

A Rough Start of a Toolset for Assessing Java/J2EE Web Apps

OWASP Austin Kickoff
27 July 2006

Matthew Franz

mdfranz@threatmind.net

franz@digitalbond.com

Overview

- *Howdy!* and Objectives
- First Principles/Concepts
- Issues with Existing Open Source Tools
- The *start* of a simple command-line web app toolset (requirements, API selection & features)
- A Non-Spectacular Demo vs Tomcat 5.0.x Admin Interface
 - Various command-line scripts
 - Crude HTML reporting
- Comments/Questions

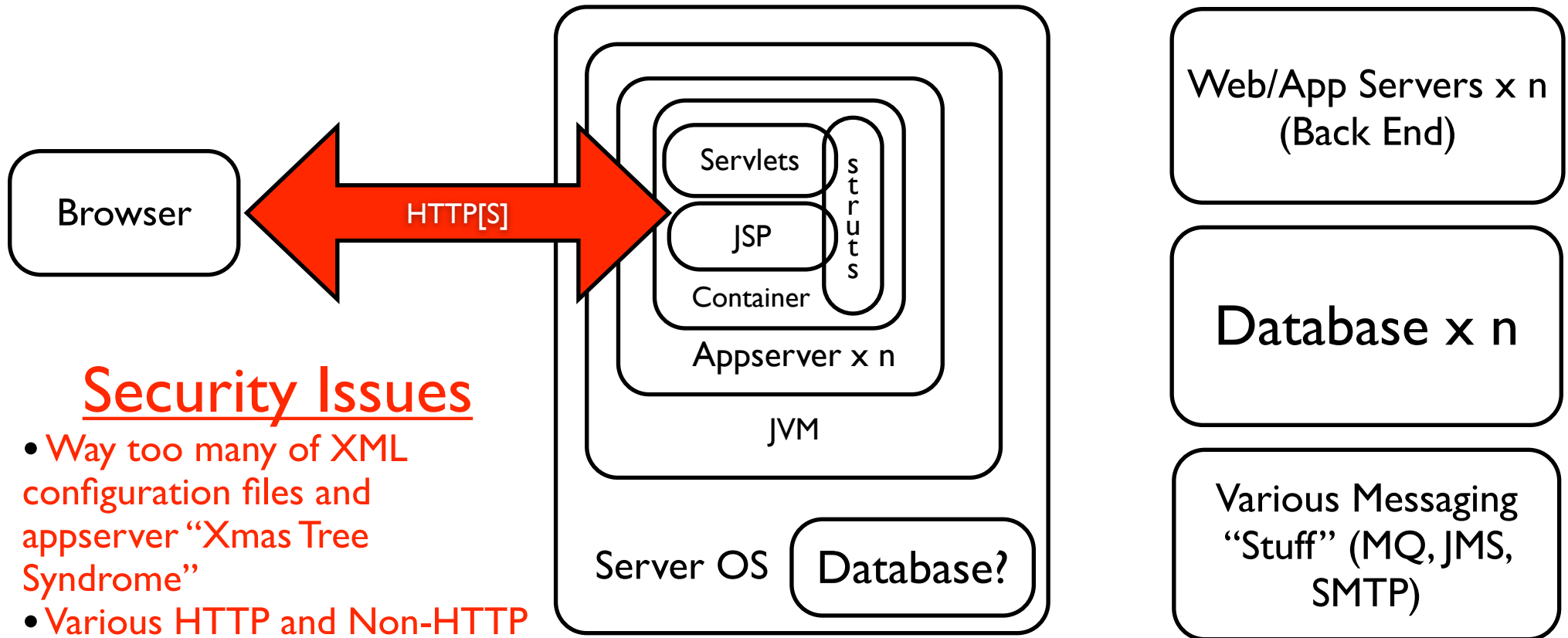
Purpose of This Talk

- Walk through the thought process on tool-set development for a Struts-based J2EE Webapp
- Provide a very superficial intro to Java/J2EE security issues
- Selfishly sanity check of some ideas

First Principles

- I want to develop a *NIX-style toolkit (meaning: command-line) for a particular Struts-based Java Web App
- I don't have to fight (or win!) the “build vs. buy” battle
- I want to learn cool stuff along the way
- I have to steer between a quick hack and a real development project

