RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

APPLICATION SECURITY –
The Invisible Onslaught Gets Worse

TRM-T09
22 July 2014

Anthony Lim

MBA FCITIL CISSL CSSLP

Member, Application Security Advisory Board
(ISC)2
Isc2.org

(ISC)²

CSSLP
Certified Secure Software Lifecycle Professional

#RSAC

Today's State: "Our Site Is Safe"

We Have Firewalls and IPS in Place

Port 80 & 443 are open for the right reasons

We Outsource

We Use Network Vulnerability Scanners

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

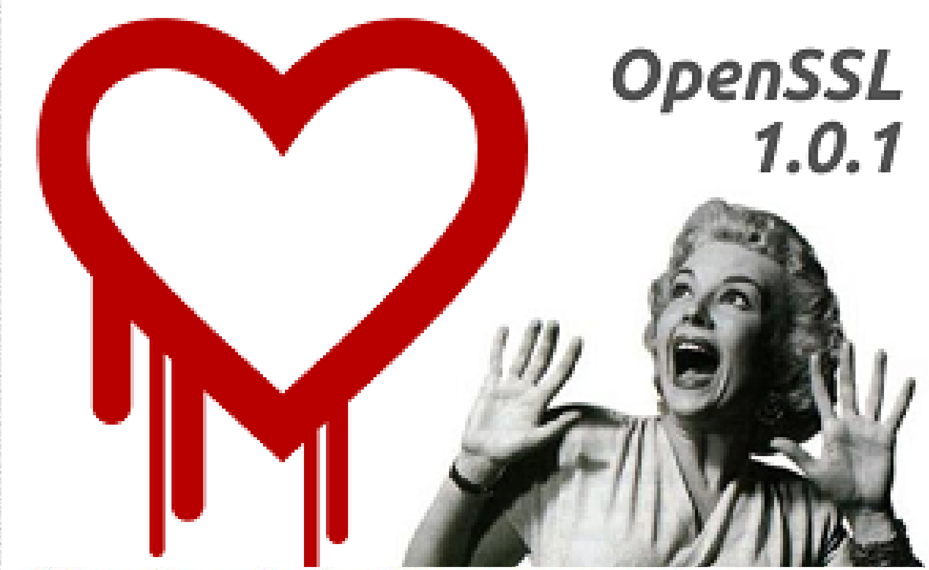
We Audit It Once a Quarter with Pen Testers

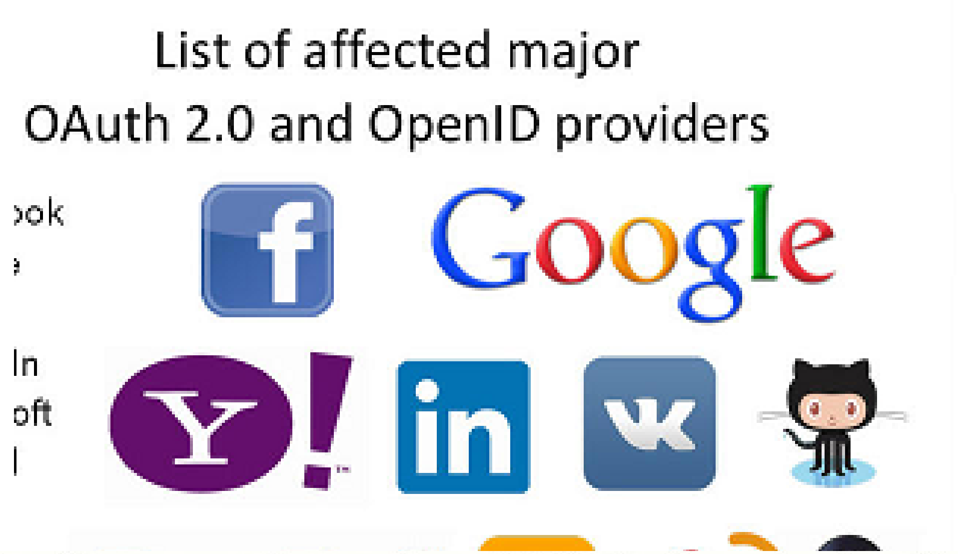
Applications are constantly changing

We Use SSL Encryption

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

... Or is it (safe) ...





After cyberattack, eBay recommends password change

Photo: Reuters

AFP
Wednesday, May 21, 2014

NEW YORK - US online giant eBay said Wednesday cyberattackers broke into its database with customer names, passwords and other personal data earlier this year.

Another zero-day vulnerability is threatening the Microsoft world

by paganinip on March 25th, 2014

g+1
My Page
Like 22

Microsoft issued a security advisory for the presence of a zero-day vulnerability in Microsoft Word products which allows a remote code execution.

Another zero-day vulnerability is threatening the Microsoft world, the news was issued

Seriously, what is happening … still?

The Hacker News™
Security in a serious way

France Telecom Orange Hacked Again, Personal Details of 1.3 Million Customers Stolen

Wednesday, May 07, 2014 Wang Wei

g+1 114 Like 621 Share 307 Tweet 123 Reddit 39 Share 12 ShareThis 552

Teen arrested for stealing tax data via Heartblee

Photo: Reuters

Share:

3 10 0

Share Tweet Share

AFP
Friday, Apr 18, 2014

OTTAWA - Federal police said on Wednesday they have arrested and charged a 19-year-old ma
with the theft of 900 Canadian taxpayers' data, which was made vulnerable by the "Heartbleed" b

B2 | HOME SATURDAY, MAY 3, 2014

Microsoft releases patch for Web browser's security flaw

By KENNY CHEE

IT MAY be safe now to use Microsoft's Web browser Internet Explorer – earlier reported to have a serious security hole – after the software giant released a patch on Thursday.

Microsoft has released a fix for its newer Windows 7 and 8 operating systems, as well as for the older Windows XP even though the American firm had previously said it would not patch the 13-year-old Windows XP because it had discontinued support for it early last month.

"We made this exception based on the proximity to the end of support for Windows XP," said Ms Adrienne Hall, Microsoft's general manager for trustworthy computing, in a blog post.

It is just as well, because fresh attacks exploiting the bug have been found targeting a version of the Web browser in Windows XP, said cyber-security firm FireEye.

Previously, attacks targeted browsers in Windows 7 and 8.

Deemed so serious that the authorities from Singapore to the US have issued warnings, the security flaw allows hackers to take control of a person's computer if he uses Internet Explorer to visit a compromised website.

Microsoft's U-turn on patching Windows XP suggests the seriousness of the bug, said Ms Macky Cruz, the security focus lead at TrendLabs, the research and development unit of security firm Trend Micro.

But cyber-security experts said they are not holding their breath for Microsoft to keep doing so.

In Singapore, some 450,000 computers were still running on XP as of February.

"We are encouraging users to upgrade to the latest versions (of Windows). It will become more and more difficult for owners of computers running Windows XP to ensure their systems are safe," Ms Cruz said.

Computers that have automat ic updates turned on in Windows would have already received the patch. Users who have not received the update can do so by opening the Windows control pa el and clicking Check for Update in the Windows Update section.

We Never Learn ???

prime.news — THE STRAITS TIMES WEDNESDAY, AUGUST 19 2009 PAGE A6

Hacker accused of stealing 130 million credit card numbers

WASHINGTON: A former government in- ... 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 the stolen data to others.

... 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 hacking into retail companies' computers with

Up to 1.5M credit card numbers stolen from Global Payments

Payments processor believes no names, addresses, or Social Security numbers were stolen in the security breach.

by Steven Musil | April 1, 2012 7:10 PM PDT

Follow

Target CEO resigns after data breach fallout

Gregg Steinhafel steps down in wake of a hack last December that affected many as 110 million Target customers.

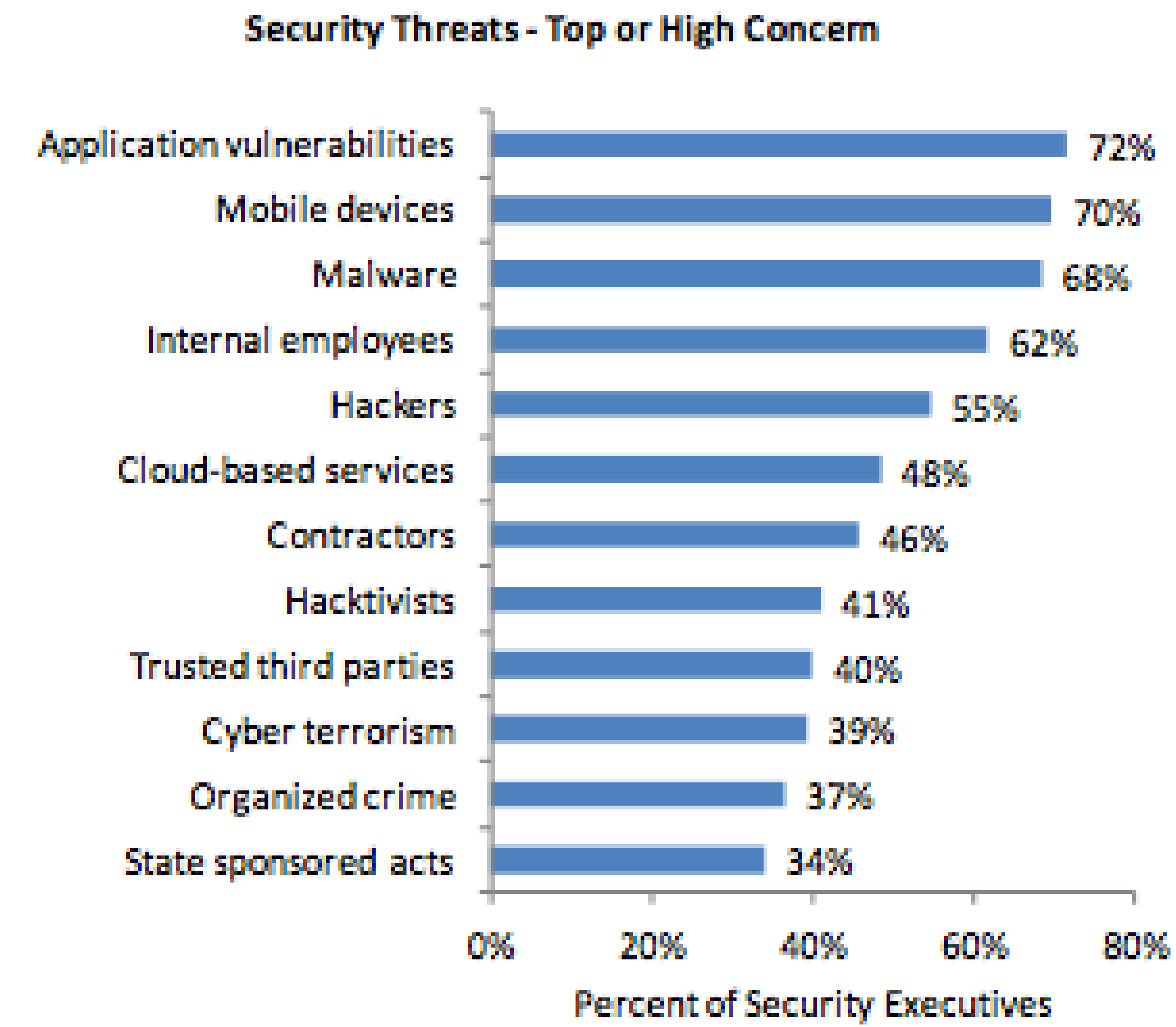
by Don Reisinger @donreisinger / May 5, 2014

Hackers Now Attack Web Applications

- Applications can be CRASHED to reveal source, logic, script or infrastructure information that can give a hacker intelligence
- Applications can be COMPROMISED to make it provide unauthorized entry access or unauthorized 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 authorized user, or send data to an unauthorized recipient, etc.

