# Web 2.0 Attacks Revealed

Kiran Maraju, CISSP, CEH, ITIL, ISO27001, SCJP

Email: Kiran_maraju@yahoo.com

## Abstract

This paper details various security concerns and risks associated with web 2.0 technologies such as Asynchronous Java script and XML (AJAX), Syndication, aggregation and notification of data in RSS or Atom feeds, mashups created by merging content from different sources. This paper also describes the security implications leading with the usage of web 2.0 technologies such as AJAX, RSS, and Mashups. Increase in application functionality leading to the emerging new web technologies (web 2.0). These new web technologies open more avenues to security threats to the online applications and users. Efficient protection mechanisms should be considered when dealing with web 2.0 technologies usage.

## Introduction

Now a days, web application security getting more prominent attention. This attention comes with the increase in the number of vulnerabilities in web applications due to the lack of proper security standards used in the development of the application.

- Cert/CC Statistics shows that 7120 Software Vulnerabilities were Reported in 2006
- 194 SQL Injection Vulnerabilities were found on BugTraq between 2005-jan and 2005-June
- Symantec highlights in its most recent Internet Security Threat Report that Web vulnerabilities constituted 69 percent of 2,249 new vulnerabilities identified for the first half of 2006, with 78 percent of "easily exploitable" vulnerabilities residing within Web applications.
- Directory Traversal is the 2nd most common attack on the internet as of the 2nd half of 2005
- Roughly 63% of the Web application vulnerabilities can be accounted for by 4 vulnerability classes: file inclusion, SQL injection, cross-site scripting, and directory traversal.

Regulations such as PCI, HIPAA,SOX etc and need for the protecting from the financial loss and reputation loss for organizations leads to surge in applications security.

Web 2.0 technologies provide collaborative, decentralized networking for online activities. It involves content participation from end users or consumers enhancements. Web 2.0 technologies involve active participation from users in terms of content contributions and content edition rather than users plays the roles of consumers in Web 1.0. Active user involvement contains activities such as Blogs, sharing information using syndications with the help of RSS/ Atom etc. Growth of technologies and user interaction increases the negative side of the online business in terms of malicious activities which affect the confidentiality, integrity and availability of information assets. These affect can lead to the unauthorized disclosure of sensitive data like SSN numbers, credit card details etc. which can lead to online business providers financial, and reputation loss.

## Asynchronous Java script and XML (AJAX) Attacks

Web 2.0 technologies typically use AJAX for implementing end user interface. AJAX uses java script scripting language for creating dynamic pages. AJAX technology uses XMLHttpRequest (XHR) object that is available from scripting language function calls that extract data from the server and loaded on the client browser without the intervention explicit call from client to server. The data is fetched and transmitted to the client browser and displayed in the form of dynamic page or in XML format automatically which is invisible to end user's knowledge ( i.e. user need not explicitly click submit button on the HTML page to fetch the data from the server). This enhances web page's interaction and speed.

Typical Ajax interaction between client and server

- A client event occurs like key/mouse events (onMouseOver/Out/ Down/Up, onKeyDown/KeyPress) etc.
- An XMLHttpRequest Object is created by the browser using Java Script function call
- The XMLHTTPRequest Object makes a call as illustrated in the following snapshot

```
var object1;
var http_request = new XMLHttpRequest();
http_request.open( "GET", url, true );
http_request.onreadystatechange = function () {
   if ( http_request.readyState == 4 ) {
      if ( http_request.status == 200 ) {
         object1 = eval( "(" + http_request.responseText + ")" );
      } else {
         alert( "Problem with the URL." );
      }
      http_request = null;
   }
}
```

- The Request is processes by the server returns an XML document containing the result
- The XMLHttpRequest Object calls the callback() function and process the result and updates the HTML DOM page as illustrated in the following snapshots

```
function callback() {
   if (req.readyState == 4) {
      if (req.status == 200) {
         // update the HTML DOM page
      }
   }
}
```

```
<script>
function setMessage(message) {
   var div1 = document.getElementById("userIdMessage");
   if (message == "invalid") {
      div1.innerHTML = "<div style=\"color:red\">Invalid User Id</ div>";
   } else {
      div1.innerHTML = "<div style=\"color:blue\">Valid User Id</ div>";
   }
}
</script>
<body>
<div id="userIdMessage"></div>
</body>
```

Cross site scripting (XSS) has been mostly growing prevalence issue of Ajax resulting in major attacks such as the Samy(infected MySpace), Yamanner(infected Yahoo email system) worms that hit the web space recent years. XSS is now becoming a client-side programming issue rather than server side programming issue with the use of Web 2.0.

