CLOUD COMPUTING SECURITY – THE SOFT SPOT

Security by Application Development Quality Assurance

Anthony Lim
MBA CISSP CSSLP FCITIL
Director, Asia Pacific, Software Security Solutions IBM, Singapore
Advisor & Secretary, Security & Governance, www.sitf.org.sg

Innovate 2010
The Rational Software Conference

Let’s build a smarter planet.
The premiere software and product delivery event.
August 10 Bangkok, Thailand
Prolog: The Security Journey Continues

- Every year - **New, More, Bigger, Better …**
  - **SYSTEMS & ARCHITECTURE**
  - **APPLICATIONS**
  - **SERVICES**
    - New Risks
    - New Vulnerabilities
    - New Hacking methods
      - Viruses, Worms, RATS, Bots …
    (Remote Access TROJANS = Spyware)
  - **GOVERNANCE & COMPLIANCE!**
    - DATA PRIVACY, POLICIES AUDIT
    - MOBILITY
    - DATA LEAKAGE /LOSS
    - S.O.A., S.A.A.S. -> **CLOUD COMPUTING**
  - APPLICATION AS A SERVICE
  - PLATFORM AS A SERVICE
  - SERVICE AS A SERVICE (?)
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-
The Wonders of Cloud Computing

PC   Laptop / Netbook   Thin Client   Mobile Device

"The Network is the computer?!"

"The Internet Is The Cloud" (or vice versa?!)

Welcome to THE SMARTER PLANET
Globalization and Globally Available Resources

Billions of mobile devices accessing the Web

Access to streams of information in the Real Time

New Possibilities

ITS ALL ABOUT SOFTWARE!
It Gets Worse

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

A hacker no longer needs a big machine
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 against Denial of Service
- Vigilant monitoring, S.I.E.M.
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 …

Asus Web site harbors threat

It is not such a Good Friday for ASUSTek Computer.

The main Web site of the Taiwanese hardware maker, known for its Asus branded PCs and motherboards, has been rigged by hackers to serve up malicious software that attempts to exploit a critical Windows vulnerability.

The attackers added an invisible frame, a so-called iframe, to the front page of the Asus.com Web site, a victim’s browser will silently connect to another Web site that tries to install a malicious script on the user’s computer.

“We’ve just confirmed multiple reports about Asus.com, a very well known hardware manufacturer compromised,” a researcher with Kaspersky Lab wrote on the company’s Viruslist.com site.

...
Hackers steal gamers’ currency

MapleStory players blame company for lax security

By Tan Weizhen

Players of the wildly popular online game MapleStory are furious with the company that hosts the game on its server, Astarot. A starot's servers were hacked into, and players are reporting missing virtual dollars worth up to $4,000.

Social networking sites targeted by hackers

Are you on Facebook? Beware of hackers

Cyber crooks targeting social networking sites

Internet enthusiasts surfing the web during the annual Campus Party in Valencia. The event, now into its 12th year, is one of the world's biggest gatherings of web fans. Experts have also spoken on the dangers of data posted on websites - names, dates of birth, addresses, job details, e-mail addresses and phone numbers - being hacked and stolen.

The report provides a six-month update from the Internet threat activity in the Asia Pacific region from July to December 2007. 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. An article in The Straits Times, dated 27 February 2009, reported that a hacker was able to sell 87,063 phishing-host computers for $1 each, compared to $1.5 per computer in previous years. The article also highlighted the importance of maintaining a strong security posture no matter where you go and what you do on the Internet.

‘Errors’ on Facebook a cyber trap

Viral application enables perpetrators to access personal data

By Serene Leo

Facebook users in Singapore are facing a threat from an application that could steal their personal information.

The viral application, which is spreading on popular social networking sites, has been reported to be generating problems for users.

According to one victim, a friend invited him to an online game called “Spread Check System” application to “connect to Facebook.” When the user clicked on it, the application asked for personal information such as name, address, and birthdate.

Virus experts said that the application may be a fake login page that steals Facebook passwords.

When Facebook users try to login to Facebook, they are directed to another website where their personal information is stored. It can be used by hackers to complicate account security.

