WEB APPLICATION SECURITY
* YOUR LAST LINE OF DEFENSE *

Anthony Lim
MBA CISSP FCITIL
Director Asia Pacific, Security
Rational Software
IBM, Singapore
<table>
<thead>
<tr>
<th>Top Priorities</th>
<th>2006 Rank</th>
<th>2007 Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Building a secure IT environment - Security threats,</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>business continuity, access control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reducing total cost of IT over time – Resource</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>utilization, growing infrastructure requirements, more</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cost effective technologies/services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Faster deployment of applications – expedite applications</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>availability or functionality enhancements to corporate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outsourcing part of IT</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Building a Utility/On-demand/Adaptive/Dynamic IT</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>environment</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In terms of Top business goals:

#1 reducing cost structure
#2 expanding business in existing or new geographies
#3 Improving customer service

APJ Continuum Survey, 2007
The Security Journey Continues

• New and More …
  • Applications
  • Services
  • Systems
    -> Vulnerabilities
    -> Hacking methods
    -> Viruses, Worms, RATS, Bots …
      (Remote Access TROJANS = Spyware)
    -> GOVERNANCE &
      COMPLIANCE!

NEW AREAS
OF IT SECURITY
WEAKNESS
ARISE ALL THE
TIME
It Gets Worse

- WAP, GPRS, EDGE, 3G
- 802.1x
- Broadband

A hacker no longer needs a big machine
Sheer Volume of Applications Keeps You From Getting Ahead of the Problems

1. Security Team Has Become a Bottleneck
2. Lack of Control and Visibility
3. Catching Problems Late in the Cycle
4. Not Monitoring Deployed Applications
5. Difficulty Managing 3rd Party Vendors

Have to do more with less, still; Risk is high, accountability is prevalent
Software Application Development Pressures

4 most common laments of the development executive

I’m being asked to:

• Deliver product faster (a lot faster!)
• Increase product innovation
• Improve quality
• Reduce cost
WE ARE HIGHLY DEPENDENT ON WEB SERVICES TODAY

- WORK / BUSINESS
  - INTERNET, INTRANET, EXTRANET
    - ERP, SCM, CRM, SAP, B2BM, B2C, COMPANY INTERNAL INFO SERVICES

- PLAY / SOCIAL NETWORKING / RECREATION
  - YouTube, Facebook, Second Life, Friendster, ITunes, MySpace, BLOGS! …

- EDUCATION / RESEARCH

- TRANSACTIONS / ONLINE SERVICES
  - INTERNET BANKING, MEMBERSHIP PORTAL, TRAVEL BOOKING, TRADING
    - B2C, C2C, Amazon, EBay E*Trade …

- COMMUNICATION

- WEB 2.0, SOA

- ONLINE STORAGE SERVICES

- ….
SO WHY ARE THESE HAPPENING?

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.

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

Hack into Obama campaign site exploited a coding flaw

SAN JOSE, Calif. (AP) -- A simple flaw in the coding of Sen. Barack Obama’s Web site led to before the important Pennsylvania primary.

Some supporters who tried to visit the community blogs section of Obama’s site started noticing Rodham Clinton’s official campaign site.

Security researchers said a hacker exploited a so-called “cross-site scripting” vulnerability in
The Alarming Reality