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

(ISC)2 2013 Global Security Workforce Survey



A Trip Down Memory Lane …

OWASP Top 10 2004

1. Unvalidated Input
2. Broken Access Control
3. Broken Authentication & Session Management
4. Cross Site Scripting (“XSS”)
5. Buffer Overflow
6. Injection Flaws
7. Improper Error Handing
8. Insecure Storage
9. Application Denial of Service
10. Insecure Configuration Management

2007

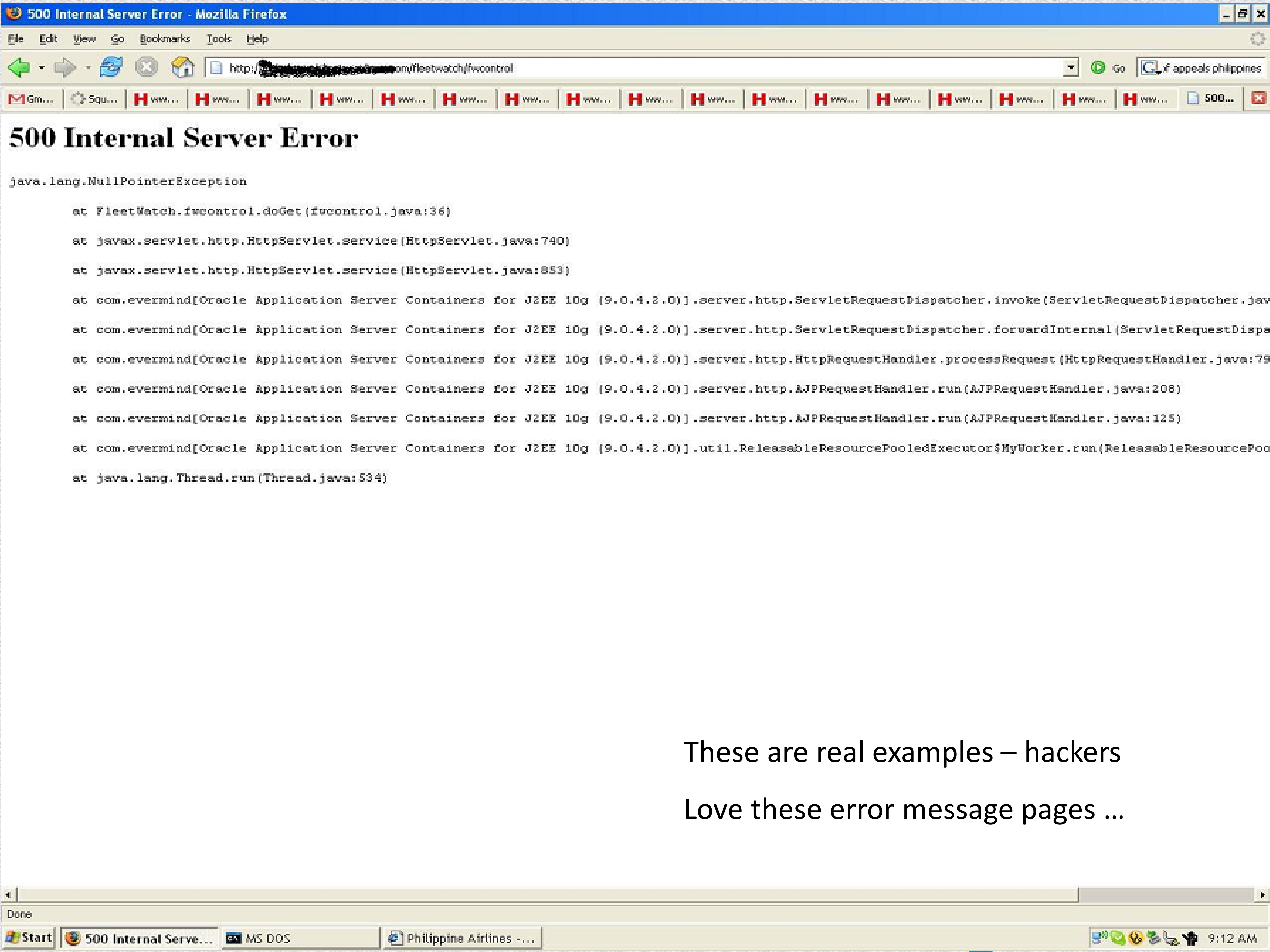
1. XSS
2. Injection Flaws
3. Malicious File Executing
4. Insecure Direct Object Reference
5. Cross Site Request Forgery (CSRF)
6. Data Leakage & Improper Error Handling
7. Broken Authentication & Session Management
8. Insecure Cryptographic Storage
9. Insecure Communications
10. Failure to restrict URL Access

OWASP
The Open Web Application Security Project

IBM X-Force Security Report

Observations on Web Application Security & Attacks

- SQL Injection vulnerabilities in public web applications dropped by 46 percent, more speciality attacks targeting **Shell Command Injection** vulnerabilities rose 2 to 3 times since 2010.
- Traditional email spam decreased by 50 percent, there was **an increase in phishing attacks** that impersonate social networking sites and mail parcel services to entice victims to click on links to web pages that may try to infect their PCs with malware.
- **New technologies such as mobile devices are creating new avenues of opportunity for attacks and new challenges for security pros**. A big increase in the number of exploits publicly released that can be used to target mobile devices—which are increasingly tapping into enterprise information through the Bring your Own Device or "BYOD" programs.



These are real examples – hackers

Love these error message pages …

Value not found: LockAfterNumberOfLoginTries - Windows Internet Explorer

[redacted]

File Edit View Favorites Tools Help

Favorites | AsiaOne | Facebook | Home | Value not found: LockA... | Page | Safety | Tools

Server Error in '/' Application.

Value not found: LockAfterNumberOfLoginTries

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.ArgumentException: Value not found: LockAfterNumberOfLoginTries

Source Error:

```
Line 7:  <html>
Line 8:  <head>
Line 9:  <title><%=AppPageTitle%></title>
Line 10: <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
Line 11: <link href="css/style.css" rel="stylesheet" type="text/css">
```

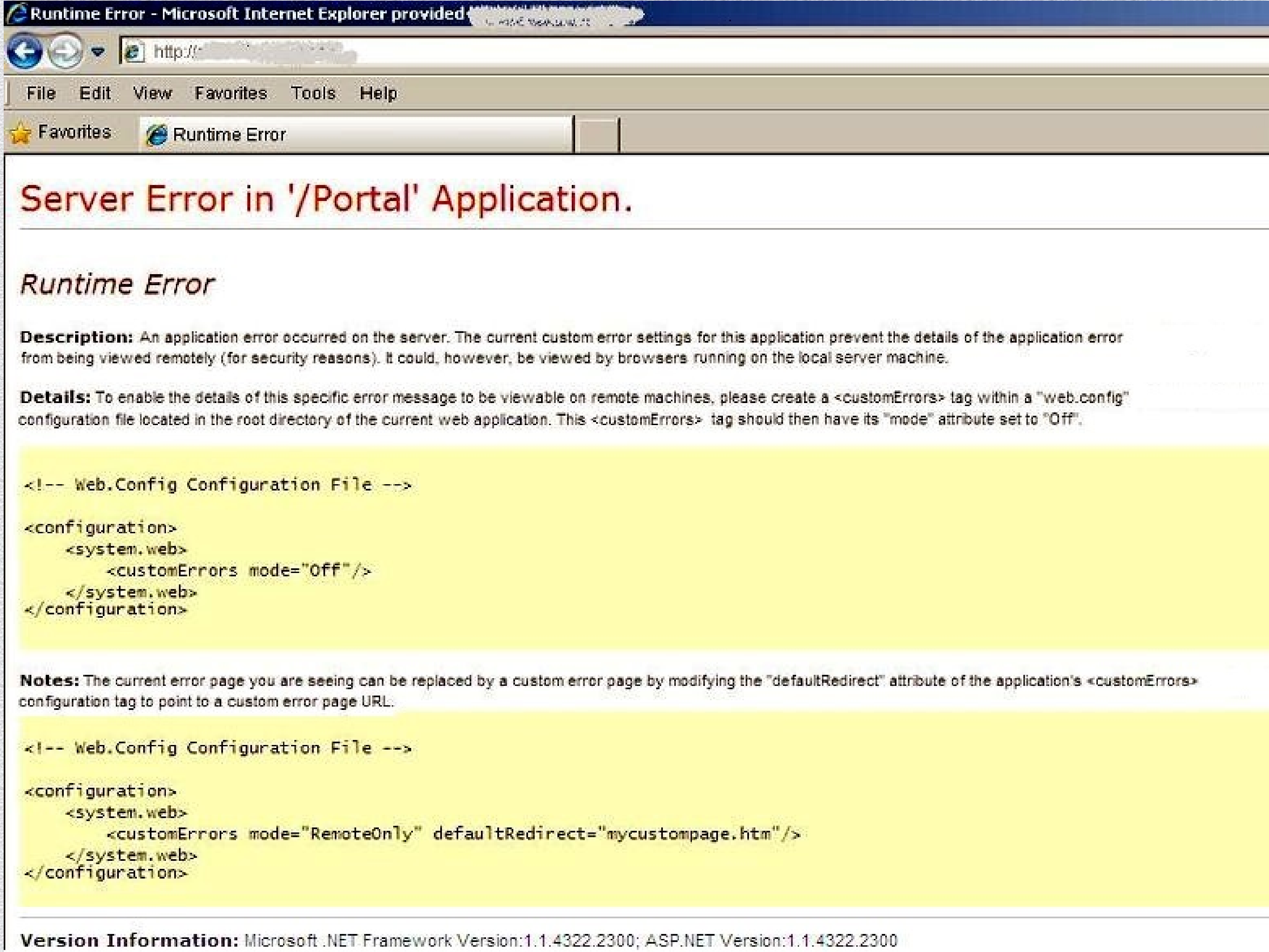
Source File: c:\Websites\MPS\mmp_port_prop_detail.aspx **Line:** 9

