Challenge: Dancing Files

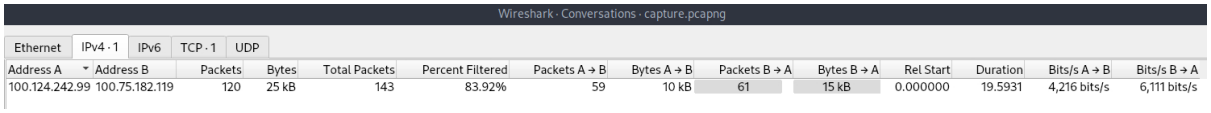
You are given a traffic capture, examine the traffic and find a way to access the cloud fileserver!

Answer: HTB{n3v4h_us3_s4mb4_w1th0ut_3ncrypt10n!!}

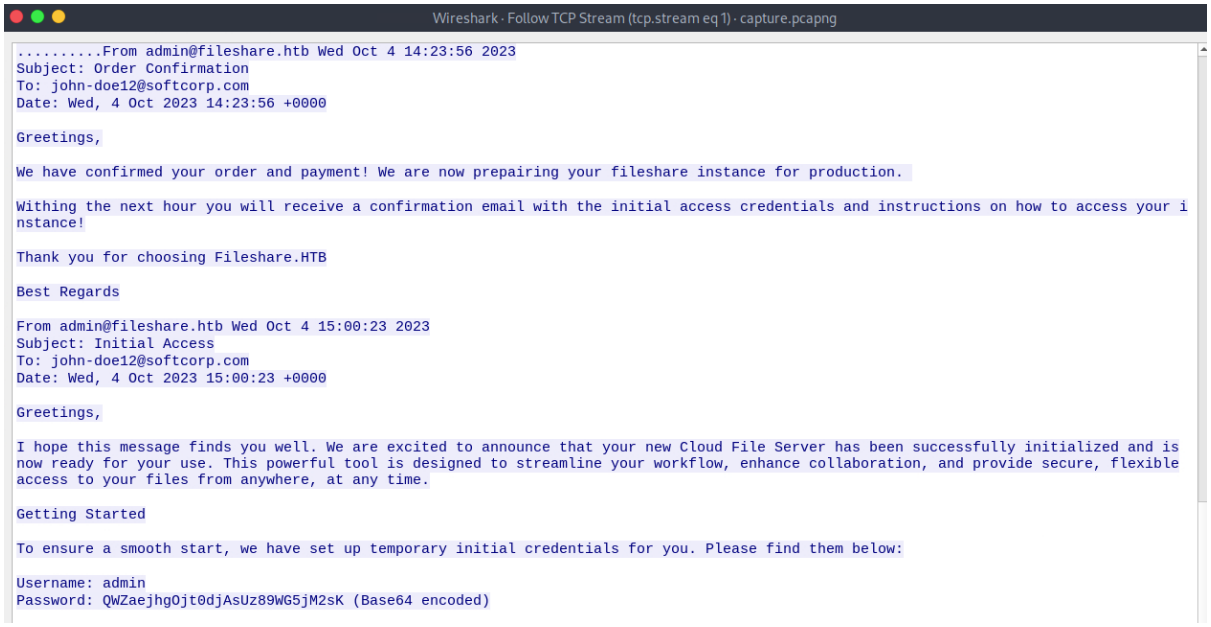
Procedure:

I got into the target and see that it is asking for a username and a password. The challenge also had a .pcap file which I could analyze on WireShark and I knew what I was looking for.

On wireshark on the conversations tab I knew that there was only 1 conversation:



