groups of data within the remote, distributed shared environment?

- **Firewalls & IPS etc to prevent network/infra hacking attacks**
  - *Standard "perimeter defense" is still first and foremost!*
- **Viruses, worms, trojans, malware, bots …**
- **Identity and access management, user provisioning**
  - Authentication & Encryption
- **Availability – prevent againt Denial of Service**
- **Vigilant monitoring, S.I.E.M.**

PER GARTNER

- Implement and maintain a security program.
- Build and maintain a secure cloud 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.

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

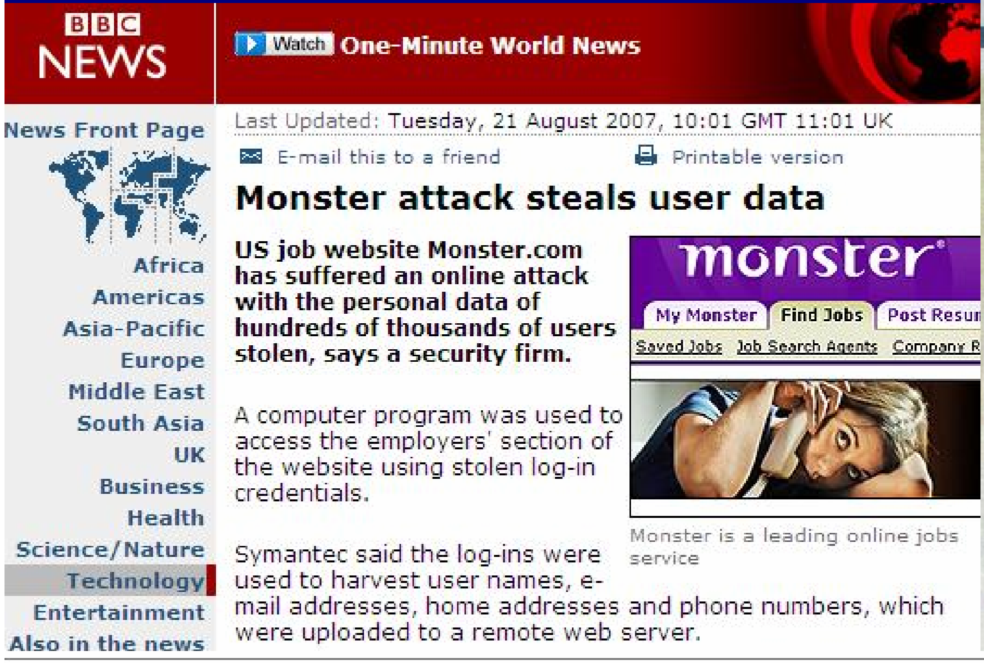
Neglect the security of the software on the network/web server

We Use SSL Encryption

Only protects data between site and user not the web application itself

SOMETHING IS STILL OUT THERE …

IBM



BBC 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

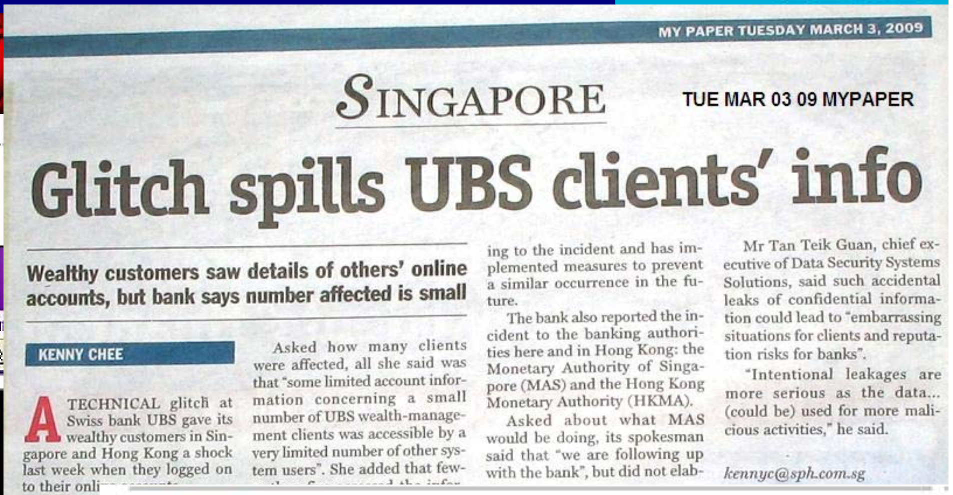
Monster attack steals user data

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.

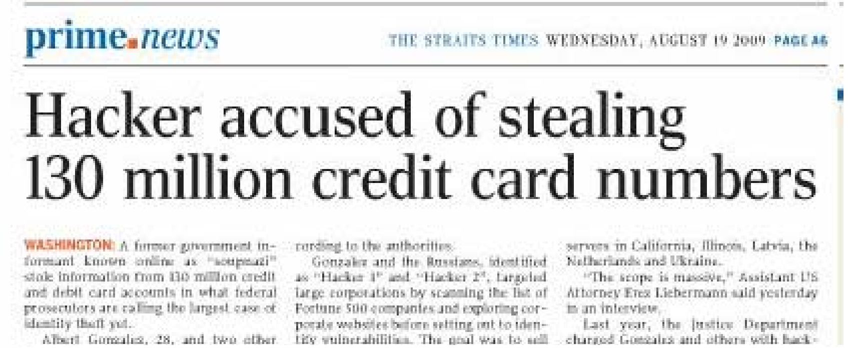
The bank also reported the incident to the banking authorities here and in Hong Kong: the Monetary Authority of Singapore (MAS) and the Hong Kong Monetary Authority (HKMA).

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

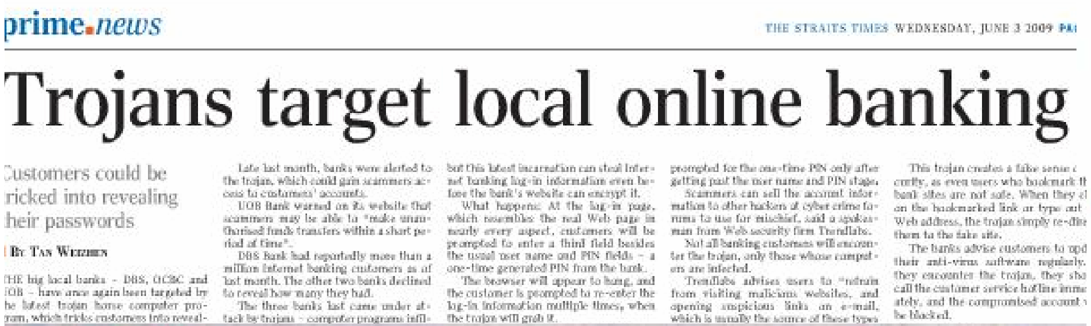
cording to the authorities.

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

Customers could be tricked into revealing their passwords

By Tan Weizhen

THE big local banks – DBS, OCBC and UOB – have once again been targeted by the latest trojan horse computer program, 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 stages.

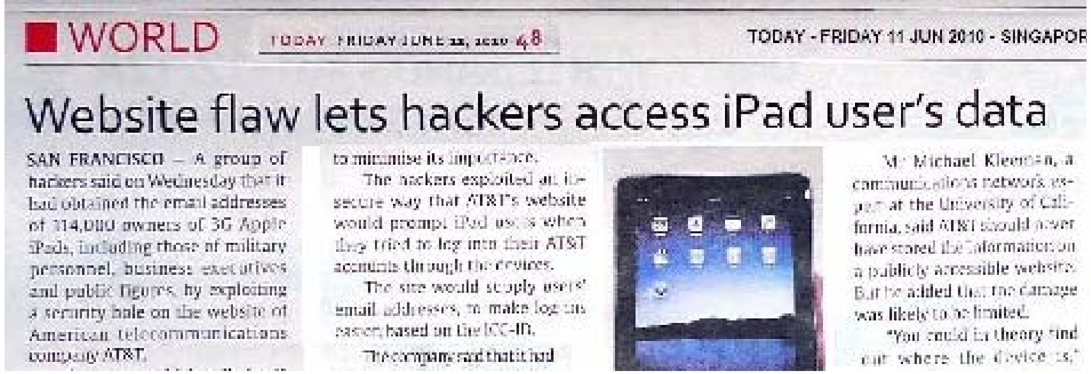
Scammers can sell the account information to other hackers at cyber crime forums to use for mischief, said a spokesman from Web security firm Trendlabs.

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 c 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.

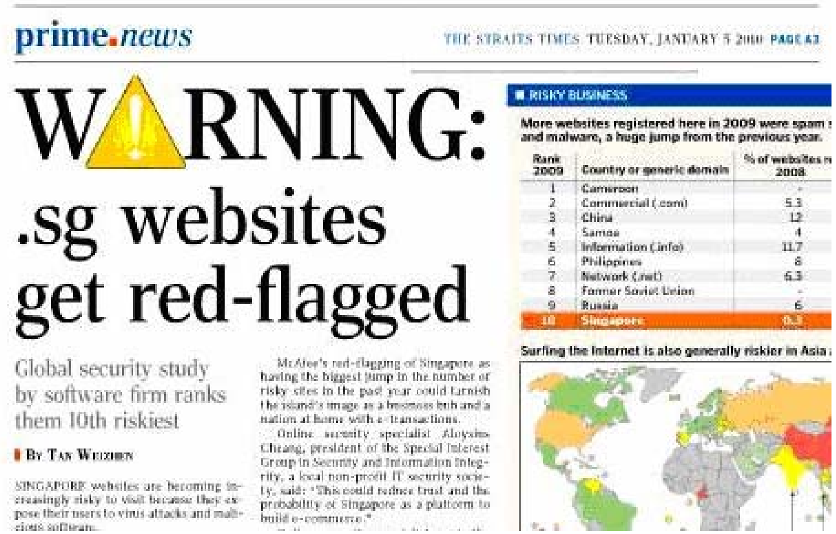
The hackers exploited an insecure way that AT&T's website would prompt iPad users when they tried to log into their AT&T accounts through the devices.

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 network expert at the University of California, said AT&T should never have stored the information on a publicly accessible website. But he added that the damage was likely to be limited.

"You could in theory find out where the device is,"



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

WARNING: .sg websites get red-flagged

Global security study by software firm ranks them 10th riskiest

By Tan Weizhen

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

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 s 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	6
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

Cloud Computing Security – The Soft Spot - Application Security Issues

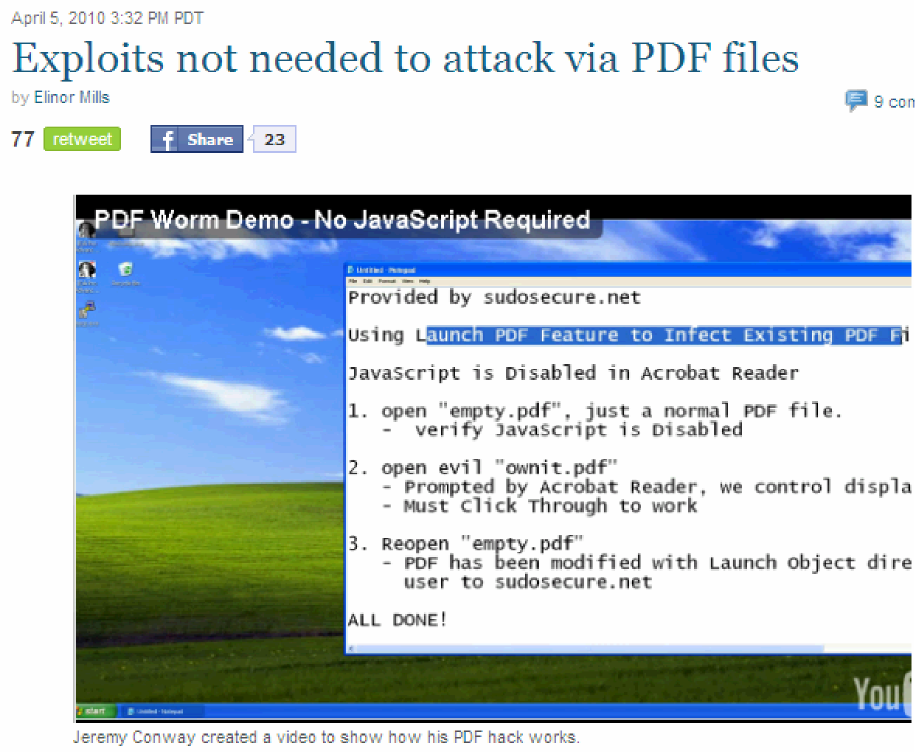
Applications can be CRASHED to reveal source, logic, script or infrastructure information that can give a hacker intelligence