Cross-site scripting (XSS) attacks occur when malicious user sends a malicious script as input to the web application to attack a different end user. The victim’s browser will have no knowledge that the script should not be trusted, and will execute the script. The malicious script can access cookies, session tokens, or other sensitive information fetched from the browser and possibility of Cookie theft, session hijacking attacks.

AJAX allows the inserting dynamically HTML pieces into the Web page at run-time. Attackers can make use of the vulnerable HTML attributes of the application and insert malicious script in the application.

The innerHTML attribute allows Java Script can be inserted as HTML fragment. Attackers can insert the malicious script as input to the innerHTML, as part of HTML fragment and browser will execute the malicious script.

The eval() function accepts a string as an argument and evaluates it as a Java Script code. Attackers can insert the malicious script in vulnerable function eval() and browser will execute the malicious script.

The following code illustrates the application page accepts user input and dynamically generates the HTML page. Malicious user can make use of this and be able to insert malicious script which will be executed and the sensitive details like cookies, session tokens can be stolen from the victim's browser.

```
<HTML>
<script type="text/javascript">
function changeText2(){
          var userInput = document.getElementById('userInput').value;
        document.getElementById('boldStuff2').innerHTML = userInput;
}
</script>
<p>Welcome to the site <div id='boldStuff2'></div> Dynamic Html </p>
<input type='text' id='userInput' value='Enter' />
<input type='button' onclick='changeText2()' value='Display'/>
</HTML>
```

## AJAX protection mechanisms

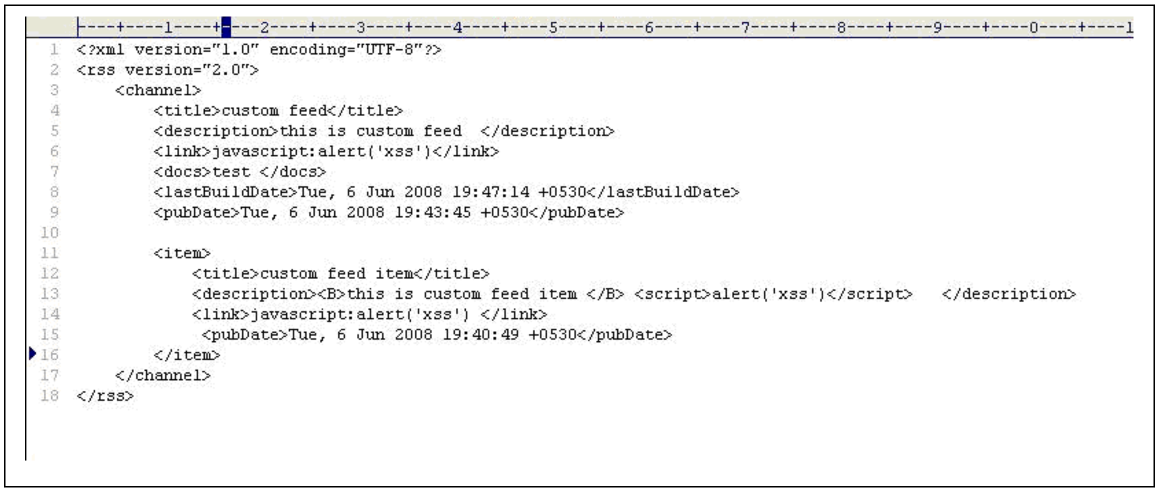
AJAX protection mechanisms are similar to typical web application protection measures like Validate all input that processed by the application both client and server level. Validate input for HTTP headers, cookies, URL parameters, POST data, and query string transmitted to server. Strict Verification checks should be performed for user input data type, length and format. Always use parameterized queries when interacting with database. Implement HTML encoded output for all the responses generated by the server.

Use the attribute “innerText” rather than “innerHtml”. A new function, parseJSON(), has been proposed as a safer alternative to eval, as it is specifically intended to process JSON data and not Java Script.

## Real Simple Syndication (RSS), ATOM

RSS, ATOM are the aggregations used to aggregate the content from multiple sources and provide the summary of full text of data in one place.
RSS feeds are used exchange information between web sites. They also used exchange details of published content like blogs, news etc.
RSS content can be read using RSS reader/feed reader/aggregator.
End user subscribes to a feed of his interest by bookmaking the feed's link into the reader that initiates the feed subscription.
The reader automatically checks the user's subscribed feeds for any latest content and downloads it to the client desktop/browser.
There are many feed aggregators exists for web based such as Bloglines, fastladder, google reader etc. and desktop based feed aggregators like feed reader, attensa, mindity etc.
It is possible to inject malicious scripts in the RSS feeds such that the feed readers can read the malicious scripts and the scripts can be executed on the feed readers that are web based or desktop based.