Stack Trace:

```
[ArgumentException: Value not found: LockAfterNumberOfLoginTries]
   Nini.Config.ConfigBase.GetInt(String key) +118
   AppFoundation.Core.Config.ConfigurationManager.Load() in C:\Documents and Settings\Ethan\My Documents\WORK\AppFoundation\AppFoundation\Core\Config\ConfigurationManager.cs:32
   AppFoundation.Core.Config.ConfigurationManager.get_Configuration() in C:\Documents and Settings\Ethan\My Documents\WORK\AppFoundation\AppFoundation\Core\Config\ConfigurationMa
   AppFoundation.Web.AppCorePage.get_AppPageTitle() in C:\Documents and Settings\Ethan\My Documents\WORK\AppFoundation\AppFoundation\Web\AppCorePage.cs:75
   ASP.mmp_port_prop_detail_aspx.__Render__control1(HtmlTextWriter __w, Control parameterContainer) in c:\Websites\MPS\mmp_port_prop_detail.aspx:9
   System.Web.UI.Control.RenderChildrenInternal(HtmlTextWriter writer, ICollection children) +98
   System.Web.UI.Control.RenderChildren(HtmlTextWriter writer) +20
   System.Web.UI.Page.Render(HtmlTextWriter writer) +26
   System.Web.UI.Control.RenderControlInternal(HtmlTextWriter writer, ControlAdapter adapter) +25
   System.Web.UI.Control.RenderControl(HtmlTextWriter writer, ControlAdapter adapter) +121
   System.Web.UI.Control.RenderControl(HtmlTextWriter writer) +22
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +2558
```

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

Done | Internet | 100%



Runtime Error - Microsoft Internet Explorer provided

http://

File Edit View Favorites Tools Help

Favorites Runtime Error

Server Error in '/Portal' Application.

Runtime Error

Description: An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It could, however, be viewed by browsers running on the local server machine.

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

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

<configuration>
    <system.web>
        <customErrors mode="Off"/>
    </system.web>
</configuration>
```

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

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

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

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

Generic Error Page - Google Chrome

https://w1.buysub.com/Error.jsp?cds_mag_code=NWO&id=1271056711152&error=

CDS Global
A Hearst Company

An error has occurred.

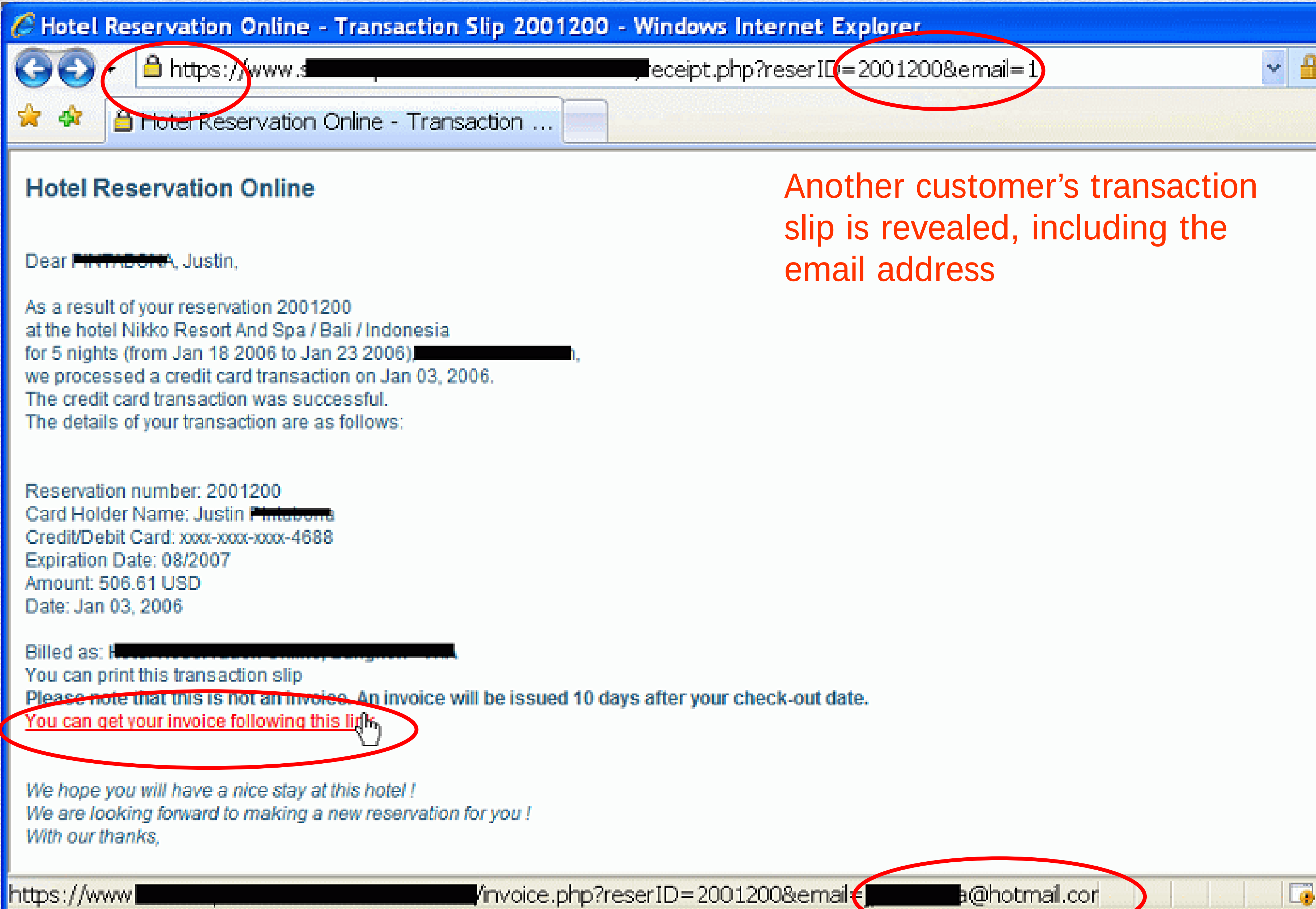
Error Description:

```
java.lang.NullPointerException at
com.cds.nm.gemini.parsers.GiftsRequestParser.getParameter(GiftsRequestParser.java(Compiled Code)) at
com.cds.nm.gemini.servlets.GeminiBaseServlet.buildErrorURL(GeminiBaseServlet.java(Compiled Code)) at
com.cds.nm.gemini.servlets.GeminiBaseServlet.processError(GeminiBaseServlet.java(Compiled Code)) at
com.cds.nm.gemini.servlets.GeminiBaseServlet.processError(GeminiBaseServlet.java(Compiled Code)) at
com.cds.nm.gemini.servlets.GiftCardServlet.doPost(GiftCardServlet.java:160) at
com.cds.nm.gemini.servlets.GiftCardServlet.doGet(GiftCardServlet.java:68) at
javax.servlet.http.HttpServlet.service(HttpServlet.java(Compiled Code)) at
com.cds.nm.gemini.servlets.session.HttpServlet.service(HttpServlet.java(Compiled Code)) at
com.cds.nm.gemini.servlets.GeminiBaseServlet.service(GeminiBaseServlet.java(Compiled Code)) at
javax.servlet.http.HttpServlet.service(HttpServlet.java(Compiled Code)) at
com.ibm.ws.webcontainer.servlet.ServletWrapper.service(ServletWrapper.java(Compiled Code)) at
com.ibm.ws.webcontainer.servlet.ServletWrapper.service(ServletWrapper.java(Compiled Code)) at
com.ibm.ws.webcontainer.filter.WebAppFilterChain.doFilter(WebAppFilterChain.java(Compiled Code)) at
com.ibm.ws.webcontainer.filter.WebAppFilterChain._doFilter(WebAppFilterChain.java(Compiled Code)) at
com.ibm.ws.webcontainer.servlet.ServletWrapper.handleRequest(ServletWrapper.java(Compiled Code)) at
com.ibm.ws.webcontainer.servlet.CacheServletWrapper.handleRequest(CacheServletWrapper.java(Compiled
Code)) at com.ibm.ws.webcontainer.WebContainer.handleRequest(WebContainer.java(Compiled Code)) at
com.ibm.ws.webcontainer.channel.WCChannelLink.ready(WCChannelLink.java(Compiled Code)) at
com.ibm.ws.http.channel.inbound.impl.HttpInboundLink.handleDiscrimination(HttpInboundLink.java(Compiled
Code)) at
com.ibm.ws.http.channel.inbound.impl.HttpInboundLink.handleNewInformation(HttpInboundLink.java(Compiled
Code)) at
com.ibm.ws.http.channel.inbound.impl.HttpICLReadCallback.complete(HttpICLReadCallback.java(Compiled Code))
at
com.ibm.ws.ssl.channel.impl.SSLReadServiceContext$SSLReadCompletedCallback.complete(SSLReadServiceContext.jav
Code)) at com.ibm.ws.tcp.channel.impl.WorkQueueManager.requestComplete(WorkQueueManager.java(Compiled
Code)) at com.ibm.ws.tcp.channel.impl.WorkQueueManager.attemptIO(WorkQueueManager.java(Compiled Code))
at com.ibm.ws.tcp.channel.impl.WorkQueueManager.workerRun(WorkQueueManager.java(Compiled Code)) at
com.ibm.ws.tcp.channel.impl.WorkQueueManager$Worker.run(WorkQueueManager.java(Compiled Code)) at
com.ibm.ws.util.ThreadPool$Worker.run(ThreadPool.java(Compiled Code))
```

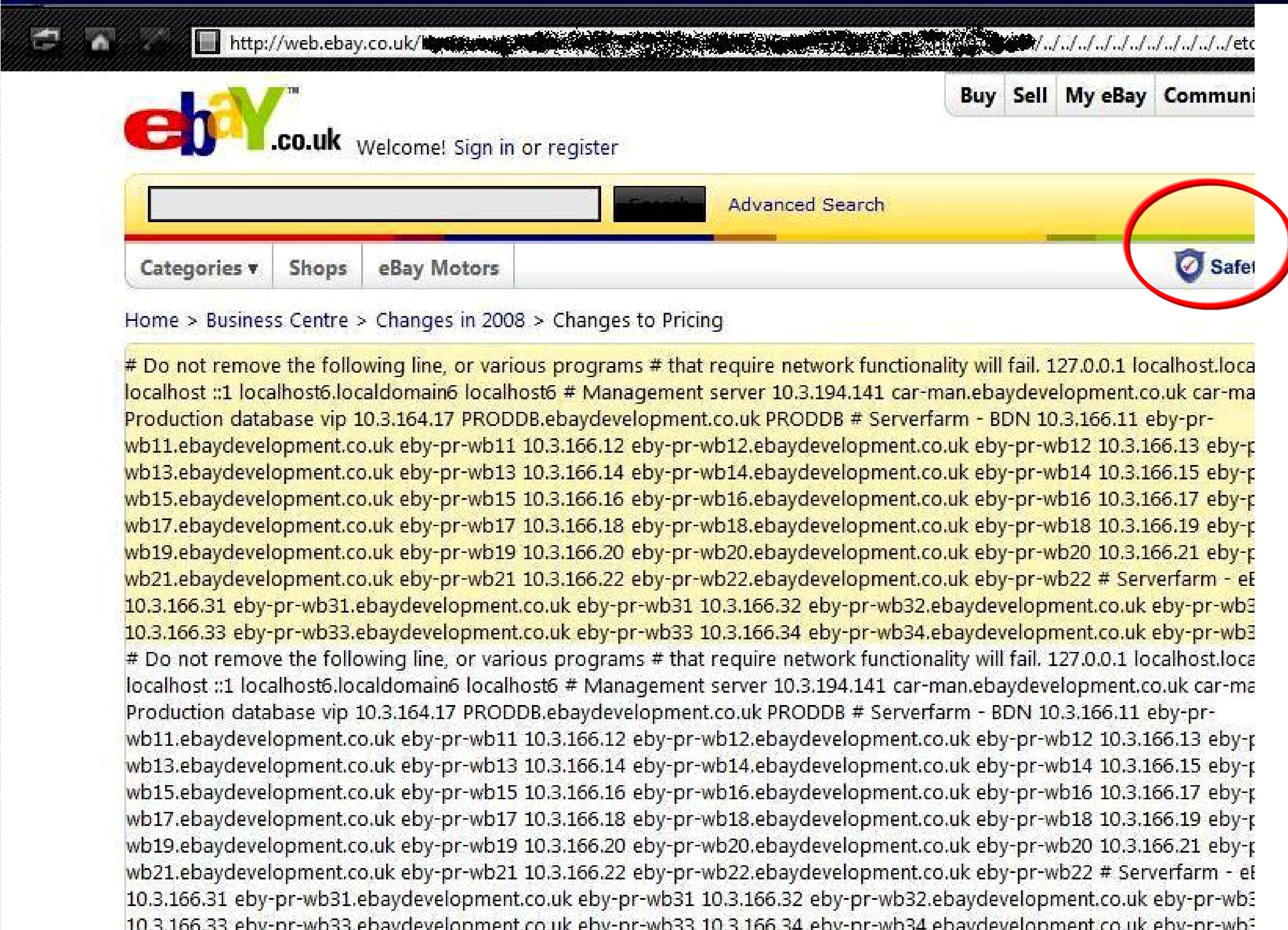
Real Example : Parameter Tampering

Reading another user's transaction

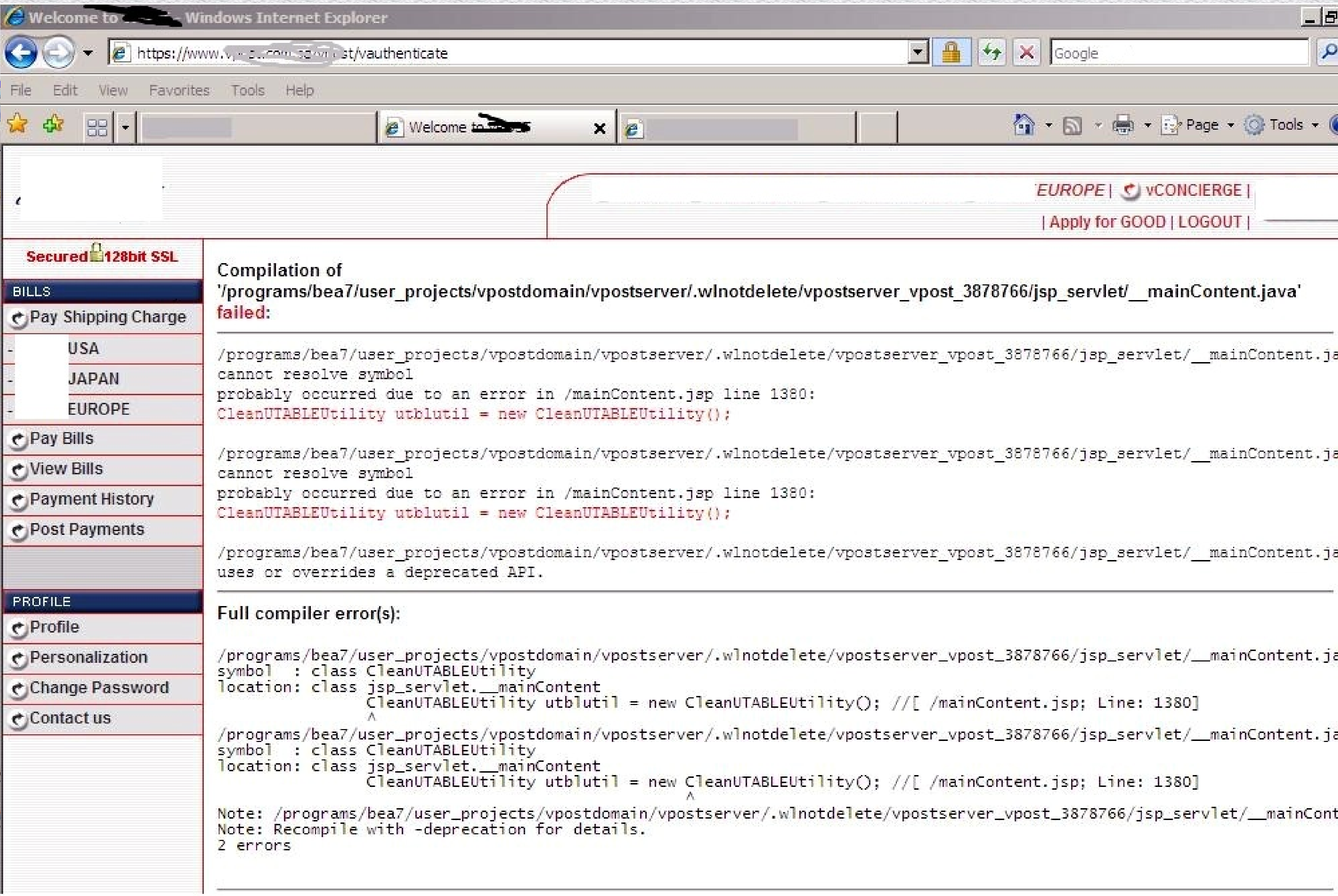
URL Rotation

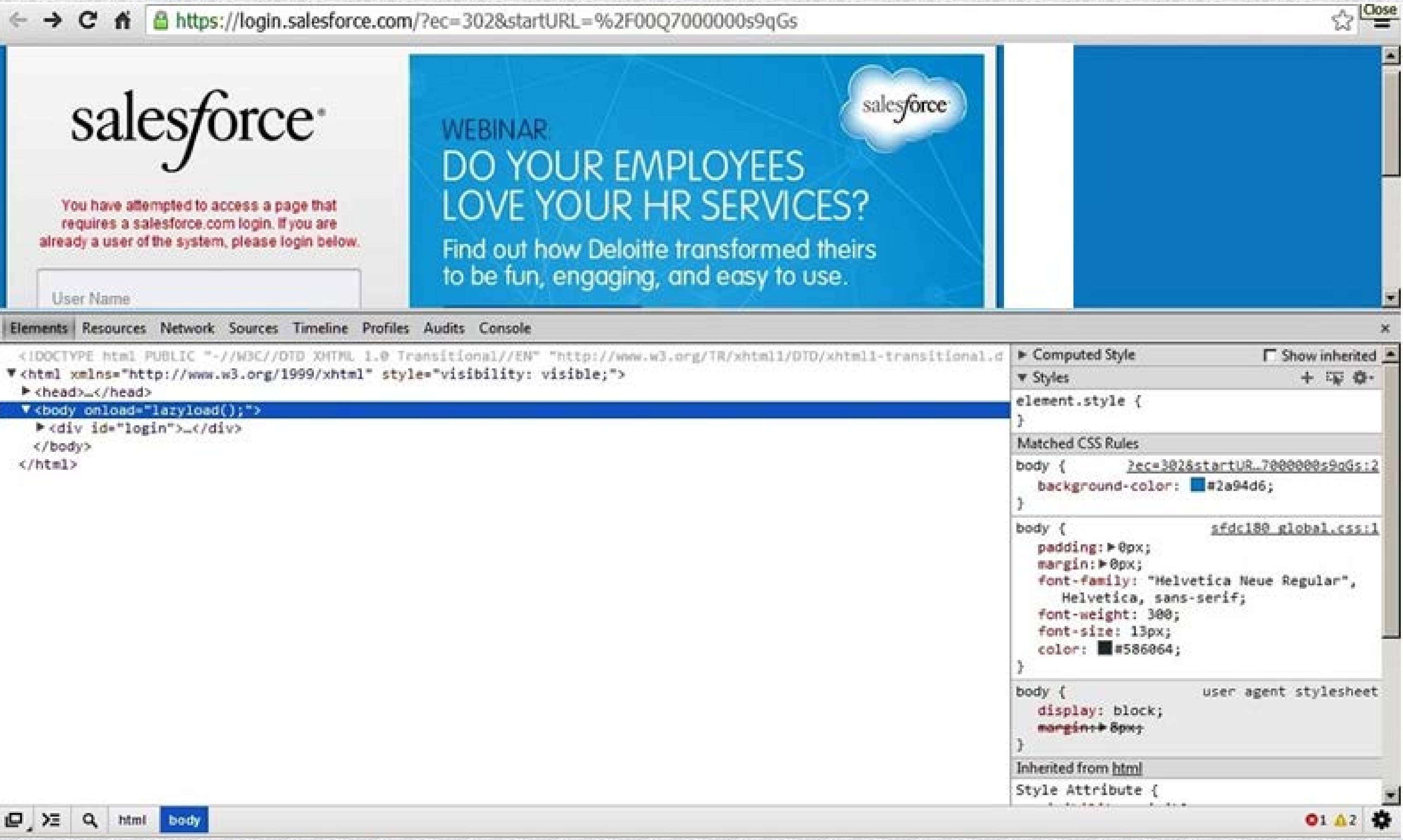


Attackers use directory traversal attacks to read arbitrary files on web servers, such as SSL private keys and password files.



Online Mail-order Payment Service




https://login.salesforce.com/?ec=302&startURL=%2F00Q7000000s9qGs
Close
salesforce
You have attempted to access a page that requires a salesforce.com login. If you are already a user of the system, please login below.
User Name
salesforce
WEBINAR
DO YOUR EMPLOYEES LOVE YOUR HR SERVICES?
Find out how Deloitte transformed theirs to be fun, engaging, and easy to use.
Elements Resources Network Sources Timeline Profiles Audits Console
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.d
<html xmlns="http://www.w3.org/1999/xhtml" style="visibility: visible;">
<head>…</head>
<body onload="lazyload();">
<div id="login">…</div>
</body>
</html>
Computed Style
Show inherited
Styles
element.style {
}
Matched CSS Rules
body { ?ec=302&startUR…7000000s9qGs:2
background-color: #2a94d6;
}
body { sfdc180_global.css:1
padding: 0px;
margin: 0px;
font-family: "Helvetica Neue Regular", Helvetica, sans-serif;
font-weight: 300;
font-size: 13px;
color: #586064;
}
body { user agent stylesheet
display: block;
margin: 8px;
}
Inherited from html
Style Attribute {
html body
1 2

Top 20 Replies by Programmers when their programs don't work...

www.geeksaresexy.net 14042014

20. That's weird...
19. It's never done that before.
18. It worked yesterday.
17. How is that possible?
16. It must be a hardware problem.
15. What did you type in wrong to get it to crash?
14. There has to be something funky in your data.
13. I haven't touched that module in weeks!
12. You must have the wrong version.
11. It's just some unlucky coincidence.
10. I can't test everything!
9. THIS can't be the source of THAT.
8. It works, but it hasn't been tested.
7. Somebody must have changed my code.
6. Did you check for a virus on your system?
5. Even though it doesn't work, how does it feel?
4. You can't use that version on your system.
3. Why do you want to do it that way?
2. Where were you when the program blew up?
1. It works on my machine.

Why Do Hackers Attack Web 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

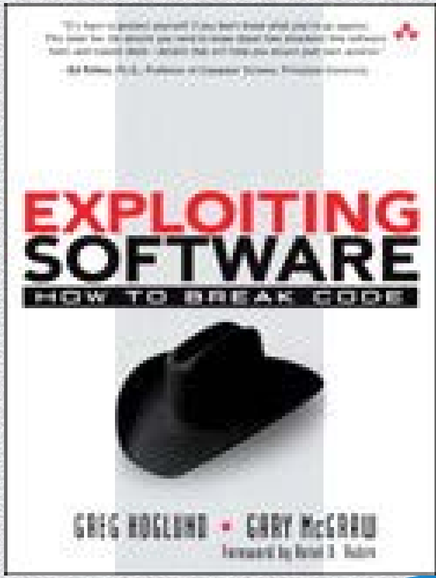
- **Because firewalls do not protect against app attacks!**
  - Very few people are actively aware of application security issues