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***



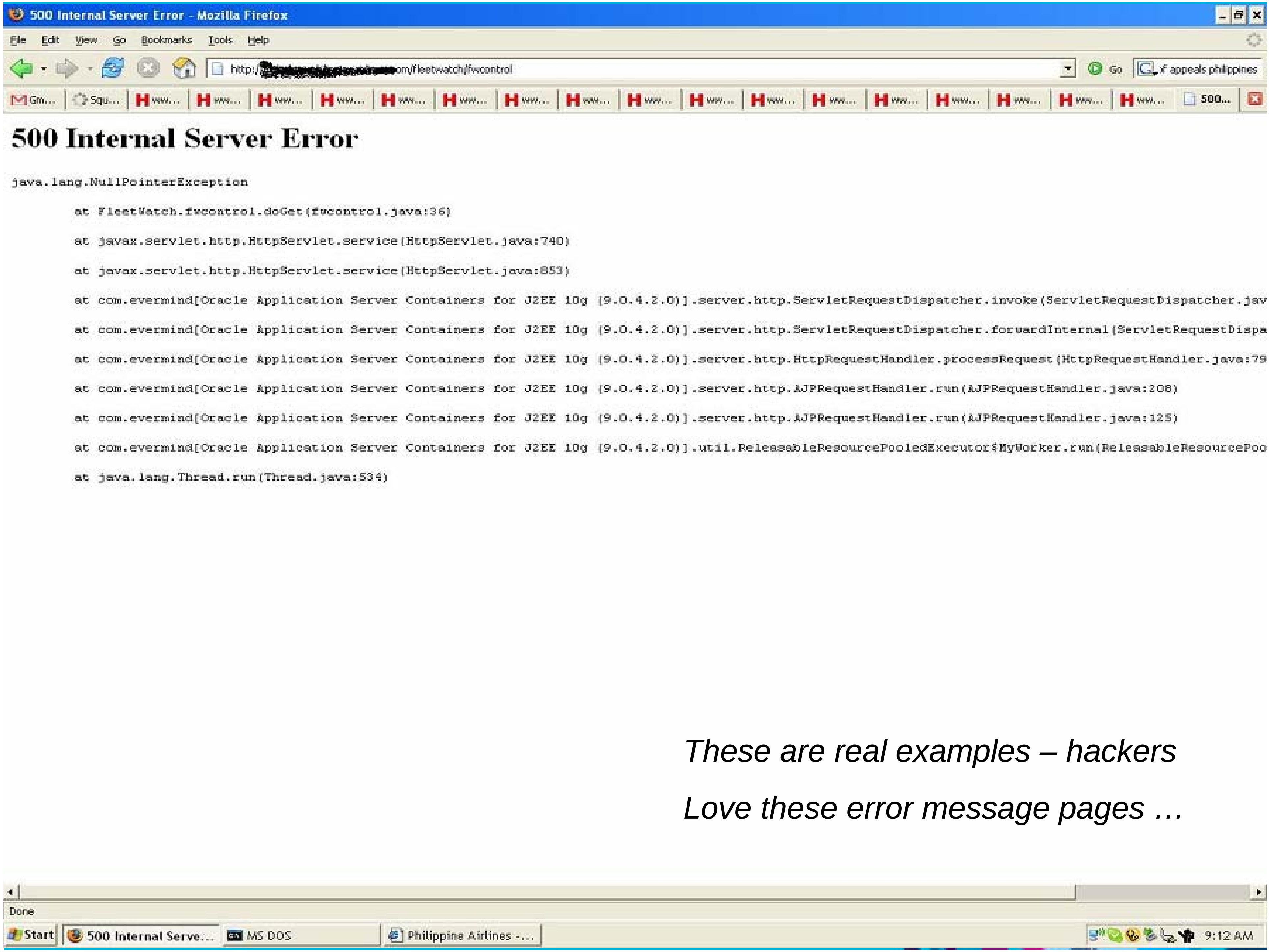
April 5, 2010 3:32 PM PDT

Exploits not needed to attack via PDF files

by Elinor Mills

```
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.

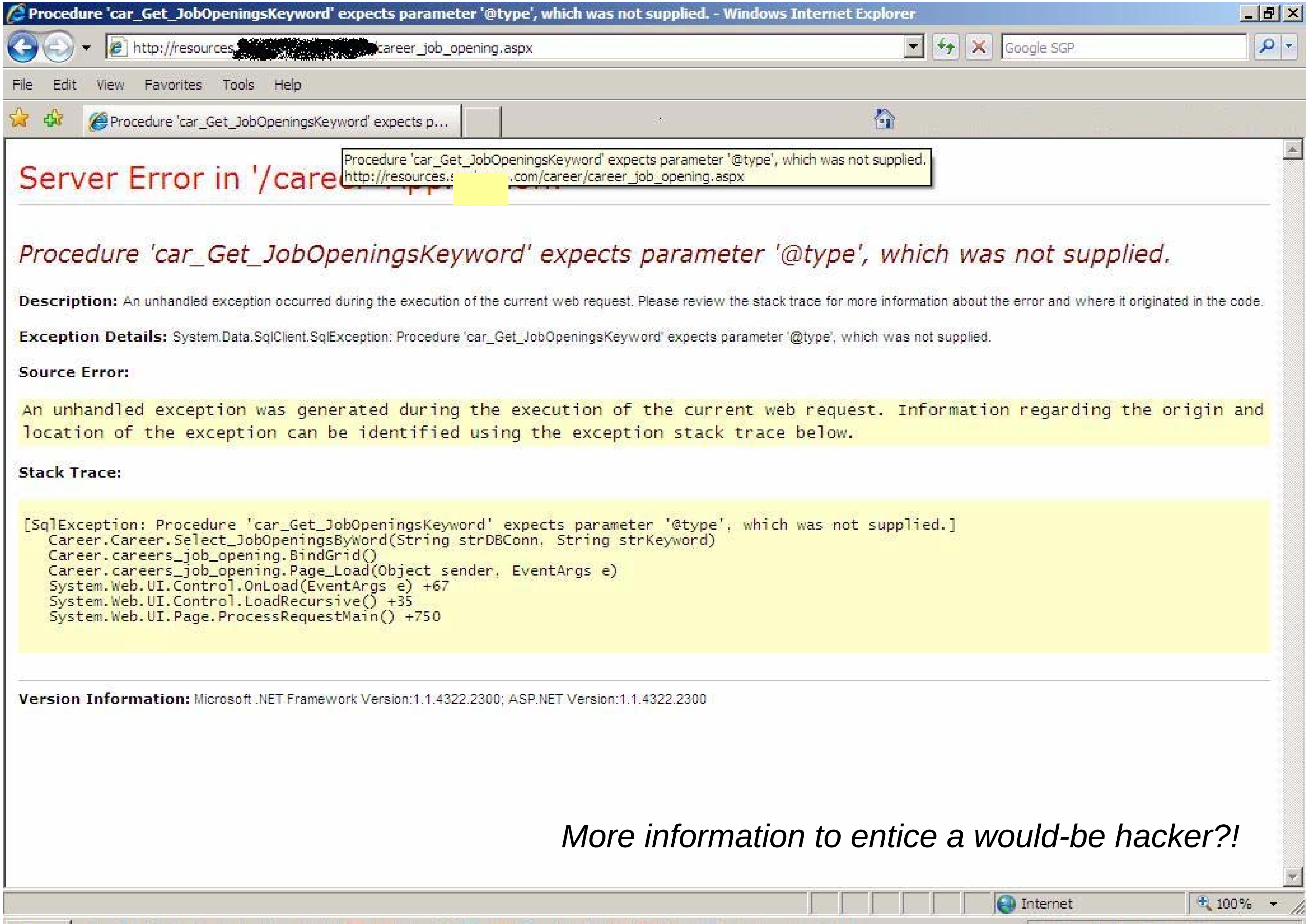


500 Internal Server Error

```
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 …



Procedure 'car_Get_JobOpeningsKeyword' expects parameter '@type', which was not supplied. - Windows Internet Explorer

http://resources[redacted]career_job_opening.aspx

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

Server Error in '/care

Procedure 'car_Get_JobOpeningsKeyword' expects parameter '@type', which was not supplied.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Procedure 'car_Get_JobOpeningsKeyword' expects parameter '@type', which was not supplied.

Source Error:

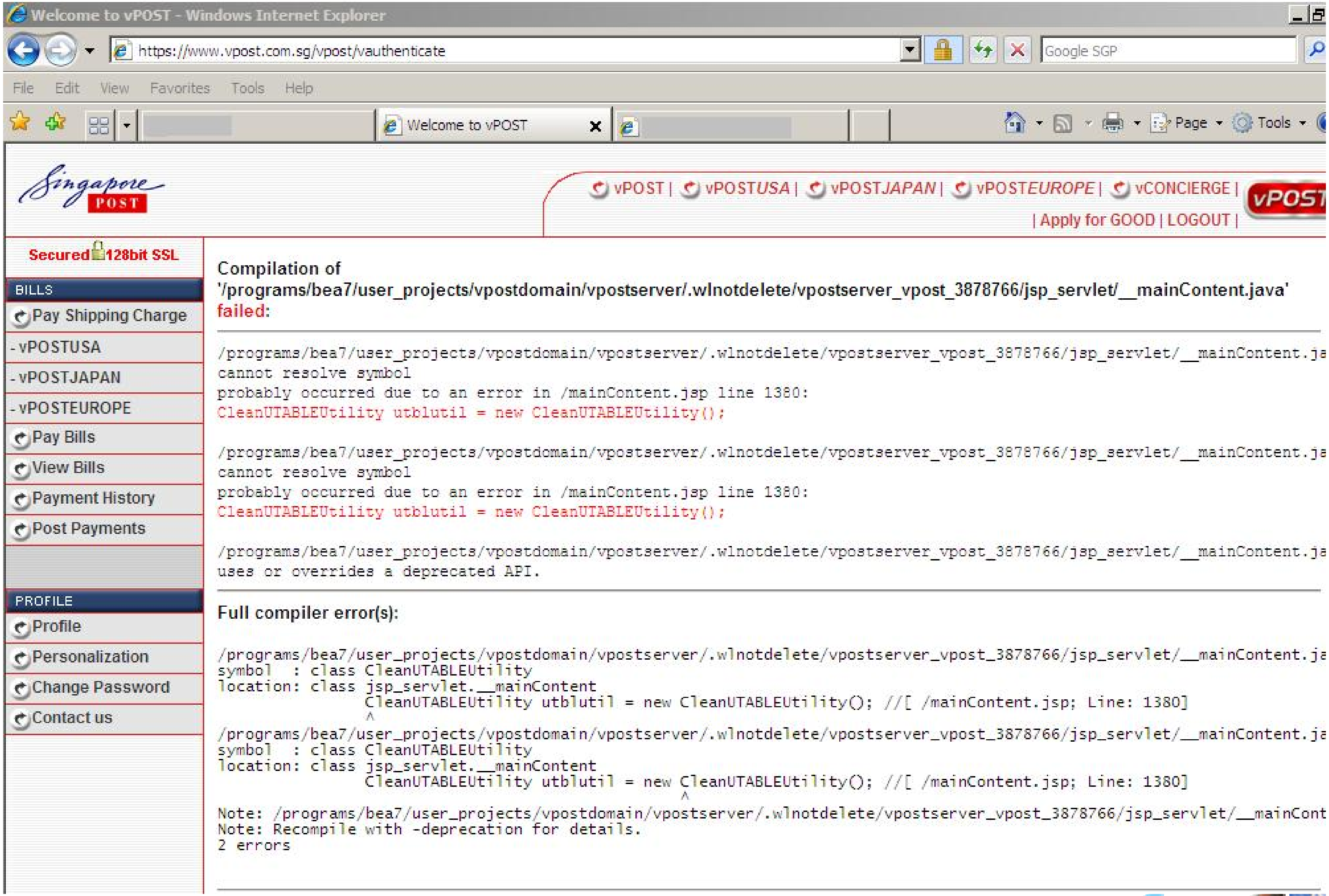
```
An unhandled exception was generated during the execution of the current web request. Information regarding the origin and
location of the exception can be identified using the exception stack trace below.
```

Stack Trace:

```
[SqlException: Procedure 'car_Get_JobOpeningsKeyword' expects parameter '@type', which was not supplied.]
   Career.Career.Select_JobOpeningsByWord(String strDBConn, String strKeyword)
   Career.careers_job_opening.BindGrid()
   Career.careers_job_opening.Page_Load(Object sender, EventArgs e)
   System.Web.UI.Control.OnLoad(EventArgs e) +67
   System.Web.UI.Control.LoadRecursive() +35
   System.Web.UI.Page.ProcessRequestMain() +750
```

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

More information to entice a would-be hacker?!