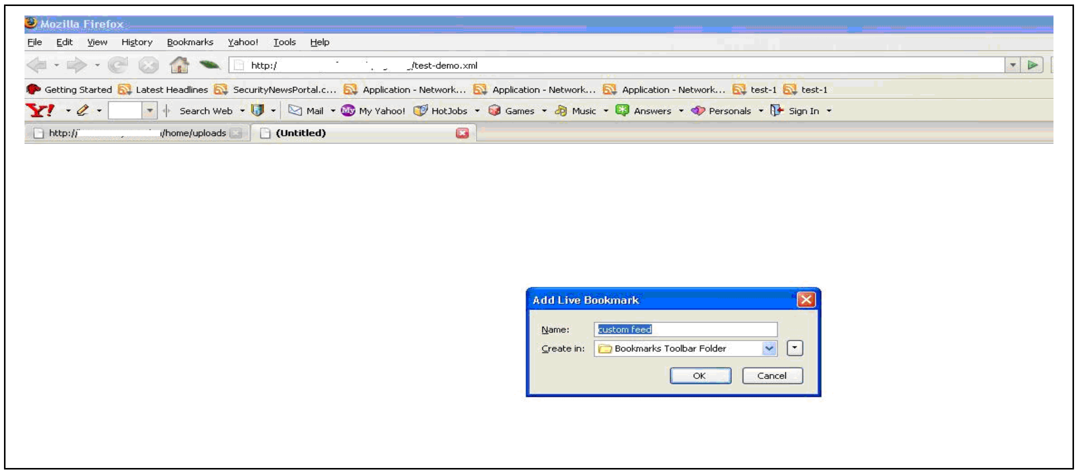
The following Attack scenario shows the Feed injection attack. Created a custom feed with malicious script included in the feed “link”, “description” tags of RSS format



```
<?xml version="1.0" encoding="UTF-8"?>
<rss version="2.0">
    <channel>
        <title>custom feed</title>
        <description>this is custom feed  </description>
        <link>javascript:alert('xss')</link>
        <docs>test </docs>
        <lastBuildDate>Tue, 6 Jun 2008 19:47:14 +0530</lastBuildDate>
        <pubDate>Tue, 6 Jun 2008 19:43:45 +0530</pubDate>

        <item>
            <title>custom feed item</title>
            <description><B>this is custom feed item </B> <script>alert('xss')</script>   </description>
            <link>javascript:alert('xss') </link>
             <pubDate>Tue, 6 Jun 2008 19:40:49 +0530</pubDate>
        </item>
    </channel>
</rss>
```

The following snapshot shows that the custom feed is added as a bookmark for the browser. So that new updates available from this custom feed will be updated by the feed reader


Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
Getting Started Latest Headlines SecurityNewsPortal.c... Application - Network... Application - Network... Application - Network... test-1 test-1
Search Web Mail My Yahoo! HotJobs Games Music Answers Personals Sign In
(Untitled)
OK Cancel