LexisNexis Data Breach
- Washington Post
  Feb 17, 2008

IndiaTimes.com Malware
- InformationWeek
  Feb 17, 2008

Mac blogs defaced by XSS
- The Register, Feb 17, 2008

Chinese hacker steals 18M identities
- HackBase.com, Feb 10, 2008

Hacker breaks into Ecuador’s presidential website
- Thaindian, Feb 11, 2008

Two Indonesian government web sites defaced
- CNET Asia, Mar 29, 2008

Hacker steals Davidson Cos client data
- Falls Tribune, Feb 4, 2008

U.S. Embassy Web Site In Manila, Defaced
- AllHeadlineNews, Mar 27, 2008

Hacking Stage 6
- Wikipedia, Feb 9 2007

Greek Ministry websites attacked
- eKathimerini, Jan 31, 2008

Drive-by Pharming in the Wild
- Symantec, Jan 21, 2008

RIAA wiped off the Net
- TheRegister, Jan 20, 2008

Italian Bank hit by XSS fraudsters
- Netcraft, Jan 8, 2008

Indian Times.com
Malware

Mac blogs defaced by XSS
- The Register, Feb 17, 2008

Chinese hacker steals 18M identities
- HackBase.com, Feb 10, 2008

Hacker breaks into Ecuador’s presidential website
- Thaindian, Feb 11, 2008

Two Indonesian government web sites defaced
- CNET Asia, Mar 29, 2008

Hacker steals Davidson Cos client data
- Falls Tribune, Feb 4, 2008

U.S. Embassy Web Site In Manila, Defaced
- AllHeadlineNews, Mar 27, 2008

Hacking Stage 6
- Wikipedia, Feb 9 2007

Greek Ministry websites attacked
- eKathimerini, Jan 31, 2008

Drive-by Pharming in the Wild
- Symantec, Jan 21, 2008

RIAA wiped off the Net
- TheRegister, Jan 20, 2008

Italian Bank hit by XSS fraudsters
- Netcraft, Jan 8, 2008
Social networking sites targeted by hackers

ANDREA SOH

JUST keep to legitimate websites and you will be safe from security threats. Think again, warns a US-headquartered computer security company.

While it used to be that Netizens could fall prey to security breaches by unknowingly visiting malicious sites or accidentally clicking on malicious e-mail attachments, these days they can be affected just by visiting regular everyday sites.

More of such websites, like those of banks, social networking and government websites, are being targeted by hackers.

In the Internet Security Threat Report released yesterday, Symantec noted that there were 878,953 phishing host computers which host phishing websites — in the second half of 2007, an increase of 167 per cent compared to the first half.

Phishing, or the theft of personal information such as bank and credit card account details, is done through creating lookalikes of these legitimate sites, e-mail and instant messaging.

Mr Stephen Trilling, Symantec Security Technology and Response vice president said: “Avoiding the dark alleys of the Internet was sufficient advice in years past. Today’s criminal is focused on compelling legitimate websites to launch attacks on end-users, which underscores the importance of maintaining a strong security posture no matter where you go and what you do on the Internet.”

The report provides a six-month update from the Internet threat activity in the Asia Pacific region from July to December last year. It includes an analysis of disclosed vulnerabilities, malicious code reports and security risks.

Also, stolen information obtained through phishing and keystroke logging, has become so plentiful that the price of stolen data has hit a new low, my paper reported on Wednesday.

A list, including a person’s name, address, date of birth, a functioning credit card number and US Social Security number, can be purchased in the underground economy for as little as US$1 ($1.40). Symantec said, Port valu, it costs between US$10 and US$150.

Symantec Singapore general manager Duan Hoi: “Social networking sites are extremely attractive because not only do the profiles on such sites contain a significant amount of personal information, users usually allow a trusted site to execute code on their computers.”

HELPDESK 电子字典

Videoographer: 电视录像员

diān shí yǔ xiàng yuán

Resume: 简历 Jiàn lì

Innovative: 创新的

chuàng xīn de
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
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.servlet.ServletRequestDispatcher.invoke(ServletRequestDispatcher.java:254)
    at com.evermind[Oracle Application Server Containers for J2EE 10g [9.0.4.2.0]].server.servlet.ServletRequestDispatcher.forwardInternal(ServletRequestDispatcher.java:799)
    at com.evermind[Oracle Application Server Containers for J2EE 10g [9.0.4.2.0]].server.HTTPRequestHandler.processRequest(HTTPRequestHandler.java:79)
    at com.evermind[Oracle Application Server Containers for J2EE 10g [9.0.4.2.0]].server.HTTPRequestHandler.run(HTTPRequestHandler.java:208)
    at com.evermind[Oracle Application Server Containers for J2EE 10g [9.0.4.2.0]].server.HTTPRequestHandler.run(HTTPRequestHandler.java:125)
    at com.evermind[Oracle Application Server Containers for J2EE 10g [9.0.4.2.0]].util.ReleaseableResourcePooledExecutor$MyWorker.run(ReleaseableResourcePooledExecutor.java:85)
    at java.lang.Thread.run(Thread.java:534)
Server Error in '/' 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.

