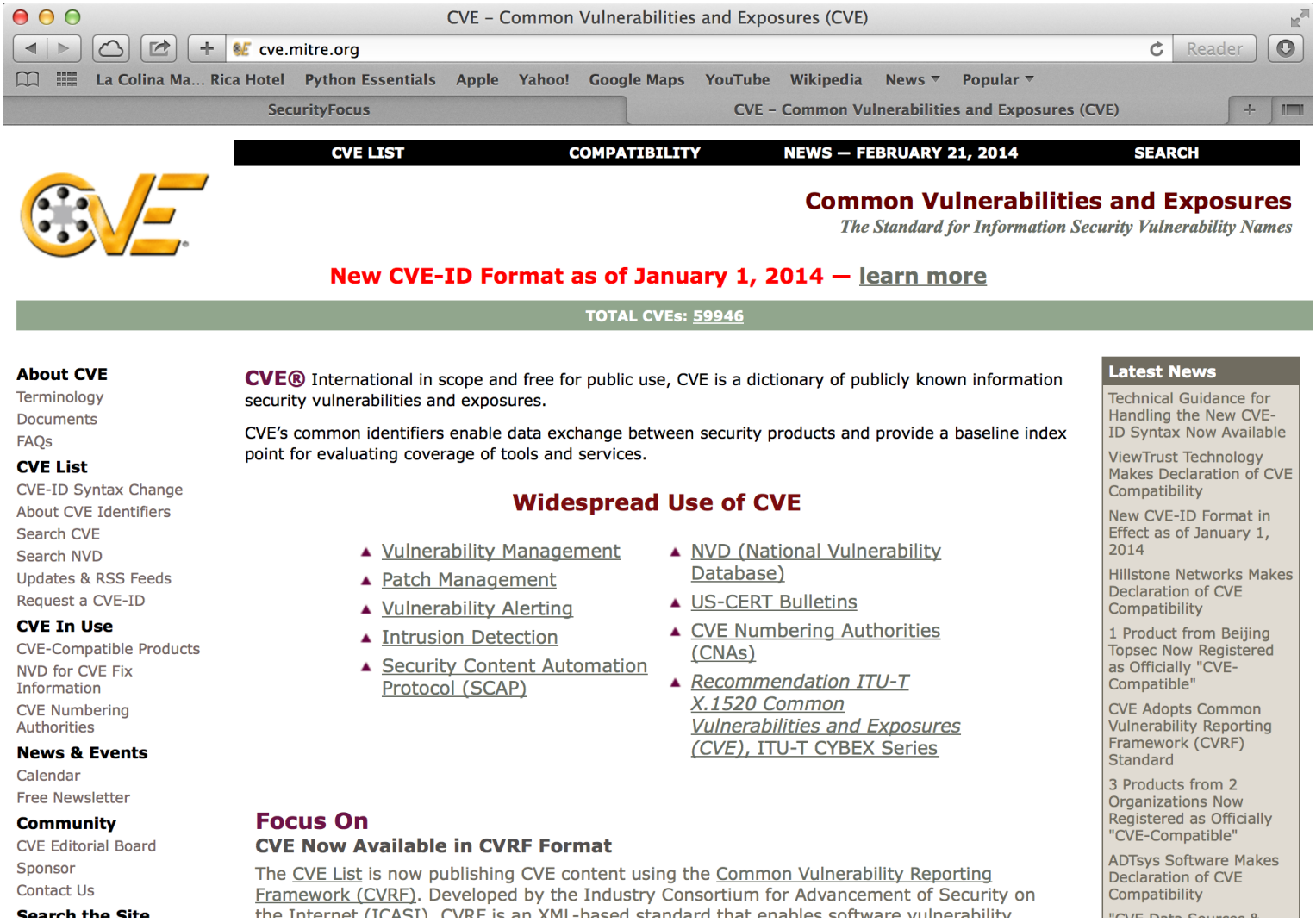
Vulnerability Monitoring

Managing Patch Updates

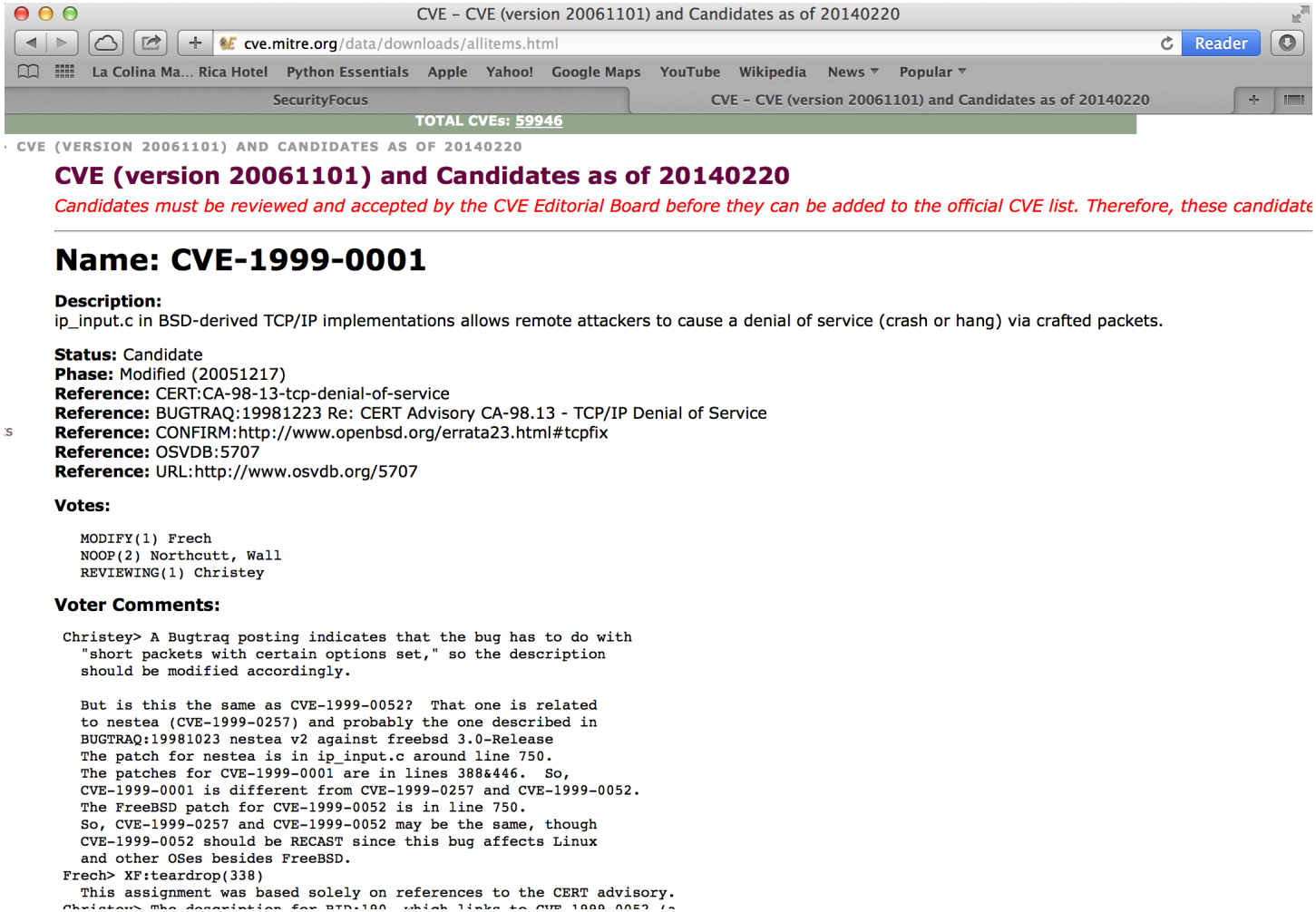
Motivation

- 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

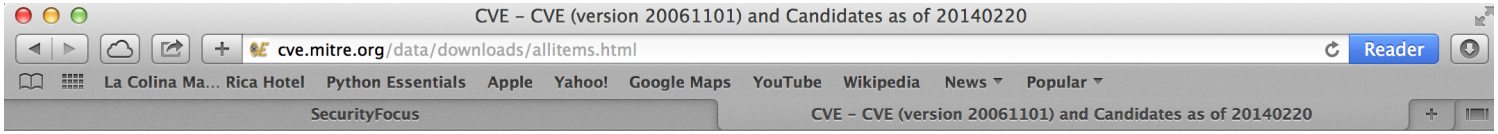
Mitre CVE Databank



Mitre – Early Vulnerability



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: MILW0RM: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

