Network Security Forum 2006

Web 2.0 新技術の表と裏
～より便利に、安全に使うには～

二木真明
CISSP

住商情報システム株式会社
情報システム部　部長付
兼 ネットワーク・セキュリティソリューション事業部　担当部長

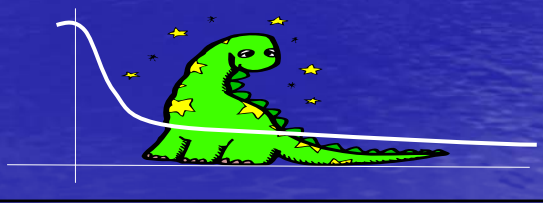
NPO日本ネットワークセキュリティ協会 幹事　技術部会長

2．0って何？？？

- 最近2．0が流行・・・・・
  - バージョンアップされた Webの使い方
  - Webを使った「マーケティング」手法とその技術的なバックアップ
  - ○×△2．0が大流行に
- Web2.0 があるならば・・・・
  - Web “Attack” 2.0 もあるに違いない・・・・

Web2.0の背景

- インターネット（Web）を活用したビジネスの発展
  - ネット商店とコンビニの対比
    - コンビニ（従来型［リアル］マーケティング）
      - 売り場面積の制約、物流コスト＝展示可能な商品の限界
      - 「売れ筋」を中心にした商品構成
      - 客は「売れ筋＋売れ筋候補」から選ぶしかない
      - 扇動的なマーケティング（宣伝）で売れ筋作り（σを最小化する手法）
    - ネット商店（Web2.0的［バーチャル］マーケティング）
      - 展示点数に限りがない。商品検索などが簡単に利用できる。流通さえ効率化できれば、はるかに多種の商品を扱える
      - 「個人の好み」を重視。品揃えの拡充。
      - 客は自分の好みで商品を買える。たとえ、それが特殊な好みであったとしても。
      - 実は、人の好みは千差万別。（σを最小化せず、さらに nσをカバー）
      - Long tail 現象



Web（ネット）の使い勝手の向上

- 検索技術の進化
  - 困ったら ○×△様にお伺い・・・「ぐ■る」・・・・
- Blogの発達、情報のシンディケーション
  - リンクとトラックバックによる双方向的情報連結
  - RSSによるサマリ・更新情報の提供
- Webクライアントの性能向上
  - Ajax など、Webベースの Rich Client化技術による操作性の向上
  - Web Service, SOA による分散アーキテクチャと多様なサービス連携、アプリケーションのポータル化

Web 2.0 注目技術

- RSS
  - Rich Site Summary / RDF Site Summary (0.9 – 1.0)
  - Really Simple Syndication (2.0)
  - MS IE7 で RSSリーダをブラウザに組み込み
- Ajax （Asynchronous Java script and XML）
  - Java Script によるバックグラウンドでのサーバとの通信（XMLデータ交換）と、再読込なしの動的表示更新
  - Google Map での利用は有名

なんだか・・
Web2. 0ってすごい！！！！

・・・・・・のか？？？？

そろそろ「裏」の話を・・・・

- 新しい「ネット技術」を使う側の問題
  - スピードが勝負の世界・・・・多くの場合「安全」は後から・・・・（むしろ、リスクを取ってでもビジネスを優先・・・・）
  - インターネットで使うのが前提・・・だから、「悪い人」でも使えてしまう・・・・（それも世界中から）
  - 流行の技術・・・・・「お子様」の遊び道具に・・・
    - ラボの中だけならばいいのだけれど、技術的に成熟する前に「使ってしまう」・・・・・・
    - 「お子様的」Web技術者ほど恐いものはない・・・
    - 攻める側は「プロ」だぜ！！

Long Tail on Web “Attack” 2.0

- 大量ウイルス攻撃、Web改竄などの派手なアピールはもう古い
- みんなそれぞれ自分なりのターゲットを絞って、コツコツやろうぜ
  - 攻撃目的、手段・手法、対象の多様化・・・
  - やっぱ、お金は儲けなきゃね （具体的な目的）

そして狙われる Web 2.0技術

- たとえば・・・・
  - RSS リーダーのクロスサイトスクリプティング（XSS）脆弱性
  - 利用者が気付かないAjax のバックグラウンドサービスへの攻撃・悪用

RSSリーダーが脆弱性を持ったら

- 不正に加工したフィードを読み込ませる
  - SPAM的にメールでフィード情報を配信
    - （フィッシング手法でユーザのリーダーに登録させる。たとえば〇△銀行オンラインサービスからのお知らせ・・・・お得な投資信託情報をリアルタイムに更新・・・とか）
  - フィードに不正なスクリプトを混入
    - キーロガーなどをダウンロードさせる・・・
    - 個人情報を送信させる・・・・
    - いろいろ出来そう・・・

RSS リーダーは簡単に作れる

- Perl XML::RSS モジュール
  - Web組込型 RSSリーダーを作るには最適
- しかし・・・・内容のチェックは自分でしなきゃいけない
- ・・・・・・・・ちょっとデモしてみましょう
- よい子はマネをしないでね！・・・・