Details: To enable the details of this specific error message to be viewable on the local server machine, please create a <customErrors> tag within a "web.config" configuration file located in the root directory of the current web application. Set the "mode" attribute to "Off" to enable details to be viewable on remote machines.

<configuration>
  <system.web>
    <customErrors mode="RemoteOnly"/>
  </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.

<configuration>
  <system.web>
    <customErrors mode="On" defaultRedirect="mycustompage.htm"/>
  </system.web>
</configuration>
An Error Has Occurred

Summary:

Unclosed quotation mark after the character string ".

Error Message:

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Size</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/27/2007</td>
<td>12:20 PM</td>
<td>1831</td>
<td>20060308_bak</td>
</tr>
<tr>
<td>7/16/2007</td>
<td>8:36 AM</td>
<td>4089</td>
<td>account.aspx</td>
</tr>
<tr>
<td>11/20/2006</td>
<td>10:05 AM</td>
<td>771</td>
<td>apply.aspx</td>
</tr>
<tr>
<td>7/16/2007</td>
<td>8:35 AM</td>
<td>446</td>
<td>customize.aspx</td>
</tr>
<tr>
<td>11/1/2006</td>
<td>8:42 PM</td>
<td>78</td>
<td>logout.aspx</td>
</tr>
<tr>
<td>7/16/2007</td>
<td>9:39 AM</td>
<td>3254</td>
<td>logout.aspx.cs</td>
</tr>
<tr>
<td>7/16/2007</td>
<td>8:21 AM</td>
<td>935</td>
<td>main.aspx</td>
</tr>
<tr>
<td>7/16/2007</td>
<td>9:36 AM</td>
<td>3951</td>
<td>main.aspx.cs</td>
</tr>
<tr>
<td>7/27/2007</td>
<td>12:20 PM</td>
<td>23</td>
<td>members</td>
</tr>
<tr>
<td>1/12/2007</td>
<td>1:55 PM</td>
<td>1414</td>
<td>moxpath.js</td>
</tr>
<tr>
<td>11/20/2006</td>
<td>10:05 AM</td>
<td>785</td>
<td>queryxpath.aspx</td>
</tr>
<tr>
<td>11/20/2006</td>
<td>10:05 AM</td>
<td>1838</td>
<td>queryxpath.aspx.cs</td>
</tr>
<tr>
<td>7/18/2007</td>
<td>5:13 PM</td>
<td>499</td>
<td>servererror.aspx</td>
</tr>
<tr>
<td>7/18/2007</td>
<td>4:13 PM</td>
<td>1700</td>
<td>transaction.aspx</td>
</tr>
<tr>
<td>7/18/2007</td>
<td>4:15 PM</td>
<td>3826</td>
<td>transaction.aspx.cs</td>
</tr>
<tr>
<td>7/17/2007</td>
<td>3:03 PM</td>
<td>3930</td>
<td>transfer.aspx</td>
</tr>
<tr>
<td>7/18/2007</td>
<td>4:51 PM</td>
<td>3505</td>
<td>transfer.aspx.cs</td>
</tr>
<tr>
<td>7/17/2007</td>
<td>2:44 PM</td>
<td>82</td>
<td>ws.asmx</td>
</tr>
</tbody>
</table>
System error

A system error occurred.

Have a look at the details, or contact your system administrator.

