Hash Fun

BACKGROUND

Hashing passwords is a relatively secure way to store credentials for users. An MD5 hash is an algorithm that converts a string into a 128 bit value. MD5 used to be a popular hashing algorithm, but has been found to be susceptible to several different attacks[1].

This lab will explore MD5 because it is easier to crack than more modern hashes like SHA3-256.

MD5 reverse for

`fbd1baa2d62ce5761cce36b9e4143c0f`

The MD5 hash:

`fbd1baa2d62ce5761cce36b9e4143c0f`

was successfully reversed into the string:

[illegible]

REQUIREMENTS

A web browser.

PART I: Create an MD5 hash of a string that would be easy to crack

1. Go to https://www.md5hashgenerator.com and enter a fairly simple string to convert to an MD5 hash. The intent of this part of the lab is to generate a hash that is easy to break, so using a well-known password or simple phrase is sufficient.

   Take a screenshot of your hash (make sure it shows the original phrase and also the hash).

EVIDENCE #1

Your Hash: **0f359740bd1cda994f8b55330c86d845**
Your String: p@ssw0rd

Use this generator to create an MD5 hash of a string:

PASTE THE IMAGE OF THE STRING AND THE HASH

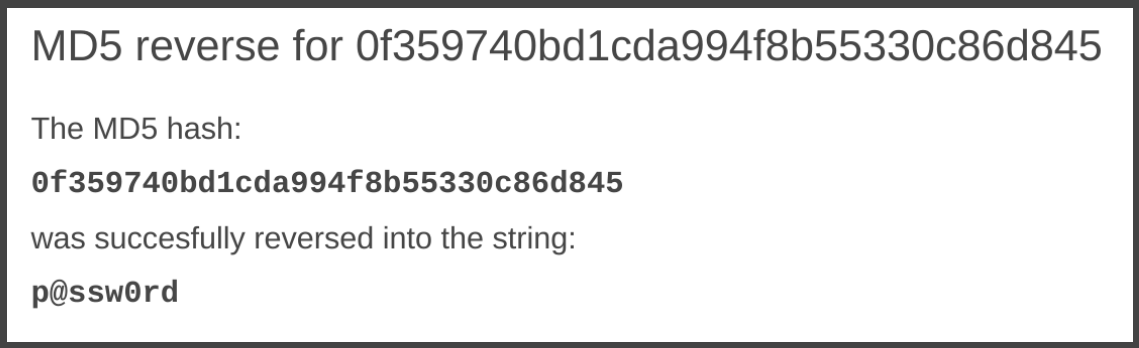
[1] MD5 [Wikipedia]

PART II: Use a reverse lookup tool to crack the hash

1. Copy the hash into your clipboard.
2. Go to https://md5.gromweb.com and paste it in, then run a reverse lookup. If the hash you created from your string is easy to crack, you will see the result here. If you were unsuccessful in the reverse lookup, try again (but save your work because you can use it for the next part of the lab).

   Take a screenshot of the hash and the reverse lookup and paste it below.

EVIDENCE #2



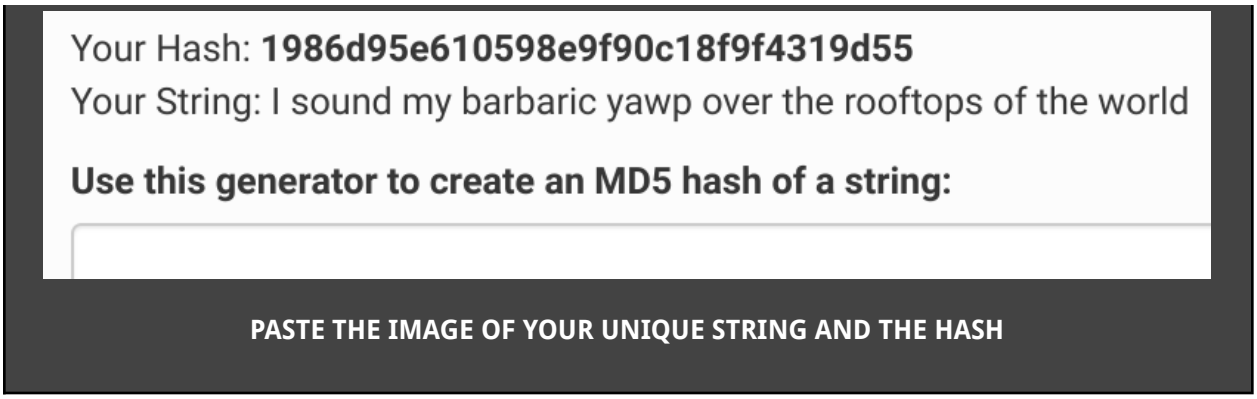
PASTE THE IMAGE OF THE HASH AND THE REVERSE LOOKUP

PART III: Create an MD5 hash of a complex phrase

1. Head back to https://www.md5hashgenerator.com and enter a complex string that probably would not appear on a rainbow table and convert it to an MD5 hash. The intent of this part of the lab is to create a hash that is impossible to crack.