＊このデモはあくまで「コンセプト」についてのデモであり、意図的に脆弱性を組み込んだ試験環境で行っています。

Ajax：見えないところで何が・・・・

- Asynchronous JavaScript
  - つまり Web ページ自身とは非同期に、JAVA Scriptとサーバ間で通信を行い、ページ全体の再読込なしに表示を更新できる
- 危険を生じる要素
  - ユーザの見えないところで通信が行われ、その結果がブラウザで「勝手に」処理される
  - 表に見えない処理は軽視されがち！？
    - もしかして、認証・・・忘れてませんよねぇ・・・・。
    - 一応、Cookieは見てるみたいですが・・・・
  - 一般の処理と同様に脆弱性が入り込む余地あり
    - XSS，＊＊＊インジェクション、・・・・・
  - インターフェイスコード（JavaScript）がまる見え・・・

ちょっとしたデモ・・・

- Ajaxを使ったデモサイトの例
- Ajaxリクエストへの直接の SQL Injection
- くどいかもしれませんが・・・・
- よい子はマネをしないでね！！・・・・

＊このデモはあくまで「コンセプト」についてのデモであり、意図的に脆弱性を組み込んだ試験環境で行っています。

Web “Attack” 2.0 シナリオ例

- たとえば不正なフィードを読ませる方法
  - SPAMまたは特定の利用者を狙ってメールで配布
  - 匿名掲示板などに掲載
  - BlogのRSS作成機構にXSS脆弱性を内包する場合、不正な加工を記事に施して、間接的にRSSへタグを埋め込むことも可
- 偽フィードは気づかれにくい
  - リンク先は本物のサイト。単に不正なスクリプトを付加しているだけ。
- 脆弱なリーダーの利用者以外にスクリプト混入を気付かせない方法も・・・
  - たとえば・・・・

Web “Attack” 2.0 シナリオ例

- XSS脆弱性とAjaxアプリ脆弱性の組み合わせ
  - XSSを利用して読ませたスクリプトで、Ajaxのサーバサイドサービスを叩く･･･とか
  - XSRF 攻撃の可能性も
    - SNSなどへの不正リンク書き込み･･･SNSワーム･･･
      - MySpace.com への攻撃(2005/10)

イントラアプリは安全か！？

- 内情を知っていれば、外部からの攻撃は可能
  - ある社員は常時、社内ポータルを開きっぱなし･･
  - ある社員はよくウイルス付きメールを開いてる･･
  - この会社のイントラは Web2.0仕様
  - 実は先月まで私はその会社にいた････
  - ･･･さて、あなたが攻撃者なら何を考えますか？

参考： http://www.blackhat.com/presentations/bh-jp-06/BH-JP-06-Grossman.pdf

まとめてみると・・・・・

Web2.0「技術」は新しくない・・・・

- Ajax
  - つまりは JavaScriptがクライアント側で動くという話
  - サーバサイドの処理は、いわゆるWebアプリと同じ
- RSS
  - いわば、サイトの要約を標準的な書式（XML）で表現しただけ
  - 最終的には、相手サイトへのWebアクセスにつながる
  - 動的更新の要約ページと考え方は同じ・・・・

Web2.0への「攻撃」も新しくない

- クロスサイトスクリプティング（XSS）
- クロスサイトリクエストフォージェリー（XSRF）
- インジェクション系攻撃
  - SQLインジェクション
  - コマンドインジェクション
  - ・・・・
- 主な手法は基本的に Web 1.0 とかわらない

ならば・・・・

- 正しいプログラマーは何をすべきか
  - セキュアなプログラミングを心がけよう
    - 参考資料：IPAセキュリティセンタ
    - http://www.ipa.go.jp/security/awareness/vendor/software.html
- 正しい運用者は何をすべきか
  - アプリケーション運用開始前の脆弱性検査を
  - 日常的なアクセス状況の管理、監視を
  - 必要ならば、補完的な防御策の検討を
    - Web/XML アプリケーションファイアウォールの利用など
    - RSS 提供にSSL＋サイト証明書を利用する。（ユーザへ確認手段を提供することでのRSSフィード詐称の撲滅）
- **基本に忠実にやること**
  - 参考資料：JNSA Web アプリケーションセキュリティWG 2005年度
    - http://www.jnsa.org/result/index.html

ひとつの問題提起

- たとえば違う視点から・・・
  - 最近、上場企業の広報部門へホームページ上のIR情報に対してマスメディアからRSSフィードの提供要請が増えている。
  - RSSフィードを詐称されることは、企業情報開示の完全性へのリスクとなりうるかもしれない。
  - フィッシング対策同様に、RSS詐称を防ぐための対策も必要になるのではないだろうか。

とはいえ・・・

- Web, インターネット利用方法の進化はビジネスの大きな変化＝ビジネスチャンスを生み出すことは間違いない。
- 新しい技術は、そのリスクを正しく見極め、対処しながら、積極的に有効利用することが必要。
- セキュアな開発環境、製品の登場に期待！
  - セキュアであること＝商用製品の最大の「売り」であってほしい・・・

ご清聴ありがとうございました。

- 参考文献
  - 入門 Ajax：高橋登史朗著　Softbank Creative刊
  - 詳解 RSS：水野貴明著　ディー・アート刊
  - 図解Web 2.0 book：小川浩／後藤康成著
    インプレス刊
  - Feed Injection In Web 2.0:　Robert Auger
  - Ajax Security Dangers: Billy Hoffman
    SPI Dynamics　/ SPI Labs
    http://www.spidynamics.com/spilabs/education/whitepapers.html

Special Thanks to:　Kurt Roemer as Author of BadStore.net