http:/ /test-demo.xml

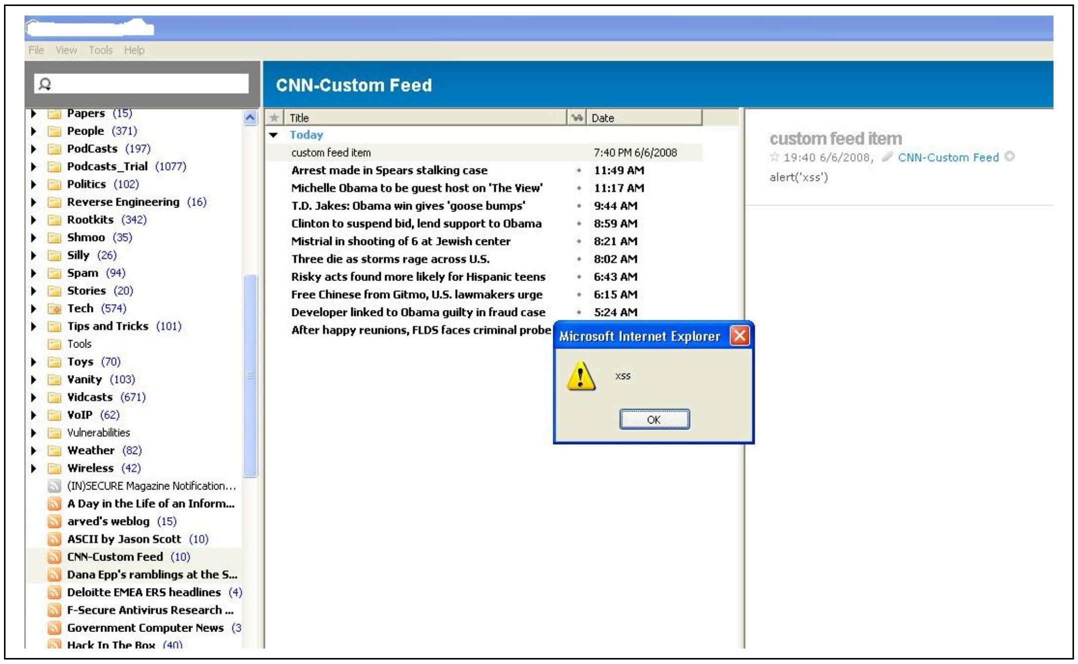
http:/ /home/uploads

Add Live Bookmark

Name: custom feed

Create in: Bookmarks Toolbar Folder

Vulnerable feed readers simply accepts the malicious feed input and execute the malicious scripts that leads to cookie, session token stealing



CNN-Custom Feed

```
Papers (15)
People (371)
PodCasts (197)
Podcasts_Trial (1077)
Politics (102)
Reverse Engineering (16)
Rootkits (342)
Shmoo (35)
Silly (26)
Spam (94)
Stories (20)
Tech (574)
Tips and Tricks (101)
Tools
Toys (70)
Vanity (103)
Vidcasts (671)
VoIP (62)
Vulnerabilities
Weather (82)
Wireless (42)
(IN)SECURE Magazine Notification...
A Day in the Life of an Inform...
arved's weblog (15)
ASCII by Jason Scott (10)
CNN-Custom Feed (10)
Dana Epp's ramblings at the S...
Deloitte EMEA ERS headlines (4)
F-Secure Antivirus Research ...
Government Computer News (3
Hack In The Box (40)
```

| Title | Date |
|---|---|
| custom feed item | 7:40 PM 6/6/2008 |
| Arrest made in Spears stalking case | 11:49 AM |
| Michelle Obama to be guest host on 'The View' | 11:17 AM |
| T.D. Jakes: Obama win gives 'goose bumps' | 9:44 AM |
| Clinton to suspend bid, lend support to Obama | 8:59 AM |
| Mistrial in shooting of 6 at Jewish center | 8:21 AM |
| Three die as storms rage across U.S. | 8:02 AM |
| Risky acts found more likely for Hispanic teens | 6:43 AM |
| Free Chinese from Gitmo, U.S. lawmakers urge | 6:15 AM |
| Developer linked to Obama guilty in fraud case | 5:24 AM |
| After happy reunions, FLDS faces criminal probe | |

custom feed item
19:40 6/6/2008, CNN-Custom Feed
alert('xss')

Microsoft Internet Explorer

xss

**Feed Injection protection mechanisms**

Though some feed readers are performing encoding of the feed input but still there are various ways to evade the prevention methods. End user should be able to discern between the genuine and malicious feeds before subscribe to them.

## Mashup

A mashup is a process of combining content from various sources (data sources) and represent in single page. The data sources can be web sites (flickr, google maps, yahoo local search etc.), web pages from any web sites, web services that expose the services to the external world, programs output, organizations internal data etc. The mashups will conglomerate the various data sources and parse them and provide a single output source that can be consumed in the form of online web applications, feeds etc.