“Simple” J2EE Component View



Security Issues

- Way too many of XML configuration files and appserver “Xmas Tree Syndrome”
- Various HTTP and Non-HTTP Transports (JMX, SOAP, RMI, JMS, MQ, SMTP)
- Authentication/Access Controls for between components?
- And the normal OWASP stuff

Problems with Existing Free/Tools

- There is a bunch of you can do with curl for cookies and forms
- GUIs are slow (especially Swing)
- Extending, automating Webscarab is easier said than done (yeah I know about BeanShell)
- Webscarab is flaky on OSX

Bottom Line - Sometimes it is easier to build small tools from scratch that do want you want, than tweaking big tools

Rough Tool Requirements

- Build a “target database” for the app from multiple sources:

Session Information (from proxies/browsing)

Files from WEB-INF directory

- Allow automated testing (spidering, fuzzing, replay) of URIs and forms
- Conduct basic tests (and generate report) for common issues:

Appserver/Container Configuration Issues (esp. info disclosure)

Data validation (or lack thereof)

Platform Issues

- Cross-Platform Scripting Language (OSX/Linux/Windows)

Originally though Python + Jython, but settled on pure Python 2.4.x

- Higher level HTTP client functions (cookies, forms, redirects, error codes, etc.)

Wanted to do Commons HTTPClient scripted with Jython, but ended up with Python urllib2 (bad docs!)

Java scripting languages (JRuby, Jython, BeanShell, etc.) are cool, but there is some pain (especially Jython because it is more/less Python 2.2 compliant)

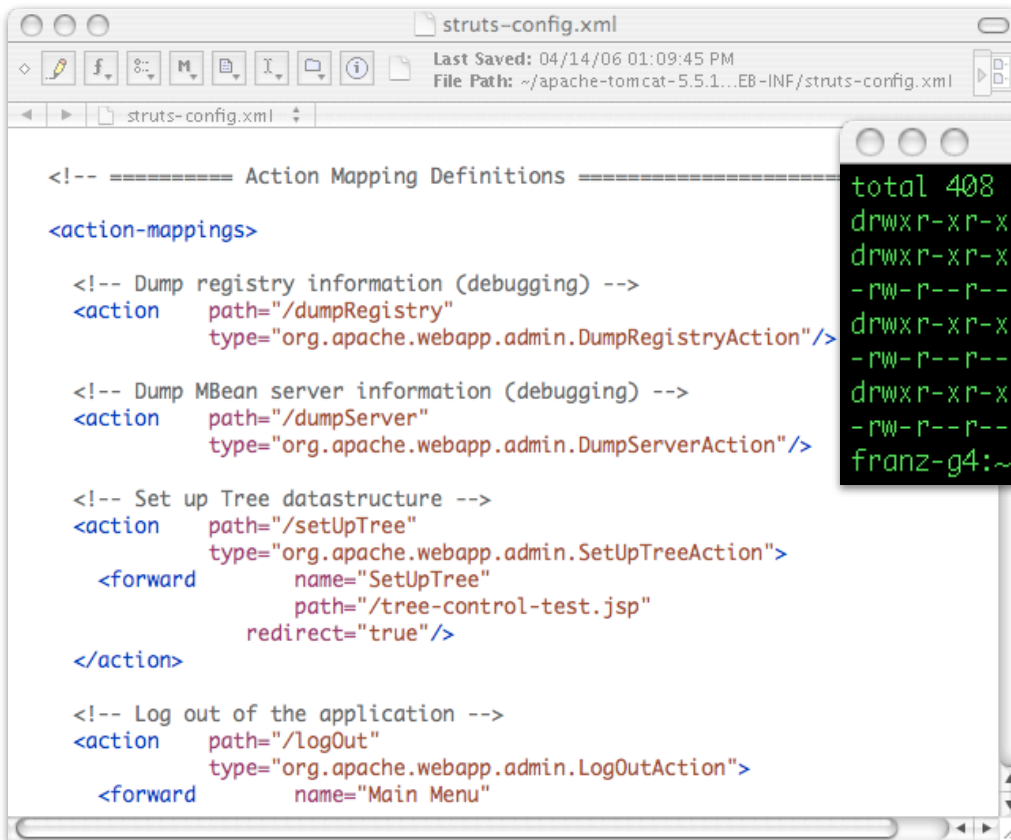
Current Tool Components

1. `strutsparse.py` - parses struts-config.xml and extracts URI, path, form
2. `parsecons.py` - reads “Conversation” files from webscarab sessions and adds to pickles
3. pickles - saved list of Python URI and Form objects
4. `pscanner.py` - reads in pickles, logs into app (or not) and creates & injects test cases and saves HTML report