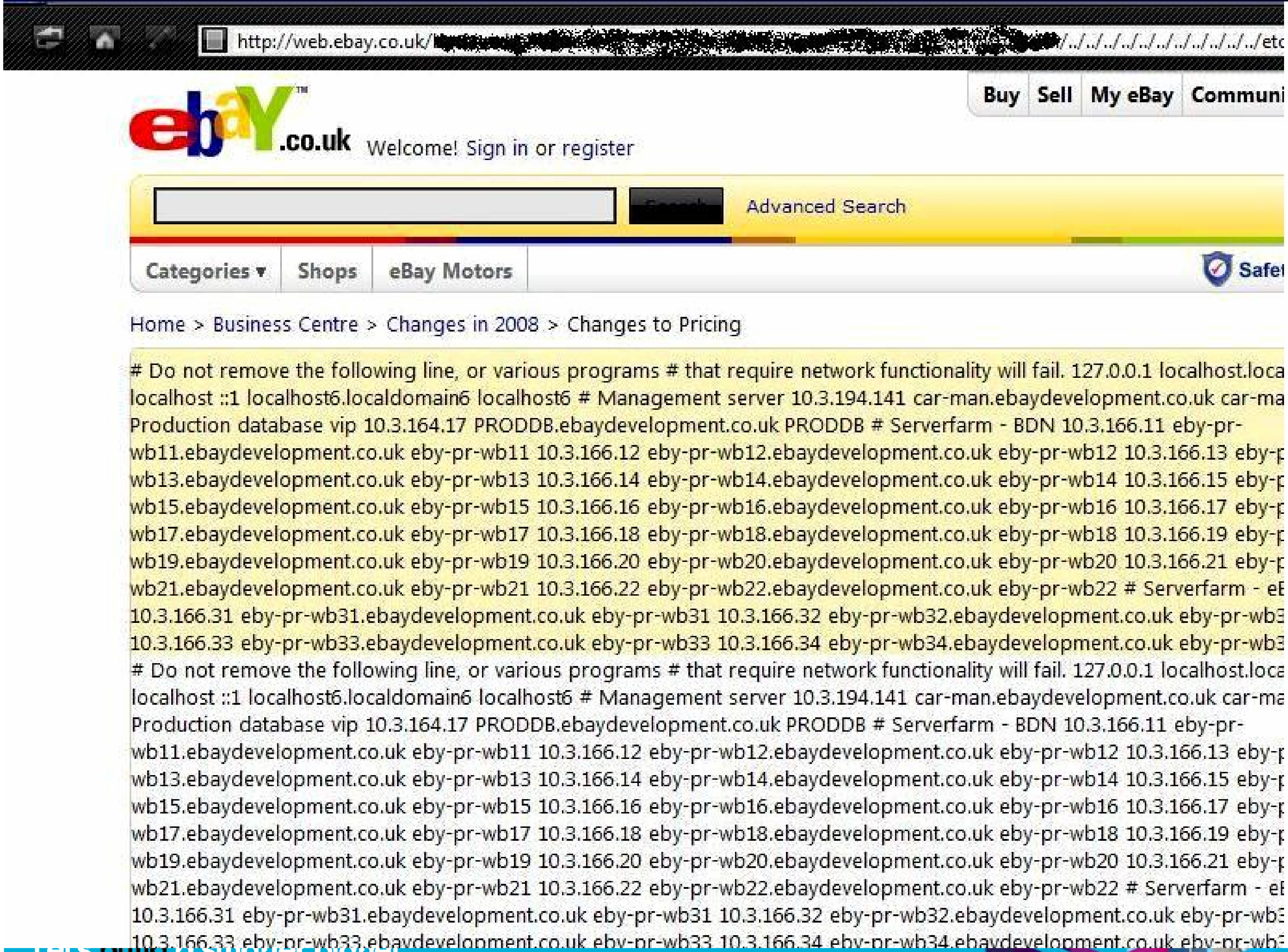
Compilation of '/programs/bea7/user_projects/vpostdomain/vpostserver/.wlnotdelete/vpostserver_vpost_3878766/jsp_servlet/__mainContent.java' failed:

```
/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

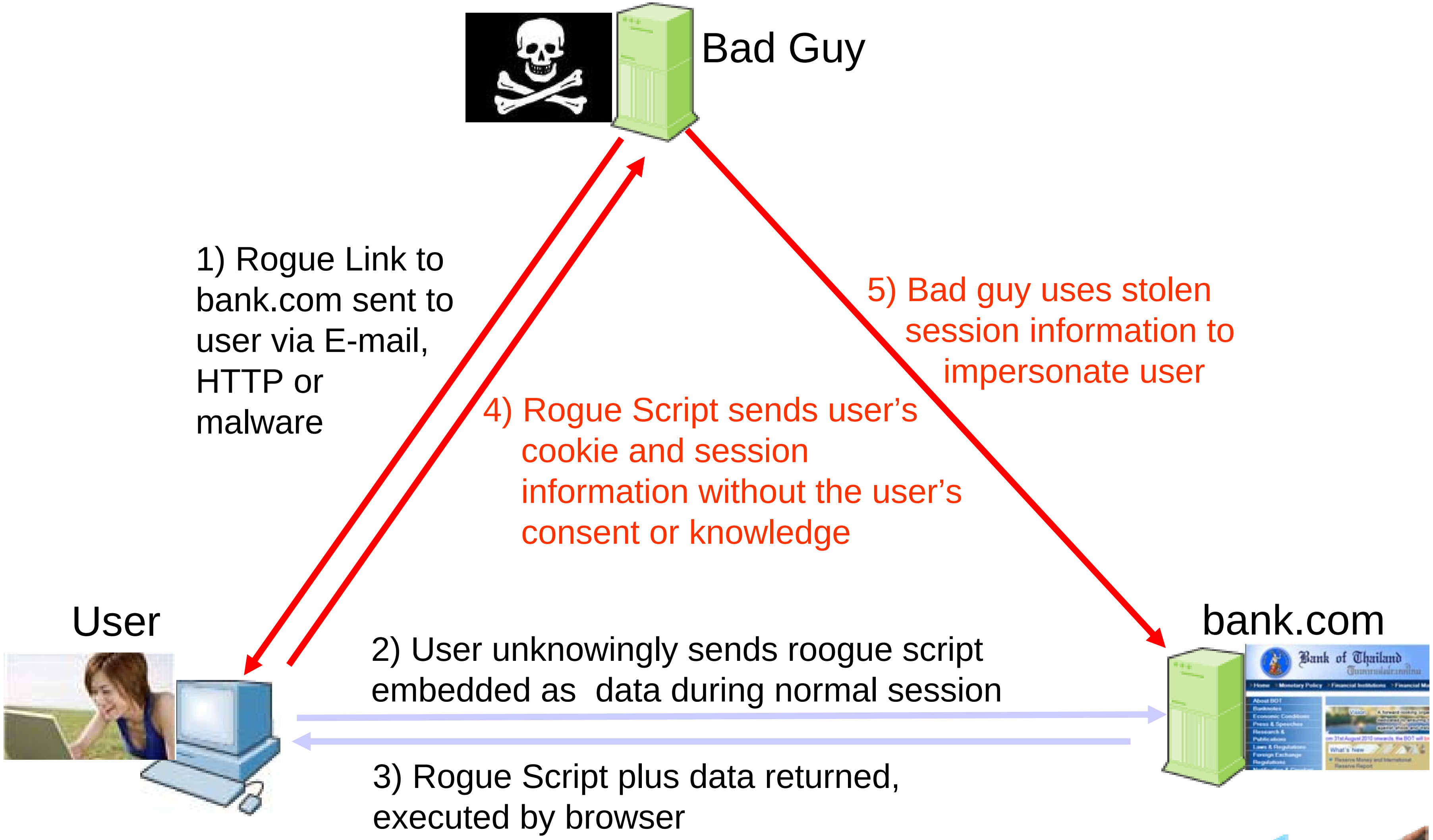
Home > Business Centre > Changes in 2008 > Changes to Pricing

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

Cross-Site Scripting

A top web-borne application attack today



Bad Guy

1) Rogue Link to bank.com sent to user via E-mail, HTTP or malware

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

5) Bad guy uses stolen session information to impersonate user

User

bank.com

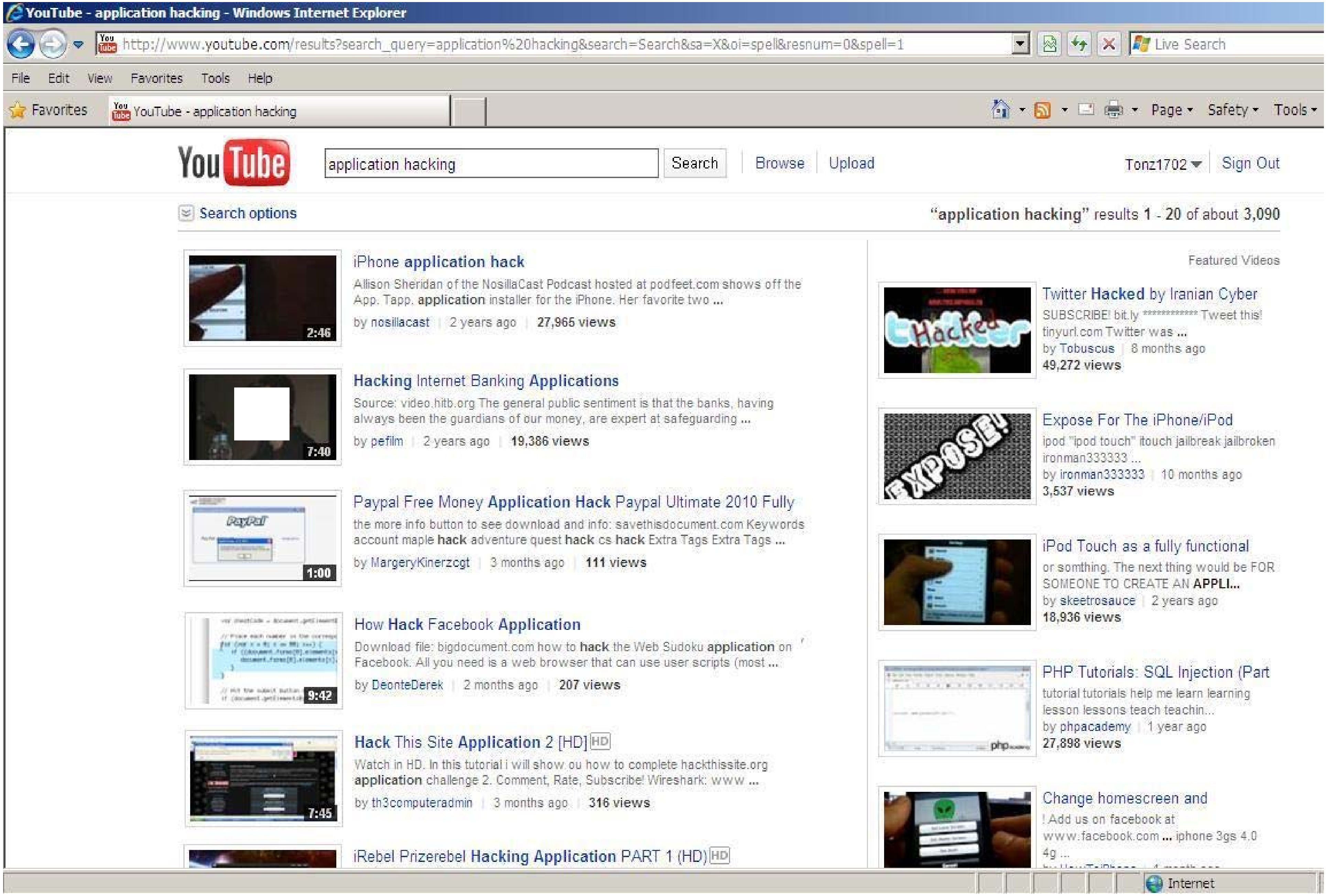
2) User unknowingly sends roogue script embedded as data during normal session

3) Rogue Script plus data returned, executed by browser

A Sample Of The ‘low hanging fruits’...

- Shell Command Execution
- HTTP PUT Defacement
- Backup Files
- Blind SQL Injection
- Debug files and Test pages
- Directory Listing
- Insecure HTTP Methods
- HTTP Response Splitting
- SOAP Web Services Issues
- XPath Injection
- Path Traversal in Parameters
- Server Side Includes
- File Upload
- Phishing Through URL redirection
- Poison Null Byte
- Buffer Overflows
- Administration Pages
- SQL Injection
- LDAP Injection
- MS FrontPage Issues
- Email Spoofing
- Cross Site Scripting
- Path Traversal in URL
- BEA WebLogic Issues
- SUN iPlanet Issues
- Oracle iAS Issues
- Format Strings
- ColdFusion Issues
- VALIDATE INPUT
- PHP Issues
- Apache HTTPd Issues
- Microsoft IIS Issues
- Privacy Issues
- Credentials Enumeration
- Tomcat Issues
- Cookie Poisoning SQL Injection

Don’t Try This At Home


YouTube - application hacking - Windows Internet Explorer
File Edit View Favorites Tools Help
Favorites
YouTube - application hacking
Page ▾ Safety ▾ Tools ▾
Live Search
Search
Browse
Upload
Tonz1702 ▾
Sign Out
Search options
Featured Videos
Internet

http://www.youtube.com/results?search_query=application%20hacking&search=Search&sa=X&oi=spell&resnum=0&spell=1

application hacking

“application hacking” results 1 - 20 of about 3,090

iPhone application hack (2:46)
Allison Sheridan of the NosillaCast Podcast hosted at podfeet.com shows off the App. Tapp. **application** installer for the iPhone. Her favorite two ...
by nosillacast | 2 years ago | 27,965 views

Hacking Internet Banking Applications (7:40)
Source: video.hitb.org The general public sentiment is that the banks, having always been the guardians of our money, are expert at safeguarding ...
by pefilm | 2 years ago | 19,386 views

Paypal Free Money Application Hack Paypal Ultimate 2010 Fully (1:00)
the more info button to see download and info: savethisdocument.com Keywords account maple **hack** adventure quest **hack** cs **hack** Extra Tags Extra Tags ...
by MargeryKinerzcgt | 3 months ago | 111 views

How Hack Facebook Application (9:42)
Download file: bigdocument.com how to **hack** the Web Sudoku **application** on Facebook. All you need is a web browser that can use user scripts (most ...
by DeonteDerek | 2 months ago | 207 views

Hack This Site Application 2 [HD] HD (7:45)
Watch in HD. In this tutorial i will show ou how to complete hackthissite.org **application** challenge 2. Comment, Rate, Subscribe! Wireshark: www ...