Graham Chilcote, a senior analyst at Symantec, said that the application could also use social networking sites to spread malware.
Hacker accused of stealing 130 million credit card numbers

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

April Gonzales, 28, and two other men have been charged with allegedly stealing more than 130 million credit and debit card numbers in the largest hacking and identity theft case in the United States.

Gonzales is already in jail in connection with hacking into 40 million other accounts, which at that time was believed to be the biggest case of its kind. Two named Russians were also indicted in the latest charges.

Gonzales, who lives in Florida and was indicted on Monday in New Jersey, is a one-time informant for the US Secret Service who had once helped to hunt hackers, said the authorities.

The agency later found out that he also had been working with criminals and fed them information on investigations, even warning off at least one individual, according to the authorities.

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

The ring targeted customers of the giant 7-Eleven convenience store and the regional Hannaford Brothers supermarket chain. It also took aim at the Heartland Payment Systems, a New Jersey-based payment processor.

The Justice Department said the new case represents the largest alleged credit and debit card data breach ever prosecuted in the US.

Gonzalez faces up to 20 years in prison if convicted on the new charges. The scheme began in October 2006 and ended last year when he was nabbed in the earlier hacking case.

Gonzalez allegedly devised a sophisticated attack to penetrate the computer networks and steal the card data.

He then sent that data to computer servers in California, Illinois, Latvia, the Netherlands and Ukraine.

“The scope is massive,” Assistant US Attorney Eric Liebmann said yesterday in an interview.

Last year, the Justice Department charged Gonzalez and others with hacking into retail companies’ computers with the theft of approximately 40 million credit cards.

At the time, that was believed to have been the biggest single case of hacking private computer networks to steal credit card data, puncturing the electronic defenses of retailers including T.J. Maxx, Barnes & Noble, Sports Authority and OfficeMax.

Prosecutors said Gonzalez was the ring-leader of the hackers in that case and caused more than US$400 million US$580 million in damage.

At the time of those charges, officials said the alleged thieves were not computer geniuses, but opportunists who used a technique called “waisting”.

This involved cramming through different areas with a laptop computer and looking for accessible wireless Internet signals.

Gonzalez faces a possible life sentence if convicted in the earlier case.

Restaurants are among the most common targets for hackers, experts said, because they often fail to update their antivirus software and other computer security systems.

Mr Scott Christie, a former federal prosecutor now in private practice, said the case shows that despite the best efforts by companies to protect data privacy, there remain individuals capable of stealing in.

“Cases like this do cause companies to sit up and take notice that this is a problem and more needs to be done,” he said. Associated Press, Reuters
School website tests show up security lapses

Personal data of staff and students are leaked easily, says online group

By Keshwan Singh

For a week, a group of members online community known as the Singapore Security Meetup Group sites of various with a leaky for phone number to be easy, unusual, was reported as we are

SSMG member and chief technology officer of an IT firm, Mr Wang Qian Chao, showed the Straits Times documents containing personal information from the website of a university, a junior college, a polytechnic, the secondary schools and a primary school which they found.

SSMG’s findings confirm this view.

The issue of data privacy had been raised in the Parliament by Mr Lee Bee Wah, an MP for Ang Mo Kio GRC.

In his written reply, the Minister for Information, Communications and the Arts Lee Hsien Yang said an inter-ministry committee had been set up to investigate the issues. As data protection at a complex issue, widespread, with extensive implication on all stakeholders, this review will take some time.

Teachers have also been reminded that it is against school policy to include IC numbers in online documents, he added.

One document on the website of the National University of Singapore (NUS) had the students’ personal details from a spreadsheet, including his address in China.

An NUS spokesman said it was users are advised not to divulge personal information in data shared on public websites, they said they do not want to take personal responsibility for any disclosure.

Mr. Polytechnic spokesman Khoo Eng Meng blamed the leak of names, IC numbers and mailing addresses of 200 students on “human error”, and said steps were taken to prevent any further.

Mr. Thoo, an IT security consultant, said users could be used in spreading malware. “To help others to know and not to make similar mistakes.”

Why leaks occur

THERE are four main reasons why data leaks and, says Mr Wong Qian Chao.