OK
Hide Details

Fehlermeldung:

at org.apache.jasper.servlet.JspServletWrapper.service(JspServlet.java:853)
at org.apache.jasper.servlet.JspServlet.service(JspServlet.java:2)
at javax.servlet.http.HttpServlet.service(HttpServlet.java:853)
at org.apache.catalina.core.ApplicationDispatcher.invoke(ApplicationDispatcher.java:976)
at org.apache.catalina.core.ApplicationDispatcher.doInclude(ApplicationDispatcher.java:924)
at org.apache.catalina.core.ApplicationDispatcher.include(ApplicationDispatcher.java:905)
at com.openems.flex.cache.CmdFlexRequestDispatcher.include(CmdFlexRequestDispatcher.java:6)
Try to modify the cookie values?

Hackers don’t use Microsoft Internet Explorer Browser
Real Example: Online Travel Reservation Portal

Change the reserID to 2001200

Hotel Reservation Online

Dear Mr. Sam,

As a result of your reservation 20031959 at the hotel Le Meridien / Jakarta / Indonesia for 2 nights (from Jan 23 2007 to Jan 25 2007), we processed a credit card transaction on Jan 15, 2007. The credit card transaction was successful. The details of your transaction are as follows:

Reservation number: 20031959
Card Holder Name: Sam
Credit/Debit Card: xxx-xxx-xxx-xxx-2196
Expiration Date: 06/2007
Amount: 240.00 SGD
Date: Jan 15, 2007

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,
Real Example: Parameter Tampering

Reading another user’s transaction – insufficient authorization

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

You can get your invoice following this link: https://www.*****/invoice.php?reserID=2001200&email=*****@hotmail.com
Parameter Tampering - Reading another user’s invoice

The same customer invoice that reveals the address and contact number

To: Justin, Mikasa
Company:
Address: 23 [redacted], Australia
Phone: 61 [redacted]

RECEIPT / TAX INVOICE #2001200

Date: Jan 30 2006

<table>
<thead>
<tr>
<th>Description</th>
<th>Nights</th>
<th>Rate</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Booking reference 2001200 at hotel: Nikko Resort And Spa / Bali / Indonesia</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Period: From Jan 18 2006 to Jan 23 2006 (5 night(s))</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ocean View Room, Breakfast Included 2 adult(s), 0 child(ren), 0 infant(s)</td>
<td>5</td>
<td>138</td>
<td>690.00 AUD</td>
</tr>
</tbody>
</table>

TOTAL AMOUNT 506.61 USD

The Payment, billed as [redacted], was received by credit card, on Jan 03, 2006, to our account from

Card Holder Name: [redacted]
Credit/Debit Card: [redacted]
Expiration Date: 08/2007

We hope you had a nice stay at this hotel!
We are looking forward to making a new reservation for you!
With our thanks,
Top Hack Attacks Today Target Web Services

Cross-site scripting has shot up the list of most common vulnerabilities

Source: US-CERT Common Vulnerabilities and Exposures
# Web Application Hacks are a **Business** Issue

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

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

2) User sends script embedded as data

3) Script/data returned, executed by browser

4) 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
Hackers Attack Apps by Exploiting Unintended Functionalities

- Intended Functionality
- Unintended Functionality
- Actual Functionality
Growth In Browser Vulnerabilities

Source: IBM Xforce 2007 Annual Report
Why Do Application Security Problems Exist

OUR GOAL IS TO WRITE BUG-FREE SOFTWARE. I'LL PAY A TEN-DOLLAR BONUS FOR EVERY BUG YOU FIND AND FIX.

YAHOO! WE'RE RICH

I HOPE THIS DRIVES THE RIGHT BEHAVIOR.

I'M GONNA WRITE ME A NEW MINIVAN THIS AFTERNOON!
Existing Solutions Don’t Address App Security

- **IT Security Solutions are usually for network and infrastructure**
  - Firewalls and IPS’s don’t block application attacks
  - Port 80, 8080 and 443 are open
  - Network scanners won’t find application vulnerabilities.
    - Nessus, ISS, Qualys, Nmap, etc.