  - **Most IT security professionals, from network & sys-admin side, have little experience or interest in software development. Programmers have little experience or interest in security or infrastructure.**
    - IT security staff are also often overworked and are focusing on other issues

- Because web sites have a large footprint; cloud makes it even bigger.

- **Because they can!**
  - **Many organizations today still lack a software development security policy!**
    - Many applications especially legacy ones still in use, were not built defensively
    - **Applications today are hundreds of thousands of lines long**
    - **It is a nightmare to QA the application, and requires discipline**
      - **So many people, even if aware, will skip or procrastinate this tedious process**
    - **Additional loss of control when outsourcing development work**

IP vs HTTP

Gartner: ITSec Spend
HW/NW 80%
App Sec 20%



Software Development Security Issues

No developer goes to work with the intention of writing bad code.

- **Developers are often <u>not trained</u> or experienced in secure coding techniques, and have never needed to worry about this before**

Developers are hired faster than they can be trained properly

- **Developers face pressures of demands for quality and functionality, and are often short on timeline, resources, information, budget, quality assurance tools investment.**

- **Plus heavy demands on outsourcing parties ….**

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

-> Choose 2

OWASP Top 10 : 2010 and 2013

2010

1. Injection
2. XSS
3. Broken Authentication & session Management
4. Insecure Direct Object References
5. Cross Site Request Forgery (CSRF)
6. Security Misconfiguration
7. Insecure Cryptographic Storage
8. Failure to restrict URL Access
9. Insufficient Transport Layer Protection
10. Unvalidated Redirects & Forwards

2013

1. Injection
2. Broken Authentication & Session Management
3. XSS
4. Insecure Direct Object References
5. Security Misconfiguration
6. Sensitive Data Exposure
7. Missing Function Level Access Control
8. CSRF
9. Using Components with Known Vulnerabilities
10. Unvalidated Redirects & Forwards

OWASP
The Open Web Application Security Project

SOME MOBILE APP SECURITY ISSUES

1. Insecure Data Storage

Eg. A Starbucks app was storing usernames, email addresses, and passwords in clear text.
Design apps in such a way that critical information such as passwords and credit card numbers do not reside directly on a device. If they do, they must be stored securely

2. Weak server-side controls

When creating their first mobile applications, businesses often expose systems that had not previously been accessible from outside of their networks. Often, these formerly sheltered systems are not fully vetted against security flaws. A number of back-end APIs assume (quite wrongly) that an app will be only thing that will access it

3. Unintended Data Leakage

(Eg Angry Birds collect alot of user personal data)
Use caution when choosing analytics providers and implementing advertising. Watching what, how, when, and where data moves can give an attacker a gold mine of information.

4. Broken cryptography

(Weak or wrong algorythms, poor key management)
Many organizations make the mistake of using strong encryption algorithms, but implement their own keys and certificates in areas that are vulnerable to attackers

5. Security Decisions via untrusted Inputs

(Eg. Weak authentication can be bypassed).
Eg. a flaw in Skype security allowed hackers to open the Skype app and dial arbitrary phone numbers using a simple link in the contents of an email.

(ISC)²

Courtesy C Fairchild, InfoWeek

MOBILE APP SECURITY ISSUES

- **Development is focused on features not security**
- **Developers are unaware of the underlying platform**
- **Users don’t even have security on their radar**
- **Users are easily social engineered**

Not different from non-mobile app-dev issues

Reversing Android Apps

**** Android apps are written in Java***

- You can use your favorite IDE with a freely downloadable Android SDK plugin (eg. Eclipse)
- Like (unobfuscated) Java apps, they can be easily reversed with the right tools
- bytecode can even be altered and apps repackaged

Courtesy Trustwave

ATTACKING IOS DEVICE

- iOS strictly enforces application boundaries and sandboxing
- Apps cannot communicate directly from other apps, or access the application directories of other apps
- Written in native ObjectiveC or even C (with the right tools)
- Based on an ARM version of the same XNU kernel from OSX
- Once you breach the walls of the fort, you own the place….

First you must Jailbreak the device -

- Involves finding a an exploit in the kernel as well as userland to allow it to run unsigned code
- Use tools like Absinthe, redsn0w limera1n to do the jailbreaking

Courtesy Trustwave

BUSINESS LOGIC ATTACKS

A Business Logic Attack (BLA) is an attack which targets the logic of a business application.

Issues to consider when developing the application –

1. **Identify Business Rules and Derive Test/Abuse Cases**
2. **Consider Time Related Business Rules**
3. **Consider Money Related Business Rules**