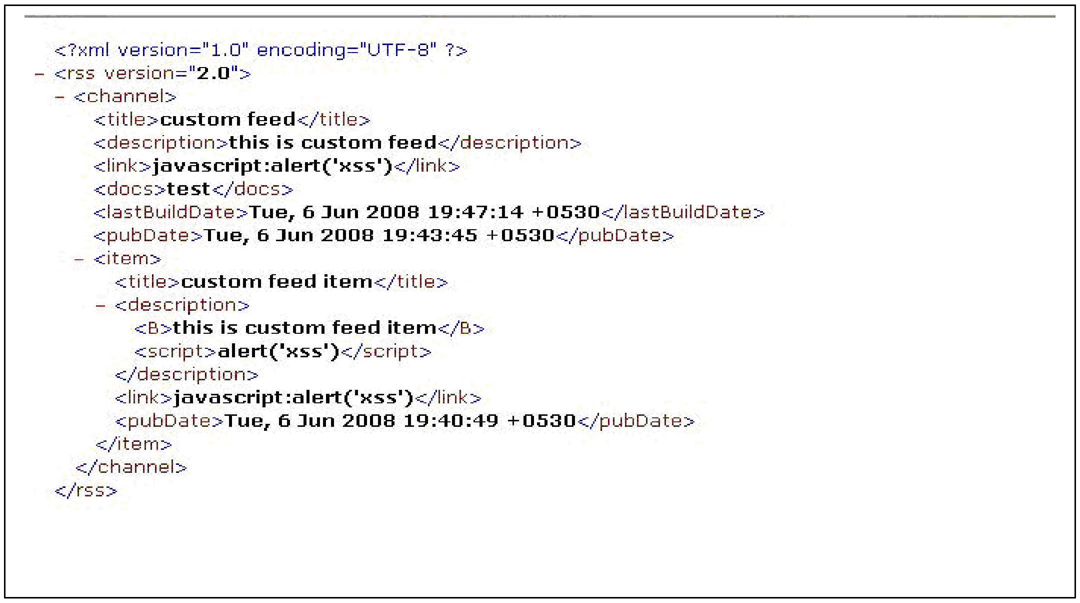
Mashups are widely used for using already existing data sources and providing a solution to the customers. There are widely used mashup services available online for example http://housingmaps.com integrated criaglist and google maps data and provide online to find a place to buy or rent in your area. Mashups are used in different from such as consumer mashups, data mashups, and business mashups.

As there is no control of data originated from the various sources these mashups provides new avenues for security threats. There is a possibility of injecting malicious scripts in one source and mix it with a genuine data source and provide a final malicious data source that can be consumed by the end users.

There are several mashup editors available.

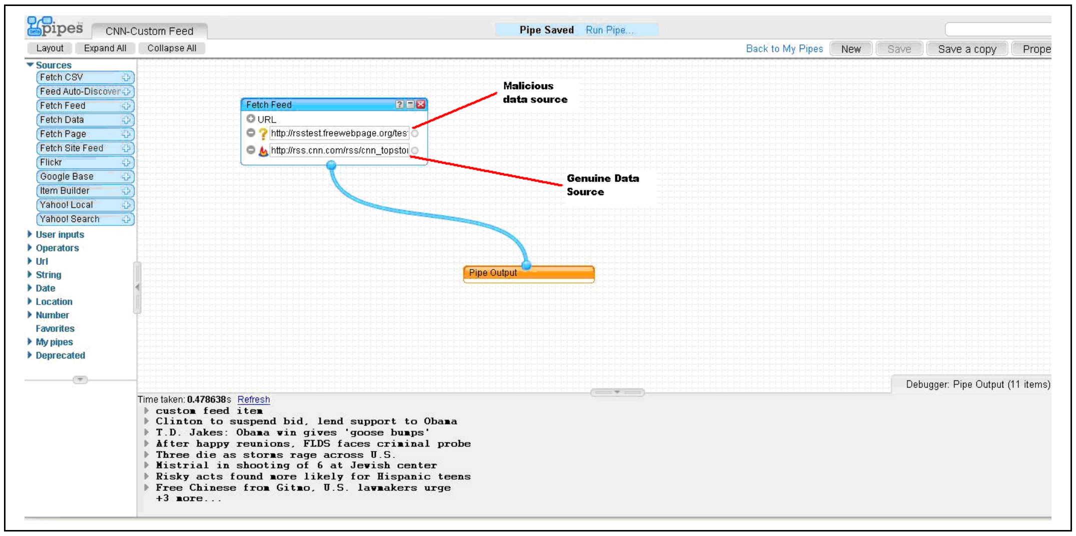
- Yahoo pipes
- Microsoft Popfly
- Intel Mash Maker
- Google Mashup Editor
- IBM QEDWiki
- Dapper
- Teqlo
- Proto
- Datamashups
- Openkapow
- LiquidApps
- Serena Mashup Composer

