Agenda

- Who am I?
- Web 1.0
- Web 2.0
- Privacy vs. Security Principles
- Past web application attacks
- Current attack trends
- Attacks of the future
Who am I?

IBM Watchfire
  ▶ Director, Security Research

Experience
  ▶ Ethical Hacker, Education
  ▶ Penetration Team, Government
  ▶ Security Research, Commercial
The World is Flat (Globalization)

- Globalization 1.0
  - Countries & Nation states

- Globalization 2.0
  - Companies and Organization

- Globalization 3.0
  - Individual

** Concepts by Thomas Friedman
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
  - ???
Web 2.0

- Marketing Term
- Significant paradigm shift
  - User generated & collaborative content
    - Social networks
    - Wikis
    - Blogs
  - Thin client computing
    - Applications on demand
    - Software as a Service
Privacy Management

- Ability of an individual or group to keep their lives and personal affairs out of public view, or to control the flow of information about themselves

- Responsibilities
  - 10 pillars of privacy
  - Policy & compliance definition
Security Management

- Condition of being protected
- Responsibilities
  - 8 principles of security
  - Security policy & management

- Information Security: preservation of confidentiality, integrity and availability
Privacy & Security Overlap

- Confidentiality
- Availability
- Integrity

- Consent
- Identifying Purposes
- Openness
- Accountability
- Individual Access
- Safeguards
- Limiting Use
- Challenging Compliance
- Limiting Collection
- Accuracy

OWASP Day - La Sapienza, 10 September 2007
Who are we against?

- Organized Crime
  - What: Data & Identity Theft
  - Why: $$$

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

- H4ck0rZ
  - What: Defacement & Denial of Service
  - Why: Ego & Credibility building
Hacking the Eras

■ Web 0.9
  ▶ Defacement
  ▶ Denial of Service

■ Web 1.0
  ▶ SQL Injection
  ▶ Command Execution
  ▶ Cookie Poisoning

■ Web 2.0
  ▶ ????
Hacking Web 2.0

■ Common attack types
  ▶ Cross-site scripting (XSS)
  ▶ Cross-site request forgery (XSRF)
  ▶ Browser Flaws

■ Technologies at risk
  ▶ Web Services
  ▶ AJ AX
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)
Web 2.0 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)
Traditional Web Service Attacks

- XML parser Denial of Service
  - DTD named entities
  - DTD parameter entities
  - Attribute blowup
- SOAP array overflow
- XML external entity file disclosure
- SOAP Web Services Injection
Web 2.0 Web Service Attacks

- Social engineering
- Cross-site scripting
- Cache poisoning
- Transport hijacking
- DNS attacks
AJAX (Asynchronous JavaScript & XML)

- Coined by Jesse James Garrett in 2005

**Advantages**
- Bandwidth
- Separation of data, format, and function

**Disadvantages**
- Browser deployment
- Response time awareness
- Search engine optimization
- User choice
- Accessibility & mobility
Fundamental Problems with AJAX

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

- Two Javascript Worms
  - Samy
  - Yamaner

- Remote Browser Hijacking
  - Major US financial firm
And here in Italy ...

- Rosario Velotta
  - Webmail XSS worm
    - Libero.it
    - Tiscali.it
    - Lycos.it
    - Excite.com
  - [http://rosario.valotta.googlepages.com/versioneitaliana](http://rosario.valotta.googlepages.com/versioneitaliana)
Putting it Together

<table>
<thead>
<tr>
<th>Name</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>off</td>
</tr>
<tr>
<td>REMOTE_ADDR</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>REMOTE_HOST</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>HTTP_ACCEPT</td>
<td>image/png;v=0.5</td>
</tr>
<tr>
<td>HTTP_ACCEPT_LANGUAGE</td>
<td>en-us,en;q=0.5</td>
</tr>
<tr>
<td>HTTP_CONNECTION</td>
<td>keep-alive</td>
</tr>
<tr>
<td>HTTP_HOST</td>
<td><a href="http://www.evlite.com">www.evlite.com</a></td>
</tr>
</tbody>
</table>
Thank-you

Questions?