by th3computeradmin | 3 months ago | 316 views

iRebel Prizerebel Hacking Application PART 1 (HD) HD

Twitter Hacked by Iranian Cyber
SUBSCRIBE! bit.ly ************ Tweet this! tinyurl.com Twitter was ...
by Tobuscus | 8 months ago
49,272 views

Expose For The iPhone/iPod
ipod "ipod touch" itouch jailbreak jailbroken ironman333333 ...
by ironman333333 | 10 months ago
3,537 views

iPod Touch as a fully functional
or somthing. The next thing would be FOR SOMEONE TO CREATE AN **APPLI...**
by skeetrosauce | 2 years ago
18,936 views

PHP Tutorials: SQL Injection (Part
tutorial tutorials help me learn learning lesson lessons teach teachin...
by phpacademy | 1 year ago
27,898 views

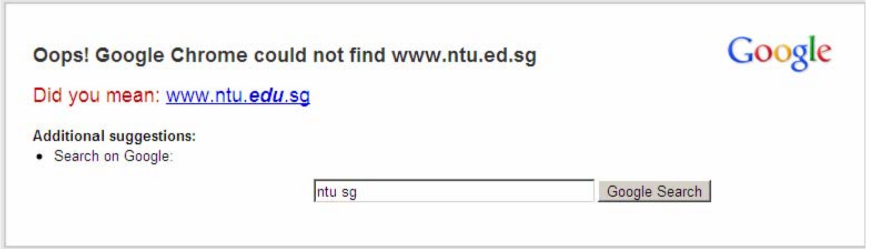
Change homescreen and
! Add us on facebook at www.facebook.com ... iphone 3gs 4.0 4g ...

WHY DO HACKERS 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.**

- **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:

- **Because they can!**
  - It is nearly impossible to write a comprehensively robust application
  - **Many organizations today still lack a software development security policy!**
    - **DEVELOPERS ARE UNDER GREAT PRESSURE OF RESOURCES, BUDGET, TIMELINE & KNOWLEDGE**
    - Developers are culturally not into secure coding practice even though they learn it.
    - Developers think differently from hackers, and often lack the right experience
    - **It is a nightmare to manually QA the application**
    - **Applications today are hundreds of thousands of lines long**

Why does software have vulnerabilities?

Singapore
Mercedes

Do more with less

200,000 lines

Today I'm being asked to:

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

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

-> Choose 2 only

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!!!
11/13 © 1995 United Feature Syndicate, Inc.(NYC)
I HOPE THIS DRIVES THE RIGHT BEHAVIOR.
I'M GONNA WRITE ME A NEW SUV THIS AFTERNOON!

Top 10 OWASP Critical Web Application Security Issues ’09

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

Top 10 OWASP Critical Web Application Security Risks ‘10

1. Injection
2. Cross-Site Scripting (XSS)
3. Broken Authentication and Session Management
4. Insecure Direct Object Reference
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

http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

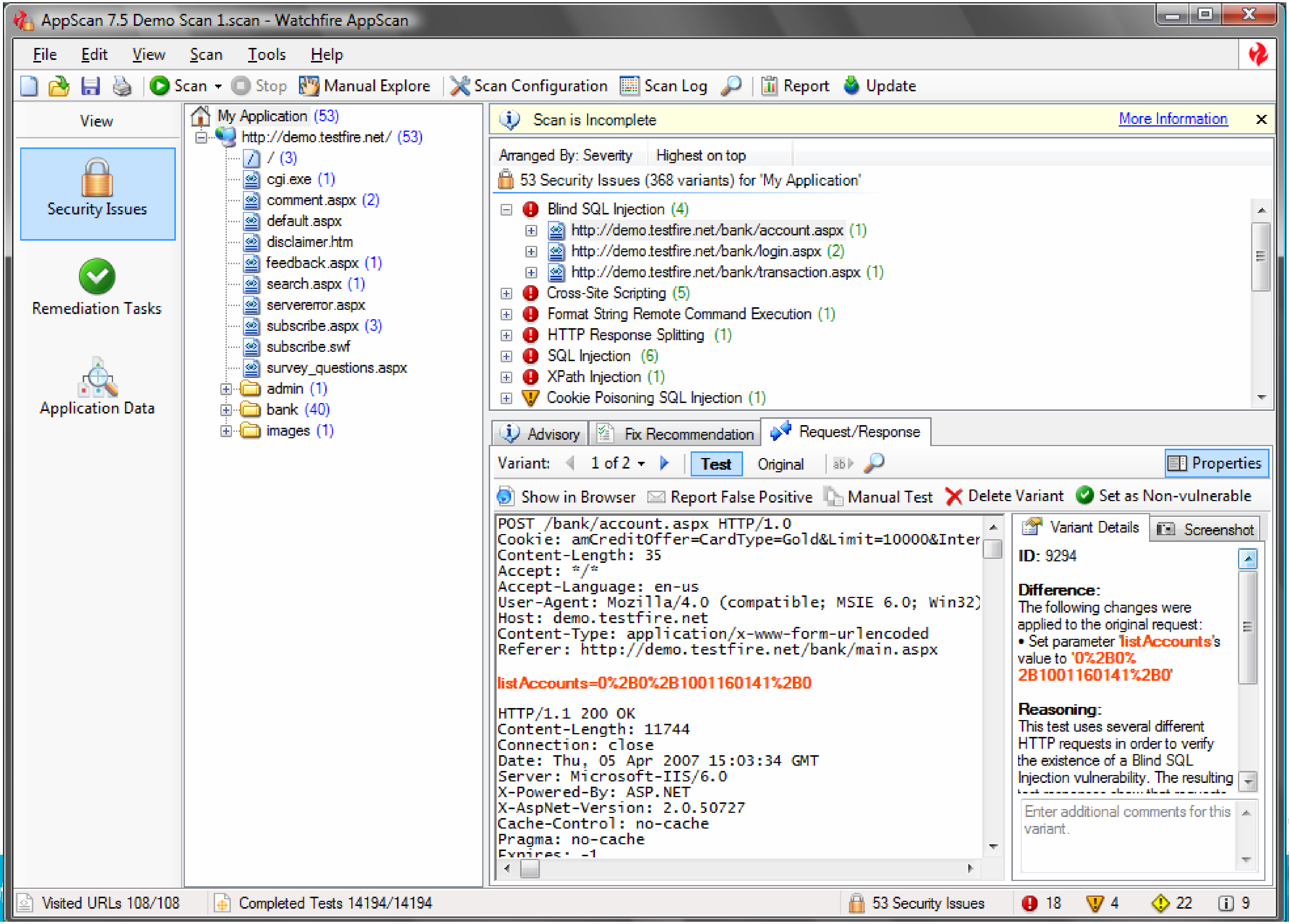
INTERNET APPLICATION SECURITY - SOLUTION

Security for Smarter Products

- Smarter Products require secure applications
- Security needs to be built into the development process and addressed throughout the development lifecycle
- Providing security for smarter products requires comprehensive security solutions deployed in concert with application lifecycle management offerings that:
  - Provide integrated testing solutions for developers, QA, Security and Compliance stakeholders
  - Leverage multiple appropriate testing technologies
  - Provide effortless security that allows development to be part of the solution
  - Support governance, reporting and dashboards
  - Can facilitate collaboration between development and security teams

You need a professional solution 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)