There are:

1. Web servers that are infected with malware, or malicious software, that diverts off information from the server.

2. Vulnerabilities in Web applications, such as poorly written applications, that allow unauthorised access.

3. Misconfigured Web servers, which reveal more information than necessary.

4. Inadequate security on Web servers without access control.

Data leakage arising from misconfigured applications could prove costly enough for application developers, their estimates. Their client’s estimate was from $10,000.

Becoming more secure

Web servers and implementing access controls can be done by the system administrator.

Let’s build a smarter planet.
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.

The group, which calls itself Goatse Security, also obtained the identification number contained in the SIM cards of the iPads used to communicate over AT&T’s network, known as an ICC-ID.

AT&T acknowledged the breach, but the company sought 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 by Tuesday turned off the feature on its website that allowed the group to find the email addresses. Apple did not respond to a request for comment.

Experts said ICC-ID numbers could, in the right hands, be used to get other information, like an iPad’s location. The breach “should be worrying people a lot,” said Mr Nick DePetrillo, an independent security consultant.

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,” he said. “But to do that, you would have to gain access to very secure databases that are not generally connected to the public Internet.” AGENCIES

- 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**
These are real examples – hackers

Love these error message pages …
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 "On" to enable the details to be viewable on remote machines.

Why is your debug tool shown to the world?
More information to entice a would-be hacker?!
Message from webpage

While attempting to load module "com.mavenlab.sph.vbintegration.v8Integration3", property "user.agent" was set to the unexpected value "unknown"

Allowed values: gecko,gecko_1_8,ie6,opera,safari

OK
<table>
<thead>
<tr>
<th>Name</th>
<th>Last Modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0391290228/</td>
<td>27-Sep-2006 08:28</td>
<td></td>
<td></td>
</tr>
<tr>
<td>05291977/</td>
<td>18-Sep-2006 04:09</td>
<td></td>
<td></td>
</tr>
<tr>
<td>240403/</td>
<td>20-Sep-2006 17:25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10136109/</td>
<td>23-Sep-2006 21:56</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ALTERC585/</td>
<td>16-Sep-2006 11:59</td>
<td>1.0K</td>
<td></td>
</tr>
<tr>
<td>_&lt;html&gt;</td>
<td>02-Oct-2006 16:18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>05291977/</td>
<td>25-Sep-2006 09:37</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19-Sep-2006 14:44</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26-Sep-2006 15:16</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26-Sep-2006 15:21</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21-Sep-2006 17:31</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>02-Oct-2006 05:17</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14-Sep-2006 22:18</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27-Sep-2006 08:36</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27-Sep-2006 11:28</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27-Sep-2006 14:37</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27-Sep-2006 16:13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26-Sep-2006 16:46</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25-Sep-2006 10:37</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21-Sep-2006 17:07</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25-Sep-2006 14:21</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20-Sep-2006 10:54</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26-Sep-2006 09:26</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22-Sep-2006 09:59</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14-Sep-2006 16:49</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>02-Oct-2006 08:55</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22-Sep-2006 16:38</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28-Sep-2006 10:55</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A File List in HTML session?!
An error has occurred.

Error Description:

Real Example: Online Travel Reservation Portal

Change the reserID to 2001200

Hotel Reservation Online

Dear [Name],

As a result of your reservation 20031959 at the hotel Le Méridien 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: [Name]
Credit/Debit Card: [Redacted]
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,

[Name]
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.[redacted]/invoice.php?reserID=2001200&email=[redacted]@hotmail.com
Parameter Tampering: Reading another user’s invoice

The same customer invoice that reveals the address and contact number.

Date: Jan 30 2006

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

TOTAL AMOUNT 506.61 USD

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

Card Holder Name: Justin Card Number: xxxxx-xxxx-xxxx-4688
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,

Boolean Logic?!
DON'T TRY THIS AT HOME!

Hacking Internet Banking Applications
Source: http://video.lib.org/2005.html The general public sentiment is that the banks, having always been the guardians ...

How to hack pete's Facebook application
Click more
http://rapidshare.com/files/4758660/hackpetesfinal.wmv Original video, (much clearer and sounds normal) Easy ...

