

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:

Wireshark · Conversations · capture.pcapng													
Ethernet	IPv4 · 1	IPv6	TCP · 1	UDP									
Address A	Address B	Packets	Bytes	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
100.124.242.99	100.75.182.119	120	25 kB	143	83.92%	59	10 kB	61	15 kB	0.000000	19.5931	4,216 bits/s	6,111 bits/s

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:

```
Wireshark · Follow TCP Stream (tcp.stream eq 1) · capture.pcapng

.....From admin@fileshare.htb Wed Oct 4 14:23:56 2023
Subject: Order Confirmation
To: john-doe12@softcorp.com
Date: Wed, 4 Oct 2023 14:23:56 +0000

Greetings,

We have confirmed your order and payment! We are now prepairing your fileshare instance for production.

Withing the next hour you will receive a confirmation email with the initial access credentials and instructions on how to access your i
nstance!

Thank you for choosing Fileshare.HTB

Best Regards

From admin@fileshare.htb Wed Oct 4 15:00:23 2023
Subject: Initial Access
To: john-doe12@softcorp.com
Date: Wed, 4 Oct 2023 15:00:23 +0000

Greetings,

I hope this message finds you well. We are excited to announce that your new Cloud File Server has been successfully initialized and is
now ready for your use. This powerful tool is designed to streamline your workflow, enhance collaboration, and provide secure, flexible
access to your files from anywhere, at any time.

Getting Started

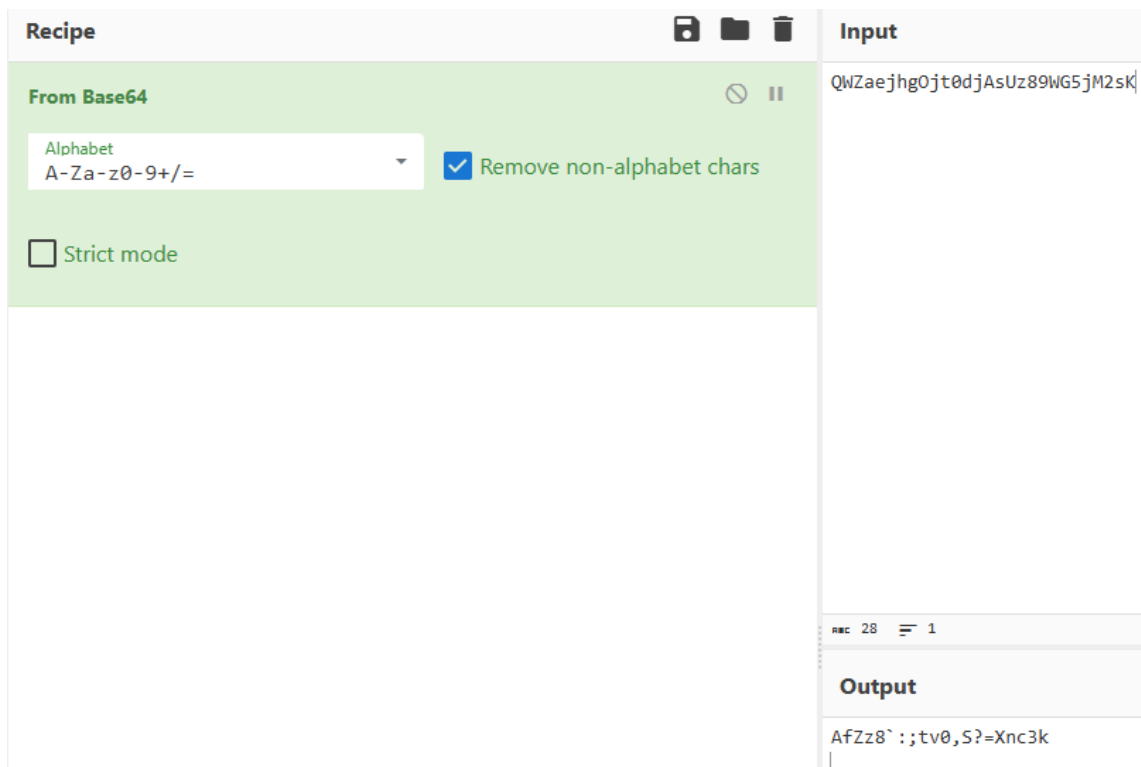
To ensure a smooth start, we have set up temporary initial credentials for you. Please find them below:

Username: admin
Password: QWZaejhgOjt0djAsUz89WG5jM2sK (Base64 encoded)
```

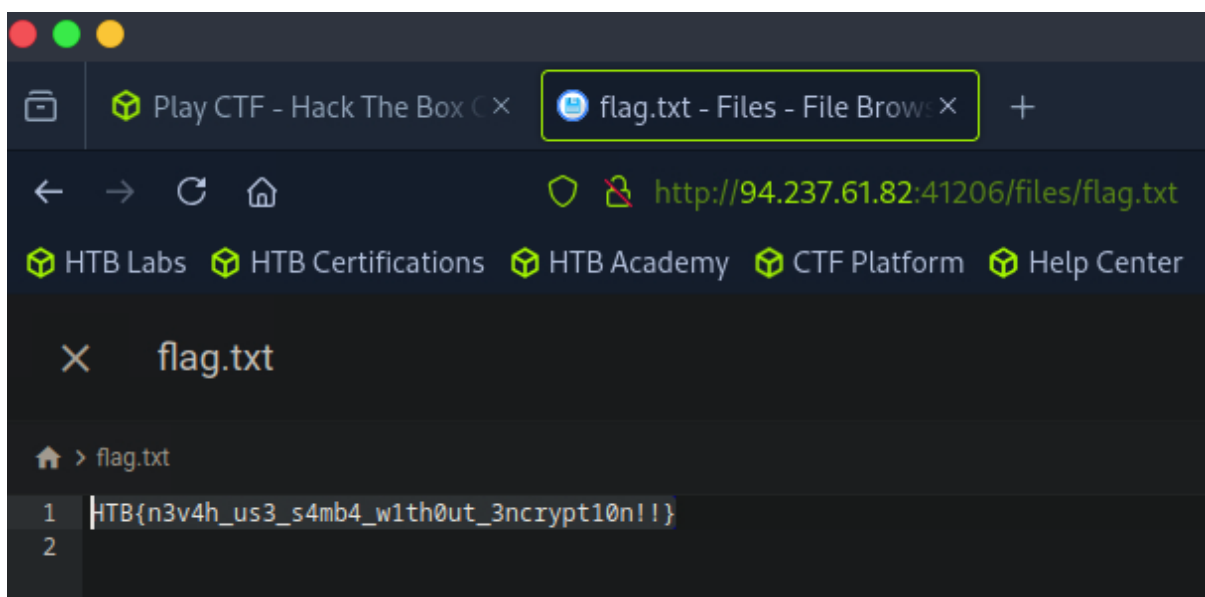
Username: admin

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.