

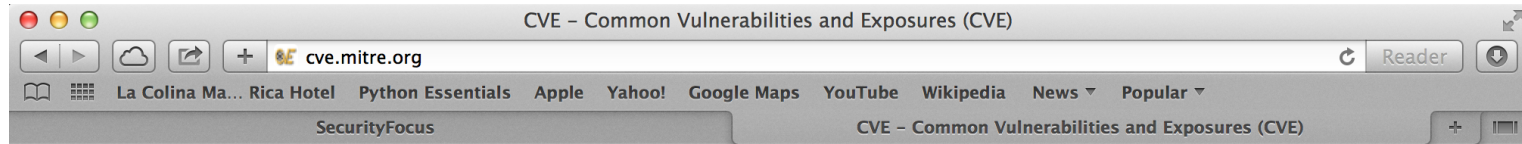
Vulnerability Monitoring

Managing Patch Updates

Motivation

- Vulnerabilities in systems are pervasive
- Many exploits can be patched but are not
- Data available but not easily aggregated
- Project overlaps with a variety of Computer Science subject areas

Mitre CVE Databank



[CVE LIST](#)

[COMPATIBILITY](#)

[NEWS — FEBRUARY 21, 2014](#)

[SEARCH](#)

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

New CVE-ID Format as of January 1, 2014 — [learn more](#)

TOTAL CVEs: 59946

About CVE

[Terminology](#)
[Documents](#)
[FAQs](#)

CVE List

[CVE-ID Syntax Change](#)
[About CVE Identifiers](#)
[Search CVE](#)
[Search NVD](#)
[Updates & RSS Feeds](#)
[Request a CVE-ID](#)

CVE In Use

[CVE-Compatible Products](#)
[NVD for CVE Fix Information](#)
[CVE Numbering Authorities](#)

News & Events

[Calendar](#)
[Free Newsletter](#)

Community

[CVE Editorial Board](#)
[Sponsor](#)
[Contact Us](#)

Search the Site

CVE® International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures.

CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

Widespread Use of CVE

- ▲ [Vulnerability Management](#)
- ▲ [Patch Management](#)
- ▲ [Vulnerability Alerting](#)
- ▲ [Intrusion Detection](#)
- ▲ [Security Content Automation Protocol \(SCAP\)](#)
- ▲ [NVD \(National Vulnerability Database\)](#)
- ▲ [US-CERT Bulletins](#)
- ▲ [CVE Numbering Authorities \(CNAs\)](#)
- ▲ [Recommendation ITU-T X.1520 Common Vulnerabilities and Exposures \(CVE\), ITU-T CYBEX Series](#)

Focus On

CVE Now Available in CVRF Format

The [CVE List](#) is now publishing CVE content using the [Common Vulnerability Reporting Framework \(CVRF\)](#). Developed by the Industry Consortium for Advancement of Security on the Internet (ICAST), CVRF is an XML-based standard that enables software vulnerability

Latest News

[Technical Guidance for Handling the New CVE-ID Syntax Now Available](#)
[ViewTrust Technology Makes Declaration of CVE Compatibility](#)
[New CVE-ID Format in Effect as of January 1, 2014](#)
[Hillstone Networks Makes Declaration of CVE Compatibility](#)
[1 Product from Beijing Topsec Now Registered as Officially "CVE-Compatible"](#)
[CVE Adopts Common Vulnerability Reporting Framework \(CVRF\) Standard](#)
[3 Products from 2 Organizations Now Registered as Officially "CVE-Compatible"](#)
[ADTsys Software Makes Declaration of CVE Compatibility](#)
[CVE Data Sources](#)

Mitre – Early Vulnerability

CVE – CVE (version 20061101) and Candidates as of 20140220

SecurityFocus

TOTAL CVEs: 59946

CVE (VERSION 20061101) AND CANDIDATES AS OF 20140220

CVE (version 20061101) and Candidates as of 20140220

Candidates must be reviewed and accepted by the CVE Editorial Board before they can be added to the official CVE list. Therefore, these candidate

Name: CVE-1999-0001

Description:
ip_input.c in BSD-derived TCP/IP implementations allows remote attackers to cause a denial of service (crash or hang) via crafted packets.