```
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
```

ID: 9294

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

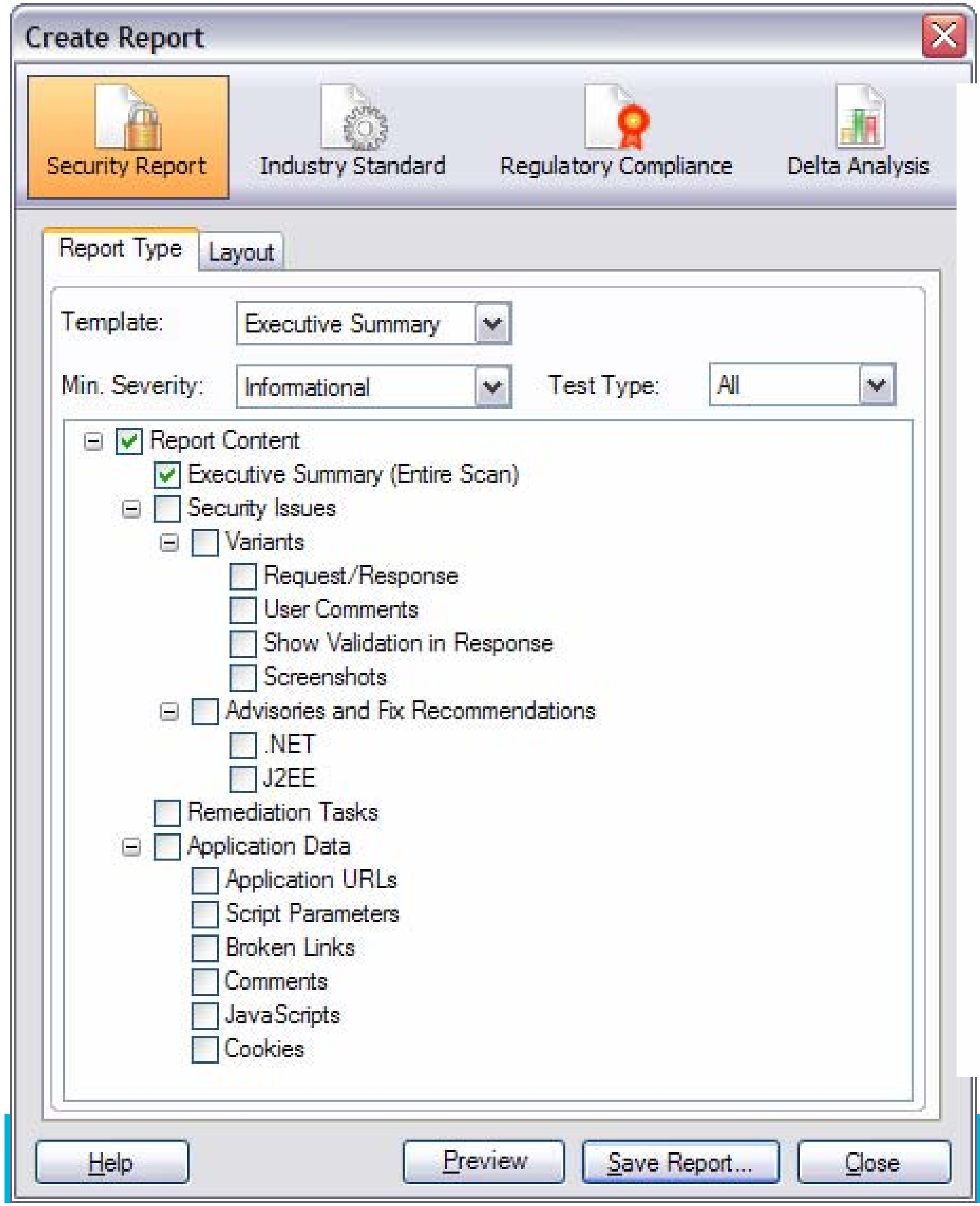
Reasoning:
This test uses several different HTTP requests in order to verify the existence of a Blind SQL Injection vulnerability. The resulting

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.



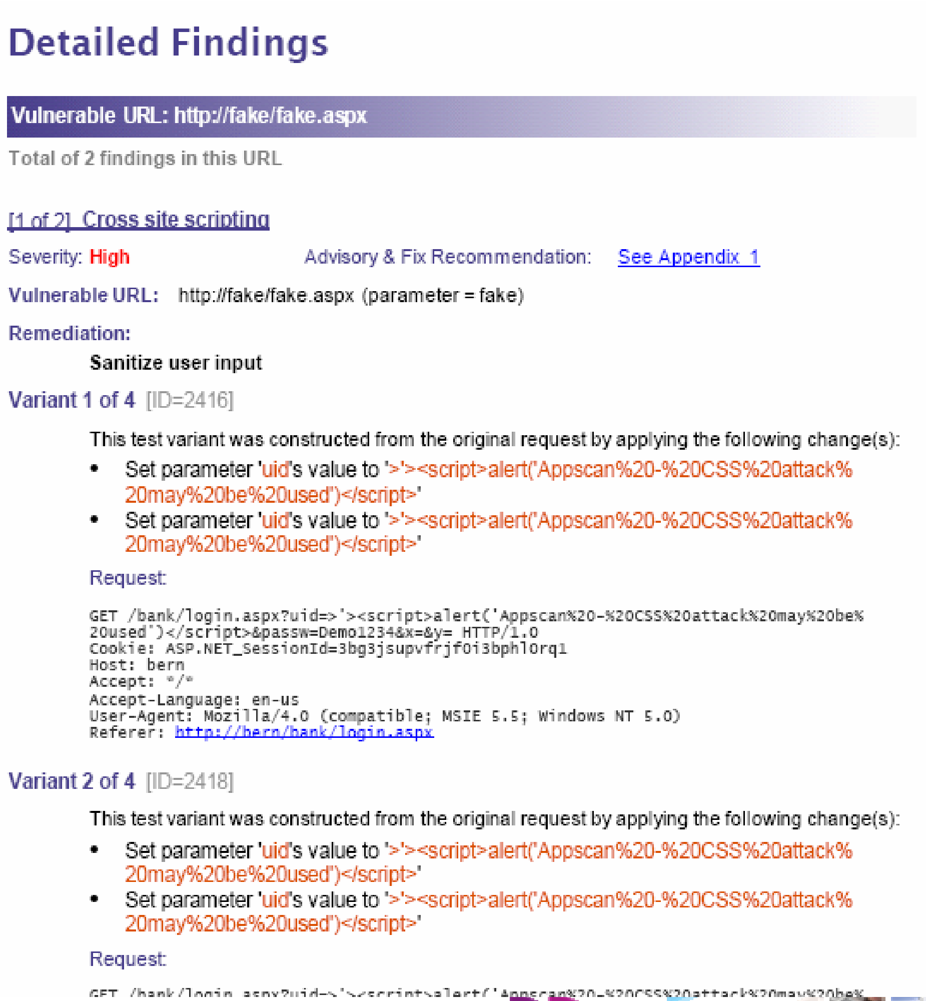
Create Report

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):

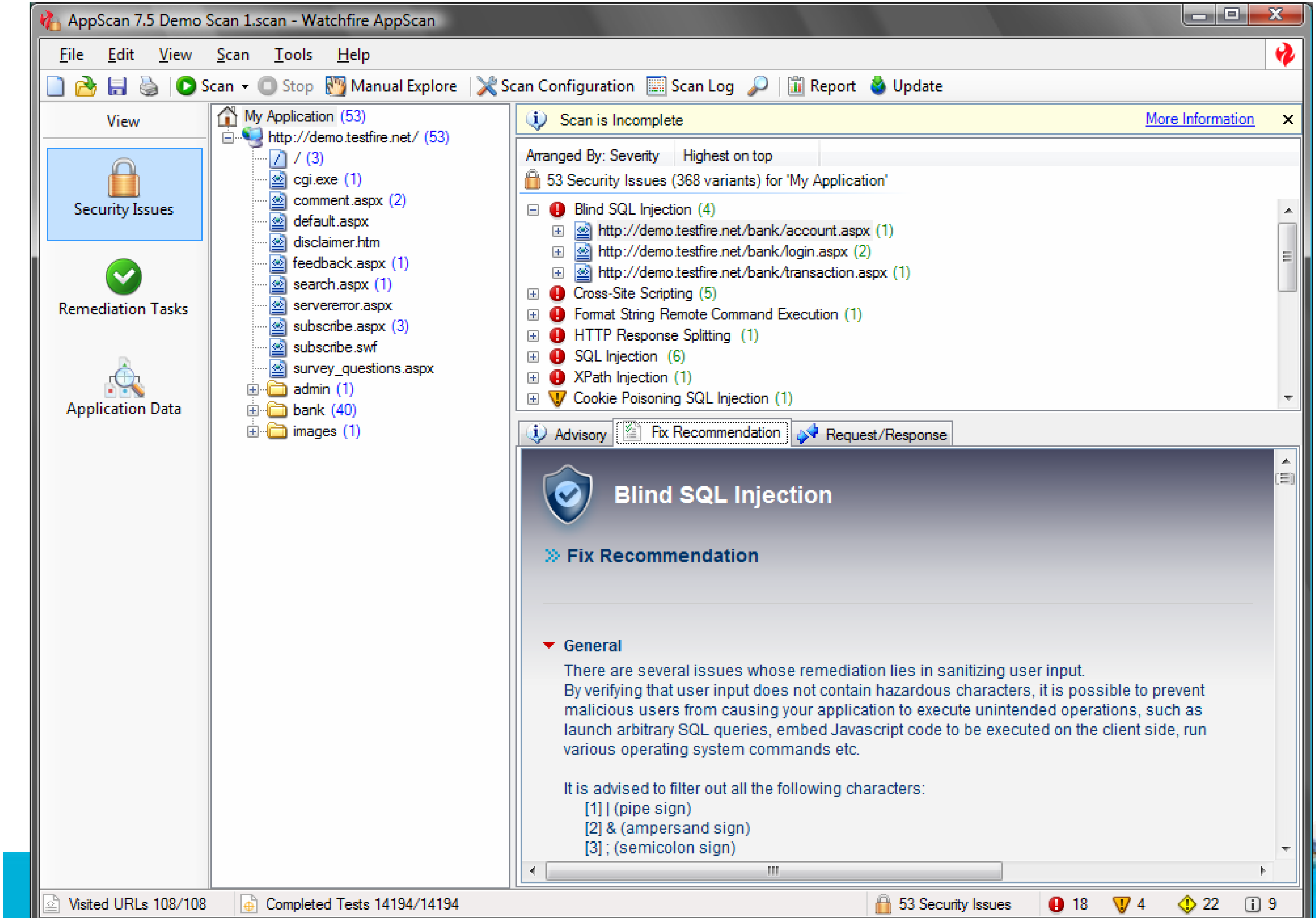
- Set parameter 'uid's value to '>'><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>'
- Set parameter 'uid's value to '>'><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>'

Request:

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

And Most Important :

Actionable Fix Recommendations



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)

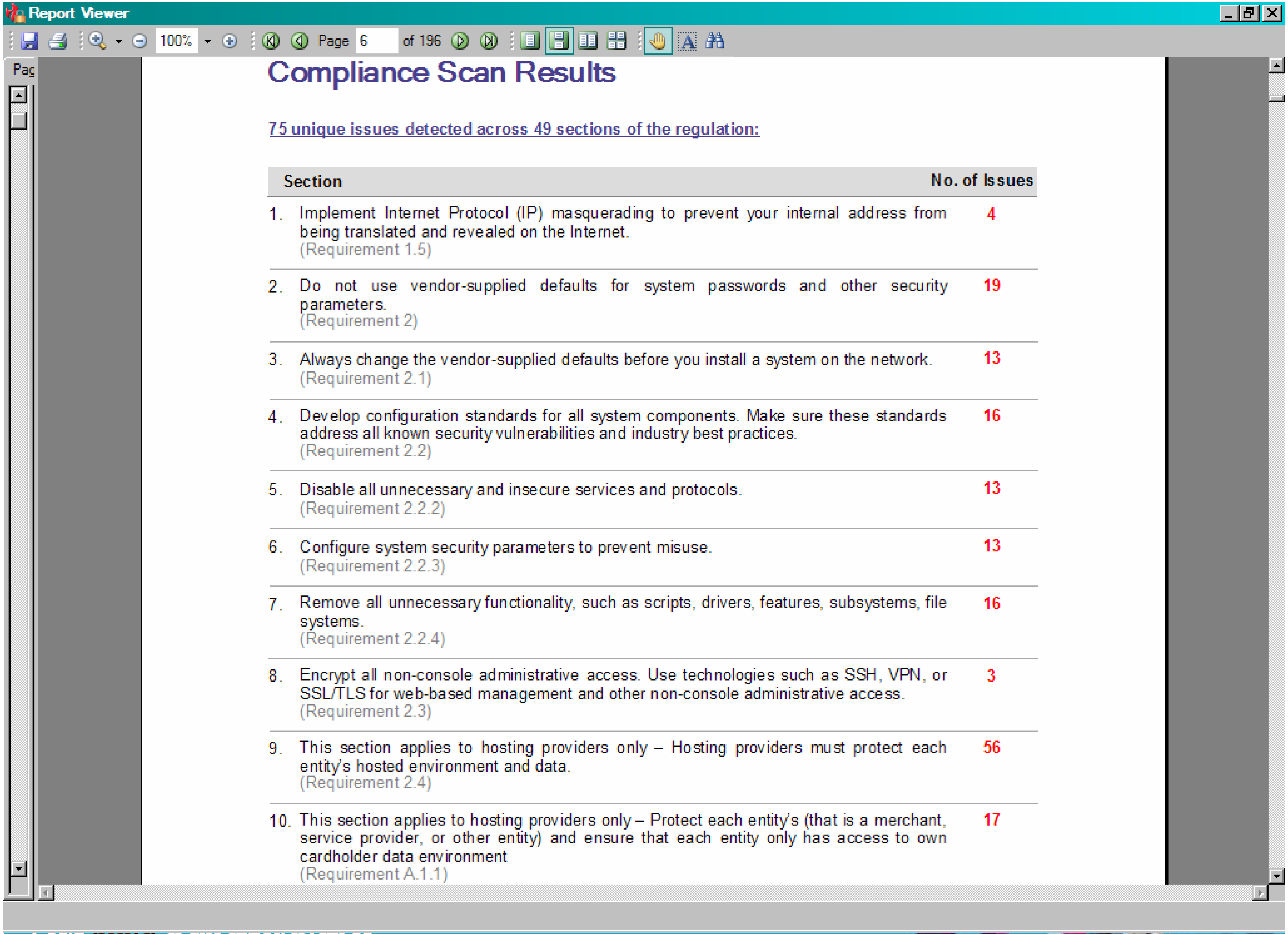
Blind SQL Injection

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)

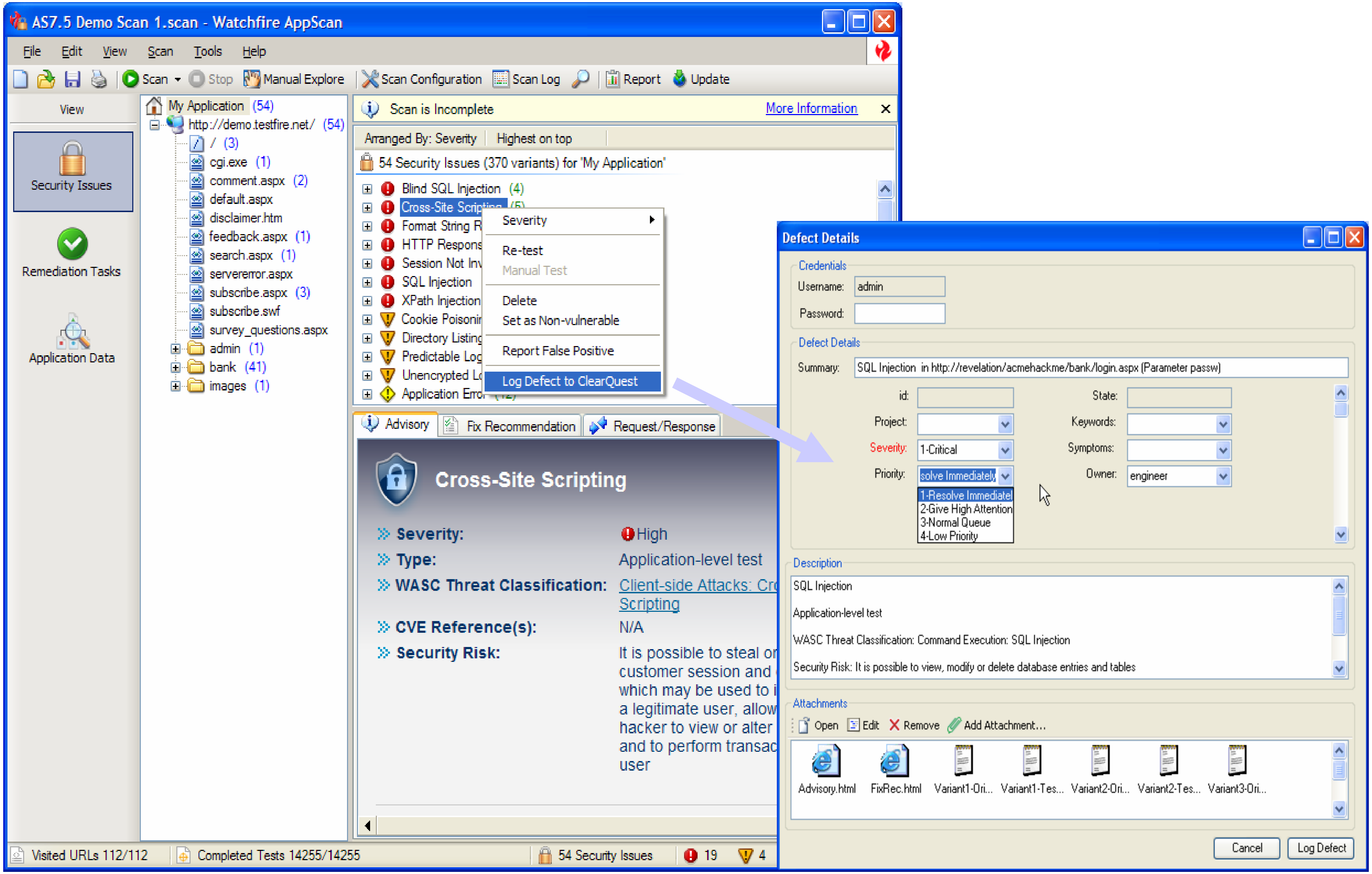


Compliance Scan Results

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

AppScan with QA Defect Logger for ClearQuest



Scan is Incomplete

54 Security Issues (370 variants) for 'My Application'

Cross-Site Scripting

Severity:	High
Type:	Application-level test
WASC Threat Classification:	Client-side Attacks: Cr… Scripting
CVE Reference(s):	N/A
