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

For this flag we did a **nmap** scan on the network and on ip **10.162.20.88** and found alot of ports open there were several http ports open we checked them all and found a **tomcat** and **jserv**. The tomcat was hosted on port **8282** so we tried to access that through the **browser**. Then we did a **gobuster directory enumeration** scan with

gobuster dir -u http://10.162.2.88:8282 -w /usr/share/wordlists/dirb/common.txt -x php,html,txt -t 30

From this we found 2 notable results which were **/axis2** and **/manager**. We **first** tried **/axis2** and **managed** to **login** as **admin** on that, but that led **no further**. Then we **tried /manager** and **found** that we had to **login**. We tried some **default credentials** like **admin:admin** and **tomcat:s3cr3t**. Then we tried to do a **dictionary attack** on that with **hydra** with the command:

hydra -l admin -P /usr/share/wordlists/rockyou.txt -f http-get://10.162.2.88:8282/manager/html -t 30

From this we got the username and password **admin:123456**.
Now **inside** the **manager** we found **/hacktheplanet-816494cc2ba913de**
With the **inspect tool** we now found the **flag**
C:\ProgramData\Tomcat9\webapps\hacktheplanet-816494cc2ba913de**flag{90b353eb2d7f8360307a57d6ac171b5bc496467fde7beb}**.jpg