The following snapshot shows vulnerable script of the malicious feed



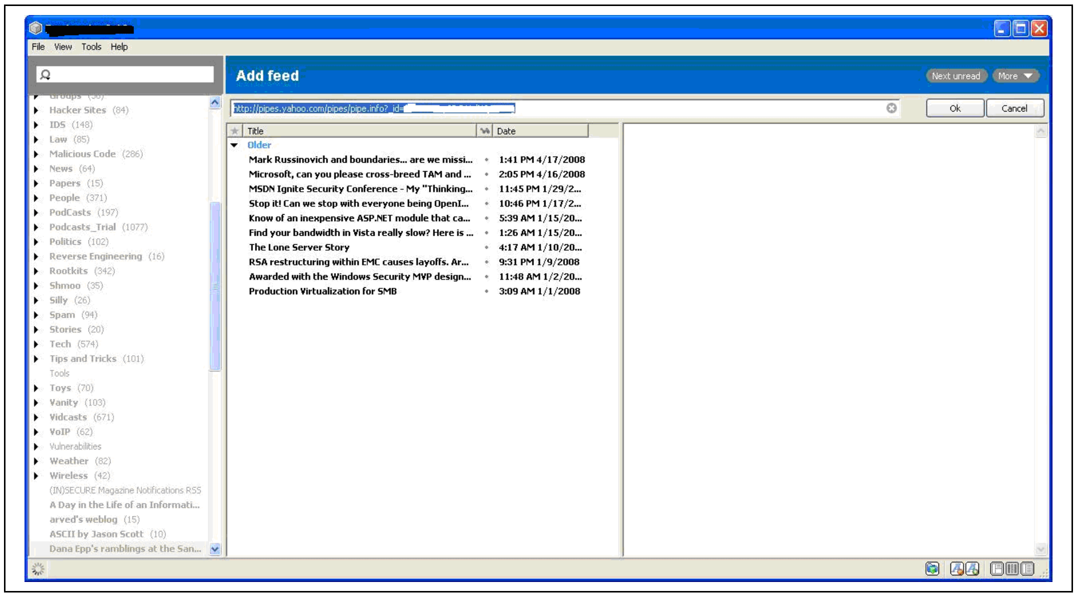
```
  <?xml version="1.0" encoding="UTF-8" ?>
- <rss version="2.0">
  - <channel>
      <title>custom feed</title>
      <description>this is custom feed</description>
      <link>javascript:alert('xss')</link>
      <docs>test</docs>
      <lastBuildDate>Tue, 6 Jun 2008 19:47:14 +0530</lastBuildDate>
      <pubDate>Tue, 6 Jun 2008 19:43:45 +0530</pubDate>
    - <item>
        <title>custom feed item</title>
      - <description>
          <B>this is custom feed item</B>
          <script>alert('xss')</script>
        </description>
        <link>javascript:alert('xss')</link>
        <pubDate>Tue, 6 Jun 2008 19:40:49 +0530</pubDate>
      </item>
    </channel>
  </rss>
```

Using mashup editors, in this case used "yahoo pipes" to create a "CNN-custom feed" mashup from malicious feed and genuine CNN feed as depicted in the following snapshot



```
Time taken: 0.478638s  Refresh
 custom feed item
 Clinton to suspend bid, lend support to Obama
 T.D. Jakes: Obama win gives 'goose bumps'
 After happy reunions, FLDS faces criminal probe
 Three die as storms rage across U.S.
 Mistrial in shooting of 6 at Jewish center
 Risky acts found more likely for Hispanic teens
 Free Chinese from Gitmo, U.S. lawmakers urge
 +3 more...
```

The following snapshot shows victim subscribes to this malicious custom feed "CNN-custom feed" in the feed aggregator client



[redacted]

