

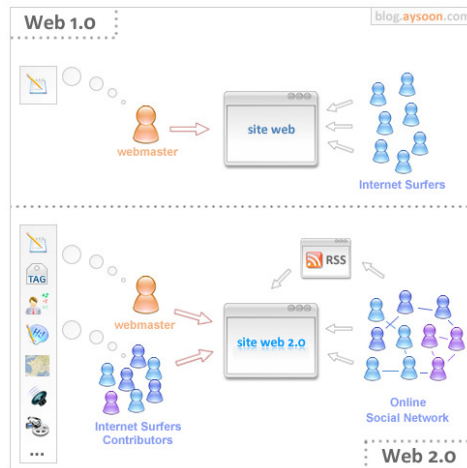
## WEB 2.0

Pericolosità nella nuova frontiera del  
web

### Introduzione al Web 2.0

- Usare la rete in maniera nuova e innovativa
- Condividere informazioni
- Basato su di un concetto «opensource »
- Possibilità di interagire, gestire, integrare contemporaneamente su piu' fonti
- Condividere, Mischiare, Riutilizzare
- Esempi: Facebook, Google Maps, Google Docs, Paypal, Flickr , Likedin

## WEB 1.0 vs WEB 2.0



## Pericolosità del Web 2.0

(fonte IDC 2009 su 1300 IT)

- 95% delle aziende permette l'accesso a siti web 2.0 ritenendoli necessarie per il loro lavoro
  - 71% Wiki
  - 66% Facebook
  - 71% LinkedIn
  - 87% Portali

## Pericolosità del Web 2.0

- **Information Leakage**
  - Utente può pubblicare delle informazioni ritenute sensibili da parte della società;
    - Difficile per il sito arrivare a controllare questo tipo di informazioni;
  - Le informazioni possono essere replicate su tantissimi siti anche inconsapevolmente;

## Pericolosità del Web 2.0

- **Phishing**
  - Utilizzare un sito compromesso per veicolare un finto sito malevolo;
  - Ricezione ed installazione di un widget malevolo via email;

## Pericolosità del Web 2.0

- **Insufficient Anti-Automation**
  - Sfruttando le particolarità del 2.0 si possono automatizzare alcuni attacchi ex: Bruteforcing, CSRF (Cross site request forgery);

## Pericolosità del Web 2.0

- **Information Integrity**
  - Correttezza delle informazioni è uno degli elementi fondamentali, compromettendo alcune informazioni e modificandole si potrebbe creare della disinformazione;

## Pericolosità del Web 2.0

- **Cross Site Request Forgery (CSRF) / Cross Gadget Request Forgery (CGRF)**
  - Visitando un sito malevolo o compromesso è possibile dirottare la vittima verso un sito autorizzato e cambiare o rubare informazioni;

## Pericolosità del Web 2.0

- **Cross Site Scripting (XSS)**
  - Sfruttando una non corretta validazione degli input è possibile far eseguire codice scripting all'utente; ex: rubare identità, visualizzazione di finte informazioni, redirectione verso siti contenenti Web malware;

## Considerazioni

- **Da tener presente che la maggioranza dei siti del Web 2.0 fa parte dei 50 più attivi dispensatori di malware.**
- Attualmente gli strumenti di protezione basati sulle segnalazioni della community sottostante come quelli implementati da YouTube e Blogspot risultano inefficaci nel quasi 80% dei casi

## Futuro?

- Aumentare la sensibilità sul tema
- Coadiuvare gli sforzi necessari a bloccare questi veicoli di ingresso ex:
  - Società che sviluppato CMS / Portali WEB 2.0, sanitizzazione degli input e maggiore attenzione al codice;
  - Browser e strumenti sempre piu' intelligenti che riscono a riconoscere in maniera preventiva il «cattivo » ;