

SQL2



HOME SURVEY MEMBERS

```
ID: -1 UNION SELECT 1, countersign FROM users limit 3, 1
First name: l
Surname : 5ff9d0165b4f92b14994e5c685cdce28
```

SEARCH MEMBER BY ID:



SUBMIT

The screenshot shows the CrackStation website's password cracking interface. At the top, there are navigation links: CrackStation, Password Hashing Security, and Defuse Security. On the right, there are links to Defuse.ca and Twitter. The main title is "Free Password Hash Cracker". Below it, a text input field contains the hash "5ff9d0165b4f92b14994e5c685cdce28". To the right of the input field is a reCAPTCHA verification box with the question "Je ne suis pas un robot". Below the input field, there is a note about supports: "Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(shat_bin)), QubesV3.1BackupDefaults". A table below shows the cracked hash: Hash (5ff9d0165b4f92b14994e5c685cdce28), Type (md5), and Result (FortyTwo). A legend at the bottom indicates color codes: green for Exact match, yellow for Partial match, and red for Not found. A link "Download CrackStation's Wordlist" is also present.

L'application concatène directement l'entrée utilisateur (le paramètre id) dans la chaîne de requête SQL, sans vérification ni échappement.

Remédiation :

Forcer à ne traiter que des nombres entiers et positifs.