4. **Consider Process Related Business Rules**
5. **Consider Human Resource Business Rules**
6. **Consider Contractual Relationship Business Rules**

Courtesy Owasp

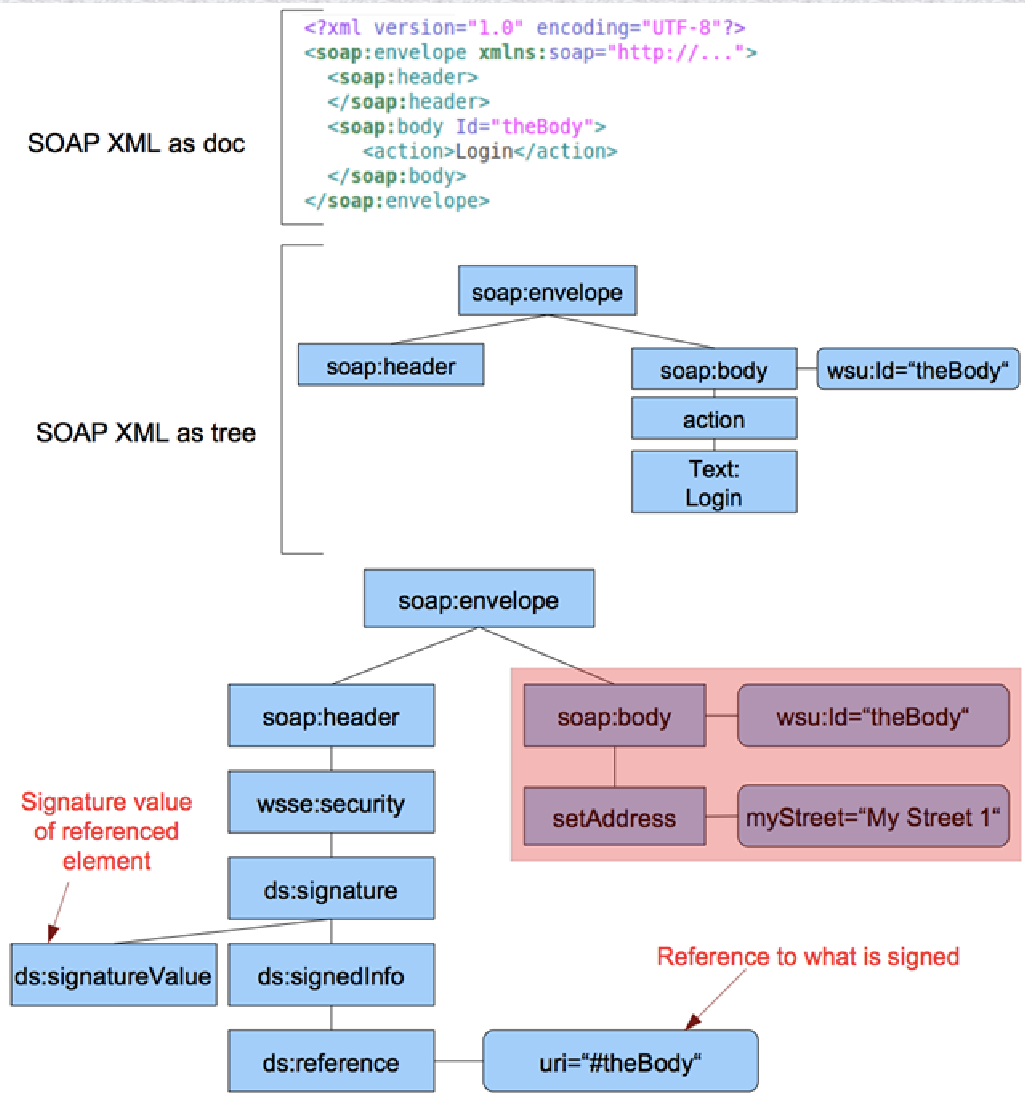
TESTING FOR BUSINESS LOGIC ATTACKS

1. **Data / Input Validation, if any**
2. **Ability to Forge Requests**
3. **Test the integrity checks, if any**
4. **Check process timings, if any** ***(eg. Password lockout OK … userid lockout?!)***
5. **Number of times function can be used, if any**
6. **Circumvention of Work Flows**
7. **Defense against application mis-use / manipulation**
8. **Test for Uploading of malicious files**
9. **Defenses for technologies used therein eg Adobe file**

(hacker does not attack the app itself but the components therein that may contain a weakness; its like … nowadays … its hard to attack a bank or military dept's site, so they attack the contractors)

SOAP BUSINESS LOGIC ATTACK

("Simple Object Access Protocol")



Theoretically you can gain admin accesss to eg. Twitter.

SOAP requests can use a security mechanism where a part of the message is signed and if any of that particular part of the message is changed it will not allow the request to be accepted. To understand more about this you need to have an in depth knowledge of what is in the SOAP request, so:

Every SOAP message has this envelope feature. In this case the request also has a header (that is empty) and a body with the ID of "theBody" and the action of Login. Because SOAP uses XML we can display the requests using both plain XML and as an XML tree.

The idea behind the signature wrapping attack is that you are tricking the business logic into accepting a malformed request.

Courtesy InfoSec Institute

BUSINESS LOGIC ATTACKS

- Authentication flags & privilege escalations
- Critical parameter manipulation & access to unauthorized information/content
- Developer's cookie tampering & business process/logic bypass
- LDAP parameter identification & critical infrastructure access
- Business constraint exploitation
- Business flow bypass
- Exploiting clients side business routines embedded in JavaScript, Flash or Silverlight
- Identity or profile extraction
- File or unauthorized URL access & business information extraction
- Denial of Services (DoS) with business logic

HACKING (STEALING) BITCOIN?!

- *Not Bitcoin per se, but their exchanges & service-providers*
- *Or attacking the private-key repositories*

Mt Gox hacked, database stolen and abused

Bitcoin blockchains are Public, making it a natural Theft deterrent

(1) Copy the keys

(2) Find a tumbler to launder your (stolen) coins

(3) Convert the Bitcoins to regular currency.

Courtesy Verge

Bitcoin bank folds after hacker robbery

Published time: March 05, 2014 03:49
Edited time: March 05, 2014 05:21

flexcoin the bitcoin bank

Flexcoin is shutting down.

On March 2nd 2014 Flexcoin was attacked and robbed of all coins in the hot wallet. The attacker made off with 896 BTC, dividing them into these two addresses:

1NDkevapt4SWYFEmquCDBSf7DLMTNVggdu

1QFcC5JitGwpFKqRDd9QNH3eGN56dCNgy6

As Flexcoin does not have the resources, assets, or otherwise to come back from this loss, ... mediately.

Screenshot from flexcoin.com

Like 1.1k Tweet 146 0 points Submit g+1 51 t

Bitcoin storage site Flexcoin announced Tuesday that it has closed after hackers robbed it of some $600,000 worth of digital currency.

Tags
Bitcoin, Currencies

"On March 2nd 2014 Flexcoin was attacked and robbed of all coins in the hot wallet. The attacker made off

Sheep is down

We are sorry to say, but we were robbed on Saturday 11/21/2013 by vendor EBOOK101. This vendor found bug in system and stole 5400 BTC - your money, our provisions, all was stolen. We were trying to resolve this problem, but we were not successful. We are sorry for your problems and inconvenience, all of current BTC will be ditributed to users, who have filled correct BTC emergency adress.

Struts Vulnerabilities in Parameters and Cookie Interceptors

We have seen one POC available in public that takes advantage of the ClassLoader being used by Tomcat. The exploit works by modifying the configuraiton settings of Tomcat (via AccessLogValve); more specifically, it changes the naming scheme of log files and the location where log files are stored to root directory, where Web application code is stored. Thereafter, when the attacker sends a request containing malicious script — such as a request containing JSP code — this will get logged into the log file, which now may have a name and extension of the attacker's choice (e.g., file1.jsp). As this log file is now in WEBROOT or someplace from which the Web server serves pages containing JSP code, the attacker can then send a GET request for file1.jsp. When the Web server processes this file, it will execute the malicious code, and the attacker gets remote code execution on the Web server. Here are POC requests to the sample Struts blank application (you can find how to set this up here).

The requests below will change the log file location and naming convention:

(Note: We are using Wget, but these requests can generally be sent via a browser as well)

