**Easy Hacking Challenge**: Take information out of an SQL table using a well-crafted search

1. **SQL Injection**

The HTML page has a search bar that you can use to access the SQLite “search” table. The table has info in it. You can search it through this search bar.

|  |  |
| --- | --- |
| search | answer |
| How long is a marathon? | 26.2188 miles |

An SQL query looks like this:

*SELECT \* FROM tables WHERE answer=’How long is a marathon?’*

SQL Injection works by exploiting the structure of the SQL search query. You can use **--** to comment out code or use **‘** to change the search query’s structure. By saying OR 1=1 or something similar, you can select all the contents of a table.

Example 1: *SELECT \* FROM tables WHERE answer=’’ OR ‘1’=’1*

Example 2: *SELECT \* FROM tables WHERE answer=’’ OR 1=1--*

Try SQL injection from the search bar on the computer.

1. **MD5 Hash Decryption**

Once you get the MD5 hash from the SQL table, you can try to find out what it means.

MD5 hash is 128 bits of encrypted nonsense to the naked eye. Ex: *5f4dcc3b5aa765d61d8327deb882cf99 = “password”*

You can decode it by comparing the MD5 hash to a list of common passwords. This website can do it for you for some MD5 hashes:

<https://md5decrypt.net/en/>

Try it out.

**(Optional) hashcat:**

You can also try to decrypt this hash using a CMD tool called hashcat and a dictionary/wordlist called rockyou.txt

echo '*5f4dcc3b5aa765d61d8327deb882cf99*' >> hashes.txt

hashcat -a 0 -m 0 hashes rockyou.txt