Simple XOR & 46esab CTF Writeup

This document is a walkthrough on one way to solve the **Simple XOR & 46esab CTFs** on **TheBlackSide**. The goal is, not only to give the solution, but also to emphasise the importance of thorough reading of the challenge's title and description.

General Information

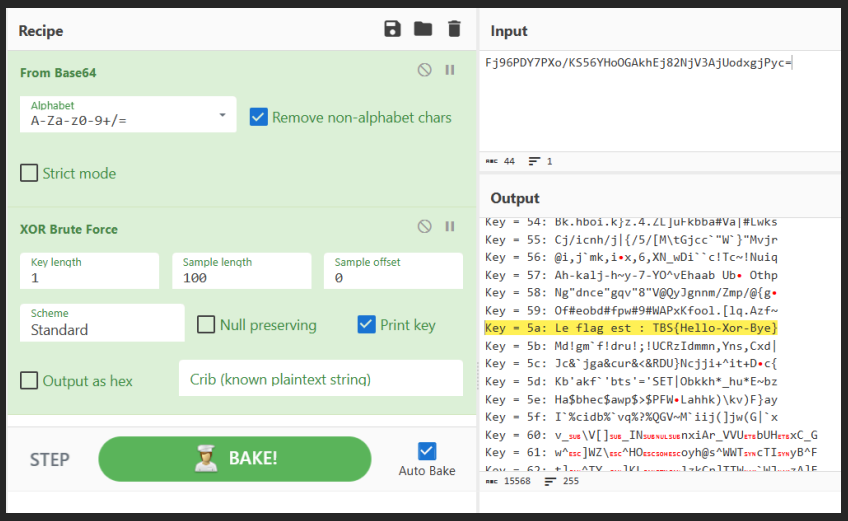
- *Difficulty:* Easy
- *Category:* Cryptography
- *Link:* Simple XOR - TheBlackSide and 46esab - TheBlackSide

Solution

"A secret piece of data has been XOR'd with a 1-byte key. Find the data in plain text!"

We have a 1-byte key (ex: 00100010), which we don't know, but we know that there are 256 possibilities, and it looks like the text ***"Fj96PDY7PXo/KS56YHoOGAkhEj82NjV3AjUodxgjPyc=",*** has been XOR'd. Now, the XOR operator is reversible, meaning that with the same key we can get the secret message.

However, brute-forcing the XOR operation on all 256 keys on the text will not give us the flag. What we have to do is carefully read the challenge's description; *"a **SECRET** piece of data has been XOR'd"* This suggests that the text underwent a second encryption process, likely using a Base64 algorithm.



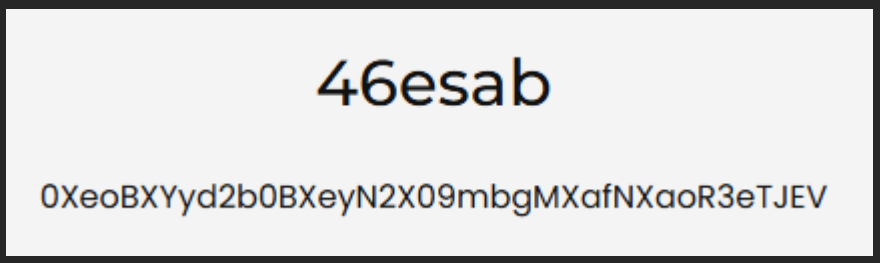
Using Cyberchef, an online cryptographic tool, we get the following flag: **Hello-Xor-Bye**

Friendly Reminder

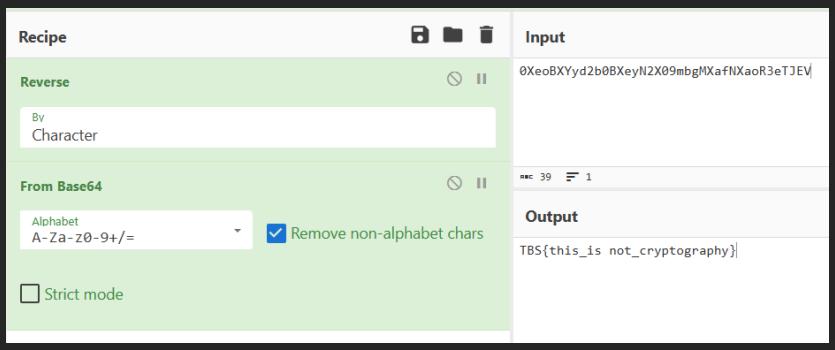
READ THE CHALLENGE TITLE & DESCRIPTION CAREFULLY !!!

Although this challenge was pretty simple, it serves as a prime example of how **hidden details** in the title/description can be pivotal to finding the solution.

Let's give another example. Here's another challenge on **TheBlackSide**:



Looking closely, **"46esab"** is **"base64"** in reverse
This suggests that the flag was most likely reversed after being encrypted using the base64 algorithm. That being said, the title tells us all we need to know to complete the challenge.



We get the following flag: **TBS{this_is not_cryptography}**