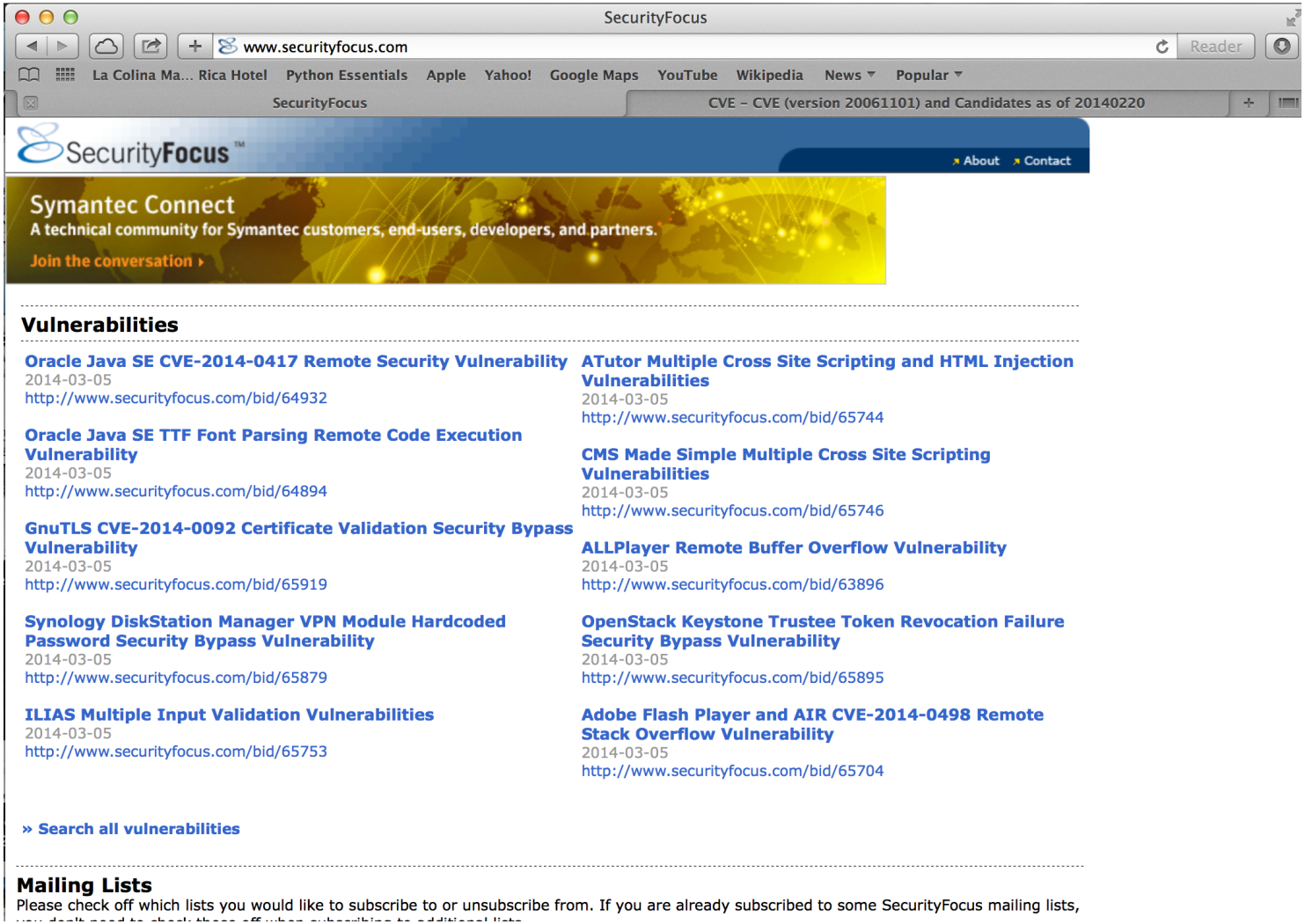
Votes:

Name: CVE-2007-6216

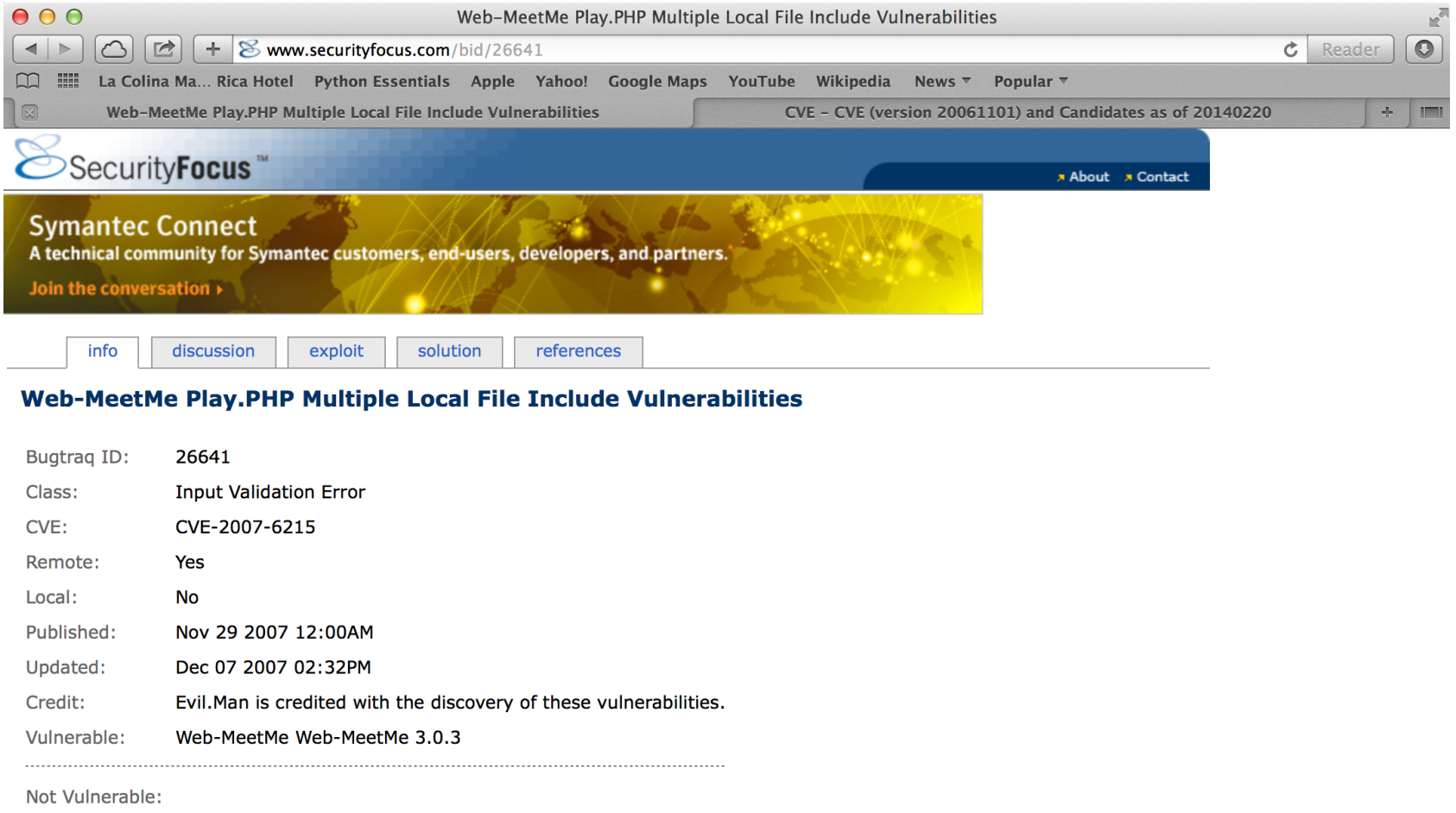
Description:
Race condition in the Fibre Channel protocol (fcp) driver and Devices filesystem (devfs) in Sun Solaris 10 allows local users to cause a denia