Security Risk:	It is possible to steal or… customer session and… which may be used to i… a legitimate user, allow… hacker to view or alter… and to perform transac… user

Visited URLs 112/112 | Completed Tests 14255/14255 | 54 Security Issues | 19 | 4

Username: admin

Password:

Summary: SQL Injection in http://revelation/acmehackme/bank/login.aspx (Parameter passw)

Severity: 1-Critical

Priority: solve Immediately

Owner: engineer

Description:

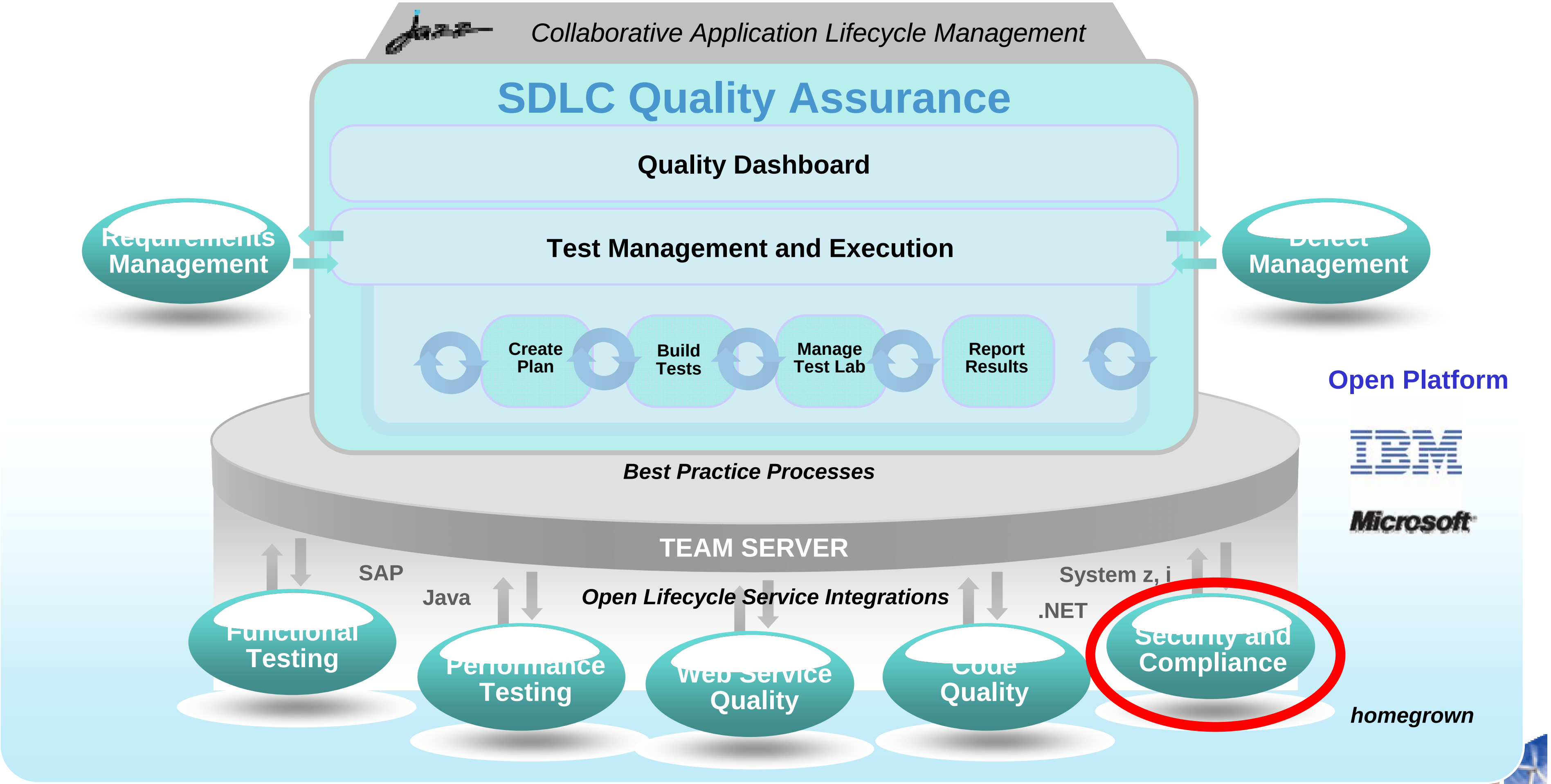
SQL Injection

Application-level test

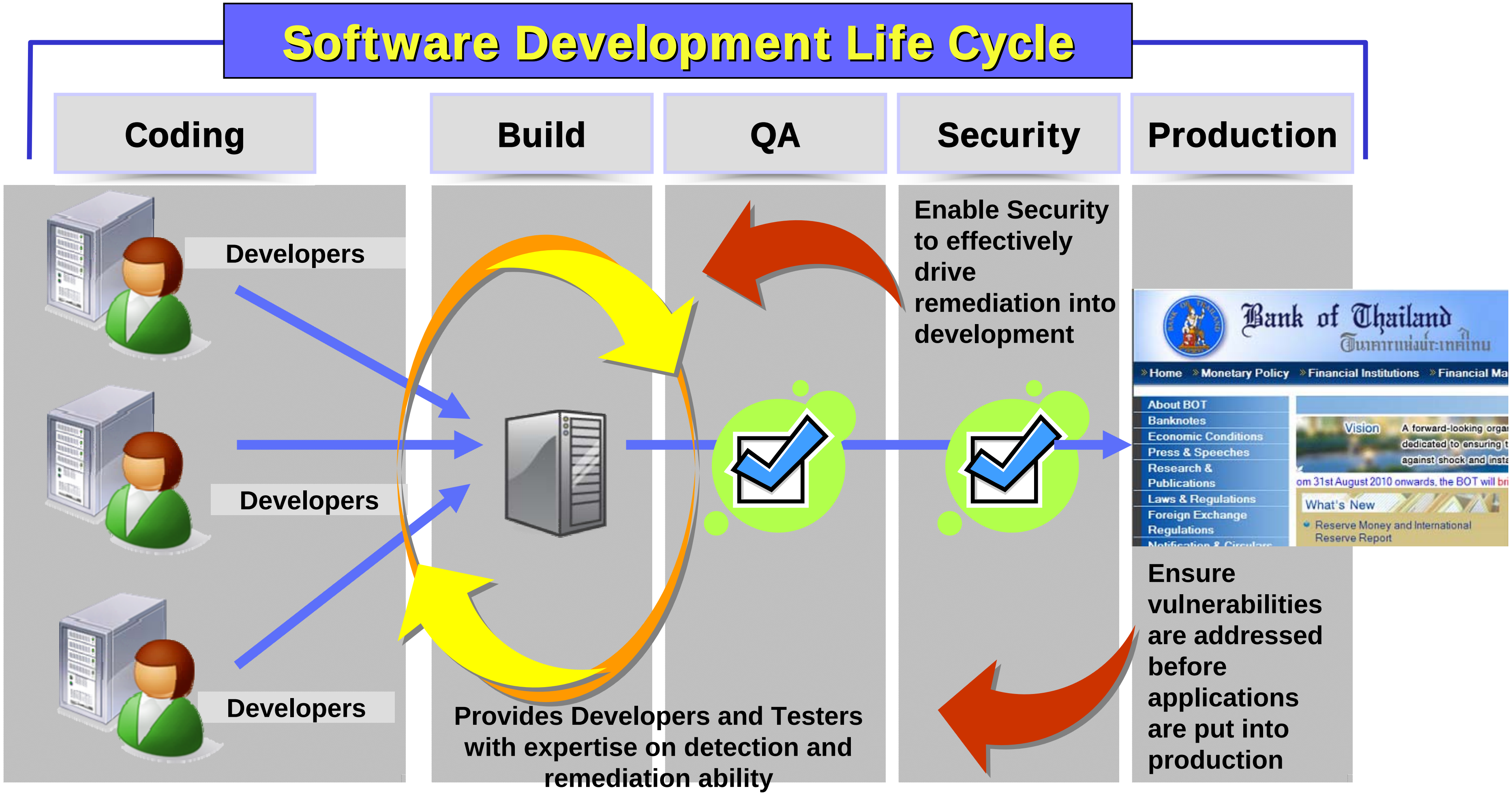
WASC Threat Classification: Command Execution: SQL Injection

Security Risk: It is possible to view, modify or delete database entries and tables

SECURITY TESTING IS PART OF SDLC QUALITY TESTING



Building security & compliance into the SDLC – further back



A forward-looking orga dedicated to ensuring t against shock and insta

om 31st August 2010 onwards, the BOT will bri

- Reserve Money and International Reserve Report

Enable Security to effectively drive remediation into development

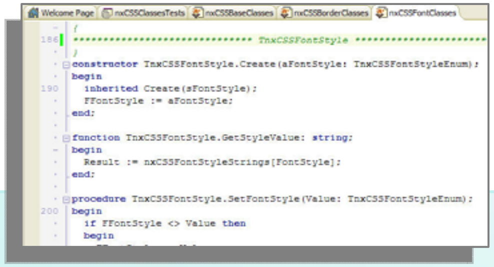
Ensure vulnerabilities are addressed before applications are put into production

Provides Developers and Testers with expertise on detection and remediation ability

Software Security Testing Technologies

Static Code Analysis = Whitebox

- Looking at the code for security issues (code-level scanning)

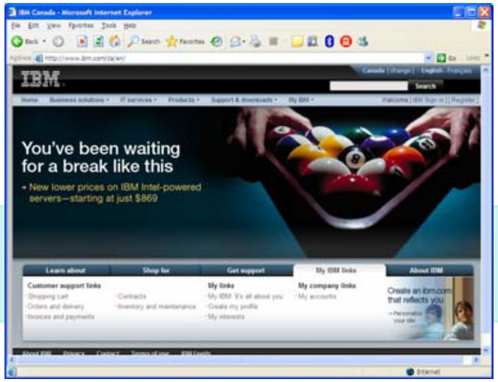