Status: Candidate

Phase: Modified (20051217)

Reference: CERT:CA-98-13-tcp-denial-of-service

Reference: BUGTRAQ:19981223 Re: CERT Advisory CA-98.13 - TCP/IP Denial of Service

Reference: CONFIRM:http://www.openbsd.org/errata23.html#tcpfix

Reference: OSVDB:5707

Reference: URL:http://www.osvdb.org/5707

Votes:

- MODIFY(1) Frech
- NOOP(2) Northcutt, Wall
- REVIEWING(1) Christey

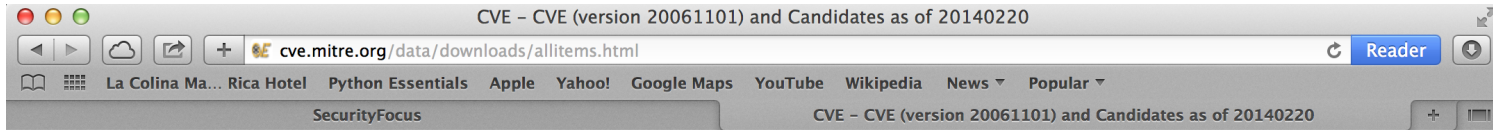
Voter Comments:

Christey> A Bugtraq posting indicates that the bug has to do with "short packets with certain options set," so the description should be modified accordingly.

But is this the same as CVE-1999-0052? That one is related to nestea (CVE-1999-0257) and probably the one described in BUGTRAQ:19981023 nestea v2 against freebsd 3.0-Release. The patch for nestea is in ip_input.c around line 750. The patches for CVE-1999-0001 are in lines 388&446. So, CVE-1999-0001 is different from CVE-1999-0257 and CVE-1999-0052. The FreeBSD patch for CVE-1999-0052 is in line 750. So, CVE-1999-0257 and CVE-1999-0052 may be the same, though CVE-1999-0052 should be RECAST since this bug affects Linux and other OSes besides FreeBSD.

Frech> XF:teardrop(338)
This assignment was based solely on references to the CERT advisory. Christey> The description for CVE-1999-0001 is "short packets with certain options set," which links to CVE-1999-0052. The

Mitre – milw0rm Play.PHP Exploit



Name: CVE-2007-6215

Description:

Multiple directory traversal vulnerabilities in play.php in Web-MeetMe 3.0.3 allow remote attackers to read arbitrary files via a .. (dot dot) in

Status: Candidate

Phase: Assigned (20071204)

Reference: MILWORM:4676

Reference: URL:<http://www.milw0rm.com/exploits/4676>

Reference: BID:26641

Reference: URL:<http://www.securityfocus.com/bid/26641>

Reference: XF:webmeetme-play-directory-traversal(38772)

Reference: URL:<http://xforce.iss.net/xforce/xfdb/38772>

Votes:

Name: CVE-2007-6216

Description:

Race condition in the Fibre Channel protocol (fcp) driver and Devices filesystem (devfs) in Sun Solaris 10 allows local users to cause a denia

Status: Candidate

Phase: Assigned (20071204)

Reference: SUNALERT:102947

Reference: URL:<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102947-1>

Reference: SUNALERT:200182

Reference: URL:<http://sunsolve.sun.com/search/document.do?assetkey=1-66-200182-1>

