El siguiente contenido está publicado con fines académicos y de concienciación. No nos hacemos responsables de las actividades que se lleven a cabo con la información mostrada a continuación.

El siguiente post forma parte de una serie de posts dedicados a mostrar las soluciones a los retos presentados en el **Evento de CiberSeguridad de Secuma 2018** celebrado en **Málaga el 15 de Noviembre de 2018.**

Cabe destacar que vamos a proceder a publicar el código fuente de cada uno de los retos (de los retos de Web) para que todo el mundo pueda bajárselo, modificarlo y conseguir así customizarlo a su gusto para lograr nuevas variantes procedentes del mismo reto que puedan inspirar a la creación de nuevos retos y/o soluciones. Así que estar atentos al **Gitlab**.

Tan sólo pedimos que siempre que se modifique el código se mencione al autor del mismo así como que se ponga a disposición del público el resultante. Dicho esto vamos a proceder a explicar, de forma detallada los pasos que seguimos así como consejos que puedan ayudar al lector y/o aclarar conceptos. Empecemos!

Cl4s1c P4r4n01d

150

"Tenemos que ayudar a la agente DiPierro, ha conseguido interceptar 3 mensajes de algunos usuarios, pero cada uno usa un cifrado distinto. ¿Puedes ayudarla? Se encontró un texto sin cifrar que decía: La **union** es la clave."