   Take a screenshot of your hash (make sure it shows the original phrase and also the hash).

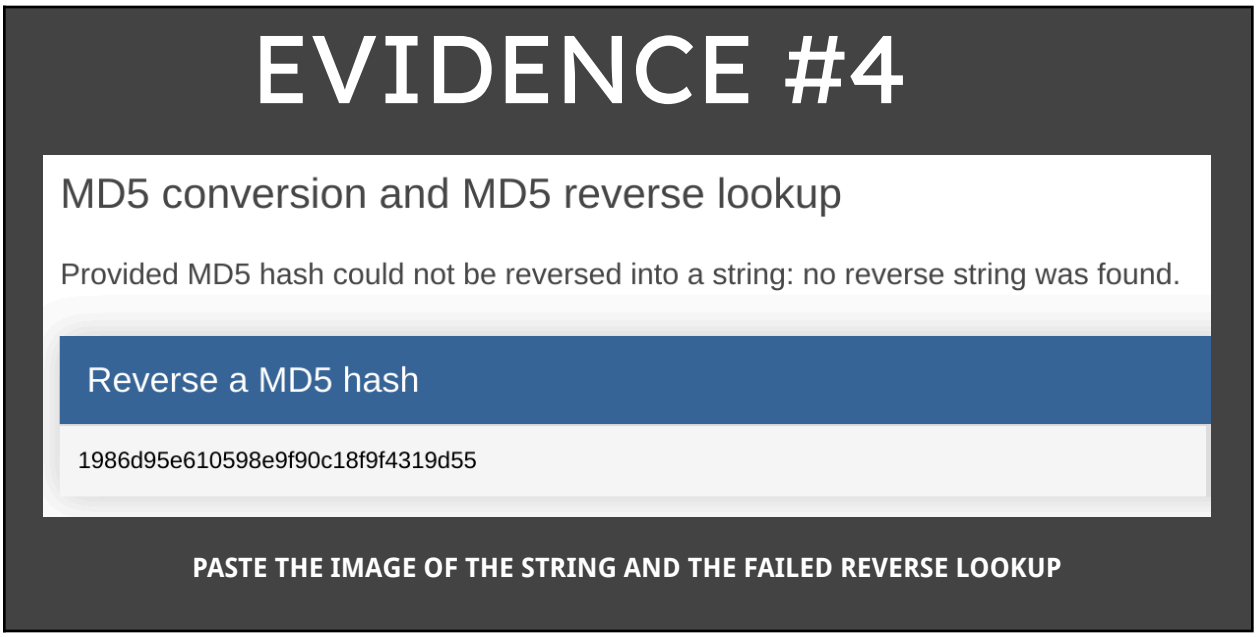
EVIDENCE #3



PART IV: Attempt a reverse lookup on a sophisticated hash

1. Copy the new hash into your clipboard.
2. Go to https://md5.gromweb.com/ and paste it into the field. Hopefully, you will not be able to crack it.

   Take a screenshot of the hash and the failed reverse lookup and paste it below.



CONCLUSION:

Does this mean that there are some MD5 hashes that cannot be reversed? Well, maybe. Maybe not. It's very likely that the rainbow table used at the reverse lookup site is not as robust as other ones. In fact, some rainbow tables can be over 500 GB large (this site has massive amounts of rainbow tables).

Does this mean that a very sophisticated string that is hashed with MD5 can never be cracked? Well, probably. But that doesn't mean that if your password is a long, unique phrase that your account is safe. This thread at StackOverflow is pretty insightful and talks to the theory that

there is very likely other strings that would reduce to your same hash, so as long as bad actors try a sufficient (read: super large) of attempts, they could conceivably crunch a string down to the same hash as your sophisticated, unique, long string (hashed). In this scenario, the bad actors won't have your password, but they'll have a password that hashes to your password's hash, which is just as good (for them).