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-devfs-dos(38767)

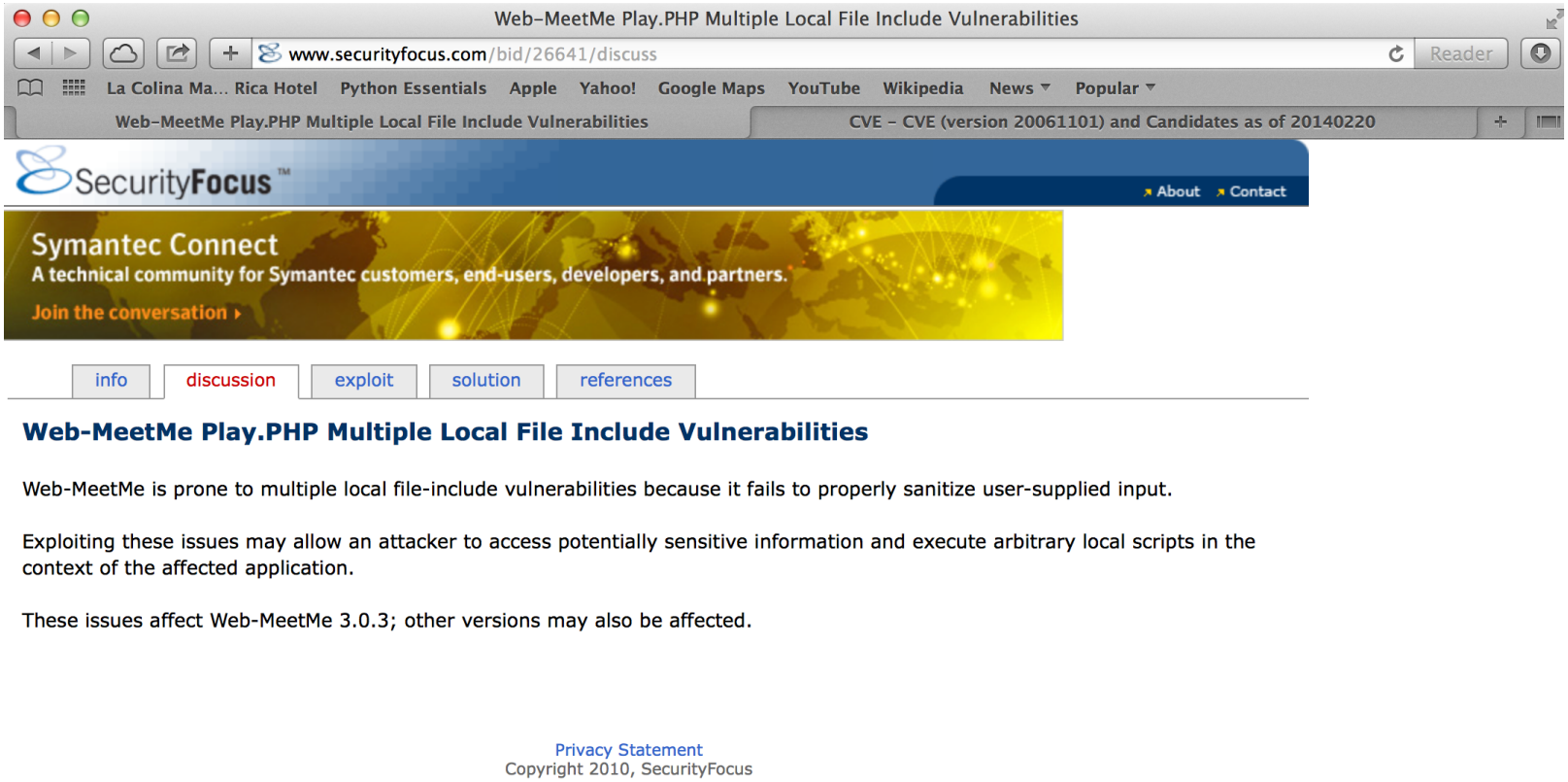
Security Focus - CVEs