Reference: BID:26653

Reference: URL:<http://www.securityfocus.com/bid/26653>

Reference: VUPEN:ADV-2007-4043

Reference: URL:<http://www.vupen.com/english/advisories/2007/4043>

Reference: OSVDB:40826

Reference: URL:<http://osvdb.org/40826>

Reference: OSVDB:40827

Reference: URL:<http://osvdb.org/40827>

Reference: SECTRACK:1019025

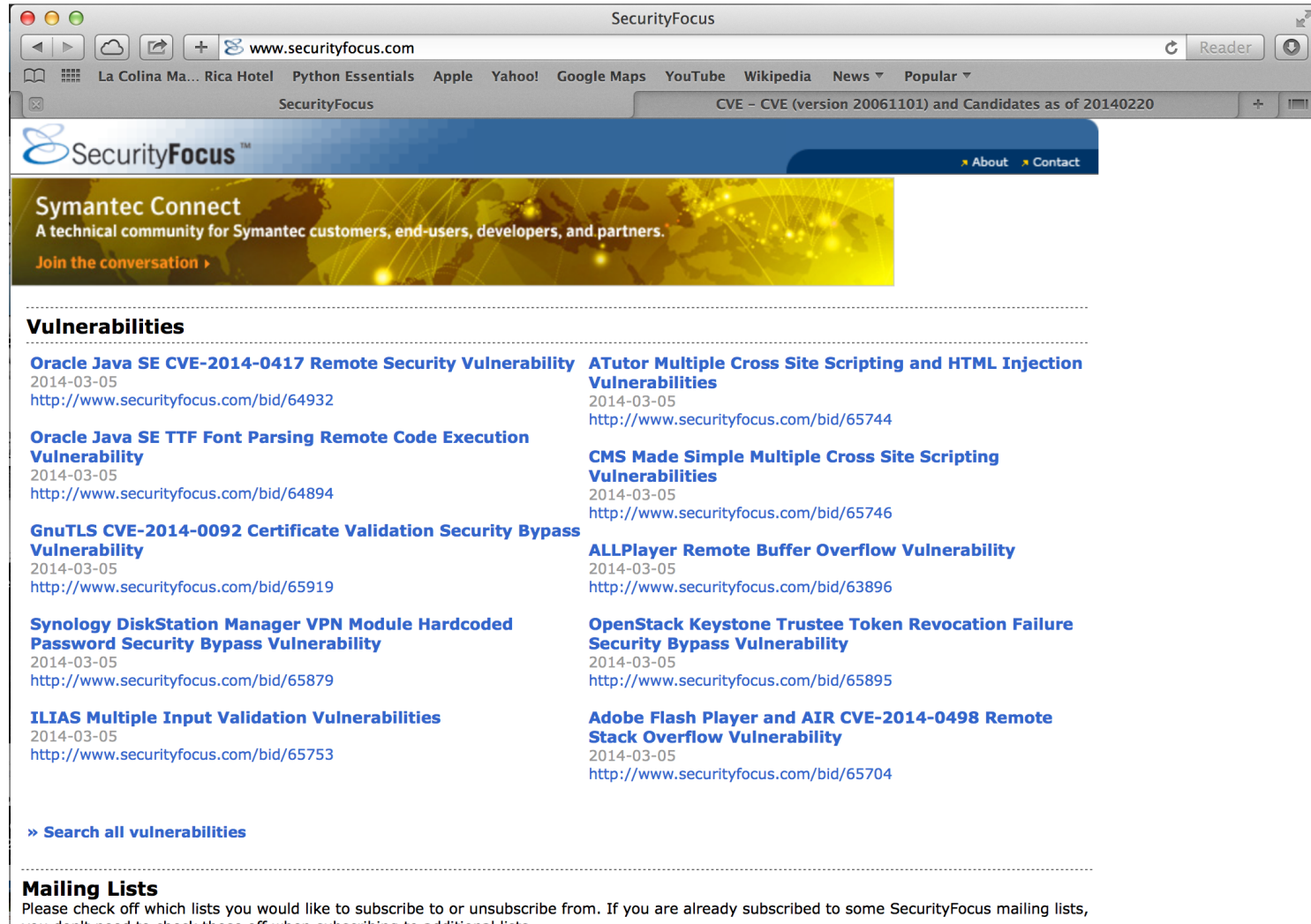
Reference: URL:<http://www.securitytracker.com/id?1019025>

Reference: SECUNIA:27867

Reference: URL:<http://secunia.com/advisories/27867>

Reference: XF:solaris-fcp-driver-race(38767)

Security Focus - CVEs



The screenshot shows a web browser window with the URL www.securityfocus.com. The page title is "SecurityFocus" and the current page is "CVE - CVE (version 20061101) and Candidates as of 20140220". The page features a navigation bar with links for "About" and "Contact". A banner for "Symantec Connect" is visible, along with a "Join the conversation" link. The main content area is titled "Vulnerabilities" and lists several CVEs with their dates and URLs. A "Search all vulnerabilities" link is provided at the bottom of the list. Below the vulnerabilities section is a "Mailing Lists" section with a heading and a paragraph of text.