Scanner Input

struts-config.xml

webscarab conversations



```
<!-- ===== Action Mapping Definitions =====>

<action-mappings>

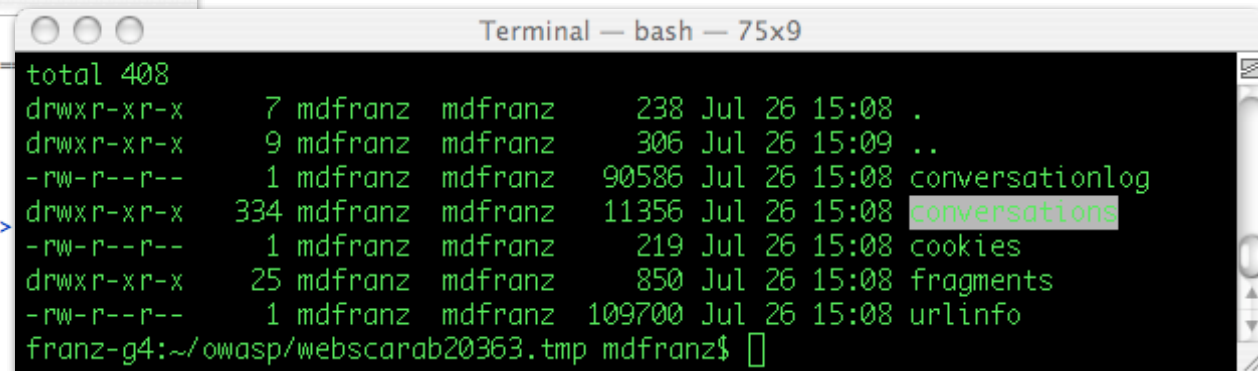
  <!-- Dump registry information (debugging) -->
  <action path="/dumpRegistry"
        type="org.apache.webapp.admin.DumpRegistryAction"/>

  <!-- Dump MBean server information (debugging) -->
  <action path="/dumpServer"
        type="org.apache.webapp.admin.DumpServerAction"/>

  <!-- Set up Tree datastructure -->
  <action path="/setUpTree"
        type="org.apache.webapp.admin.SetUpTreeAction">
    <forward name="SetUpTree"
            path="/tree-control-test.jsp"
            redirect="true"/>
  </action>

  <!-- Log out of the application -->
  <action path="/logout"
        type="org.apache.webapp.admin.LogOutAction">
    <forward name="Main Menu"
            path="/tree-control-test.jsp"
            redirect="true"/>
  </action>

</action-mappings>
```



```
total 408
drwxr-xr-x  7 mdfranz mdfranz  238 Jul 26 15:08 .
drwxr-xr-x  9 mdfranz mdfranz  306 Jul 26 15:09 ..
-rw-r--r--  1 mdfranz mdfranz 90586 Jul 26 15:08 conversationlog
drwxr-xr-x 334 mdfranz mdfranz 11356 Jul 26 15:08 conversations
-rw-r--r--  1 mdfranz mdfranz  219 Jul 26 15:08 cookies
drwxr-xr-x  25 mdfranz mdfranz   850 Jul 26 15:08 fragments
-rw-r--r--  1 mdfranz mdfranz 109700 Jul 26 15:08 urlinfo
franz-g4:~/owasp/webscarab20363.tmp mdfranz$
```

URI/Form DB
(Python Pickles)