```
wget http://127.0.0.1/struts2-blank/example/HelloWorld.action?Class.classLoader.resources.context.parent.pipeline.first.directo

wget http://127.0.0.1/struts2-blank/example/HelloWorld.action?Class.classLoader.resources.context.parent.pipeline.first.prefix=

wget http://127.0.0.1/struts2-blank/example/HelloWorld.action?Class.classLoader.resources.context.parent.pipeline.first.suffix=

wget http://127.0.0.1/struts2-blank/example/HelloWorld.action?Class.classLoader.resources.context.parent.pipeline.first.fileDat
```

Then, if we send the request with jsp code, it gets stored into log file. Note that we are using Netcat to avoid URL encodings:

Lessons / Conclusions:

-difficulty of getting blacklisting and whitelisting right

- importance of code and patch reviews (in this case one same vulnerability hits both parameter & cookie inteceptors)

- importance of patching itself.

◆http://securityintelligence.com/struts-vulnerabilities-analysis-parameters-cookie-interceptors-impact-exploitation/#.U4CNP2eKDDo

WhiteHat Security 2013 Top 10 New Attacks

1. Mutation XSS

- capable of bypassing high-end filter systems by utilizing the browser and its often unknown capabilities

2. BREACH Compression Attack

- Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext, is a compression attack similar to CRIME (Compression Ratio Info-leak Made Easy)

3. HTML5 Pixel-Perfect Timing Attacks

4. "Lucky 13" attack

- against TLS (Transport Layer Security) and Datagram-TLS (DTLS)
- TLS MAC includes 13 bytes of header information, which lets the attack happen

5. Weaknesses in RC4 Encryption in TLS.

WhiteHat SECURITY

WhiteHat Security 2013 Top 10 New Attacks

6. XML Out-of-Band Data Retrieval

7. Million Browser Botnet

- using web advertising services to spread malware

8. DOM-based XSS (aka "Type 0 XSS")

- ("Document Object Model")

- attack payload is executed by modifying the DOM "environment" in the victim's browser used by the original client- side script.

9. TOR Hidden-Service Passive De-Cloaking

- Broken link reveals source

10. HTML5 Hard Disk Filler™ API

Special Mention : **Serialized YAML Remote Code Execution**

- with Rails 2.3 and 3.0

Where Do We Go From Here

(towards safer software applications)

For Developers -

- Ask for secure code training
- Design your features securely
- Adopt secure coding standards and practices
- Refactor existing code to use safer constructs
- Review and apply the OWASP Development Guide and controls
- Test your code for security defects
- Have a security testing regime

Courtesy Owasp

Where Do We Go From Here

(towards safer software applications)

For Application Owners -

- Work through the OWASP Secure Software Contract Annex with the software producers
- Ensure business requirements include non-functional requirements (NFRs) such as security requirements
- Encourage designs which include secure by default features, defense in depth and simplicity in design
- Employ (or train) developers who have a strong security background
- Test for security defects throughout the project: design, build, test, and deployment
- Allow resources, budget and time in the project plan to remediate security issues

Courtesy Owasp

Where Do We Go From Here

(towards safer software applications)

For C-Level Executives -

- For off the shelf software, ensure purchasing policies and contracts include security requirements
- For custom code, adopt secure coding principles in your policies and standards
- Train your developers in secure coding techniques and ensure they keep these skills up to date
- Include security-relevant code analysis tools in your budget
- Notify your software producers of the importance of security to your bottom line
- Train your architects, designers, and business people in web application security fundamentals
- Consider using third-party code auditors, who can provide an independent assessment
- Adopt responsible disclosure practices and build a process to properly respond to vulnerability reports for your products

Courtesy Owasp

Five Tips for Improved Application Security

Per IBM (up to 80% improvement!)

1.Get trained on secure coding practices.

*Management should support and fund this effort

2.Use only stored procedures for database calls.

This helps prevent SQL injection attacks, which abuse database statements sent as SQL command strings instead of using parameterized procedures. If you don’t understand how SQL injection attacks work, see step 1.

3.Sanitize user input.

This will stop cross-site scripting (XSS) and cross-site request forgery (XSRF) attacks. SQLI targets Web servers, XSS/XSRF targets clients by tainting the HTML that’s served to the browser. Again, if you don’t understand how XSS/XSRF attacks work, see step 1.

Five Tips for Improved Application Security

Per IBM (up to 80% improvement!)

4.Integrate source and dynamic application security testing into your development process.

SAST and DAST aren't substitutes for secure coding practices, but they will help you catch what you might miss; to err is human. Beyond the benefits of catching latent security vulnerabilities, these solutions integrate with your source control solution and can help train developers by giving detailed information about how vulnerability manifests itself. Application scanning solutions can also identify chronic defects so you can focus your training efforts.

5.Instrument granular and meaningful events and errors.

One of the major reasons there are so many gray bubbles in the graphic on public disclosures is because organizations are unable to perform complete and timely forensics investigations. This is in part due to a lack of technology and process — no log management, SIEM solutions or not collecting the right telemetry — but many systems also produce generic or esoteric events.

(ISC)2 10 Secure Software Best Practices

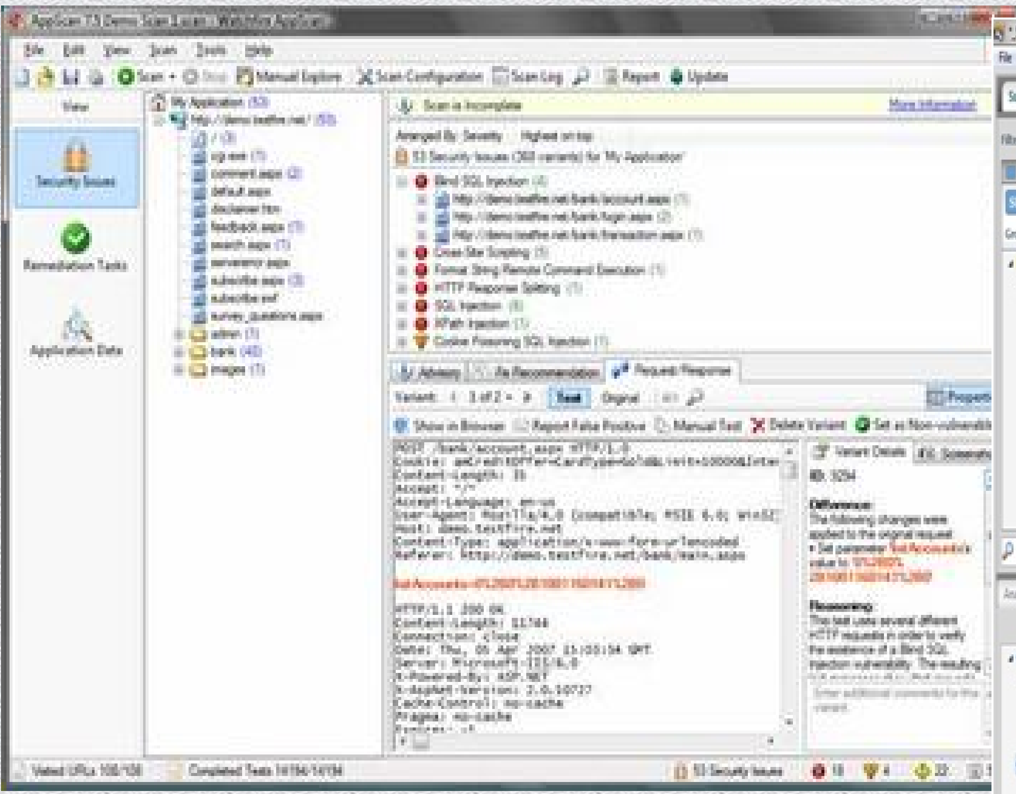
1. Protect the Brand Your Customers Trust
2. Know Your Business and Support it with Secure Solutions
3. Understand the Technology of the Software
4. Ensure Compliance to Governance, Regulations, and Privacy
5. Know the Basic Tenets of Software Security
6. Ensure the Protection of Sensitive Information
7. Design Software with Secure Features
8. Develop Software with Secure Features
9. Deploy Software with Secure Features
10. Educate Yourself and Others on How to Build Secure Software

ISC)2 Characteristics of Insecure Code

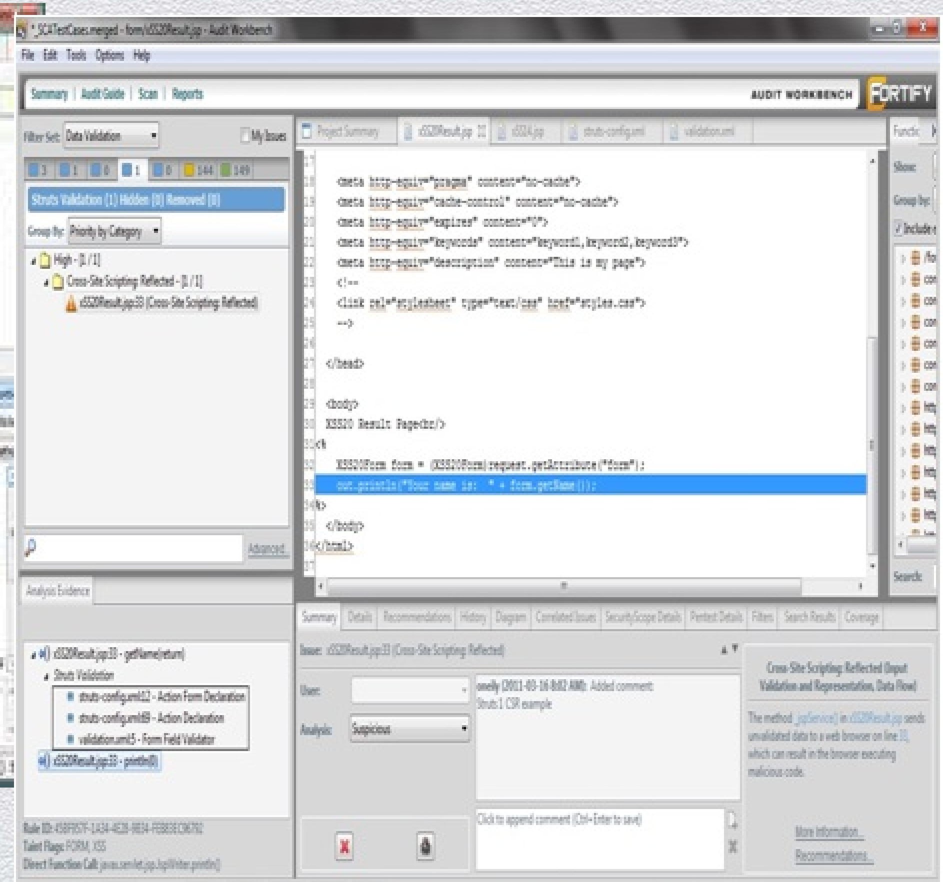
I	Injectable Code
N	Non-Repudiation Mechanisms not Present
S	Spoofable Code
E	Exceptions and Errors not Properly Handled
C	Cryptographically Weak Code
U	Unsafe/Unused Functions and Routines in Code
R	Reversible Code
E	Elevated Privileges Required to Run

PROFESSIONAL SOFTWARE QA TOOLS

"WHITE BOX" (static code analyzer) and "BLACK BOX" (dynamic application analyzer)
- automate application-development testing, Q.A. and vulnerability management process
- providing comprehensive reports of security issues with remediation guidance.



IBM Appscan



HP Fortify

Other Application Security Solutions

<u>Outsourced Penetration Test Services</u>

* Whether on-site or remote   eg. WH, CX, Big 4, SI

<u>Issues to consider</u>

* The good ones are very expensive, and its hard to say who's really "good"

- May not actually <u>solve</u> the problem

<u>Web Application Firewalls (WAF)</u>

<u>Advantages</u>

* Convenient; easy to install and run; plug-and-play

* Immediately stops 70% of common web attacks

<u>Issues to consider</u>

* Difficult to configure, and need to configure often in line with app changes

- Does not fix the problem; issues still in the software, staff not learning.

(ISC)^2 Survey & Global Information Security Workforce Study -Stats

- **<u>59% not following a rigorous Security process</u>**
- 26% have no hint of Security within their development lifecycle
- **48% claim to audit procedures regularly**
- 69% Blame Culture as reason for current practices
- 57% blame lack of Education
- 70% claim to have insufficient guidance for key technology models

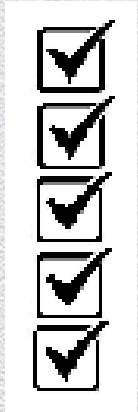