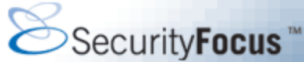
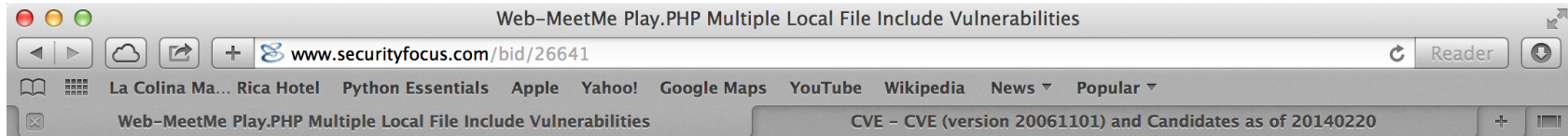
Vulnerabilities

Oracle Java SE CVE-2014-0417 Remote Security Vulnerability 2014-03-05 http://www.securityfocus.com/bid/64932	ATutor Multiple Cross Site Scripting and HTML Injection Vulnerabilities 2014-03-05 http://www.securityfocus.com/bid/65744
Oracle Java SE TTF Font Parsing Remote Code Execution Vulnerability 2014-03-05 http://www.securityfocus.com/bid/64894	CMS Made Simple Multiple Cross Site Scripting Vulnerabilities 2014-03-05 http://www.securityfocus.com/bid/65746
GnuTLS CVE-2014-0092 Certificate Validation Security Bypass Vulnerability 2014-03-05 http://www.securityfocus.com/bid/65919	ALLPlayer Remote Buffer Overflow Vulnerability 2014-03-05 http://www.securityfocus.com/bid/63896
Synology DiskStation Manager VPN Module Hardcoded Password Security Bypass Vulnerability 2014-03-05 http://www.securityfocus.com/bid/65879	OpenStack Keystone Trustee Token Revocation Failure Security Bypass Vulnerability 2014-03-05 http://www.securityfocus.com/bid/65895
ILIAS Multiple Input Validation Vulnerabilities 2014-03-05 http://www.securityfocus.com/bid/65753	Adobe Flash Player and AIR CVE-2014-0498 Remote Stack Overflow Vulnerability 2014-03-05 http://www.securityfocus.com/bid/65704

[» Search all vulnerabilities](#)

Mailing Lists
Please check off which lists you would like to subscribe to or unsubscribe from. If you are already subscribed to some SecurityFocus mailing lists, you do not need to check those off when subscribing to additional lists.

Play.PHP - Info



[About](#) [Contact](#)

Symantec Connect

A technical community for Symantec customers, end-users, developers, and partners.

[Join the conversation](#)

[info](#)

[discussion](#)

[exploit](#)

[solution](#)

[references](#)

Web-MeetMe Play.PHP Multiple Local File Include Vulnerabilities

Bugtraq ID: 26641
Class: Input Validation Error
CVE: CVE-2007-6215
Remote: Yes
Local: No
Published: Nov 29 2007 12:00AM
Updated: Dec 07 2007 02:32PM
Credit: Evil.Man is credited with the discovery of these vulnerabilities.
Vulnerable: Web-MeetMe Web-MeetMe 3.0.3

Not Vulnerable:

Play.PHP - Discussion

Web-MeetMe Play.PHP Multiple Local File Include Vulnerabilities

www.securityfocus.com/bid/26641/discuss

SecurityFocus™

Symantec Connect
A technical community for Symantec customers, end-users, developers, and partners.
Join the conversation >

info discussion exploit solution references

Web-MeetMe Play.PHP Multiple Local File Include Vulnerabilities

Web-MeetMe is prone to multiple local file-include vulnerabilities because it fails to properly sanitize user-supplied input.

Exploiting these issues may allow an attacker to access potentially sensitive information and execute arbitrary local scripts in the context of the affected application.

