Category:

MISC

Name:

Hash

Message:

A team of cybercriminals was recently busted, but before that they managed to delete an entire directory containing vital information. However, law enforcement managed to recover the directory compressed as deleted_files.zip with 100 text files inside. Also, 3 mysterious hash values were left behind by the bad guys.

- 6cff6c25e4198e2b26fb5c7118694092ada6bdc7ef1a344b86d36929cd2d40f5
- 5aa6d31bc63069d9e85f810a14d96e085d822b06b7de9516599aa3d209ba9614
- ae6448234393c9ccf7895c0b98e52dac65248eda15016b4b247e3fb1ef1087e3

Your mission is to identify the files that match these hash values and then retrieve the hidden flag they've tried so hard to conceal.

Hint:

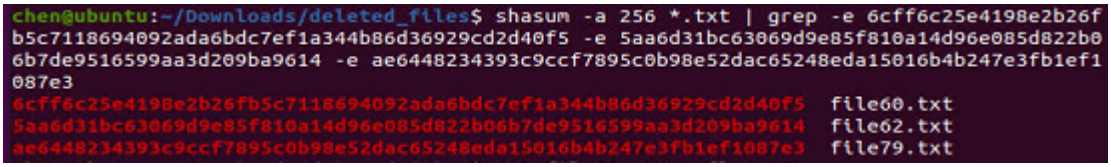
- The hash values provided use a common cryptographic algorithm.
- Found the matching files with the given hash values? Decoding tools like CyberChef may help with the last step!

Objective:

Identify the three files in deleted_files.zip that match the given hash values, combine the strings found in each file, decode the base64-encoded string, and reveal the flag.

Instructions:

1. Extract the deleted_files.zip archive to get the 100 text files. The challenge provides three hash values but doesn't specify which hashing algorithm is used. The hash values are 64 characters long, which is a typical length for SHA-256 hashes.
2. To find the files that match the given hashes, you need to calculate the SHA-256 hash of the files with the provided hash values. the result shows that the matching files are file60.txt, file62.txt and file79.txt.



3. Once you've identified the three files, open each one and locate the flag fragment within. The combined string "Q1NHX0ZMQUd7aDRzaF9icm93bnNfd2l0aF9vbmlvbnNfNF9icmU0a2Y0c3R9" is a base64-encoded message. Finally decode the message to get the flag! Online decoders such as CyberChef should help you in this process.

Flag is:

CSG_FLAG{h4sh_browns_with_onions_4_bre4kf4st}