

File Actions Edit View Help

```
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5 hash.txt
```

Unknown ciphertext format name requested

```
(kali@kali)-[~]
```

```
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=dynamic=md5($p) hash.txt
```

Dyna expression syntax error around this part of expression

md5(): System

Invalid token found

exiting now

```
(kali@kali)-[~]
```

```
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5 hash.txt
```

Unknown ciphertext format name requested

```
(kali@kali)-[~]
```

```
$ john --wordlist[]=/usr/share/wordlists/rockyou.txt hash.txt
```

Unknown option: "--wordlist[]=/usr/share/wordlists/rockyou.txt"

```
(kali@kali)-[~]
```

```
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5 hash.txt
```

Unknown ciphertext format name requested

```
(kali@kali)-[~]
```

```
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5 has
```

Unknown ciphertext format name requested

```
(kali@kali)-[~]
```

```
$ john --format=raw-md5 hash.txt
```

Using default input encoding: UTF-8

Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])

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

Proceeding with single, rules:Single

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

Almost done: Processing the remaining buffered candidate passwords, if any.

Proceeding with wordlist:/usr/share/john/password.lst

password (?)

abc123 (?)

letmein (?)

Proceeding with incremental:ASCII

charley (?)

4g 0:00:00:00 DONE 3/3 (2024-02-28 17:39) 11.42g/s 509022p/s 509022c/s 510668C/s stevy13..chertsu

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

Session completed.

```
(kali@kali)-[~]
```

```
$
```

Damn Vulnerable Web

Not secure 192.168.51.101/damn-vulnerable-web/sql/md55E6...

## Vulnerability: SQL Injection

User ID:

### More info

<http://www.securiteam.com/securityreviews/5DP0W1P70E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout