Web Hacking LIVE!

The monsters under the bed are real...

2004 World Tour

NETCONTINUUM

Agenda

Wichita ISSA – August 6th, 2004

- The Application Security Dilemma
- How Bad is it, Really?
- Overview of Application Architectures
- Uncovering Dangerous Vulnerabilities
- Demonstration of Hacking Techniques
- Vulnerability Remediation Options
- Summary and Next Steps

Why Application Security Matters

Data Disclosure

Customer Confidentiality

Customer List

Name	Main Contact	YTD Revenue
ACME Corp	John Michaels	$893, 56
Anderson Technologies	Sandra Watson	$599,670
Azure Systems	Mitch Wilson	$395,00
Best Industries	Muchael Le	
Cascade Inc.	Rob Smith	
Diamond Technology	Bruce Leah	
Echelon Manufacturing	Jennifer Bl	

User ID:

Password:

Identity Theft

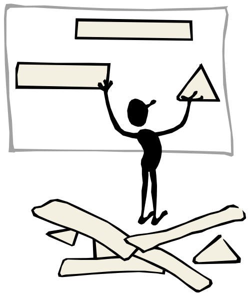
Data Theft

NETCONTINUUM

The Application Security Dilemma

Functionality

- Allow seamless application access to the world’s customers
- Make the application easy to use, friendly and feature-rich
- Constantly update the application to meet ever-changing business needs



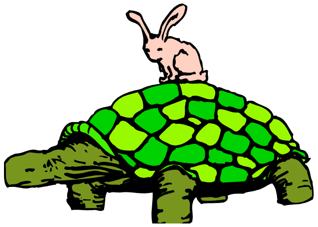
Security

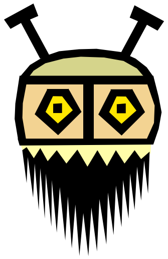
- Protect sensitive data from unauthorized prying eyes
- Make the application impervious to attack and compromise
- Minimize changes and complexity to maintain control and establish a security baseline

The Security Manager’s Dilemma

Impossible Request

- Improve performance. More speed!
- Constantly patch and watch for signatures of known attacks!
- Save Money! Cut the budget!



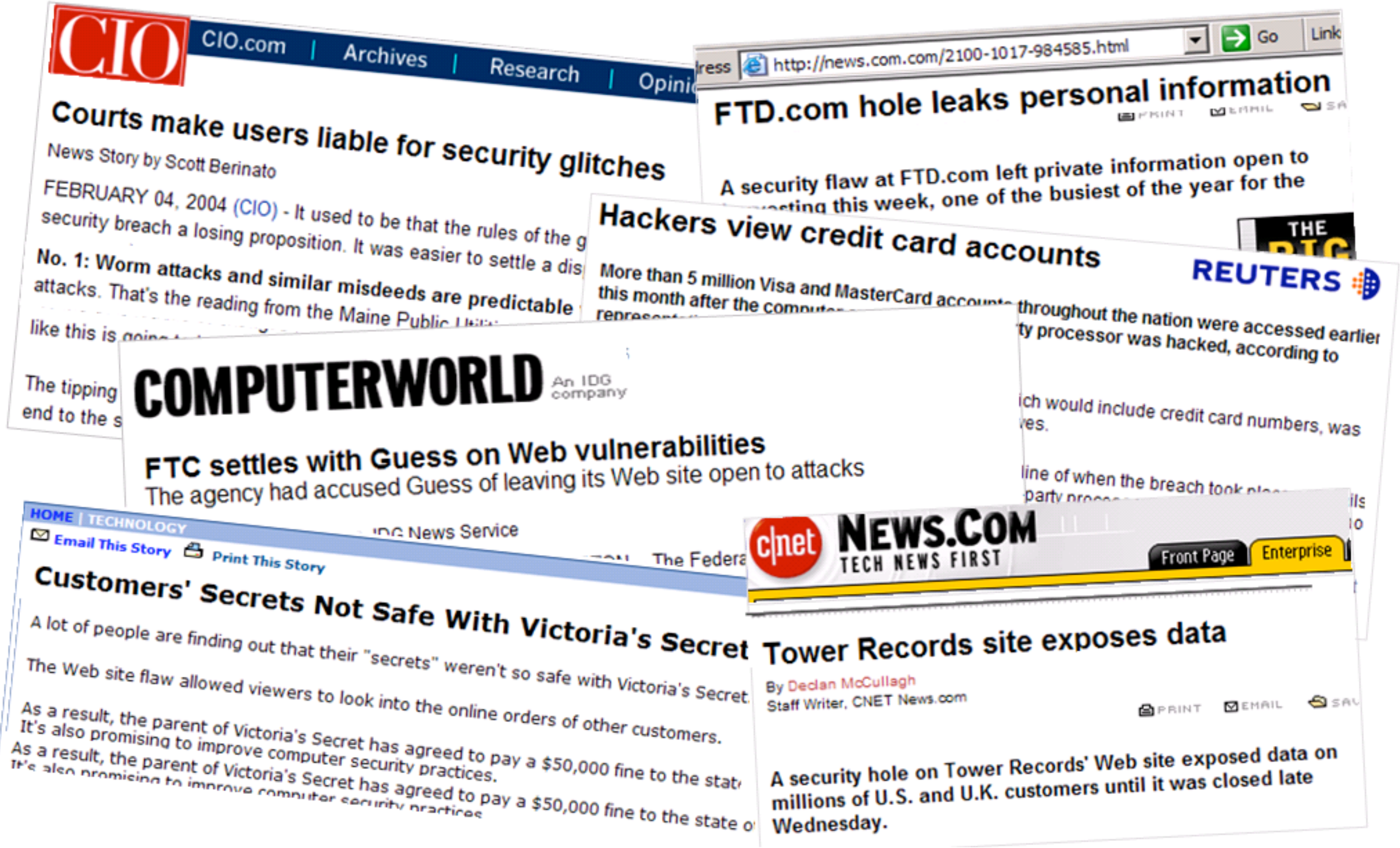


Reality Check

- Must inspect all traffic for attacks
- Secret Knowledge and Zero-Day Attacks have no known signatures
- What do I give up this time?

NETCONTINUUM

The Old Way of Doing Things Clearly Isn't Working



CIO | CIO.com | Archives | Research | Opini

Courts make users liable for security glitches

News Story by Scott Berinato

FEBRUARY 04, 2004 (CIO) - It used to be that the rules of the g security breach a losing proposition. It was easier to settle a dis

No. 1: Worm attacks and similar misdeeds are predictable

attacks. That's the reading from the Maine Public Utili

like this is goin

The tipping end to the s

ress http://news.com.com/2100-1017-984585.html Go Link

FTD.com hole leaks personal information

PRINT EMAIL SA

A security flaw at FTD.com left private information open to ...esting this week, one of the busiest of the year for the

THE BIG

Hackers view credit card accounts

REUTERS

More than 5 million Visa and MasterCard accounts throughout the nation were accessed earlier this month after the computer ...ty processor was hacked, according to represent

...ich would include credit card numbers, was ...ves.

...line of when the breach took place ...party proce

...ils ...o

COMPUTERWORLD An IDG company

FTC settles with Guess on Web vulnerabilities

The agency had accused Guess of leaving its Web site open to attacks

IDG News Service

The Federa

HOME | TECHNOLOGY

Email This Story Print This Story

Customers' Secrets Not Safe With Victoria's Secret

A lot of people are finding out that their "secrets" weren't so safe with Victoria's Secret.

The Web site flaw allowed viewers to look into the online orders of other customers.

As a result, the parent of Victoria's Secret has agreed to pay a $50,000 fine to the stat It's also promising to improve computer security practices.

As a result, the parent of Victoria's Secret has agreed to pay a $50,000 fine to the state o It's also promising to improve computer security practices

c|net NEWS.COM TECH NEWS FIRST Front Page Enterprise

Tower Records site exposes data

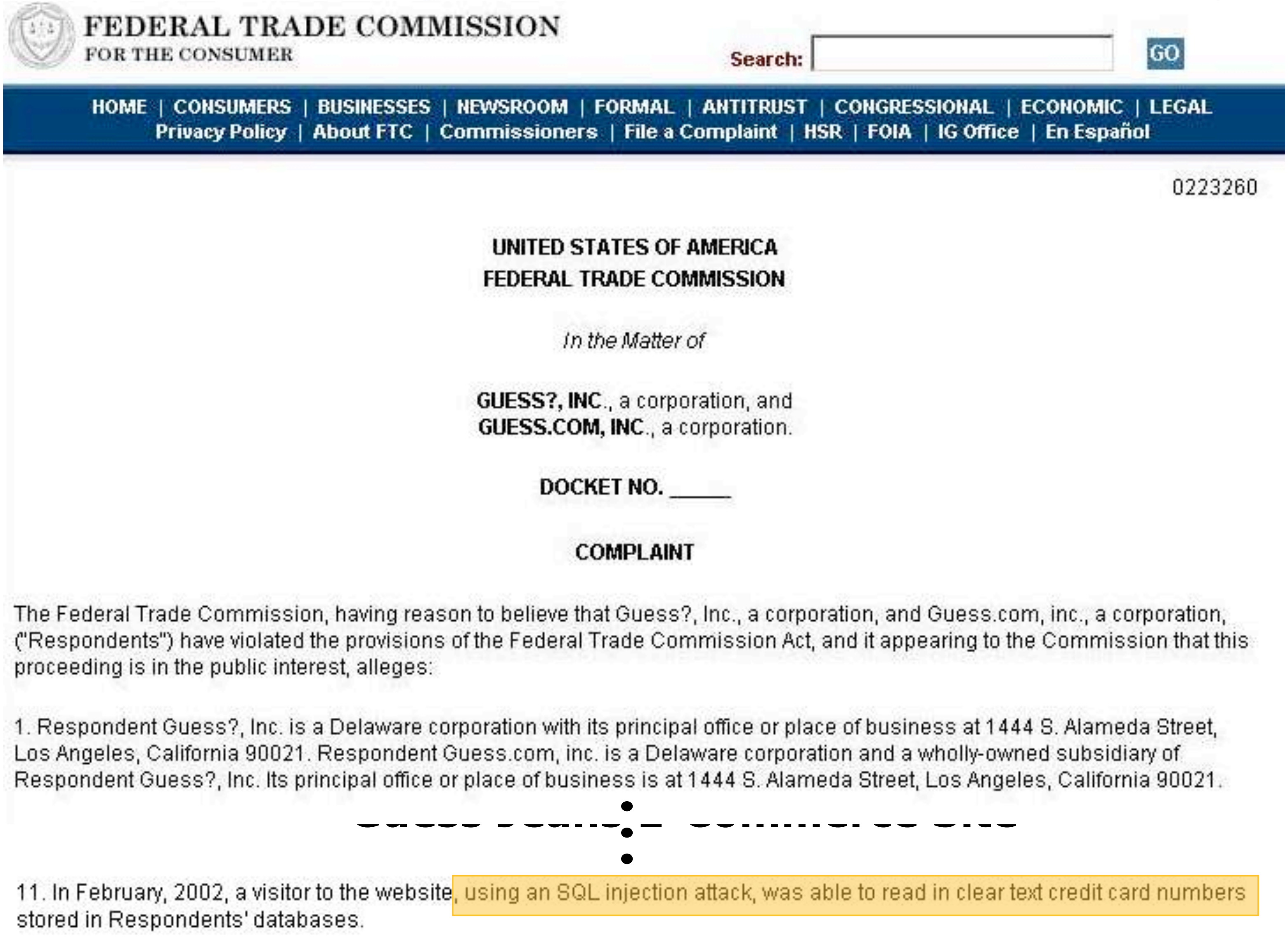
By Declan McCullagh
Staff Writer, CNET News.com

PRINT EMAIL SAV

A security hole on Tower Records' Web site exposed data on millions of U.S. and U.K. customers until it was closed late Wednesday.

NETCONTINUUM

Guess.com SQL Attack


FEDERAL TRADE COMMISSION
FOR THE CONSUMER
Search:
GO
HOME | CONSUMERS | BUSINESSES | NEWSROOM | FORMAL | ANTITRUST | CONGRESSIONAL | ECONOMIC | LEGAL
Privacy Policy | About FTC | Commissioners | File a Complaint | HSR | FOIA | IG Office | En Español

0223260

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of

GUESS?, INC., a corporation, and
GUESS.COM, INC., a corporation.

DOCKET NO. _____

COMPLAINT

The Federal Trade Commission, having reason to believe that Guess?, Inc., a corporation, and Guess.com, inc., a corporation, ("Respondents") have violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Guess?, Inc. is a Delaware corporation with its principal office or place of business at 1444 S. Alameda Street, Los Angeles, California 90021. Respondent Guess.com, inc. is a Delaware corporation and a wholly-owned subsidiary of Respondent Guess?, Inc. Its principal office or place of business is at 1444 S. Alameda Street, Los Angeles, California 90021.

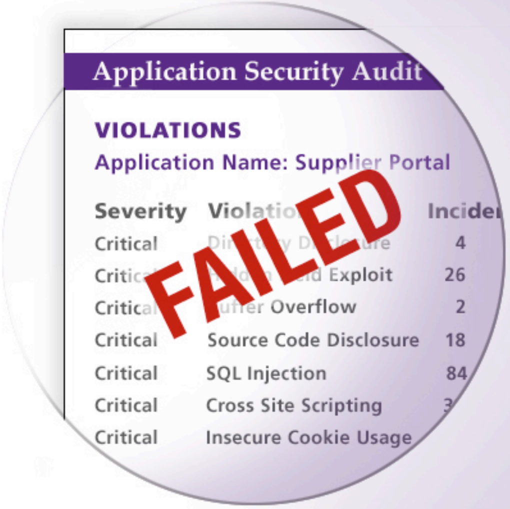
⋮

11. In February, 2002, a visitor to the website, using an SQL injection attack, was able to read in clear text credit card numbers stored in Respondents' databases.

Source: www.ftc.gov/os/2003/06/guesscmp.htm

NETCONTINUUM

External Pressure is Growing



Application Security Audit

VIOLATIONS

Application Name: Supplier Portal

Severity	Violatio	Incide
Critical	Directory Disclosure	4
Critic	[illegible] Exploit	26
Critica	uffer Overflow	2
Critical	Source Code Disclosure	18
Critical	SQL Injection	84
Critical	Cross Site Scripting	3
Critical	Insecure Cookie Usage	

FAILED

- Government regulations
- Industry regulations
- Internal auditors
- Tough new privacy laws

Sarbanes-Oxley

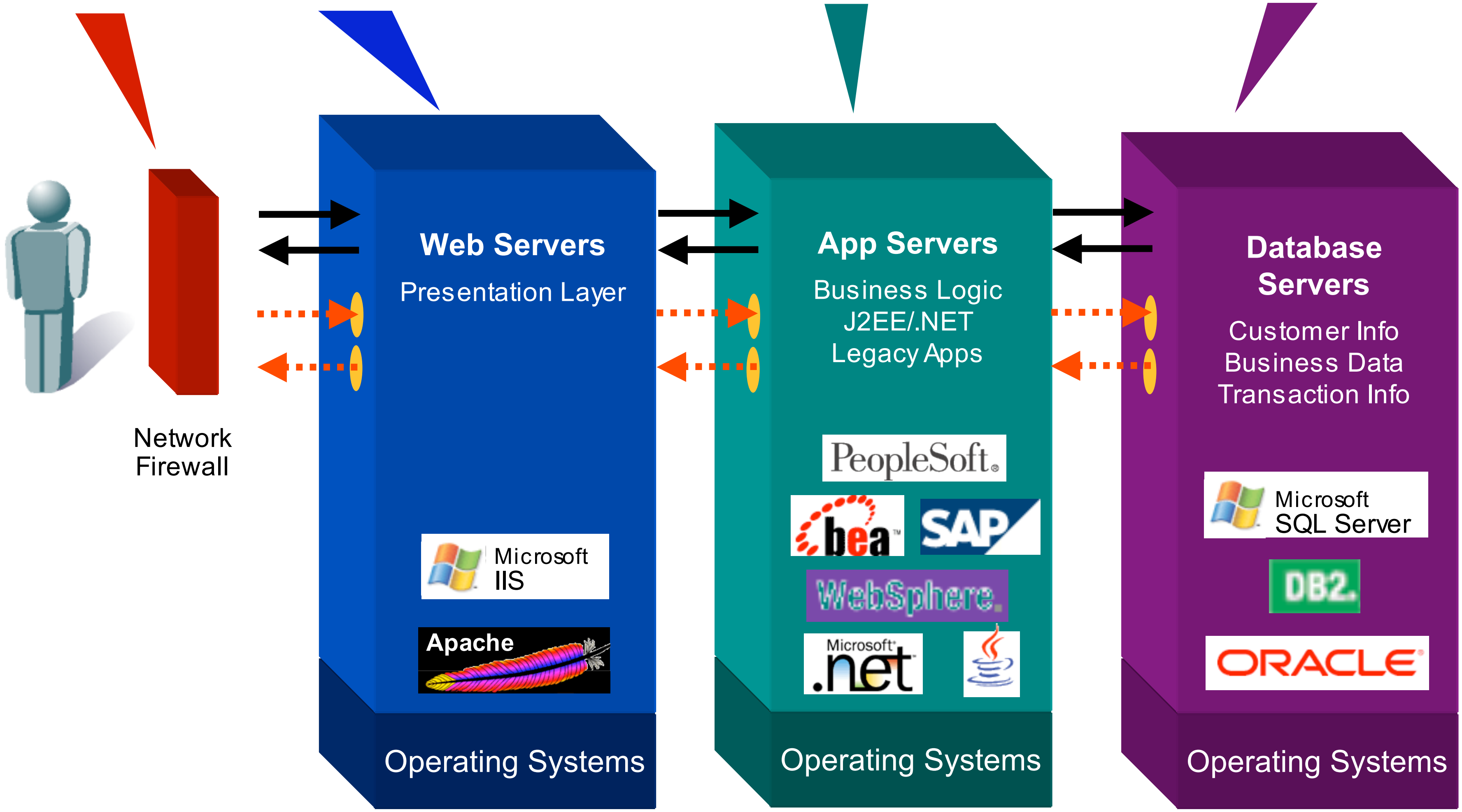
GLB

HIPAA

CA SB-1386

Securing Applications is Complex

http ://www.none.to/script ?submenu=update&uid =1'+or+like'%25admin%25';--%00



Linux Solaris AIX Windows

NETCONTINUUM

List of Application Attack Techniques Grows Every Day

Top Application Threat Classes

1. Cross-Site Scripting
2. SQL Injection
3. Command Injection
4. Cookie/Session Poisoning
5. Parameter/Form Tampering
6. Buffer Overflow
7. Directory Traversal/Forceful Browsing
8. Cryptographic Interception
9. Cookie Snooping
10. Authentication Hijacking
11. Log Tampering
12. Error Message Interception
13. Attack Obfuscation
14. Application Platform Exploits
15. DMZ Protocol Exploits
16. Security Management Attacks
17. Web Services Attacks
18. Zero Day Attacks
19. Network Access Attacks
20. TCP Fragmentation
21. Denial of Service

Business Impact:

- Access to unpublished pages
- Unauthorized app access
- Password theft
- Privacy and Identity theft
- Theft of customer data
- Modification of data
- Disruption of service
- Website defacement
- Recovery and cleanup
- Loss of Customer Confidence

Uncovering the Problem

Determining vulnerabilities in web applications:

Tools

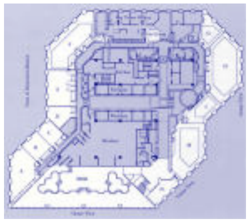
- Learn what assessment tools are available, and test them
- Use automated tools whenever possible, or script one
- Test the security of the network, servers, OS, web servers, middleware, business logic, databases, and browsers

Techniques

- Think like an Attacker!!! Where do you want to go today?
- Use de-compilation techniques to review source code
- Be curious – try "strange" techniques and "fuzzing"
  - What can an unauthenticated user do?
  - What can an authenticated user do?
- Document everything you do (and what you didn't do)!

Get written permission from someone authorized to give it to you!!!

To Block Attack Methods You Must First Understand Attacker's Methodology



Planning

Site Reconnaissance

Getting In

Attack obfuscation

Theft of legitimate credentials

Forceful browsing

On the Inside

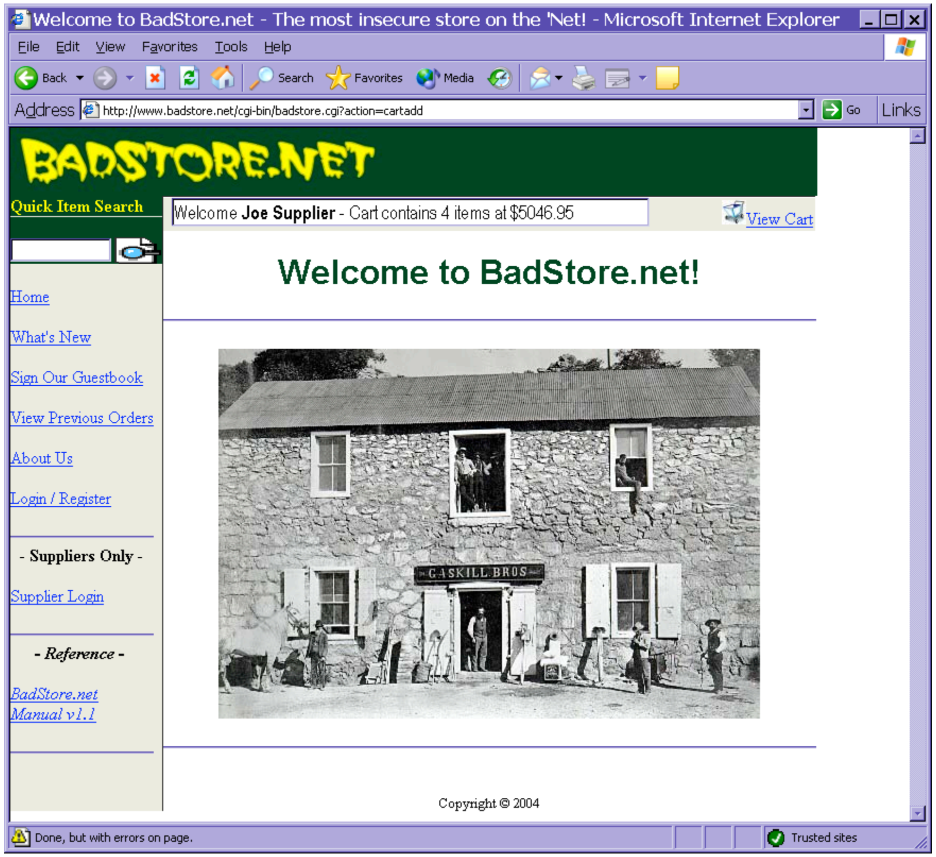
Parameter and input manipulation

Getting Away With It

Log tampering

NETCONTINUUM

Hacking Demonstration



http://www.badstore.net/cgi-bin/badstore.cgi?action=cartadd

Welcome **Joe Supplier** - Cart contains 4 items at $5046.95

Welcome to BadStore.net!