- **IT Security professionals are typically from the network /infrastructure area, and usually have little experience in software application development**

- **Developers are usually not trained in or mandated to security.**
  - 64% of developers are not confident in their ability to write secure applications – Microsoft Developer Research
  - Developers do not care about security, they think its someone else’s job
    - (even though they are the root cause)

- **Security teams are focused on other issues (network, desktops, etc) and overwhelmed**
  - *They don’t want to have to deal with another new issue that they don’t understand*

- **No defined policy, accountability or process to deal with the issue (not many people understand application attacks today)**
Why would anyone want to attack a web site?
The Fact: Attacks targeted at a new area

<table>
<thead>
<tr>
<th>Security</th>
<th>Spender</th>
</tr>
</thead>
<tbody>
<tr>
<td>% of Attacks</td>
<td>% of Dollars</td>
</tr>
<tr>
<td>75%</td>
<td>10%</td>
</tr>
<tr>
<td>25%</td>
<td>90%</td>
</tr>
</tbody>
</table>

In an organization, IT Security people and developers are poles apart

Sources: Gartner, IDC, Watchfire
Regulation & Compliance

- It is part of doing business
- Business Continuity
- An environment of TRUST
  - For doing business
  - Ensure Orderliness in Internet world
  - Promote Economic growth

- More than just Confidentiality, Integrity and Availability
- Privacy

People never learn – there will be another Edison Chen case – that’s why I still have a job today
Requirement 6.5 calls for developers to use OWASP (Open Web Application Security Project) guidelines to prevent common coding errors. Secure coding practices can be a co-factor leading to more thoughtfully written applications that are easier to maintain because they are documented and tested.
IBM Rational AppScan SDLC Ecosystem

IBM Rational AppScan Enterprise / Reporting Console

- **AppScan Developer Ed**: (Eclipse IDE)
- **AppScan Ent. QuickScan**: (web client)
- **AppScan Developer Ed**: for build systems (scanning agent)
- **AppScan Tester Ed**: (scanning agent)
- **AppScan Tester Ed**: (QA client)
- **AppScan Enterprise user**: (web client)
- **AppScan Standard Ed**: (desktop)

**Build**

- **Rational BuildForge**
- **Rational ClearQuest**
- **Rational Quality Manager**

**Security**

- **Security and Compliance Testing, oversight, control, policy, in-depth tests**

**QA**

- **Security / compliance testing incorporated into testing & remediation workflows**

**Code**

- **Build security testing into the IDE**
- **Automate Security / Compliance testing in the Build Process**

**IBM Rational Web Based Training for AppScan**
Rational Appscan – Functional Benefits

- Configure and tune scans to help ensure coverage for each application.

- Review and analyze results to help eliminate false positives and negatives, identify patterns, prioritize key issues and highlight key remediation tasks.

- Track remediation progress by maintaining trend data, tracking resolution of key issues from scan to scan and reporting on remediation effectiveness.

- Train your QA staff to use Rational AppScan throughout the Web application delivery lifecycle and help build security and compliance management into your applications from the ground up.

- Realtime results views that enable users to act on issues before a scan is complete.

- DON’T REALLY NEED TO HAVE I.T. SECURITY KNOWLEDGE OR EXPERIENCE
Rational Appscan – Basic Features

- **Scans anything and every thing web (HTTP/HTML, SOAP/XML)**
  - Java (Jsp), Microsoft/DotNet (Asp), Php, Ajax, Python, ...
- **Non-invasive hacker-simulation of over 14,000 permutations of 200+ attacks**
- **Rich reporting and granular remediation-assisting functions (very important)**
  - What is the purpose of scanning – to fix the issues
  - Separate Report Options for Executive, Security, Developers
  - Advanced remediation and fix recommendations for unmatched accuracy and efficiency
- **Constant and automatic updating over time of new fixes and defenses backed by worldwide R&D**
- **Over 44 global regulatory-compliance, best-practice and industry-standard testing bases out-of-the-box**
  - Eg Sarbanes Oxley, PCI, Basel II, ISO-27001, OWASP Top 10, ...
  - Can customize your own test/policy criteria
- **Used by more than 2000 organizations in the world**
Rational AppScan – Some Key Features

