HackTheBox – Market Dump Write Up

Tools:

- Wireshark (Kali Linux)
- CyberChef (https://gchq.github.io/CyberChef/)

Walkthrough:

Step	Description
1	The file extracted from the zip file is "MarketDump.pcapng".
2	Wireshark was used to analyze the pcap file.
3	Upon inspecting the TCP stream of a specific packet, there was a list of American Express card numbers found but one card number was encrypted.
4	The encrypted text was decoded in CyberChef by using the Magic method. After decrypting the cipher text, the flag was obtained and found to be decoded from Base58.

Flag is HTB{Please decrypt yourself}