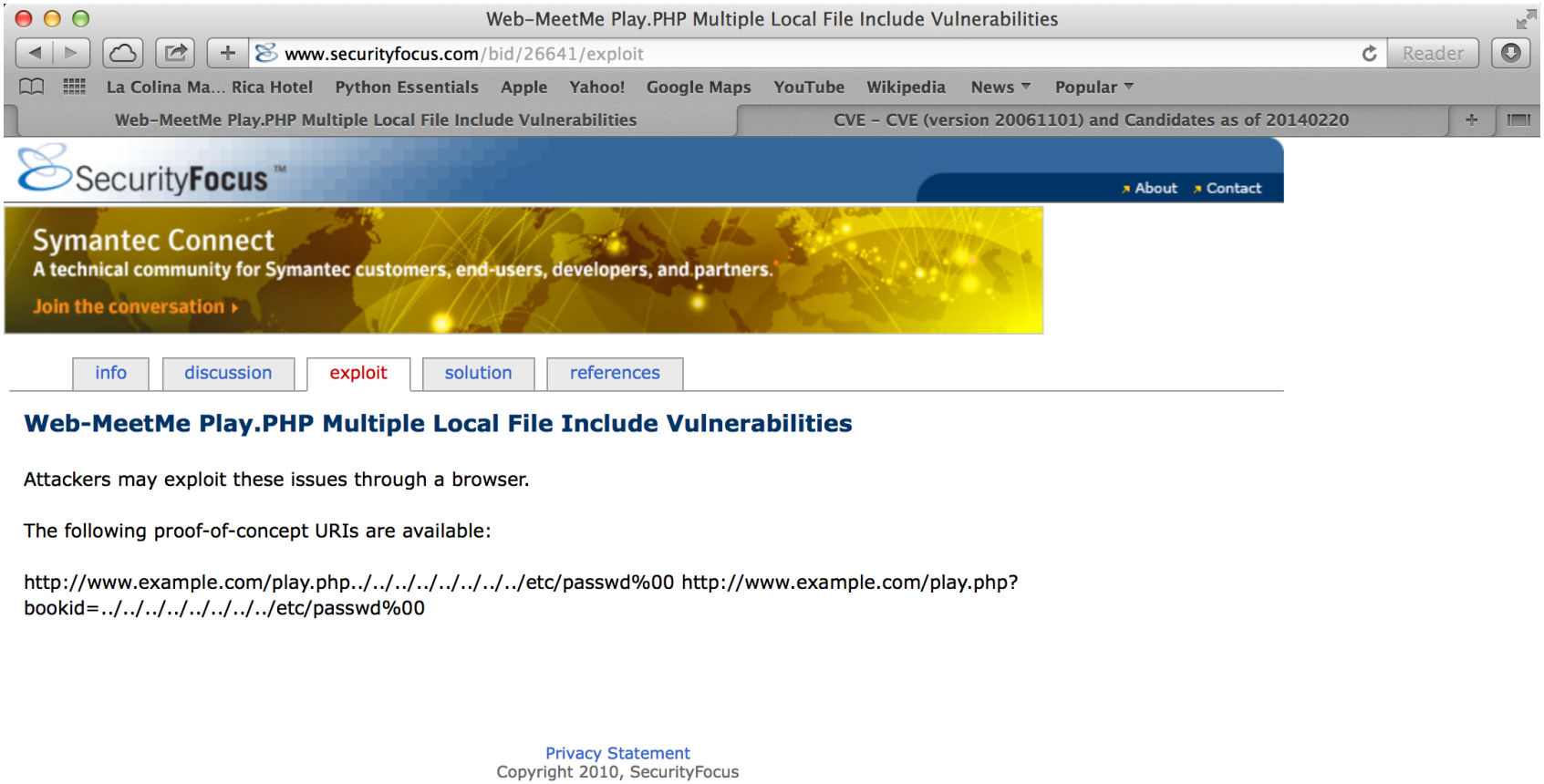
Play.PHP - Info



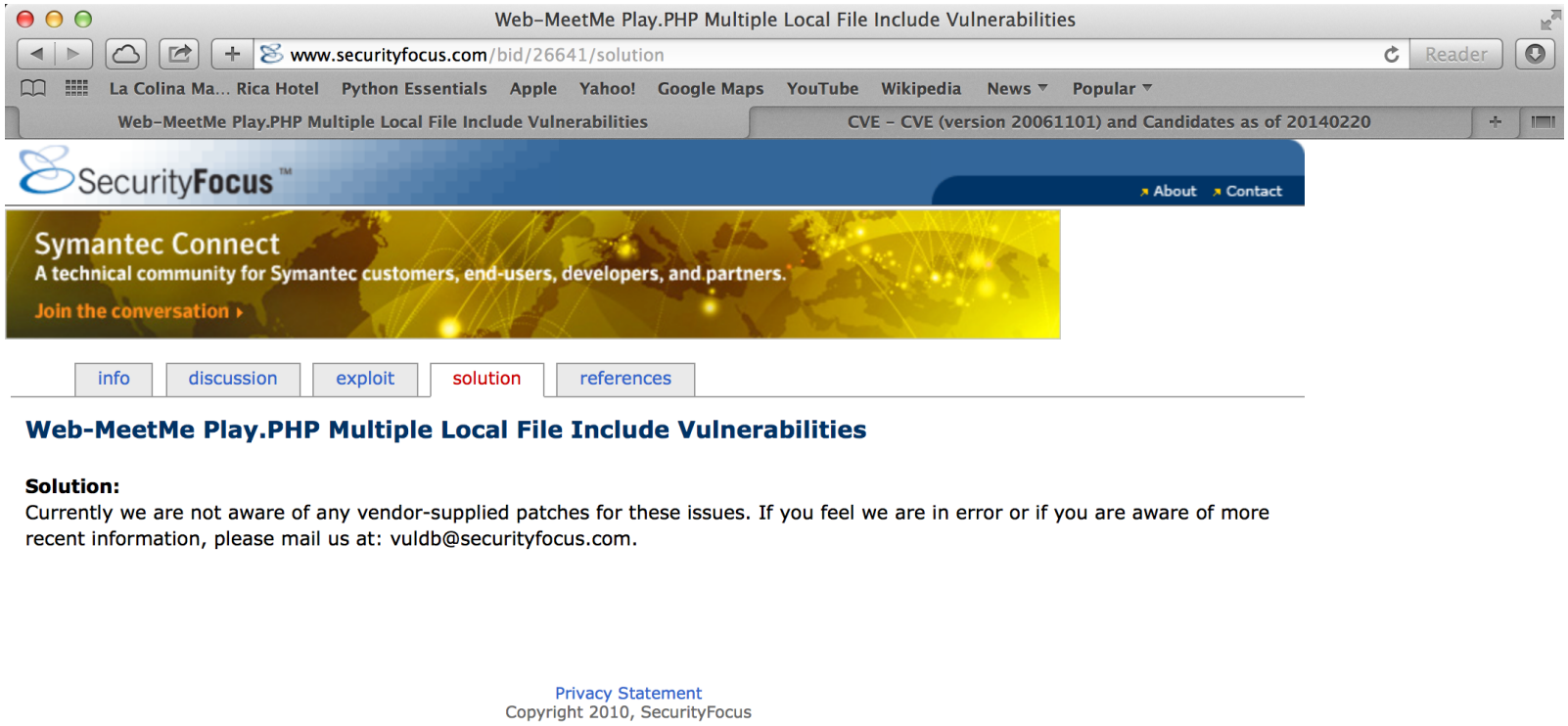
Play.PHP - Discussion