```
{
****************************** TnxCSSFontStyle ******************************
}
constructor TnxCSSFontStyle.Create(aFontStyle: TnxCSSFontStyleEnum);
begin
  inherited Create(sFontStyle);
  FFontStyle := aFontStyle;
end;

function TnxCSSFontStyle.GetStyleValue: string;
begin
  Result := nxCSSFontStyleStrings[FontStyle];
end;

procedure TnxCSSFontStyle.SetFontStyle(Value: TnxCSSFontStyleEnum);
begin
  if FFontStyle <> Value then
  begin
```

Code integrity

Dynamic Analysis = Blackbox

- Sending tests to a functioning application



IBM Canada - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
http://www.ibm.com/ca/en/
IBM
Search
Home Business solutions IT services Products Support & downloads My IBM
Learn about
Shop for
Get support
My IBM links
About IBM
Internet

You've been waiting for a break like this

- New lower prices on IBM Intel-powered servers—starting at just $869

Customer support links

Shopping cart · Orders and delivery · Invoices and payments · Contracts · Inventory and maintenance

My links

My IBM: It's all about you · Create my profile · My interests

My company links

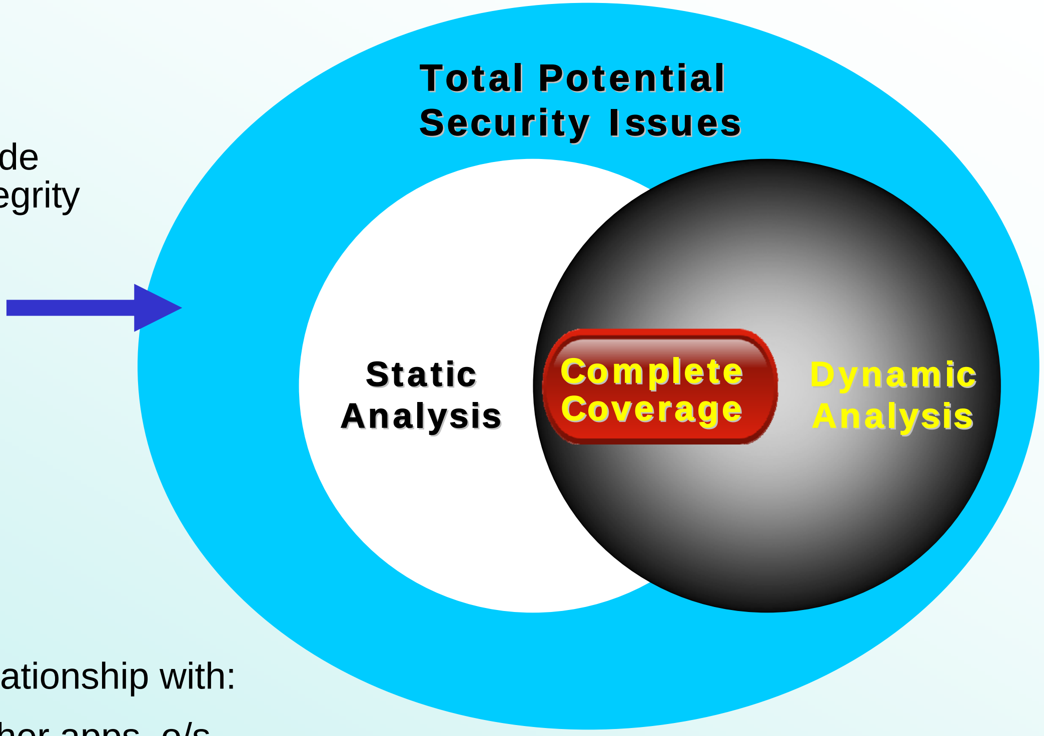
My accounts

Create an ibm.com that reflects you

Relationship with:

-Other apps, o/s

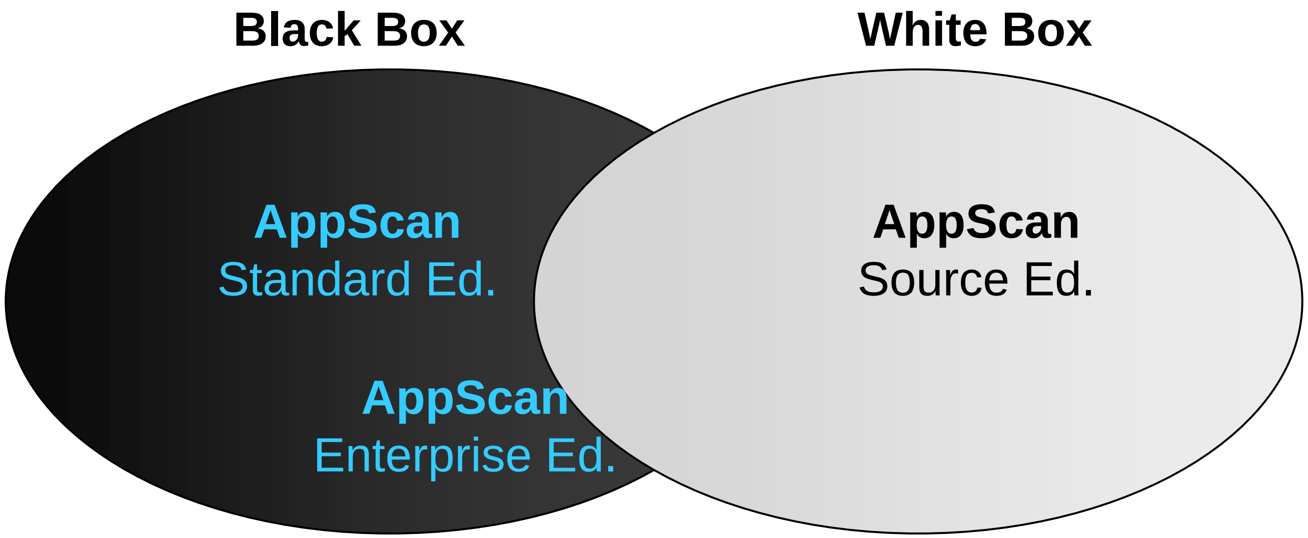
-Middleware, infra



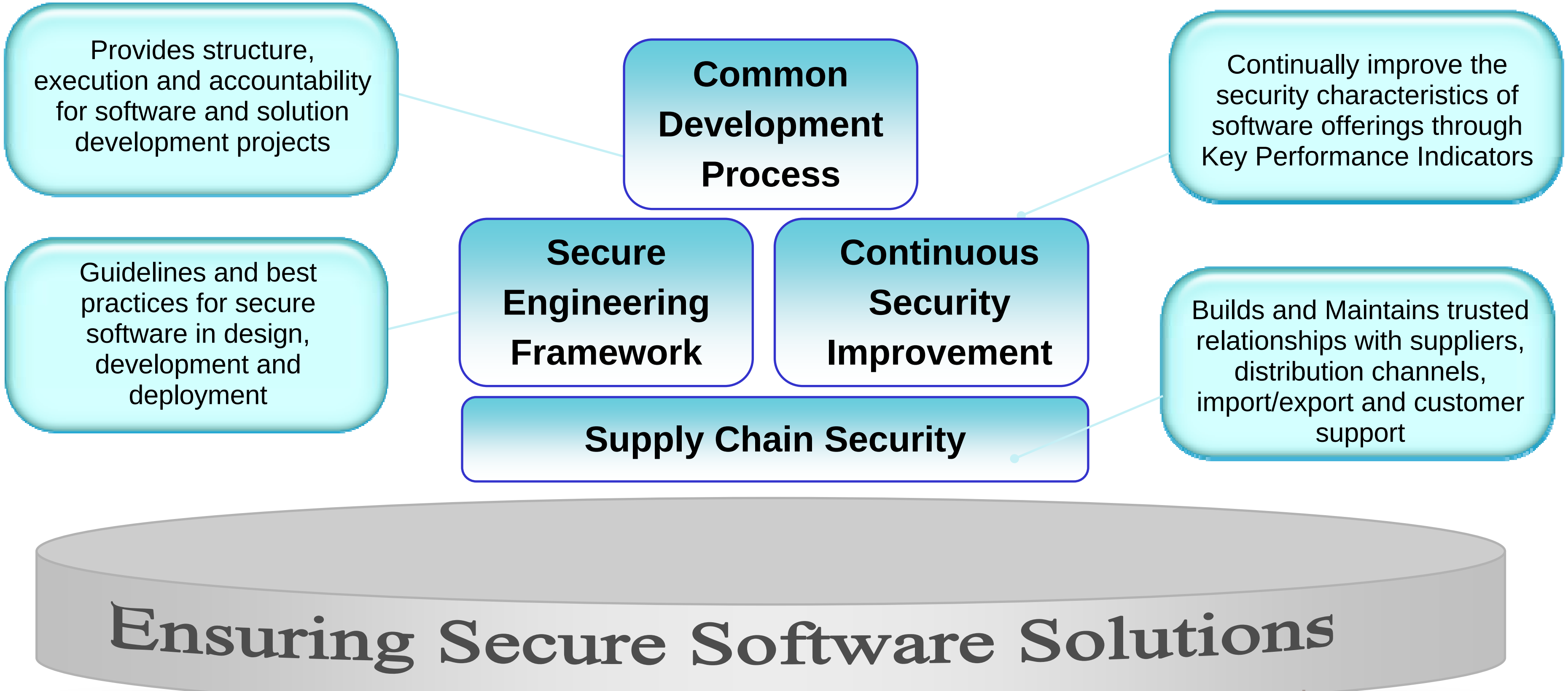
Application Development Security Testing Domains

BLACK BOX *IBM Rational Appscan Standard Edition*	WHITE BOX *IBM Rational Appscan Source Edition*
Dynamic APPLICATION Analysis	**Static CODE Analysis**
Good for security folks who are not experienced in application development	Good for developers who are not experienced in security
Don't need to worry about code	Provides learning for developers
Simulates real-world exploit attack	**Good for interim audit of half-written code**
Tests for relation between App and other apps, O/S, middleware, network	Can test for more than just HTTP /HTML code - eg. C, C++, C#, Perl, Codefusion, Javascript …
Like IPS, checks for "unknown" threats	Like Firewall, checks for "known" threats

- **Two approaches to web application security scanning**
  - Black-box - Automates attacker actions
  - White-box - Automates code auditing
- Challenges and issue coverage are different
- Complete solution – ***involve more people in the organization***
- Objective – ***build the knowledge, minimize future errors & risks***



IBM Secure Engineering Initiative


Provides structure, execution and accountability for software and solution development projects
Common Development Process
Continually improve the security characteristics of software offerings through Key Performance Indicators
Guidelines and best practices for secure software in design, development and deployment
Secure Engineering Framework
Continuous Security Improvement
Builds and Maintains trusted relationships with suppliers, distribution channels, import/export and customer support
Supply Chain Security
Ensuring Secure Software Solutions

Link to Security Engineering Framework: http://www.redbooks.ibm.com/redpieces/abstracts/redp4641.html?Open

- IBM develops products and solutions for sale.
- IBM develops and operates solutions and services for its own internal use.
- IBM develops and operates solutions and services on behalf of customers.

NEW

IBM

…for Review February 24, 2010 3:41 pm

REDP-4641-00

Security in Development: The IBM Secure Engineering Framework

Redguides for Business Leaders

Danny Allan
Tim Hahn
Andras Szakal
Jim Whitmore
Axel Buecker

- Investigating common development processes and the IBM Integrated Product Development process
- Emphasizing security awareness and requirements in the software development process
- Discussing test and vulnerability assessments

Redbooks

Introducing IBM Secure by Design

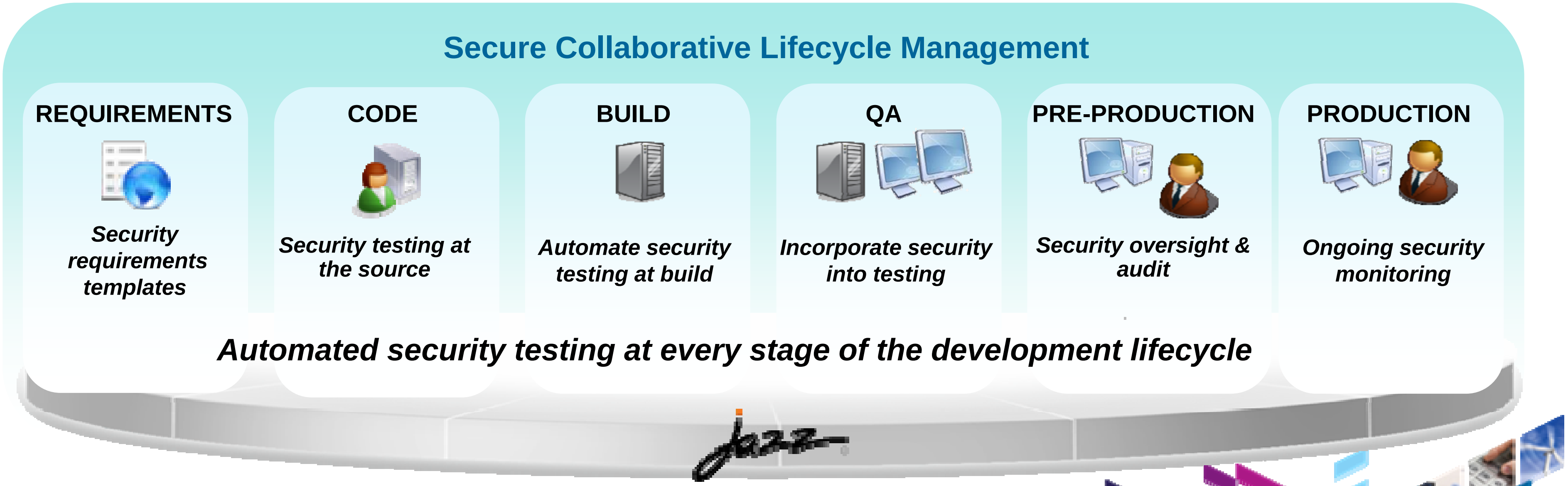