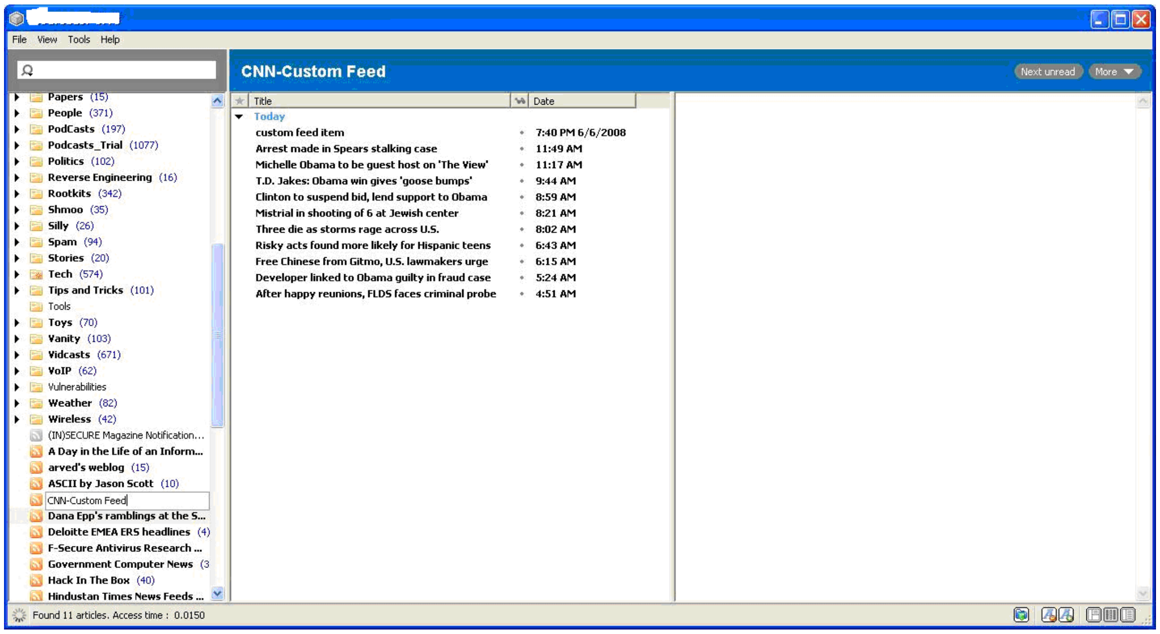
**Add feed**

http://pipes.yahoo.com/pipes/pipe.info?_id=[redacted]

Groups (30)
Hacker Sites (84)
IDS (148)
Law (85)
Malicious Code (286)
News (64)
Papers (15)
People (371)
PodCasts (197)
Podcasts_Trial (1077)
Politics (102)
Reverse Engineering (16)
Rootkits (342)
Shmoo (35)
Silly (26)
Spam (94)
Stories (20)
Tech (574)
Tips and Tricks (101)
Tools
Toys (70)
Vanity (103)
Vidcasts (671)
VoIP (62)
Vulnerabilities
Weather (82)
Wireless (42)
(IN)SECURE Magazine Notifications RSS
A Day in the Life of an Informati...
arved's weblog (15)
ASCII by Jason Scott (10)
Dana Epp's ramblings at the San...

| Title | Date |
|---|---|
| Older | |
| Mark Russinovich and boundaries... are we missi... | 1:41 PM 4/17/2008 |
| Microsoft, can you please cross-breed TAM and ... | 2:05 PM 4/16/2008 |
| MSDN Ignite Security Conference - My "Thinking... | 11:45 PM 1/29/2... |
| Stop it! Can we stop with everyone being OpenI... | 10:46 PM 1/17/2... |
| Know of an inexpensive ASP.NET module that ca... | 5:39 AM 1/15/20... |
| Find your bandwidth in Vista really slow? Here is ... | 1:26 AM 1/15/20... |
| The Lone Server Story | 4:17 AM 1/10/20... |
| RSA restructuring within EMC causes layoffs. Ar... | 9:31 PM 1/9/2008 |
| Awarded with the Windows Security MVP design... | 11:48 AM 1/2/20... |
| Production Virtualization for SMB | 3:09 AM 1/1/2008 |

The following snapshot illustrates the vulnerable feed aggregator fetches the data from the malicious mashup”CNN-Custom feed”



[redacted]

