Hacker Attacks on the Horizon: Web 2.0 Attack Vectors

Danny Allan
Director, Security Research
dallan@us.ibm.com
Agenda

- HISTORY
- Web Eras & Trends
- SECURITY
- Web 2.0 Attack Vectors
- VISION
- Securing Web 2.0
Web Eras

- **Web 0.9**
  - August 6, 1991
  - Static HTML content

- **Web 1.0**
  - Mid 1995
  - Applications
    - .asp, .cfm, .do, .php

- **Web 2.0**
  - O’Reilly Media uses the term in 2004
What is Web 2.0?

- **Marketing Term**
- **Significant paradigm shift**
  - Collaborative Communities
    - Social networks
    - Wikis
    - Blogs
  - Modularity
    - Applications on demand
    - Software as a Service
    - Mash-ups
The Myth: “Our Site Is Safe”

- We Have Firewalls in Place
- We Audit It Once a Quarter with Pen Testers
- We Use Network Vulnerability Scanners
- We Use SSL Encryption
The Alarming Truth

LexisNexis Data Breach
- Washington Post
  Feb 17, 2008

Data Breach
- Washington Post
  Feb 17, 2008

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

Malware
- InformationWeek
  Feb 17, 2008

Greek Ministry websites hit by hacker intrusion
- eKathimerini, Jan 31, 2008

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

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

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

Hacking Stage 6
- Wikipedia, Feb 9, 2007

Your Free MacWorld Expo Platinum Pass
- CNet, Jan 14, 2008

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

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

Hacker takes down Pennsylvania gvt
- AP, Jan 6, 2008

RIAА wiped off the Net
- TheRegister, Jan 20 2008

Your Free MacWorld Expo Platinum Pass
- CNet, Jan 14, 2008

Greek Ministry websites hit by hacker intrusion
- eKathimerini, Jan 31, 2008

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

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

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

Hacking Stage 6
- Wikipedia, Feb 9, 2007

Your Free MacWorld Expo Platinum Pass
- CNet, Jan 14, 2008

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

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

Hacker takes down Pennsylvania gvt
- AP, Jan 6, 2008

RIAА wiped off the Net
- TheRegister, Jan 20 2008

The Alarming Truth

LexisNexis Data Breach
- Washington Post
  Feb 17, 2008

Data Breach
- Washington Post
  Feb 17, 2008

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

Malware
- InformationWeek
  Feb 17, 2008

Greek Ministry websites hit by hacker intrusion
- eKathimerini, Jan 31, 2008

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

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

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

Hacking Stage 6
- Wikipedia, Feb 9, 2007

Your Free MacWorld Expo Platinum Pass
- CNet, Jan 14, 2008

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

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

Hacker takes down Pennsylvania gvt
- AP, Jan 6, 2008

RIAА wiped off the Net
- TheRegister, Jan 20 2008
Attacks of Previous Eras

- **Web 0.9**
  - Defacement
  - Denial of Service

- **Web 1.0**
  - SQL Injection
  - Command Execution
Hacker Attacks of the Future

- **Attacks by Type**
  - Cross-site scripting (XSS)
  - Cross-site request forgery (CSRF)
  - Browser & Plugin Flaws

- **Technologies at risk**
  - AJAX
  - Web Services
  - Browsers
Web 2.0 Terms

- Rich Internet Applications
- AJAX
- Mash-ups

Web 2.0
Agenda

**HISTORY**

Web Eras & Trends

**SECURITY**

Web 2.0 Attack Vectors

**VISION**

Securing Web 2.0
Where are the attacks?

- **Desktop**
  - Antivirus Protection

- **Transport**
  - Encryption (SSL)

- **Network**
  - Firewalls / Advanced Routers

- **Web Applications**
  - Web Servers
  - Web Application
  - Databases
  - Backend Server
Who are we against?

- **Organized Crime**
  - What: Data & Identity Theft
  - Why: Ca$h

- **Espionage (Nation State & Corporate)**
  - What: Data Theft & Intellectual Property
  - Why: Competitive Advantage

- **H4ck0rZ**
  - What: Defacement & Denial of Service
  - Why: Ego & Credibility building
2006 Vulnerability Statistics (31,373 sites)

Traditional Web Services? (W3C definition)

- “A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards” (W3C)
Traditional Web Service Attacks

- XML parser Denial of Service
  - DTD named & parameter entities
  - Attribute blowup
- SOAP array overflow
- XML external entity file disclosure
- SOAP Web Services Injection
AJAX Web Services

- A Web 2.0 service is a software system designed to support interoperable machine-to-machine interaction over a network. This software system allows organizations to focus on the application being designed while consuming services from third parties to enrich the functionality. (eg. Google Maps, Spelling Cow)
Fundamental Problems with AJAX

- Architectural & framework weaknesses
- Authentication & authorization
- Attack surface fragmentation
- Transport
- Communication management
- Can not trust the client
Web 2.0 Attacks

- **JavaScript hijacking**
  - Brian Chess, Jacob West

- **Prototype hijacking**
  - Stefano Di Paola, Giorgio Fedon

- **Cache Poisoning**
  - Amit Klein, Stefano Di Paola, Giorgio Fedon

- **DNS Attacks**
  - Princeton Research (Feb 2005)
AJAX Web Service Attacks

- Social engineering
- Cross-site scripting
- Cache poisoning
- Transport hijacking
- DNS attacks
1. Cross-Site Scripting (XSS)

- **What is it?**
  - Malicious script echoed back into HTML returned from a trusted site, and runs under trusted context

- **What are the implications?**
  - Session Tokens stolen (browser security circumvented)
  - Complete page content compromised
  - Future pages in browser compromised
2. Injection Flaws

- **What is it?**
  - User-supplied data is sent to an interpreter as part of a command, query or data.

- **What are the implications?**
  - SQL Injection – Access/modify data in DB
  - SSI Injection – Execute commands on server and access sensitive data
  - LDAP Injection – Bypass authentication
  - …
5. Cross Site Request Forgery (CSRF/XSRF)

- **What is it?**
  - Tricking a victim into sending an unwitting (often blind) request to another site, using the user’s session and/or network access.

- **What are the implications?**
  - Internal network compromised
  - User’s web-based accounts exploited
Web 2.0 Demonstration Attacks
Agenda

HISTORY
Web Eras & Trends

SECURITY
Web 2.0 Attack Vectors

VISION
Securing Web 2.0
Asking the Wrong Question

- Business Owner
  - Why isn’t the app working?

- Developer
  - What’s wrong with the code?

- QA Test
  - Where are the bugs?

- Security Auditor
  - What is our risk exposure?

What are the root causes?
Understanding the Root Causes

1. Takes the focus off the symptoms
2. Eliminates over-reporting
3. Highlights pro-active security
4. Can help build education programs
5. CHASING VULNERABILITIES DOESN’T WORK
Online Risk Management for the Enterprise

People

Process

Technology
Building Security & Compliance into the SDLC

- Coding
  - Developers

- Build
  - Provides Developers and Testers with expertise on detection and remediation ability

- QA
  - Enable Security to effectively drive remediation into development

- Security
  - Ensure vulnerabilities are addressed before applications are put into production

- Production
  - Developers

Enable Security to effectively drive remediation into development.
Questions?

Danny Allan

dallan@us.ibm.com

www.watchfire.com/securityzone