“Scanning” Functions

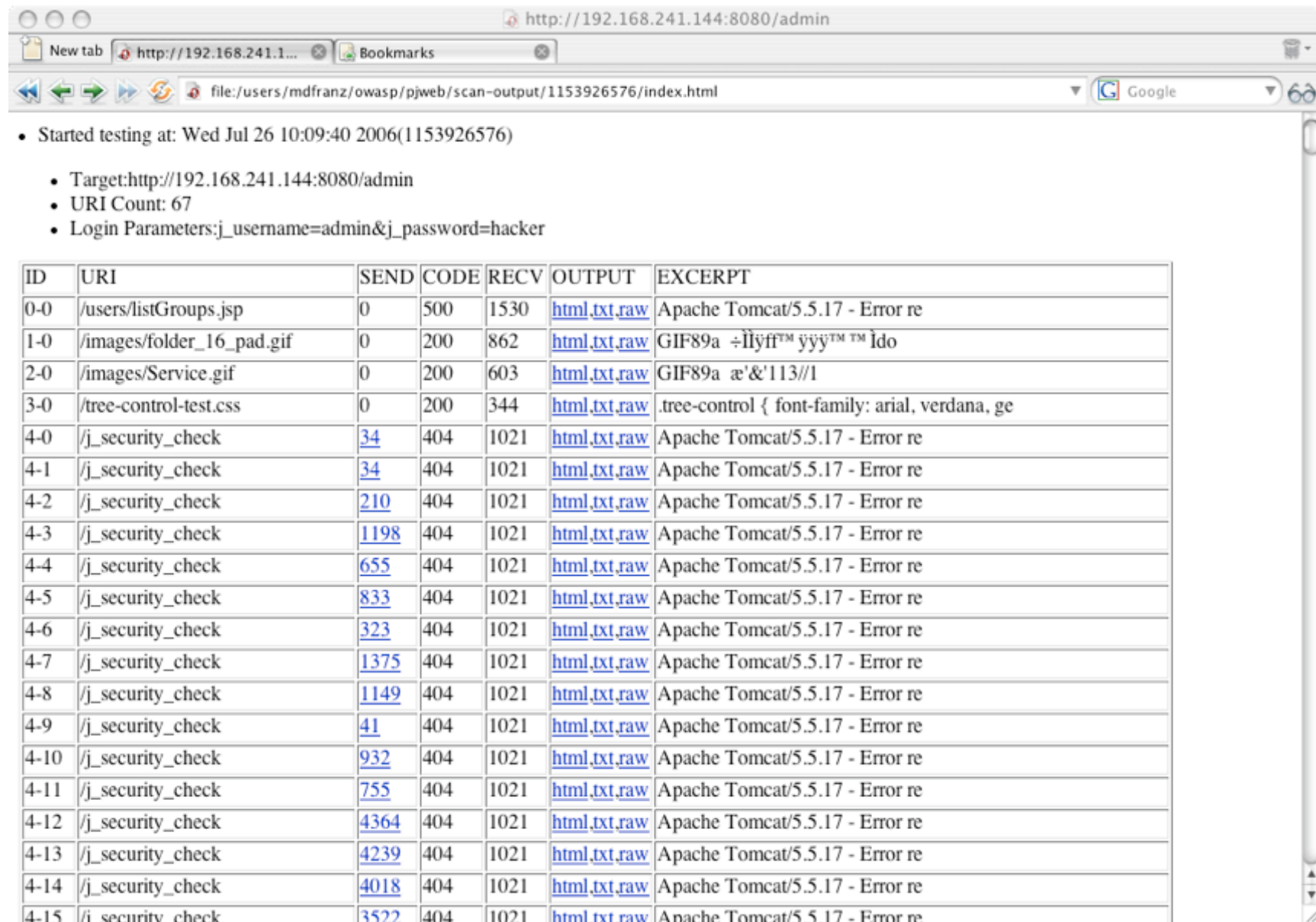
- URI-Crawl at various authentication levels
- Form “replay” (to Servlets/jsp) for different users
- Form mangling (based on existing sessions)