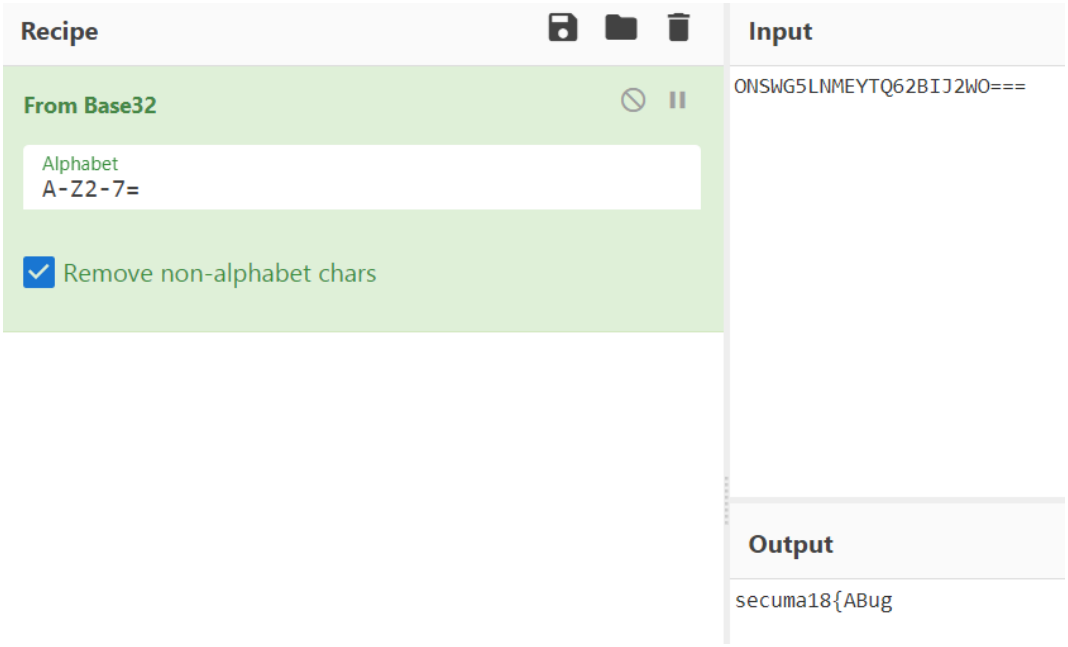
BAnkS: ONSWG5LNMEYTQ62BIJ2WO===

irVInG: Cf_V3j3eDhah_n

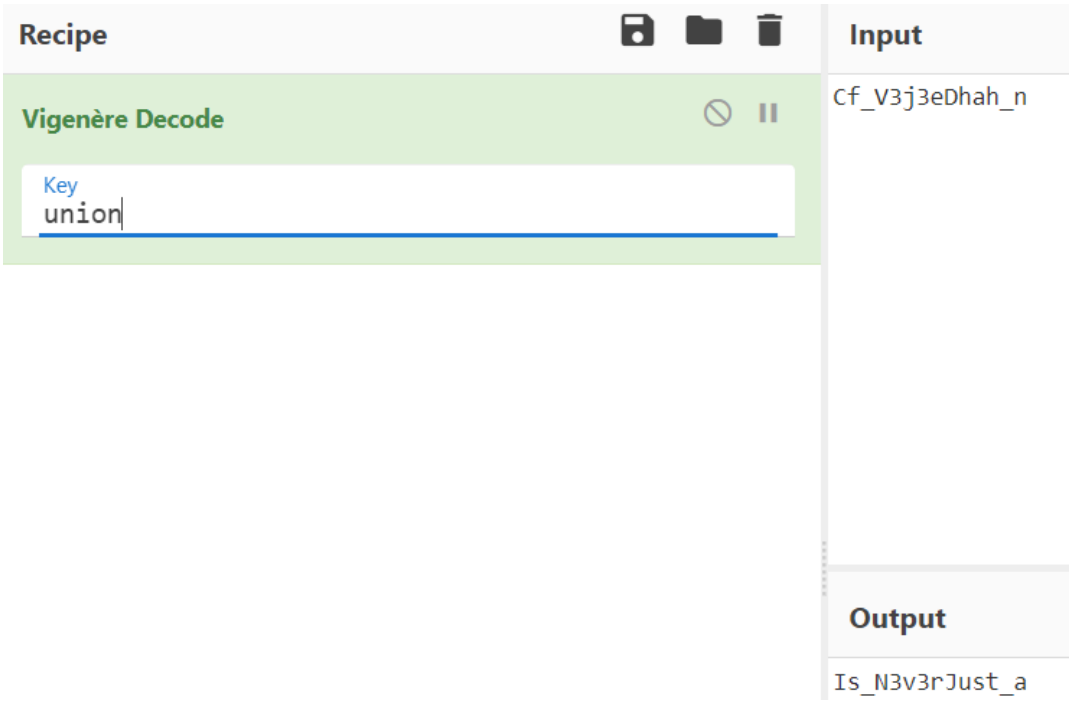
RObоT: _K1qryi3}

En este reto podemos ver tres mensajes cifrados, se nos dice que cada uno usa un cifrado distinto y en cada uno de ellos al principio hay como unos nombres con ciertas letras en mayúscula, que pueden ser pistas para descifrar cada uno de ellos.

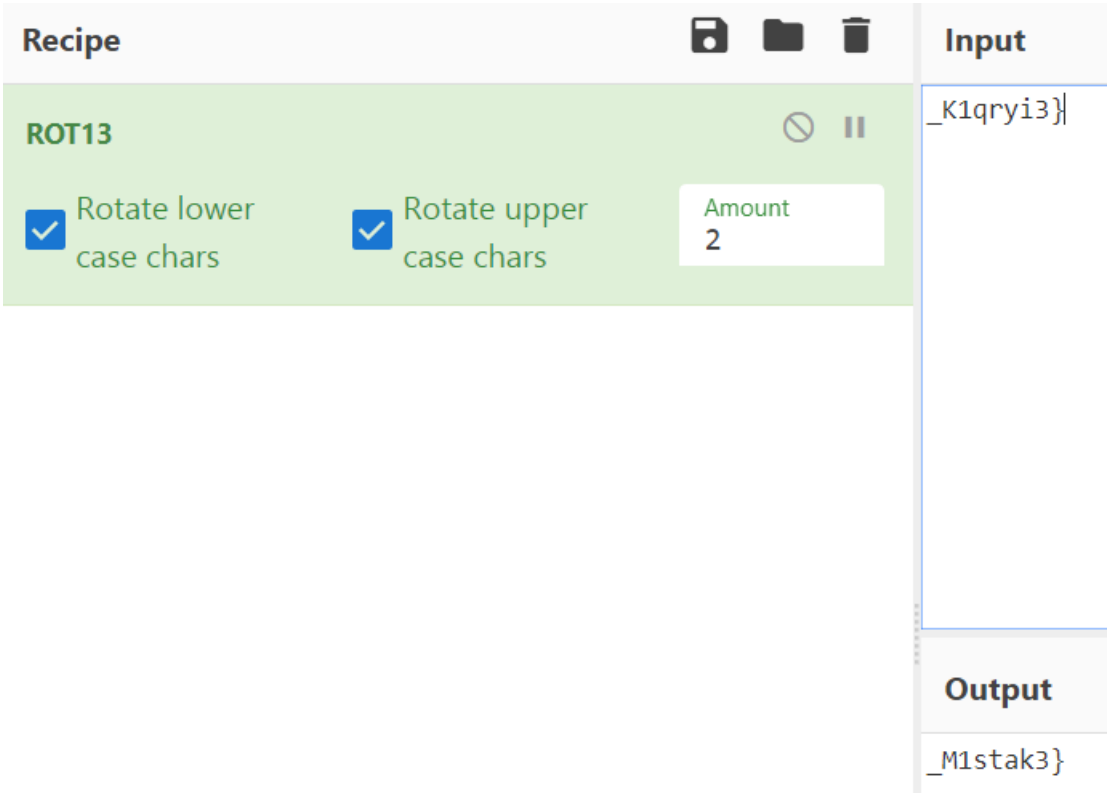
Si nos fijamos en el nombre del primer mensaje las letras en mayúscula forman **BAS**, por lo que podemos pensar, viendo el formato del mensaje cifrado, que puede tratarse de un **base64**, al comprobarlo vemos que no tiene mucho sentido (**8Ô...Í0F.C.. ..**<), decido probar con otras bases y finalmente con **base32** obtenemos lo que parece ser el principio de una flag, por lo que el resto de la flag deben ser los otros dos mensajes.



Del nombre del segundo mensaje destaca **VIG**, y eso nos recuerda al cifrado **Vigenere**, para este tipo de cifrado, necesitamos conocer una **clave**, si volvemos al enunciado, la última frase decía que *la **union** es la clave*, probamos a descifrar con la clave '**union**' y obtenemos otra parte de la flag.



Para finalizar este reto, en el último mensaje, tenemos en mayúsculas **ROT**, por lo que intuimos que debe ser algún tipo de rotación, lo normal que se suele probar es **Rot13** pero al ver que no llegamos a un mensaje con algo de sentido, probamos distintas rotaciones y hasta dar con algo que parece tener sentido utilizando **Rot2.**



Simplemente queda unir los 3 fragmentos de la FLAG!:
secuma18{ABugIs_N3v3rJust_a_M1stak3}

Para la realización de los retos nos hemos servido de la herramienta
https://gchq.github.io/CyberChef/

Espero que os haya gustado ;)
by **@Verdej0**