These issues affect Web-MeetMe 3.0.3; other versions may also be affected.

Play.PHP - Exploit

Web-MeetMe Play.PHP Multiple Local File Include Vulnerabilities

www.securityfocus.com/bid/26641/exploit

La Colina Ma... Rica Hotel Python Essentials Apple Yahoo! Google Maps YouTube Wikipedia News Popular

Web-MeetMe Play.PHP Multiple Local File Include Vulnerabilities CVE - CVE (version 20061101) and Candidates as of 20140220

SecurityFocus™ About Contact

Symantec Connect
A technical community for Symantec customers, end-users, developers, and partners.
Join the conversation >

info discussion **exploit** solution references

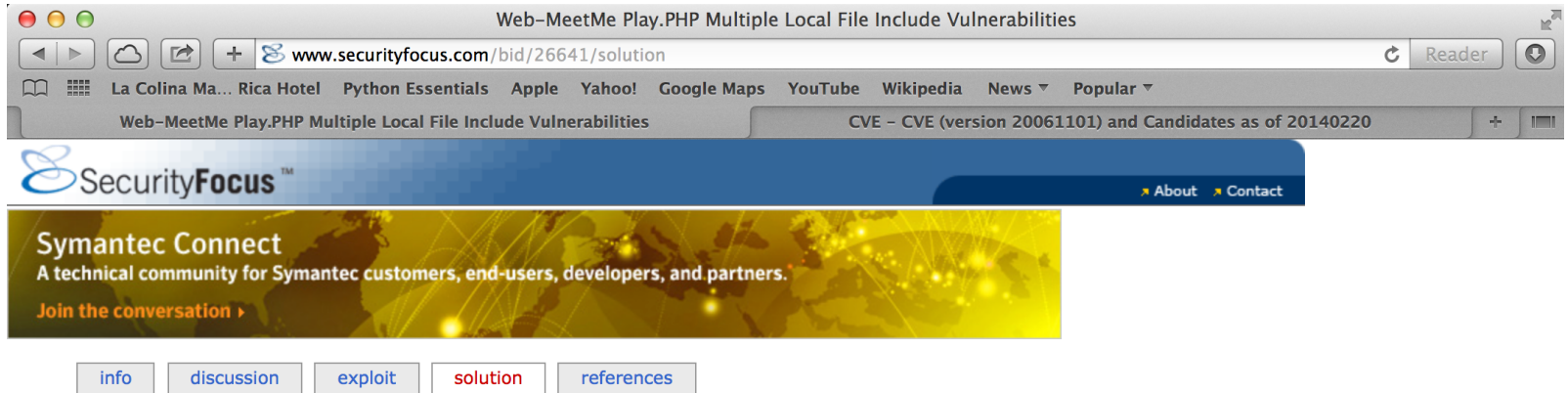
Web-MeetMe Play.PHP Multiple Local File Include Vulnerabilities

Attackers may exploit these issues through a browser.

The following proof-of-concept URIs are available:

`http://www.example.com/play.php../../../../../../../../etc/passwd%00` `http://www.example.com/play.php?bookid=../../../../../../../../etc/passwd%00`

Play.PHP - Solution



Web-MeetMe Play.PHP Multiple Local File Include Vulnerabilities

www.securityfocus.com/bid/26641/solution

La Colina Ma... Rica Hotel Python Essentials Apple Yahoo! Google Maps YouTube Wikipedia News Popular

Web-MeetMe Play.PHP Multiple Local File Include Vulnerabilities CVE - CVE (version 20061101) and Candidates as of 20140220

SecurityFocus™ About Contact

Symantec Connect
A technical community for Symantec customers, end-users, developers, and partners.
Join the conversation >

info discussion exploit **solution** references

Web-MeetMe Play.PHP Multiple Local File Include Vulnerabilities

Solution:

Currently we are not aware of any vendor-supplied patches for these issues. If you feel we are in error or if you are aware of more recent information, please mail us at: vuldb@securityfocus.com.

