

# Changing hash values to Passwords

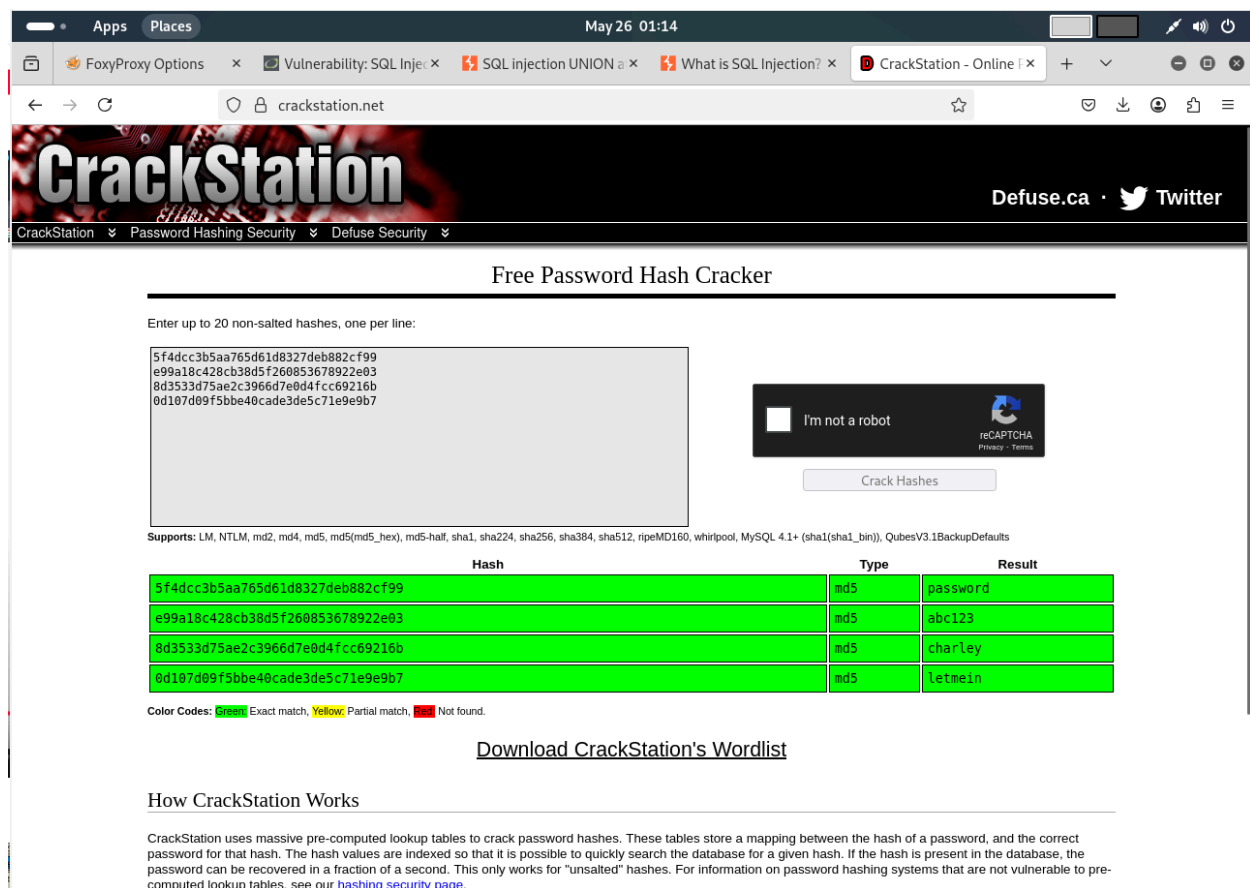
## Optional:

To convert the obtained hash values into readable passwords there are many ways like using inbuilt methods like John the ripper, hashcat, etc

To make things easier I used an online hash decoder

[Crackstation.net](https://crackstation.net)

Just copy the hashes into the online web of crackstation and enter and it will crack the hashes



The screenshot shows the CrackStation website interface. At the top, there's a navigation bar with the CrackStation logo and links to Defuse.ca and Twitter. Below the navigation bar, the main heading is "Free Password Hash Cracker". A text input field contains five MD5 hashes. To the right of the input field is a reCAPTCHA widget. Below the input field, a table displays the results of the cracking process. The table has three columns: Hash, Type, and Result. The results show that all five hashes were successfully cracked into passwords. Below the table, there's a legend for color codes: Green for Exact match, Yellow for Partial match, and Red for Not found. At the bottom, there's a link to "Download CrackStation's Wordlist" and a section titled "How CrackStation Works" which explains the site's methodology.

Enter up to 20 non-salted hashes, one per line:

```
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
```

I'm not a robot

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password
e99a18c428cb38d5f260853678922e03	md5	abc123
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

[Download CrackStation's Wordlist](#)

### How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our [hashing security page](#).