Popping

Transformation

- XSS/Injection (a work in progress)
- Manual Form/URI Entry

Crude HTML Reports

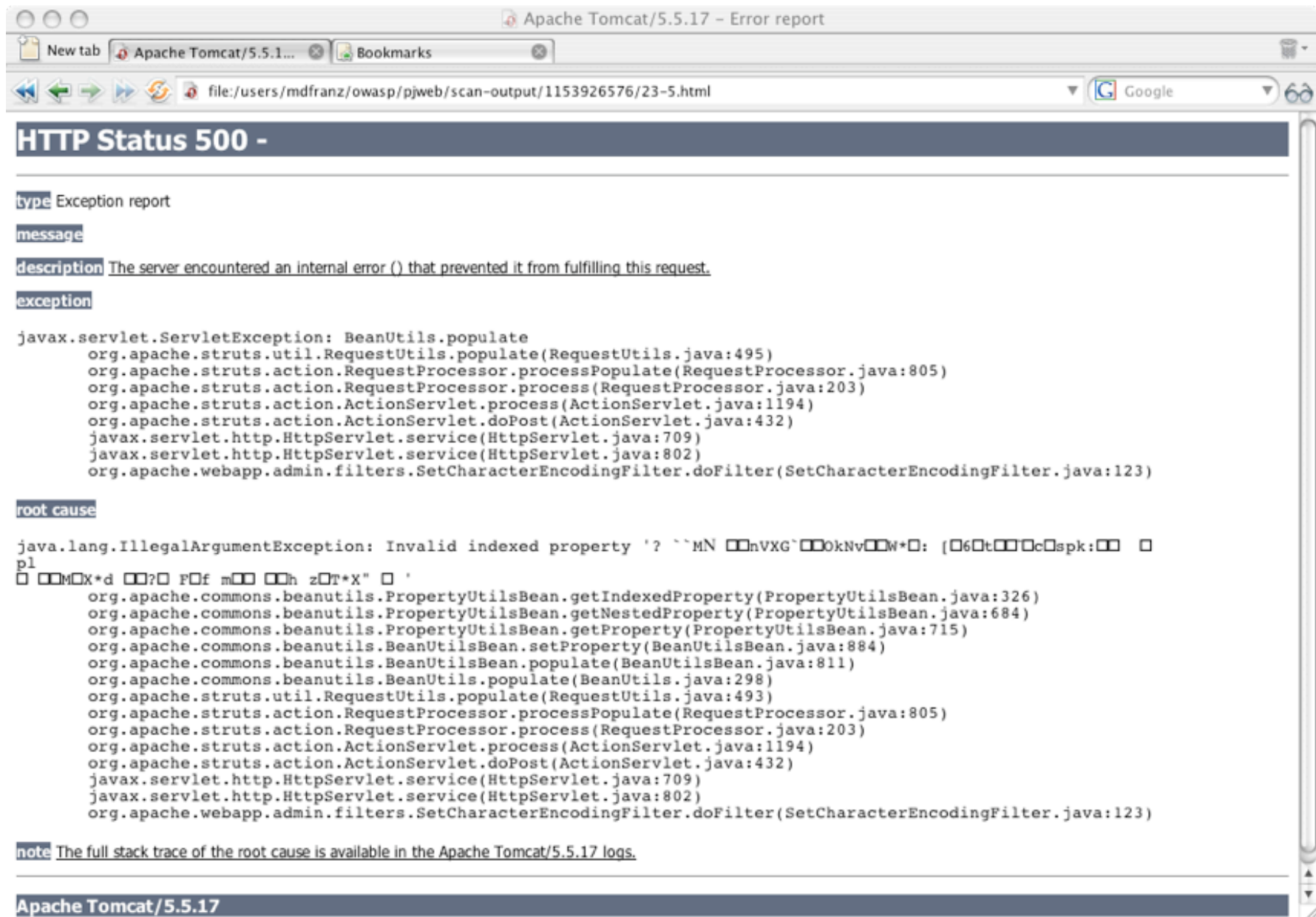


Started testing at: Wed Jul 26 10:09:40 2006(1153926576)

- Target: http://192.168.241.144:8080/admin
- URI Count: 67
- Login Parameters: j_username=admin&j_password=hacker