Copyright © 2004

Done, but with errors on page.

Top Application Threat Classes

1. Cross-Site Scripting
2. SQL Injection
3. Command Injection
4. Cookie/Session Poisoning
5. Parameter/Form Tampering
6. Buffer Overflow
7. Directory Traversal/Forceful Browsing
8. Cryptographic Interception
9. Cookie Snooping
10. Authentication Hijacking
11. Log Tampering
12. Error Message Interception
13. Attack Obfuscation
14. Application Platform Exploits
15. DMZ Protocol Exploits
16. Security Management Attacks
17. Web Services Attacks
18. Zero Day Attacks
19. Network Access Attacks
20. TCP Fragmentation
21. Denial of Service

NETCONTINUUM

Can’t We Just Go Fix the Code?

Every 1000 lines of code averages 15 critical security defects
(US Dept of Defense)

The average security defect takes 75 minutes to diagnose and 6 hours to fix.
(5-year Pentagon Study)

The average business application has 150,000-250,000 lines of code.
(Software Magazine)

Going back and fixing application security flaws cost companies $59 billion last year
(Research Triangle Institute)

“Trying to keep up by simply fixing code and patching is just too hard… customers have to have better defenses at the application perimeter”

- Steve Ballmer, Microsoft, 2003

You've identified problems – now what?

Your remediation options are:

- Block – application security gateways block current and future threats at the perimeter – now you have breathing room!
- Patch – *if* a patch is available, by all means, apply it!
- Recode – *if* you have control over the application and can fix it in a timely manner and within a reasonable budget
- Replace the Application – sometimes, the application is just too broken or too outdated, and is best replaced
- Ignore – and hope the guards are nice to you...

"Most applications will never be secure enough to meet evolving threats. Companies must also install a layer of protection between the application and potential attackers."

- Gartner, 2003

Action plan

To mitigate web application vulnerabilities:

1. Know the risk your organization is willing to accept, clearly defining “acceptable loss”
2. Implement a “Defense in Depth” protection architecture to block attacks against critical data
3. Develop a deep understanding of the usage and features of your most crucial web applications
4. Regularly test all layers of your web applications with automated and manual tools and techniques
5. Perform periodic forensic review of logs and error messages to prove information assurance
6. Think Like an Attacker while actively protecting!!!
7. Trust nobody – validate all application input

Thank You!

NETCONTINUUM

Kurt R. Roemer, CISSP
Chief Security Officer
NetContinuum
847-548-5390 Office
847-420-7846 Mobile
kroemer@netcontinuum.com
http://www.netcontinuum.com

Application Firewalls are Now Industry Best-Practice

40% of the Fortune 500 will deploy Web Application Firewalls during 2004.

- Enterprise Security Buying Survey
Forrester Research, 2004

70% of all threats today are application-layer attacks that traditional firewalls can't block.

- Web Hacking Exposed, 2003

"Most applications will <u>never</u> be secure enough to meet evolving threats. Companies must install application firewalls in front of key apps."

- Gartner, 2003

NETCONTINUUM

The NetContinuum Advantage

- ✓ Unparalleled ASIC-based platform
- ✓ Powerful methods-based approach stops attacks cold
- ✓ Protects *known* platform attacks proactively
- ✓ Protects *custom code* that has no signatures or patches
- ✓ Protects with no changes to apps, servers or networks

"NetContinuum is the leader
in application firewalls"

Gartner