CryptoVault Web + Crypto Challenge Writeup

Challenge Overview

CryptoVault is a web application claiming to securely store encrypted messages. The hint suggested an old trick, indicating classic vulnerabilities.

Step 1 – Explore the Web App

Accessing the homepage revealed a login button redirecting to /login with a username and password form.

Step 2 – SQL Injection Bypass

Using the payload admin' -- in the username field bypassed authentication and logged in as admin.

Step 3 – Retrieve Encrypted Notes

The admin panel revealed Base64 encoded encrypted messages for multiple users.

Step 4 – Identify Encryption Layers

First layer was Base64 decoding. The second layer was a repeating XOR cipher.

Step 5 – Decrypt Messages

Using known plaintext SECE{ revealed the XOR key CryptoVault2025. Decrypting all messages revealed the final flag.

Final Flag

SECE{w3lc0m3_t0_th3_cr7pt0_v4ult_0f_s3cr3ts_4nd_h1dd3n_m3ss4g3s_m4st3r_h4ck3r}

Techniques Used

SQL Injection, Base64 decoding, XOR cryptanalysis, known plaintext attack.

Lessons Learned

Base64 is not encryption, repeating XOR is weak, and old web vulnerabilities still work.