Sense of Security Pty Ltd
(ABN 14 098 237 908)
306, 66 King St
Sydney NSW 2000
Australia

Tel: +61 (0)2 9290 4444
Fax: +61 (0)2 9290 4455
info@senseofsecurity.com.au

Managing and Securing

Web 2.0

4 March 2009

What is Web 2.0?

- Web 2.0 refers to today's "second generation" of Web technologies
  - includes AJAX, RSS feeds, online forums, and mashups.

- In general Web 2.0 covers broader development trends:
  - Rich Internet Applications (RIA): Feature rich web sites; mimic thick client applications.
  - Collaboration and Participation: Generating and sharing content in real time; wikis, extranets, blogs, social networking sites, online forums.
  - Syndication: RSS or Atom feeds and mashups. Broadcasting of data.

Look familiar?

Social Networks

facebook

myspace a place for friends

bebo

hi5

Instant Messaging

meebo

RSS

Google Reader

Tagging

del.icio.us

digg

reddit

Personalised Home Pages

iGoogle

netvibes

MY YAHOO!

Windows Live

Pageflakes

Widgets

Windows

Google Desktop

YAHOO! WIDGETS

Source: Worklight

Sense of Security

Security that enables business

Why should you care about Web 2.0?

- Consumer (i.e. "Web 2.0") technologies are already finding their way into the enterprise.
  - Employees use (sanctioned and unsanctioned) consumer tools to perform day-to-day business tasks
  - Enterprise applications use consumer technologies to provide the latest and greatest in usability and functionality
  - Examples include: instant messaging, blogs, mashups, wikis

- ……..and Web Applications are the focus of attacks
  - Web applications in general have become the Achilles heel of Corporate IT Security.
  - Nearly 55% of all vulnerability disclosures in 2008 affect Web applications
  - SQL injection jumped 134 percent and replaced cross-site scripting as the predominant type of Web application vulnerability (several hundred thousand per day at the end of 2008).

    (Source IBM)

It’s real

- 78% of IT organizations are concerned about the risks of employee-driven, unsanctioned use of Web 2.0 tools and technologies

  Source: Forrester Research

- 50% of respondents said they "customize their work environment moderately or aggressively" (including the use of unsanctioned tools) and will continue to do so.

  Source: Gartner Research poll

Awareness

- One of the objectives of this seminar
  - Generate awareness around the secure use of Web 2.0 services and technologies to do business (because you can do it securely)
  - Present valuable information about the risks associated with the use of Web 2.0 services and technologies for business (because you should be careful)

Web 2.0 Security Issues

- The main security issues that must be addressed include the following:
  - User Authentication
  - Access control (authorisation)
  - Data security
  - Credential security
  - Client security
  - Acceptable use of new tools, such as:
    - RSS
    - Instant messaging
    - Blogs
    - Wikis
    - Bookmarking and tagging
    - Personalised homepages
    - Social networks

Different, but same same

While Web 2.0 sites may have some fancy user interfaces and provide the ability to interact and share information in new ways, the principles guiding secure development, deployment and maintenance remain the same as traditional web methods.

RIA Threats

- RIA's push application logic to the client
  - Can include access controls and session management.
  - Client code is easily manipulated by attackers
  - Flash, AJAX, Java (can be decompiled on client side)
- Server methods are exposed
  - Servers need to interact more openly with clients
  - Provides another attack vector and larger attack footprint
- XML data response is processed directly by JavaScript
  - Increases the threat of Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) attacks.
- Large number of small modules
  - Every module is potential target for attack, in total representing a larger attack footprint
  - State tracking and validation issues for modules that work with shared parameters.

Ref: Imperva Inc

Mitigating RIA Threats

- Separate data from application code
  - Use separate modules for generating display structures and filling in content.
- Do not directly execute XML data as script
  - Do not use the JavaScript eval method to render XML data.
- Encode all XML data
  - This prevents many types of attacks, from XSS to SQL injection, because dangerous characters like brackets, quotes, and ampersands are interpreted by the browser and the application server as harmless character strings.
- Never use client side code to perform security related tasks.
- Always validate input at the server.
- Always apply access controls and session management at the server.

Collaboration Threats

Current problems exists because sites allow users to

- Contribute malicious HTML
  - Eg scripts and page redirects
- Upload malicious files
  - Worms and viruses.

Mitigating Collaboration Threats

- Encode all data
  - All user-supplied data displayed to other users should always be encoded. Encoding user data ensures that this data is interpreted by the client as plain text, not dangerous scripts.
- Automated user input validation
  - Validate all of the data to prevent script injection, file inclusion, command injection and other attacks. All of the validation should be performed at the server side.
- Prevent malicious users from posting viruses and malware
  - Restrict the types of files that users can upload to known, accepted file formats like GIF images.

Syndication Threats

- Syndicated data like RSS feeds and mashups present multiple threats.
- Malicious content can invoke client side vulnerabilities.
  - Vulnerabilities include buffer overflows and client side execution.
- Local zone attacks
  - Many RSS readers translate RSS feeds to HTML and then store the HTML files on the local disk, users are even more exposed to dangerous exploits.
- Lack of transparency
  - difficult for end users to identify the initial source of data. Data may originate from multiple sources and be proxied, parsed, and aggregated before being displayed in the Web browser. This lack of transparency opens up the door for malicious script injections and other client side attacks.
- Unknown data sources
  - Companies that republish content from external sites can inadvertently spread attacks

Ref: Imperva Inc

Mitigating Syndication Threats

- Sanitise dangerous content
  - Do not distribute unknown scripts, files, and HTML markup
- Select upstream content providers carefully.
  - Evaluate the integrity and the security of external sites before republishing third party data.
- Keep up-to-date (or seek regular expert advice)
  - Know the vulnerabilities associated with the various RSS readers. If a content provider is hacked, then sites that republish the content providers' data must either strip the malicious content or find alternative data sources.

Top Web 2.0 Threats

Web 2.0 is different but still the same ….

1. Insufficient Authentication Controls
2. Cross Site Scripting (XSS)
3. Cross Site Request Forgery (CSRF)
4. Phishing
5. Information Leakage
6. Injection Flaws
7. Information Integrity
8. Insufficient Anti-automation

Secure Enterprise 2.0 Forum 2009

What should you be concerned about?

- Which technologies are acceptable for enterprise use?
- How can organisations best leverage these new technologies to do more business while minimising risk?
- What are the rules for acceptable use of Web 2.0 technologies and how can they be enforced?
- When facing the collaborative nature of Web 2.0 tools and technologies, how can organisations maintain current levels of information security?

Thank You

Thank You

Sense of Security Pty Ltd
Tel: +61 2 9290 4444
info@senseofsecurity.com
www.senseofsecurity.com