How to download Hacking Application
This video is a part of http://www.youtube.com/watch?v=cl-ZKxKio this video and http://www.youtube.com/watch?v ...

How to Hack Facebook
Detailed instructions below: Tool needed: Internet Browser (I used firefox with google toolbar) Facebook Account Mood ...

Playlist Results for application hacking
frienster myspace facebook hackers (15 Videos)

Hacking SQL Server
In this presentation at the Jacksonville SQL Server Users Group, Bayer White plays the part of a developer protecting his ...

DON'T TRY THIS AT HOME!
WHY DO HACKERS TODAY ATTACK APPLICATIONS?

- Because they know you have firewalls
  - So it's not very convenient to attack the network anymore
  - But they still want to attack ‘cos they still want to steal data …

- Because firewalls do not protect against app attacks!
  - So the hackers are having a field day!
  - Very few people are *actively aware* of application security issues

- Because web sites have a large footprint
  - No need to worry anymore about cumbersome IP addresses

- Because they can!
  - It is difficult or impossible to write a comprehensively robust application
    - Developers are yet to have secure coding as second nature
    - Developers think differently from hackers
    - *Cheap, Fast, Good* – choose two, you can’t have it all
    - It is a nightmare to manually QA the application
    - Many companies today still do not have a software security QA policy or resource
Software Application Development Pressures

Today I’m being asked to:
• Deliver product faster (a lot faster!)
• Increase product innovation
• Improve quality
• Reduce cost
• Deliver a secure product (?)

• Cheap
• Fast
• Good

- Choose 2
<table>
<thead>
<tr>
<th>2009</th>
<th>2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unvalidated Input</td>
<td>Injection</td>
</tr>
<tr>
<td>Broken Access Control</td>
<td>Cross-Site Scripting (XSS)</td>
</tr>
<tr>
<td>Broken Authentication and Session Management</td>
<td>Broken Authentication and Session Management</td>
</tr>
<tr>
<td>Cross Site Scripting Flaws</td>
<td>Insecure Direct Object References</td>
</tr>
<tr>
<td>Buffer Overflows</td>
<td>Cross-Site Request Forgery (CSRF)</td>
</tr>
<tr>
<td>Injection Flaws</td>
<td>Security Misconfiguration</td>
</tr>
<tr>
<td>Improper Error Handling</td>
<td>Insecure Cryptographic Storage</td>
</tr>
<tr>
<td>Insecure Storage</td>
<td>Failure to Restrict URL Access</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>Insufficient Transport Layer Protection</td>
</tr>
<tr>
<td>Insecure Configuration Management</td>
<td>Unvalidated Redirects and Forwards</td>
</tr>
</tbody>
</table>
WHY DO APPLICATION SECURITY PROBLEMS EXIST?

- IT security solutions and professionals are normally from the network/infrastructure/sysadmin side
  - They usually have little or no experience in application development
  - And developers typically don’t know or don’t care about security or networking

- Most companies today still do not have an application security QA policy or resource
  - IT security staff are focused on other things and are swarmed
    - App Sec is their job but they don’t understand it and don’t want to deal with it
    - Developers think it’s not their job or problem to have security in coding
    - People who outsource expect the 3rd party to security-QA for them

- It is cultural currently to not associate security with coding
  - “Buffer Overflow” has been around for 25 years!
  - “Input Validation” is still often overlooked.
SECURITY TESTING IS PART OF SDLC QUALITY TESTING
You need a professional solution to Identify Vulnerabilities
With Rich Report Options

44 Regulatory Compliance Standards, for Executive, Security, Developers.

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?video=''&<script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')'/script>&password=Demo123&login=6y HTTP/1.0
Cookie: ASP.NET_SessionId=3b93fsufvfrj03rbhf10rql
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?video=''&<script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')'/script>&password=Demo123&login=6y HTTP/1.0
Cookie: ASP.NET_SessionId=3b93fsufvfrj03rbhf10rql
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
And Most Important:
Actionable Fix Recommendations

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:
- | (pipe sign)
- & (ampersand sign)
- ; (semicolon sign)
Compliance Scan Results

