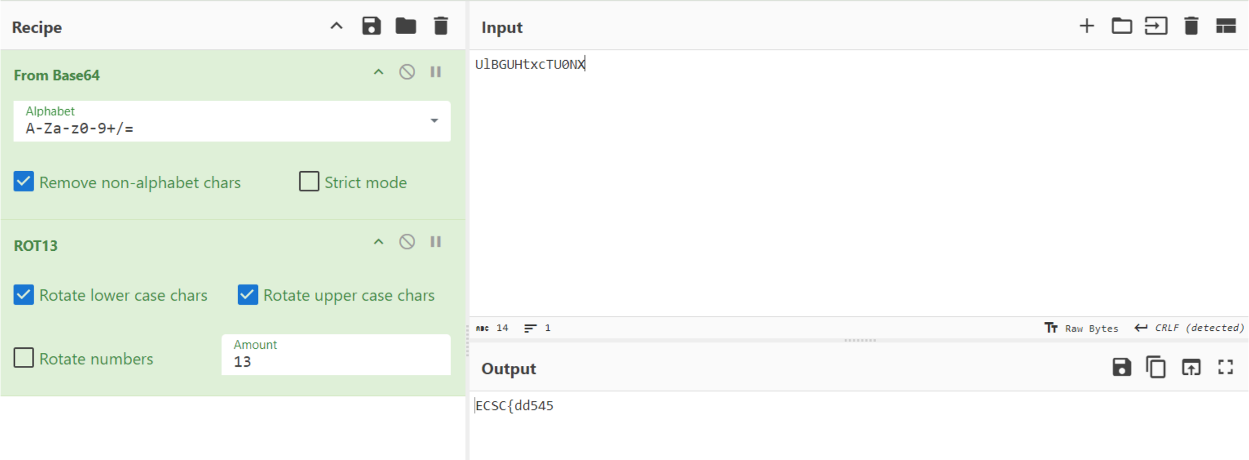
After looking through the capture, we see there is some http traffic so we export all HTTP objects and start investigating them. After reading the file called crypto we realize that TxTWizard is used, which is a website that performs encryption entirely in your browser. No data is transmitted to any server, so the encryption data must be somewhere around these files.

After looking through the PKCS5 files we see they contain plaintext data. In PKCS5(6) we see that the plaintext is a base64-ish string, so we play arounf a bit in cyberchef:



Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

ROT13

☑ Rotate lower case chars ☑ Rotate upper case chars

☐ Rotate numbers

Amount
13

Input

```
UlBGUHtxcTU0NX
```

Output

```
ECSC{dd545
```

Eureka! We found part of the flag. To extract all the flag data, we use “**grep -hoP 'plainText=.*?&' stuff/* | sed 's/plainText=//; s/&//' | tr -d '\n'**” to extract what is between plaintext= and &. Some extra data is also extracted, so we need to delete a bit of to obtain the flag. Also, if you decode the flag but it is not accepted, make sure you delete the part that appears twice, “f744a3573b1dc0bc53cec201f50f95c8520bec9”.

Made with love by: AndreiCat