1. AppScan SDK & AppScan eXtensions Framework
2. Python-based Web app security testing platform
3. Enhanced AJAX support
4. Adaptive Test Process
5. Concurrent Scanning
6. Non-Vulnerable Tracking & Report False Negative
Integrated Computer Based Training

*Key to adoption across the organization is education*

**AppScan Knowledge OnDemand**

- **Self-service** – more convenient than traditional training
  - Participants no longer have to schedule time “out of the office”

- **Self-paced** – greater information retention
  - With digestible content modules, participants no longer experience information overload

- **Just-in-time reference-ability**
  - Full access to searchable, online content for 12 months

- **Structure**
  - Courses are individual modules
  - Typically 15 minutes or less
Identify Vulnerabilities
**Report**

**Detailed Findings**

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

Total of 2 findings in this URL

<table>
<thead>
<tr>
<th>[1 of 2] Cross site scripting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Severity:</strong> High</td>
</tr>
<tr>
<td><strong>Advisory &amp; Fix Recommendation:</strong> See Appendix 1</td>
</tr>
</tbody>
</table>

**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='&lt;script&gt;alert('Appscan%20-%20CSS%20attack%20may%20be%20used')&lt;/script&gt;';&amp;password=Demo1234&amp;x=y HTTP/1.0

Host: bank

Accept: */*

Accept-Language: en-us

User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)

Referer: http://bank/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='&lt;script&gt;alert('Appscan%20-%20CSS%20attack%20may%20be%20used')&lt;/script&gt;';&amp;password=Demo1234&amp;x=y HTTP/1.0

Host: bank

Accept: */*

Accept-Language: en-us

User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)

Referer: http://bank/bank/login.aspx
**Actionable Fix Recommendations**

1. Ensure that accessed files reside in the virtual path and have certain extensions; remove special characters from user input.

Completing this remediation task will address the following issues:

- Poison Null Byte Files Retrieval

Details:

- Ensure that the requested file resides in the virtual path of the web server.
- Make sure that only certain extensions can be opened.
- Remove special characters (Meta-characters) from the user's input, e.g. the pipe ("|"), character.
- Use 'explicit open' mode for files in Perl CGI Scripts.
Forthcoming AppScan DE (Mid Sep 08)

- Security Testing in your Development Environment (Architect, RAD or Eclipse)
- Integration with source code, WebSphere, ClearQuest
- Can interoperate with AppScan Enterprise for central licensing, permissions and oversight
Appscan: Scan Expert Recommendations

- Detect AJAX Frameworks
  - Turn on JavaScript Execution
- Case Sensitive Path
  - Deselect the Case-Sensitive option
- Detect Flash Objects
  - Turn on Flash parsing for URLs
Appscan: Explore the application many ways
Appscan: Or build your own test policy
Appscan: Industry Standard and Compliance Reports

Over 40 Standards Out of the box
AppScan Enterprise – Dashboards and Metrics
Appscan Enterprise: Access Control
**AppScan Enterprise / IBM Rational ClearQuest Integration**

![AppScan Enterprise / IBM Rational ClearQuest Integration](image)

On the screenshot, we see a webpage from IBM Rational Software Development Conference 2008. The page is titled "AppScan Enterprise / IBM Rational ClearQuest Integration". It appears to be a demonstration of the integration features between AppScan Enterprise and IBM Rational ClearQuest.

The screenshot shows the interface of AppScan Enterprise, with a focus on security issues. It is displayed under the Folders section with a list of security issues. The summary indicates there are 51 issues of 23 different types across 32 URLs.