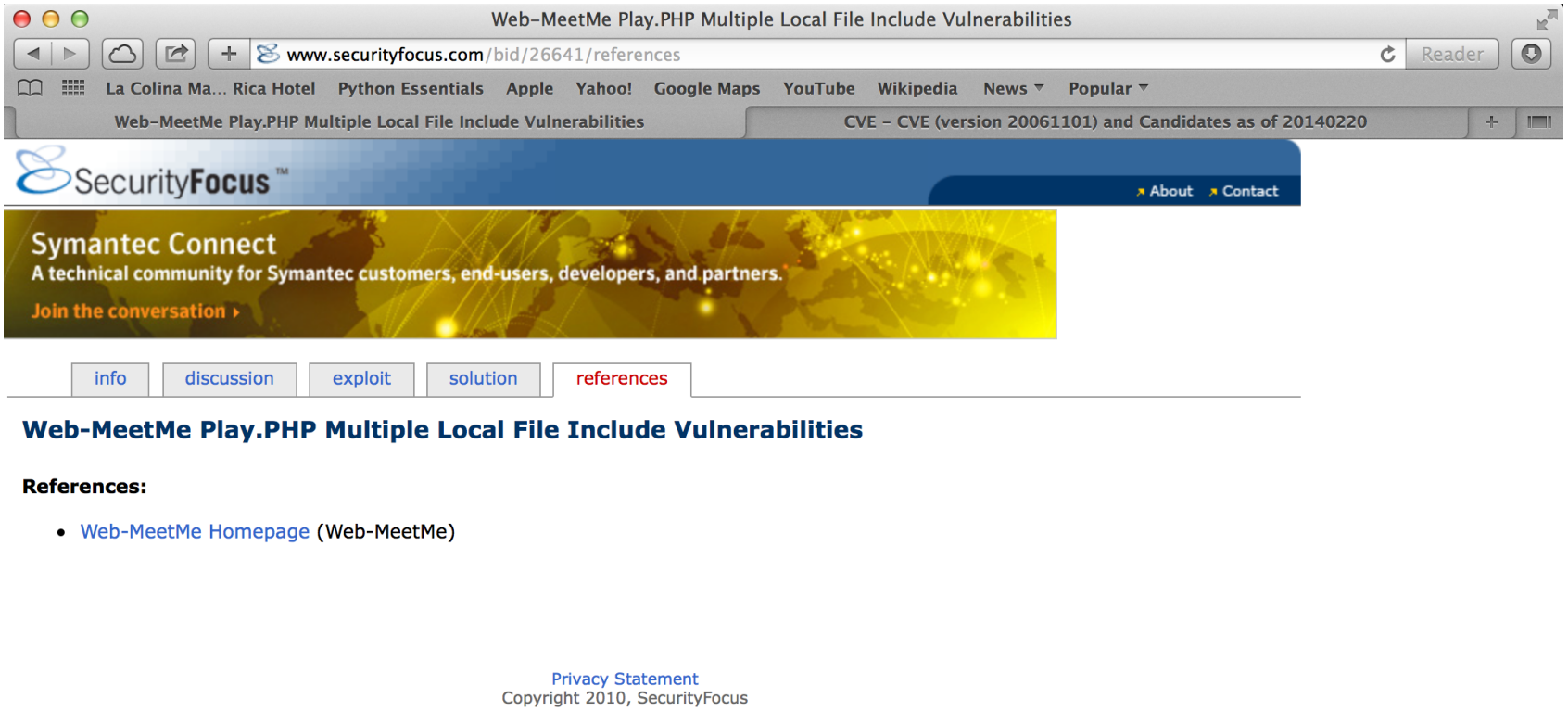
Play.PHP - Exploit



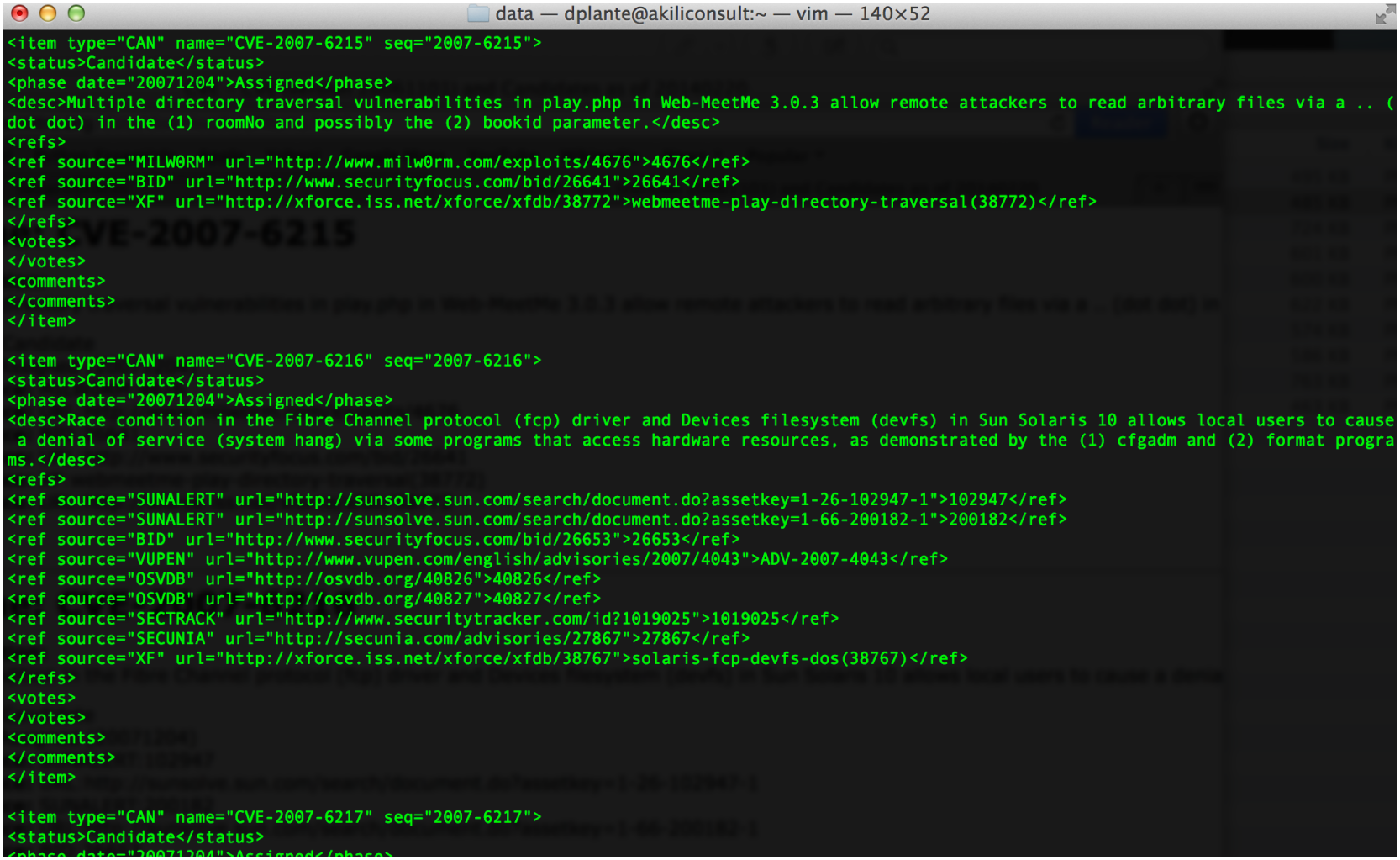
Play.PHP - Solution



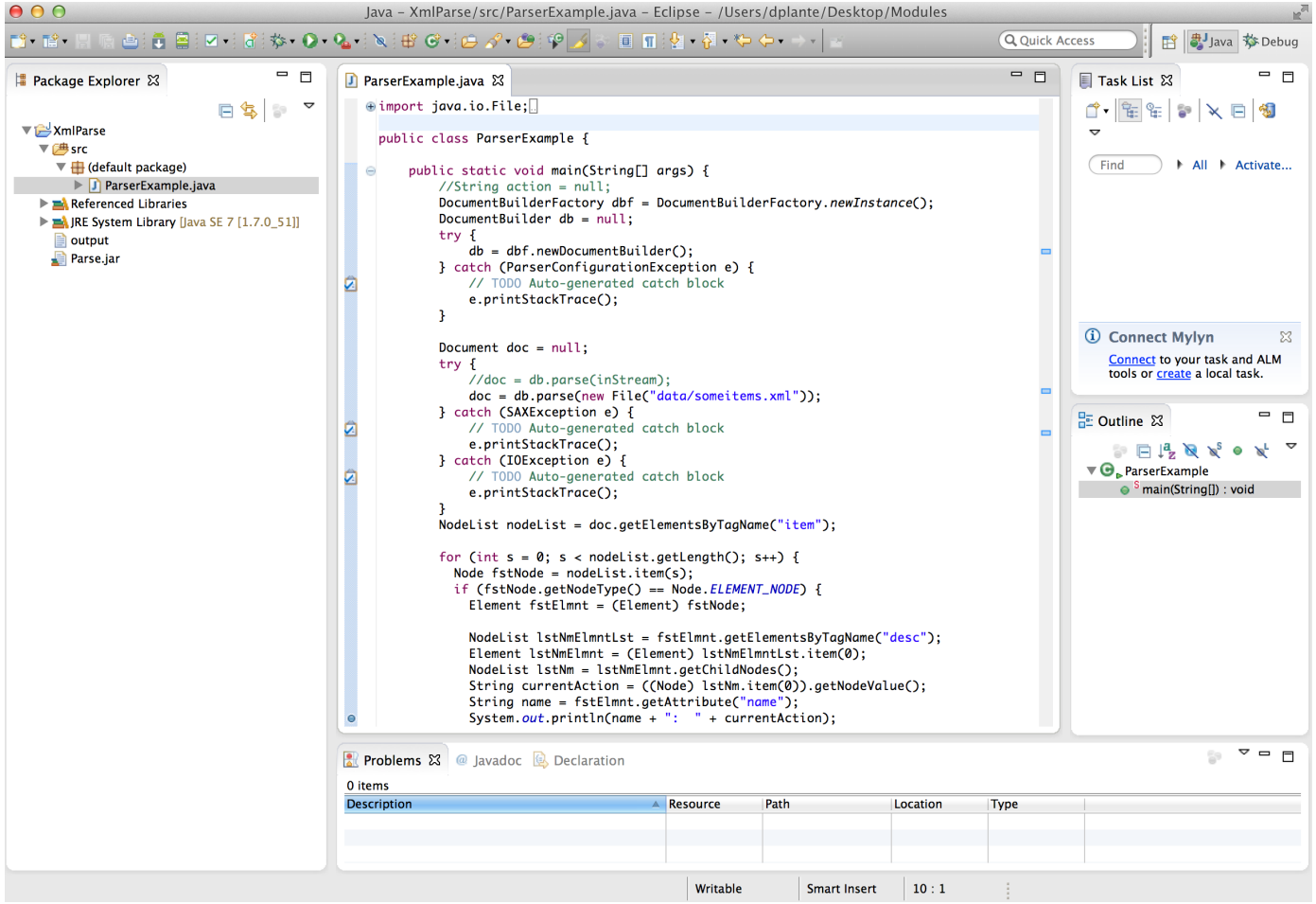
Play.PHP - References



CVE – XML File


data — dplante@akiliconsult:~ — vim — 140×52
<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>

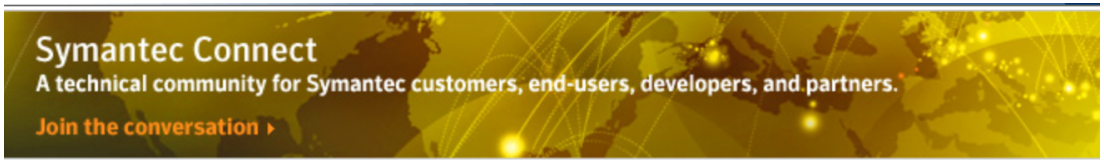
XML Parser – Sample in JAVA



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)