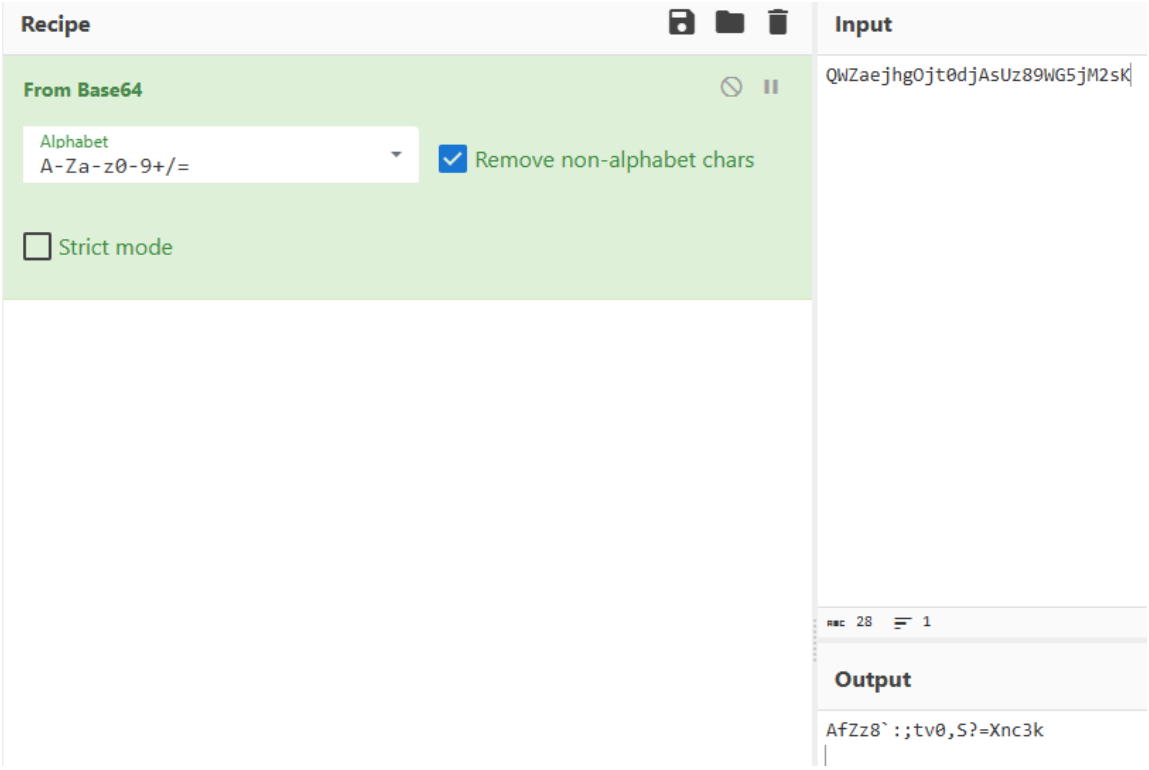
With this, I followed the TCP stream and at first everything seemed encrypted, however if you keep going down you could observe some clear text and found the credentials you are looking for:



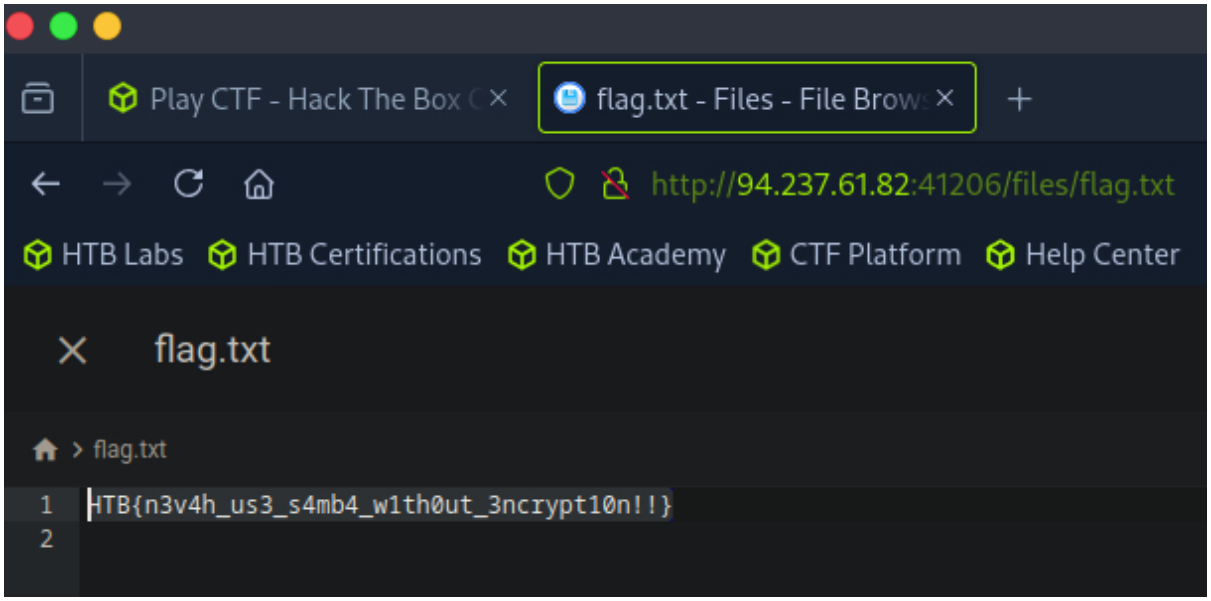
Username: admin

Password: QWZaejhgOjt0djAsUz89WG5jM2sK (but it says is Base64 encoded)

I put the password on cyberchef and got the following password:



So the real password is: AfZz8`:;tv0,S?=Xnc3k . With this, I already had the credentials to enter the page, and in there you can observe a flag.txt file with the flag:



Mitigation Strategy: To prevent credential leakage over the network, all authentication data should be transmitted exclusively over encrypted channels using HTTPS with properly configured TLS. Plaintext or weakly encoded credentials, such as those using Base64, must never be sent over the network, as they can be easily intercepted and decoded by attackers. Additionally, strong authentication practices should be implemented, including hashing passwords before storage and avoiding sending raw passwords over the network altogether. Regular network monitoring and penetration

testing should be conducted to detect any accidental exposures during development or deployment. By securing communication channels and adopting secure credential handling practices, the risk of credential theft through traffic capture can be effectively minimized.