ID	URI	SEND	CODE	RECV	OUTPUT	EXCERPT
0-0	/users/listGroups.jsp	0	500	1530	html.txt.raw	Apache Tomcat/5.5.17 - Error re
1-0	/images/folder_16_pad.gif	0	200	862	html.txt.raw	GIF89a ÷llyf™ yyy™ ™ İdo
2-0	/images/Service.gif	0	200	603	html.txt.raw	GIF89a æ'&'113//1
3-0	/tree-control-test.css	0	200	344	html.txt.raw	.tree-control { font-family: arial, verdana, ge
4-0	/j_security_check	34	404	1021	html.txt.raw	Apache Tomcat/5.5.17 - Error re
4-1	/j_security_check	34	404	1021	html.txt.raw	Apache Tomcat/5.5.17 - Error re
4-2	/j_security_check	210	404	1021	html.txt.raw	Apache Tomcat/5.5.17 - Error re
4-3	/j_security_check	1198	404	1021	html.txt.raw	Apache Tomcat/5.5.17 - Error re
4-4	/j_security_check	655	404	1021	html.txt.raw	Apache Tomcat/5.5.17 - Error re
4-5	/j_security_check	833	404	1021	html.txt.raw	Apache Tomcat/5.5.17 - Error re
4-6	/j_security_check	323	404	1021	html.txt.raw	Apache Tomcat/5.5.17 - Error re
4-7	/j_security_check	1375	404	1021	html.txt.raw	Apache Tomcat/5.5.17 - Error re
4-8	/j_security_check	1149	404	1021	html.txt.raw	Apache Tomcat/5.5.17 - Error re
4-9	/j_security_check	41	404	1021	html.txt.raw	Apache Tomcat/5.5.17 - Error re
4-10	/j_security_check	932	404	1021	html.txt.raw	Apache Tomcat/5.5.17 - Error re
4-11	/j_security_check	755	404	1021	html.txt.raw	Apache Tomcat/5.5.17 - Error re
4-12	/j_security_check	4364	404	1021	html.txt.raw	Apache Tomcat/5.5.17 - Error re
4-13	/j_security_check	4239	404	1021	html.txt.raw	Apache Tomcat/5.5.17 - Error re
4-14	/j_security_check	4018	404	1021	html.txt.raw	Apache Tomcat/5.5.17 - Error re
4-15	/j_security_check	3522	404	1021	html.txt.raw	Apache Tomcat/5.5.17 - Error re

A Server Response



The screenshot shows a web browser window titled "Apache Tomcat/5.5.17 - Error report". The address bar shows the file path: "file:/users/mdfranz/owasp/pjweb/scan-output/1153926576/23-5.html". The page content is as follows:

HTTP Status 500 -

type Exception report

message

description The server encountered an internal error () that prevented it from fulfilling this request.

exception

```
javax.servlet.ServletException: BeanUtils.populate
    org.apache.struts.util.RequestUtils.populate(RequestUtils.java:495)
    org.apache.struts.action.RequestProcessor.processPopulate(RequestProcessor.java:805)
    org.apache.struts.action.RequestProcessor.process(RequestProcessor.java:203)
    org.apache.struts.action.ActionServlet.process(ActionServlet.java:1194)
    org.apache.struts.action.ActionServlet.doPost(ActionServlet.java:432)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:709)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
    org.apache.webapp.admin.filters.SetCharacterEncodingFilter.doFilter(SetCharacterEncodingFilter.java:123)
```

root cause

```
java.lang.IllegalArgumentException: Invalid indexed property '? `MN   nVXG`  0kNv  W* : [ 6 t   c spk:    
pl
    M X*d   ?  P f m     h z T*X"   '
    org.apache.commons.beanutils.PropertyUtilsBean.getIndexedProperty(PropertyUtilsBean.java:326)
    org.apache.commons.beanutils.PropertyUtilsBean.getNestedProperty(PropertyUtilsBean.java:684)
    org.apache.commons.beanutils.PropertyUtilsBean.getProperty(PropertyUtilsBean.java:715)
    org.apache.commons.beanutils.BeanUtilsBean.setProperty(BeanUtilsBean.java:884)
    org.apache.commons.beanutils.BeanUtilsBean.populate(BeanUtilsBean.java:811)
    org.apache.commons.beanutils.BeanUtils.populate(BeanUtils.java:298)
    org.apache.struts.util.RequestUtils.populate(RequestUtils.java:493)
    org.apache.struts.action.RequestProcessor.processPopulate(RequestProcessor.java:805)
    org.apache.struts.action.RequestProcessor.process(RequestProcessor.java:203)
    org.apache.struts.action.ActionServlet.process(ActionServlet.java:1194)
    org.apache.struts.action.ActionServlet.doPost(ActionServlet.java:432)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:709)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
    org.apache.webapp.admin.filters.SetCharacterEncodingFilter.doFilter(SetCharacterEncodingFilter.java:123)
```

note The full stack trace of the root cause is available in the Apache Tomcat/5.5.17 logs.

Apache Tomcat/5.5.17

Conclusions

- Don't be afraid to write your tools for you apps (if I can do it...)

There are decent HTTP (and above) Java/Python APIs

- Consider all sources of data for generating testcases/attacks, not just external ones (spiders & proxies)

Exploit Java (and .NET ??) “XML-hell”