The worst reason to have security is Governance & Regulation

-**You must know why you want security, not because someone said so**

- we end up trying all sorts of ways to get by or get past the feared (or hated) auditor …

59% of staff will try to bypass a security process

A
U
D
I
T



EMPOWERING THE HUMAN RESOURCE ELEMENT

Continuing Education and Certification

Security CERTIFICATION for Application Development & Security Teams

www.isc2.org

CISSP

'COS DEVELOPERS NEVER HAD TO WORRY ABOUT THIS BEFORE … UNTIL NOW

CSSLP®

The **Certified Secure Software Lifecycle Professional** (CSSLP) Certification Program will show software lifecycle stakeholders not only how to implement security, but how to glean security requirements, design, architect, test and deploy secure software.

An Overview of the Steps:

(ISC)² ® 5-day CSSLP CBK® Education Program

Educate yourself and learn security best practices and industry standards for the software lifecycle through the CSSLP Education Program.(ISC)² provides education your way to fit your life and schedule.Completing this course will, not only teach all of the material contained within each of CSSLP seven domains but, give you the expertise to establish a security plan across your software development lifecycle, regardless of your methodology.

The CSSLP Exam

Prove your knowledge and experience by taking the CSSLP exam which is available worldwide.

Download the CSSLP Candidate Information Bulletin.

(ISC)² Membership

Once you successfully pass the exam and endorsement process, you'll be part of a globally recognized family of over 68,000 professionals. You'll have access to our full

(ISC)2 Certified Secure Software Lifecycle Professional (CSSLP®) Domains

- Secure Software Concepts
- Secure Software Requirements
- Secure Software Design
- Secure Software Implementation/Coding
- Secure Software Testing
- Software Acceptance
- Software Deployment, Operations, Maintenance, and Disposal
- SUPPLY CHAIN & Software Acquisition

(ISC)²®

Security in the Skies

Cloud computing security concerns, threats, and controls

Mano Paul, CSSLP, CISSP, AMBCI, MCAD, MCSD, Network+, ECSA

Introduction

The Internet, often represented as a cloud in architectural diagrams, has changed the way of life for both the individual and businesses. This whitepaper highlights the security concerns that are evident in cloud computing, with particular focus on information assurance, and provides strategies to adopt when evaluating cloud service providers and when designing, developing, and deploying applications that will operate in the cloud. It also gives guidance on what some of the next steps need to be for secure cloud computing.

What is Cloud Computing?

Cloud computing is one of the most highly discussed topics within the typical organization, according to the 2011 (ISC)² Global Information Security Workforce Study (GISWS) conducted by Frost and Sullivan. But what is cloud computing? Is it a silver lining in computing, or is it a harbinger of an impending perfect storm?

Institute of Standards and Technology (NIST) developed: *Cloud Computing – A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*

Architecture and Service Models

The cloud computing architecture is primarily a multi-tenant, service based architecture. It has a distinct consumer front-end and the

"The three primary service models in cloud computing are IaaS, PaaS and SaaS"

(ISC)²®

Assuring Software Security Through Testing

White, Black and Somewhere In Between

Mano Paul, CSSLP, CISSP, AMBCI, MCAD, MCSD, Network+, ECSA

Introduction

Take any software development project plan today and it is more than likely that the plan will not have a line item with time allocated exclusively for security testing. It is only a matter of time before software deployed or released without attestation of its ability to withstand attacks will be hacked. It is not a question of if the software will be hacked, but when it will be hacked.

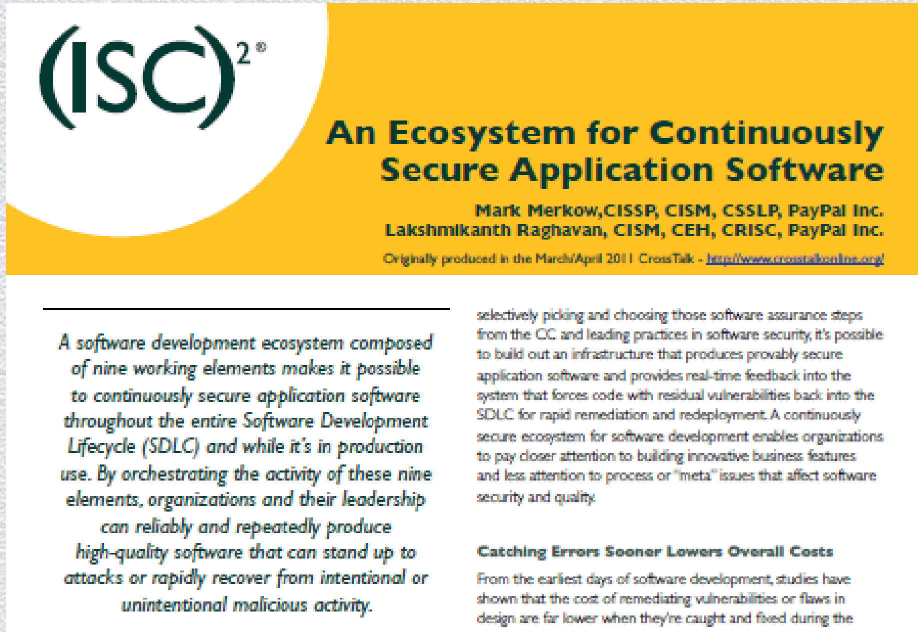
(ISC)²®'s whitepaper, *Code (In)Security*, highlights various considerations that need to be taken into account to develop code that is secure. But merely developing secure code without attesting to its assurance capabilities is akin to operating an automobile without checking to ensure that the brakes work as expected. With such an outlook, a crash becomes not just possible but inevitable. This paper will discuss the need for attesting software assurance, the different types of testing as it pertains to functionality and assurance, a security tester's profile, and some proven strategies to incorporate security testing into the software development lifecycle (SDLC).

Figure 1. Software Quality Components

Recoverability
Reliability
Resiliency
Software Quality

(ISC)2 CSSLP New Domain - Supply Chain and Software Acquisition

- Supplier Risk Assessment
- Supplier Sourcing
- Software Developement Test
- Software Delivery, Operations & Maintenance
- Supplier Transitioning



An Ecosystem for Continuously Secure Application Software

Mark Merkow, CISSP, CISM, CSSLP, PayPal Inc.
Lakshmikanth Raghavan, CISM, CEH, CRISC, PayPal Inc.

Originally produced in the March/April 2011 CrossTalk - http://www.crosstalkonline.org/

A software development ecosystem composed of nine working elements makes it possible to continuously secure application software throughout the entire Software Development Lifecycle (SDLC) and while it's in production use. By orchestrating the activity of these nine elements, organizations and their leadership can reliably and repeatedly produce high-quality software that can stand up to attacks or rapidly recover from intentional or unintentional malicious activity.

selectively picking and choosing those software assurance steps from the CC and leading practices in software security, it's possible to build out an infrastructure that produces provably secure application software and provides real-time feedback into the system that forces code with residual vulnerabilities back into the SDLC for rapid remediation and redeployment. A continuously secure ecosystem for software development enables organizations to pay closer attention to building innovative business features and less attention to process or "meta" issues that affect software security and quality.

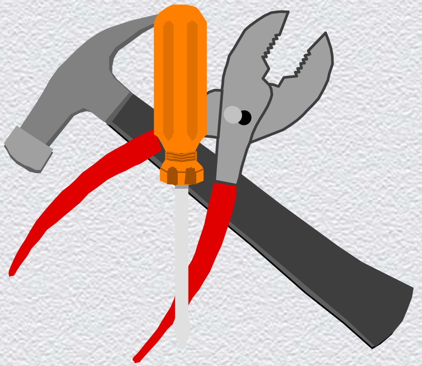
Catching Errors Sooner Lowers Overall Costs

From the earliest days of software development, studies have shown that the cost of remediating vulnerabilities or flaws in design are far lower when they're caught and fixed during the

Conclusion: 2 Components to I.T. Security

Technical Component

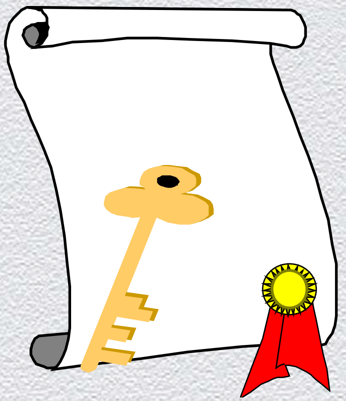
- Access Control
- Authenticated Access
- Encryption & Privacy
- Policy-based traffic filtering
- Enterprise Management etc



I.T. SECURITY TODAY IS NO LONGER A TECHNOLOGY THING – IT IS A HUMAN AND SOCIAL MATTER!

Human & Policy Component

- Education
- Enforcement
- Reinforcement
- Diligence & Vigilance
- CLEAR OWNERSHIP

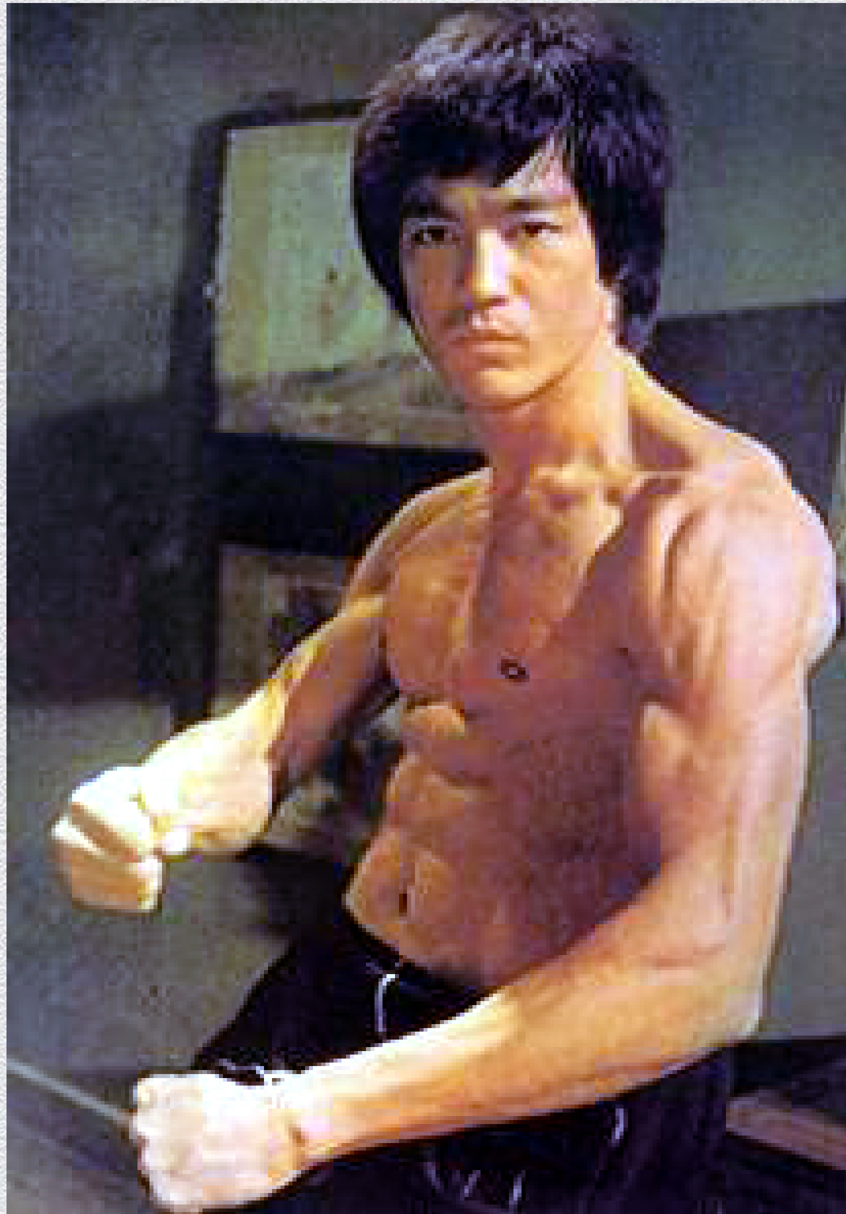


AS LONG AS HUMANS BEHAVE LIKE HUMANS WE WILL STILL HAVE A JOB IN I.T. SECURITY!

Technologies today can provide the technical component. Only commitment at the highest levels can the human factor be successful.

Application Security : Conclusion – Security by Application Development Q.A

- **The Application Must Defend Itself** **(ie. Write the programs properly)**
  - Network security solutions do not stop application attacks
  - Existing network security solutions do not automatically work well in cloud environments
- **THIS IS THE BEST AND ONLY WAY TO MINIMISE SOFTWARE ATTACKS**
- Both security and development teams need to be in harmony
- **DEVELOPERS NEED TO BE TRAINED APPROPRIATELY IN SECURE CODING**
- **MANAGEMENT MUST ACTIVELY SUPPORT AND FINANCE A SOFTWARE SECURITY POLICY, RESOURCE AND ONGOING PRACTICE**



(ISC)²

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

THANK YOU

Application Security – *The Invisible Onslaught Gets Worse*

Anthony Lim
Member, Application Security Advisory Board
(ISC)2 isc2.org