### Security Issues

**Last Updated:** 1/22/2007 5:56:22 PM

**Summary:**
- There are 51 issues of 23 different types across 32 URLs.

**Items 1-51 of 51**

<table>
<thead>
<tr>
<th>Action</th>
<th>Export to Excel</th>
<th>Issue</th>
<th>Defect Id</th>
<th>Test URL</th>
<th>Element</th>
<th>Issue Type</th>
<th>Threat Class</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>33</td>
<td>12453</td>
<td><a href="http://revelation/acme">http://revelation/acme</a>... Submit</td>
<td>Blind SQL Injection</td>
<td>Command Execution: S...</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>35</td>
<td>12459</td>
<td><a href="http://revelation/acme">http://revelation/acme</a>... uid</td>
<td>Blind SQL Injection</td>
<td>Command Execution: S...</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>45</td>
<td>13240</td>
<td><a href="http://revelation/acme">http://revelation/acme</a>... comments</td>
<td>Blind SQL Injection</td>
<td>Command Execution: S...</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>61</td>
<td>13235</td>
<td><a href="http://revelation/acme">http://revelation/acme</a>... passw</td>
<td>Blind SQL Injection</td>
<td>Command Execution: S...</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>62</td>
<td>14111</td>
<td><a href="http://revelation/acme">http://revelation/acme</a>... content</td>
<td>Poison Null Byte Files R... Information Disclosure...</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Submit Defect</td>
<td>44</td>
<td>14329</td>
<td><a href="http://revelation/acme">http://revelation/acme</a>... uid</td>
<td>SQL Injection</td>
<td>Command Execution: S...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Open</td>
<td>38</td>
<td></td>
<td><a href="http://revelation/acme">http://revelation/acme</a>... passw</td>
<td>SQL Injection</td>
<td>Command Execution: S...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Open</td>
<td>29</td>
<td></td>
<td><a href="http://revelation/acme">http://revelation/acme</a>... listAccounts</td>
<td>SQL Injection</td>
<td>Command Execution: S...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Open</td>
<td>64</td>
<td></td>
<td><a href="http://revelation/acme">http://revelation/acme</a>... passw</td>
<td>Login Page SQL Injection</td>
<td>Command Execution: S...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Open</td>
<td>24</td>
<td></td>
<td><a href="http://revelation/acme">http://revelation/acme</a>...</td>
<td>Directory Listing</td>
<td>Information Disclosure...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Open</td>
<td>60</td>
<td></td>
<td><a href="http://revelation/acme">http://revelation/acme</a>...</td>
<td>Predictable Login Cred... Authentication: Brute ...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IBM Rational & Watchfire Product Synergy

SDLC

Requirements | Design | Code | Build | QA | Security | Compliance

IBM Rational

- Requisite Pro
- ROSE, RAM, Software Architect
- RAD
- ClearCase, Build Forge
- CQ, CQTM, RFT, RPT

Watchfire

- AppScan & AppScan Enterprise
- WebXM
- Privacy, Quality, Accessibility

#1 in Market Share for Application Security
- Gartner & IDC
  * Twice *
Building security & compliance into the SDLC

SDLC

Coding

Build

QA

Security

Production

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

Enable Security to effectively drive remediation into development
Conclusion: Application QA for Security

- **The Application Must Defend Itself**
  - You cannot depend on firewall or infrastructure security to do so

- **Bridging the GAP between Software development and Information Security**

- **QA Testing for Security must now be integrated and strategic**

- **We need to move security QA testing back to earlier in the SDLC**
  - at production or pre-production stage is late and expensive to fix
  - Developers need to learn to write code defensively and securely
SDLC QA - YOUR LAST LINE OF DEFENSE
Web Application Security - Research Resources

- www.owasp.org
- webappsec.org
- www.ibm.com/software/awdtools/appscan/
- www.ibm.com/software/software/rational
  - Look for “Quality Management”
  - And “Web Application Security”
WEB APPLICATION SECURITY
YOUR LAST LINE OF DEFENSE

Anthony Lim
Director, Asia Pacific, Security, Rational Software

Thank You