Automate security testing early & often throughout the development lifecycle

- 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

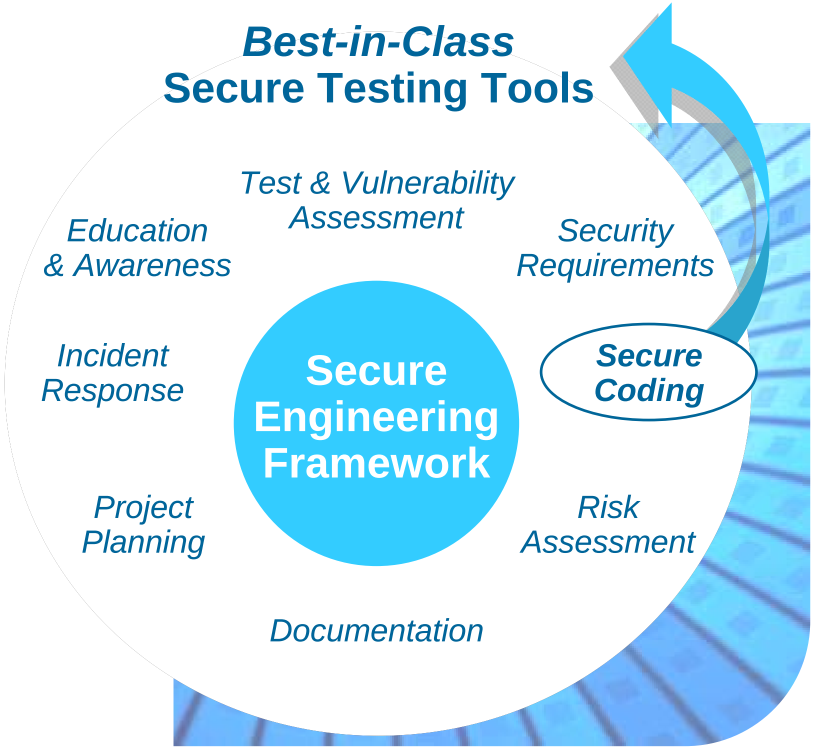
REQUIREMENTS	CODE	BUILD	QA	PRE-PRODUCTION	PRODUCTION
Security requirements templates	*Security testing at the source*	*Automate security testing at build*	*Incorporate security into testing*	*Security oversight & audit*	*Ongoing security monitoring*

Automated security testing at every stage of the development lifecycle

Delivering new Secure by Design tools and frameworks

Implement security best practices and tools into each phase of the lifecycle

- A proven security blueprint for building and deploying secure software in both application and manufactured product scenarios
- Enables on time, on budget delivery of secure software via automated source code testing
- Manage the proliferation of portal and Web applications with more scalable, high performance identity and access management



"Utilizing IBM's leading AppScan family of application security solutions has proven to be of significant value to our customers in reducing their overall risk and demonstrating compliance."

- Joey Peloquin, Director, Application Security, Fishnet Security

Conclusion:

SECURITY BY APPLICATION DEVELOPMENT QUALITY

- **The Application Must Defend Itself**
  - Firewalls & IPS etc cannot stop an application attack
- **Application Security must be strategic, not ad hoc or afterthought**
- **Both security and development teams need to be in harmony**
- **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**

Lower Compliance & Security Costs by:

- **Ensuring Security Quality in the Application up front**
- **Not having to do a lot of rework after production**

Don’t worry – IBM to the rescue

Securing the SDLC: A Business Perspective

ISC2TV | December 14, 2009

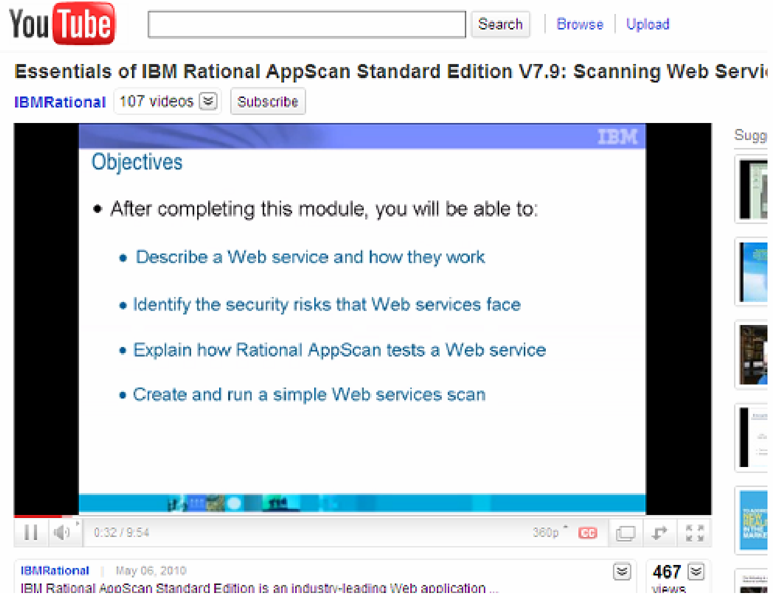
You Tube
Search
Browse
Upload
Sign

Innovate 2010 Application Security and Compliance

Ibminnovate
42 videos
Subscribe
0:50 / 1:19
360p
Suggestions
Innovate 2010 Cloud Computing
by ibminnovate
59 views
Patrick Kane's 2010 Stanley Cup Winning Goal
68,071 views
Innovate 2010 Modeling, Architecture and Constr...
by ibminnovate
Innovate 2010 Walker Royce Chief Software Daily
by ibminnovate
Innovate 2010 Grady Booch Chief Scientist IBM R...
by ibminnovate
106 views
Innovate 2010 Jazz Solutions
25
views

ibminnovate | June 10, 2010

Danny Allan talks about the importance in application security and compliance



Essentials of IBM Rational AppScan Standard Edition V7.9: Scanning Web Servi

Objectives

- After completing this module, you will be able to:
  - Describe a Web service and how they work
  - Identify the security risks that Web services face
  - Explain how Rational AppScan tests a Web service
  - Create and run a simple Web services scan

IBMRational | May 06, 2010

IBM Rational AppScan Standard Edition is an industry-leading Web application ...

You Tube
application security anthony
Search
Browse
Upload
Sign Out

Why web application security is important

questexhk
48 videos
Subscribe
What makes current web security practices useless?
0:09 / 5:09
360p
192
views
Like
Save to
Share
<Embed>
Suggestions
Web Application Security Fundamentals pt 5
by PCISboonbox
218 views
8:07
Web Application Security in todays challenging ...
by WFRational
214 views
2:21
Software Testing vs. Software Quality Assurance...
by portnovschool
17,719 views
4:12
Web application security issues and solutions
by helpnetsecurity
1,412 views
3:46
Web Security Today
by DeepNines
19 views
0:36
Owasp5034 Part2 - LOTUS NOTES AND DOMINO WEB
by mediarchives
201 views
9:00

questexhk | November 06, 2008

Anthony Lim continues the discussion around web application security, how hac...

Thank You

ขอบคุณครับ

www.ibm.com/software/rational

www.ibm.com/security

www.isc2.org

www.owasp.org