Play.PHP - References

The screenshot shows a web browser window with the following details:

- Address bar: www.securityfocus.com/bid/26641/references
- Page Title: Web-MeetMe Play.PHP Multiple Local File Include Vulnerabilities
- Navigation: Back, Forward, Home, Reload, Reader, Print
- Search: La Colina Ma... Rica Hotel Python Essentials Apple Yahoo! Google Maps YouTube Wikipedia News Popular
- Page Content: SecurityFocus logo, Symantec Connect banner, and a breadcrumb trail: info | discussion | exploit | solution | **references**

Web-MeetMe Play.PHP Multiple Local File Include Vulnerabilities

References:

- [Web-MeetMe Homepage](#) (Web-MeetMe)

CVE – XML File

```
data — dplante@akiliconsult:~ — vim — 140x52
<item type="CAN" name="CVE-2007-6215" seq="2007-6215">
<status>Candidate</status>
<phase date="20071204">Assigned</phase>
<desc>Multiple directory traversal vulnerabilities in play.php in Web-MeetMe 3.0.3 allow remote attackers to read arbitrary files via a .. (
dot dot) in the (1) roomNo and possibly the (2) bookid parameter.</desc>
<refs>
<ref source="MILW0RM" url="http://www.milw0rm.com/exploits/4676">4676</ref>
<ref source="BID" url="http://www.securityfocus.com/bid/26641">26641</ref>
<ref source="XF" url="http://xforce.iss.net/xforce/xfdb/38772">webmeetme-play-directory-traversal(38772)</ref>
</refs>
<votes>
</votes>
<comments>
</comments>
</item>

<item type="CAN" name="CVE-2007-6216" seq="2007-6216">
<status>Candidate</status>
<phase date="20071204">Assigned</phase>
<desc>Race condition in the Fibre Channel protocol (fcp) driver and Devices filesystem (devfs) in Sun Solaris 10 allows local users to cause
a denial of service (system hang) via some programs that access hardware resources, as demonstrated by the (1) cfgadm and (2) format progra
ms.</desc>
<refs>
<ref source="SUNALERT" url="http://sunsolve.sun.com/search/document.do?assetkey=1-26-102947-1">102947</ref>
<ref source="SUNALERT" url="http://sunsolve.sun.com/search/document.do?assetkey=1-66-200182-1">200182</ref>
<ref source="BID" url="http://www.securityfocus.com/bid/26653">26653</ref>
<ref source="VUPEN" url="http://www.vupen.com/english/advisories/2007/4043">ADV-2007-4043</ref>
<ref source="OSVDB" url="http://osvdb.org/40826">40826</ref>
<ref source="OSVDB" url="http://osvdb.org/40827">40827</ref>
<ref source="SECTRACK" url="http://www.securitytracker.com/id?1019025">1019025</ref>
<ref source="SECUNIA" url="http://secunia.com/advisories/27867">27867</ref>
<ref source="XF" url="http://xforce.iss.net/xforce/xfdb/38767">solaris-fcp-devfs-dos(38767)</ref>
</refs>
<votes>
</votes>
<comments>
</comments>
</item>

<item type="CAN" name="CVE-2007-6217" seq="2007-6217">
<status>Candidate</status>
<phase date="20071204">Assigned</phase>
```


XML Parser – Sample in JAVA

The screenshot displays the Eclipse IDE interface with the following components:

- Package Explorer:** Shows a project named 'XmlParse' with a source folder 'src' containing 'ParserExample.java'. It also lists 'Referenced Libraries' including 'JRE System Library [Java SE 7 [1.7.0_51]]', 'output', and 'Parse.jar'.
- Editor:** Displays the source code for 'ParserExample.java'. The code imports 'java.io.File' and defines a 'main' method that uses 'DocumentBuilderFactory' to parse an XML file ('data/someitems.xml'). It iterates through the root element's children, printing the name and content of each element.
- Task List:** Contains a search bar and a 'Connect Mylyn' button with a link to connect to task and ALM tools.
- Outline:** Shows the class structure with 'ParserExample' and its 'main(String[]) : void' method.
- Problems:** Shows '0 items' in the table below.

```
import java.io.File;

public class ParserExample {

    public static void main(String[] args) {
        //String action = null;
        DocumentBuilderFactory dbf = DocumentBuilderFactory.newInstance();
        DocumentBuilder db = null;
        try {
            db = dbf.newDocumentBuilder();
        } catch (ParserConfigurationException e) {
            // TODO Auto-generated catch block
            e.printStackTrace();
        }

        Document doc = null;
        try {
            //doc = db.parse(inStream);
            doc = db.parse(new File("data/someitems.xml"));
        } catch (SAXException e) {
            // TODO Auto-generated catch block
            e.printStackTrace();
        } catch (IOException e) {
            // TODO Auto-generated catch block
            e.printStackTrace();
        }
        NodeList nodeList = doc.getElementsByTagName("item");

        for (int s = 0; s < nodeList.getLength(); s++) {
            Node fstNode = nodeList.item(s);
            if (fstNode.getNodeType() == Node.ELEMENT_NODE) {
                Element fstElmnt = (Element) fstNode;

                NodeList lstNmElmntLst = fstElmnt.getElementsByTagName("desc");
                Element lstNmElmnt = (Element) lstNmElmntLst.item(0);
                NodeList lstNm = lstNmElmnt.getChildNodes();
                String currentAction = ((Node) lstNm.item(0)).getNodeValue();
                String name = fstElmnt.getAttribute("name");
                System.out.println(name + " : " + currentAction);
            }
        }
    }
}
```

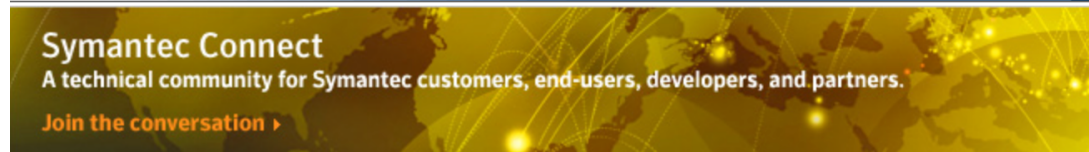
Description	Resource	Path	Location	Type

Writable Smart Insert 10 : 1

Support for Project

- PatchAdvisor, Inc. found problem too difficult to solve
- Data mined and categorized highly valuable

PostgreSQL Exploit Example

[info](#)[discussion](#)[exploit](#)[solution](#)[references](#)

PostgreSQL CVE-2014-0061 Security Bypass Vulnerability

Bugtraq ID: 65724
Class: Access Validation Error
CVE: CVE-2014-0061
Remote: Yes
Local: No
Published: Feb 20 2014 12:00AM
Updated: Mar 05 2014 01:02AM
Credit: Andres Freund
Vulnerable: Ubuntu Ubuntu Linux 10.04 LTS
RedHat Enterprise Linux Desktop Workstation 5 client
Red Hat Enterprise Linux Workstation 6
Red Hat Enterprise Linux Server 6
Red Hat Enterprise Linux HPC Node Optional 6
Red Hat Enterprise Linux HPC Node 6
Red Hat Enterprise Linux Desktop Optional 6
Red Hat Enterprise Linux Desktop 6
Red Hat Enterprise Linux Desktop 5 client
Red Hat Enterprise Linux 5 Server
PostgreSQL PostgreSQL 9.1.3
PostgreSQL PostgreSQL 9.0.7
PostgreSQL PostgreSQL 9.0.3
PostgreSQL PostgreSQL 9.0.1
PostgreSQL PostgreSQL 9.0
PostgreSQL PostgreSQL 8.4.11

Possible Module Directions

- Data Structures
 - Manage small collection of CVE data in ADTs
- Machine Learning/Data Mining
 - Mine patterns in XML and HTML pages to more accurately classify exploits
- Databases
 - Manage all data in SQL and NoSQL databases

Data Structures Class

- Parse XML data and store in data structures
- Data in form of:
 - (OS, Application/Program, Data)
- Various options for working with data
 - HashMap to associate (CVE, Data)
 - Sorted List of OS and Applications

Data Structures Class

- OS and Applications may be loaded by hand at first
- May require sorting algorithm to be programmed and used (e.g. MergeSort)
- GUI to allow selection of data for entered OS or Application (or both)