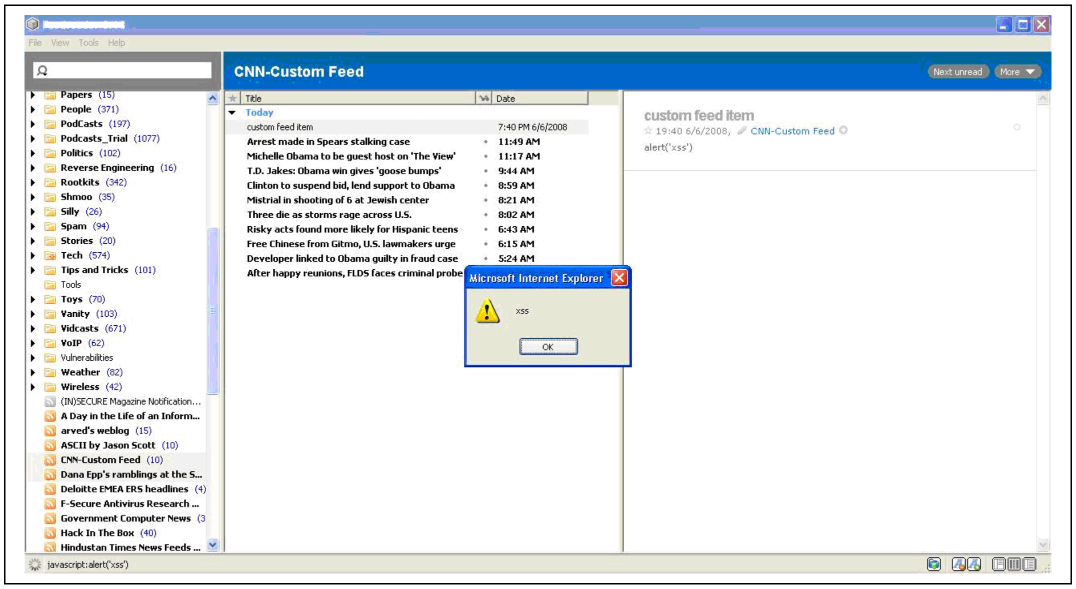
**CNN-Custom Feed**

Papers (15)
People (371)
PodCasts (197)
Podcasts_Trial (1077)
Politics (102)
Reverse Engineering (16)
Rootkits (342)
Shmoo (35)
Silly (26)
Spam (94)
Stories (20)
Tech (574)
Tips and Tricks (101)
Tools
Toys (70)
Vanity (103)
Vidcasts (671)
VoIP (62)
Vulnerabilities
Weather (82)
Wireless (42)
(IN)SECURE Magazine Notification...
A Day in the Life of an Inform...
arved's weblog (15)
ASCII by Jason Scott (10)
CNN-Custom Feed
Dana Epp's ramblings at the S...
Deloitte EMEA ERS headlines (4)
F-Secure Antivirus Research ...
Government Computer News (3
Hack In The Box (40)
Hindustan Times News Feeds ...

| Title | Date |
|---|---|
| Today | |
| custom feed item | 7:40 PM 6/6/2008 |
| Arrest made in Spears stalking case | 11:49 AM |
| Michelle Obama to be guest host on 'The View' | 11:17 AM |
| T.D. Jakes: Obama win gives 'goose bumps' | 9:44 AM |
| Clinton to suspend bid, lend support to Obama | 8:59 AM |
| Mistrial in shooting of 6 at Jewish center | 8:21 AM |
| Three die as storms rage across U.S. | 8:02 AM |
| Risky acts found more likely for Hispanic teens | 6:43 AM |
| Free Chinese from Gitmo, U.S. lawmakers urge | 6:15 AM |
| Developer linked to Obama guilty in fraud case | 5:24 AM |
| After happy reunions, FLDS faces criminal probe | 4:51 AM |

Found 11 articles. Access time : 0.0150

The vulnerable injected script gets executed on the feed aggregator client leads to cross site scripting vulnerability that can be used to cookie, session tokens stealing as shown in the following snapshot



[redacted]

**CNN-Custom Feed**

Papers (15)
People (371)
PodCasts (197)
Podcasts_Trial (1077)
Politics (102)
Reverse Engineering (16)
Rootkits (342)
Shmoo (35)
Silly (26)
Spam (94)
Stories (20)
Tech (574)
Tips and Tricks (101)
Tools
Toys (70)
Vanity (103)
Vidcasts (671)
VoIP (62)
Vulnerabilities
Weather (82)
Wireless (42)
(IN)SECURE Magazine Notification...
A Day in the Life of an Inform...
arved's weblog (15)
ASCII by Jason Scott (10)
CNN-Custom Feed (10)
Dana Epp's ramblings at the S...
Deloitte EMEA ERS headlines (4)
F-Secure Antivirus Research ...
Government Computer News (3
Hack In The Box (40)
Hindustan Times News Feeds ...

| Title | Date |
|---|---|
| Today | |
| custom feed item | 7:40 PM 6/6/2008 |
| Arrest made in Spears stalking case | 11:49 AM |
| Michelle Obama to be guest host on 'The View' | 11:17 AM |
| T.D. Jakes: Obama win gives 'goose bumps' | 9:44 AM |
| Clinton to suspend bid, lend support to Obama | 8:59 AM |
| Mistrial in shooting of 6 at Jewish center | 8:21 AM |
| Three die as storms rage across U.S. | 8:02 AM |
| Risky acts found more likely for Hispanic teens | 6:43 AM |
| Free Chinese from Gitmo, U.S. lawmakers urge | 6:15 AM |
| Developer linked to Obama guilty in fraud case | 5:24 AM |
| After happy reunions, FLDS faces criminal probe | |

custom feed item
19:40 6/6/2008, CNN-Custom Feed
alert('xss')

Microsoft Internet Explorer
xss

```
javascript:alert('xss')
```

## Mashup protection mechanisms

Proper input sanitization should be performed when creating or consuming the mashups and control of data should be performed by the verification of origin policy of various data sources. End users should be aware of the implications leading to subscribing/consuming data from the untrusted data sources.

## References

- http://java.sun.com/developer/technicalArticles/J2EE/AJAX/
- http://www.owasp.org
- http://mashable.com/2007/07/08/mashups/
- http://www.programmableweb.com/