75 unique issues detected across 49 sections of the regulation:

<table>
<thead>
<tr>
<th>Section</th>
<th>No. of Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Implement Internet Protocol (IP) masquerading to prevent your internal address from being translated and revealed on the Internet. (Requirement 1.5)</td>
<td>4</td>
</tr>
<tr>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters. (Requirement 2)</td>
<td>19</td>
</tr>
<tr>
<td>3. Always change the vendor-supplied defaults before you install a system on the network. (Requirement 2.1)</td>
<td>13</td>
</tr>
<tr>
<td>4. Develop configuration standards for all system components. Make sure these standards address all known security vulnerabilities and industry best practices. (Requirement 2.2)</td>
<td>16</td>
</tr>
<tr>
<td>5. Disable all unnecessary and insecure services and protocols. (Requirement 2.2.2)</td>
<td>13</td>
</tr>
<tr>
<td>6. Configure system security parameters to prevent misuse. (Requirement 2.2.3)</td>
<td>13</td>
</tr>
<tr>
<td>7. Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems. (Requirement 2.2.4)</td>
<td>16</td>
</tr>
<tr>
<td>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)</td>
<td>3</td>
</tr>
<tr>
<td>9. This section applies to hosting providers only – Hosting providers must protect each entity’s hosted environment and data. (Requirement 2.4)</td>
<td>56</td>
</tr>
<tr>
<td>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)</td>
<td>17</td>
</tr>
</tbody>
</table>
Building security & compliance into the SDLC – further back

**Software Development Life Cycle**

<table>
<thead>
<tr>
<th>Coding</th>
<th>Build</th>
<th>QA</th>
<th>Security</th>
<th>Production</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developers</td>
<td></td>
<td></td>
<td>Enable Security to effectively drive remediation into development</td>
<td></td>
</tr>
<tr>
<td>Developers</td>
<td></td>
<td>Provides Developers and Testers with expertise on detection and remediation ability</td>
<td>Ensure vulnerabilities are addressed before applications are put into production</td>
<td></td>
</tr>
<tr>
<td>Developers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Application Development Security Testing Domains

<table>
<thead>
<tr>
<th>&quot;BLACK BOX&quot;</th>
<th>WHITE BOX</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IBM Rational Appscan Source Edition</strong></td>
<td><strong>IBM Rational Appscan Standard Edition</strong></td>
</tr>
<tr>
<td><strong>Dynamic APPLICATION Analysis</strong></td>
<td><strong>State CODE Analysis</strong></td>
</tr>
<tr>
<td>Good for security folks who are not experienced in application development</td>
<td>Good for developers who are not experienced in security</td>
</tr>
<tr>
<td>Don't need to worry about code</td>
<td>Provides learning for developers</td>
</tr>
<tr>
<td>Simulates real-world exploit attack</td>
<td>Good for interim audit of half-written code</td>
</tr>
<tr>
<td>Tests for relation between App and other apps, O/S, middleware, network</td>
<td>Can test for more than just HTTP/HTML code - eg. C, C++, C#, Perl, Codefusion, Javascript …</td>
</tr>
<tr>
<td>Like IPS, checks for &quot;unknown&quot; threats</td>
<td>Like Firewall, checks for &quot;known&quot; threats</td>
</tr>
</tbody>
</table>
Conclusion: Application Development Quality for Security

The Application Must Defend Itself

- "Traditional" FIREWALLS AND IPS WILL NOT STOP APPLICATION ATTACKS
- YOU CANNOT STOP AN APPLICATION ATTACK FROM HAPPENING
- The best way to protect against an application attack is to ensure the robustness of the application, that it's written properly, if not defensively, that it's QA'ed for bugs, vulnerabilities, logic errors etc

- 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

Lower Compliance & Security Costs by:

- Ensuring Security Quality in the Application up front
- Not having to do a lot of rework after production
- Automated software security scanning & remediation solution backed by world class R&D
Thank You

Anthony LIM
MBA CISSP CSSLP FCITIL
ISC2

CLOUD COMPUTING SECURITY – THE SOFT SPOT

www.isc2.org

www.ibm.com/security

www.owasp.org