Note: We first **found** the **flag** the **non-intended way** with the same password to ftp as ssh.

We continued on the ip **10.162.20.88:8282** (**tomcat** server) in **/manager**, where we could **upload** a **war file**. We noticed that when **trying** to make a **reverse shell** we could **not get** a **netcat connection** to it when listening and it gave **no response**. We **could deploy .war files** to the **manager** and we tried **different versions** of a **reverse shell without success**.
We thought **maybe outbound connections** were **blocked**.
We **searched online** for some other **shell** code executables and **found** a **webshell**.

From here we got their code
https://gist.github.com/nikallass/5ceef8c8c02d58ca2c69a29a92d2f461 and used the commands **nano index.js** and **pasted** the code. Then **compiled** the code **into a .war** file with:
mkdir webshell
cp index.js webshell
cd webshell
jar -cvf ../webshellP1.war *
We **uploaded** the **war file** in the **tomcat server** and **deployed** it.

When going into **http://10.162.20.88:8282/webshell** here we **got** a **webshell** we could **execute commands remotely** on the **target machine** and **display** the **output on** the **website**. **Next** we **stacked two commands** so that the **webshell displayed** all the **directories** with the command:
cd C:\ & dir /s /b /o:gn
This **dumps all** the **files on** the **system** and **displays** them **on** the **webpage**. We then found the flag by doing **Ctrl+F** "**flag**" and **got** the **flags 4,5 and 6**.
Flag 6 we found was:
flag{cd699a4b257eb56c70b1037cc9ebeab7091b76a3a8d427}