28 FEBBRAIO 2024

REPORT - EPICODE

S6L3

PRESENTED BY

Alessandro Marasca

PASSWORD CRACKING

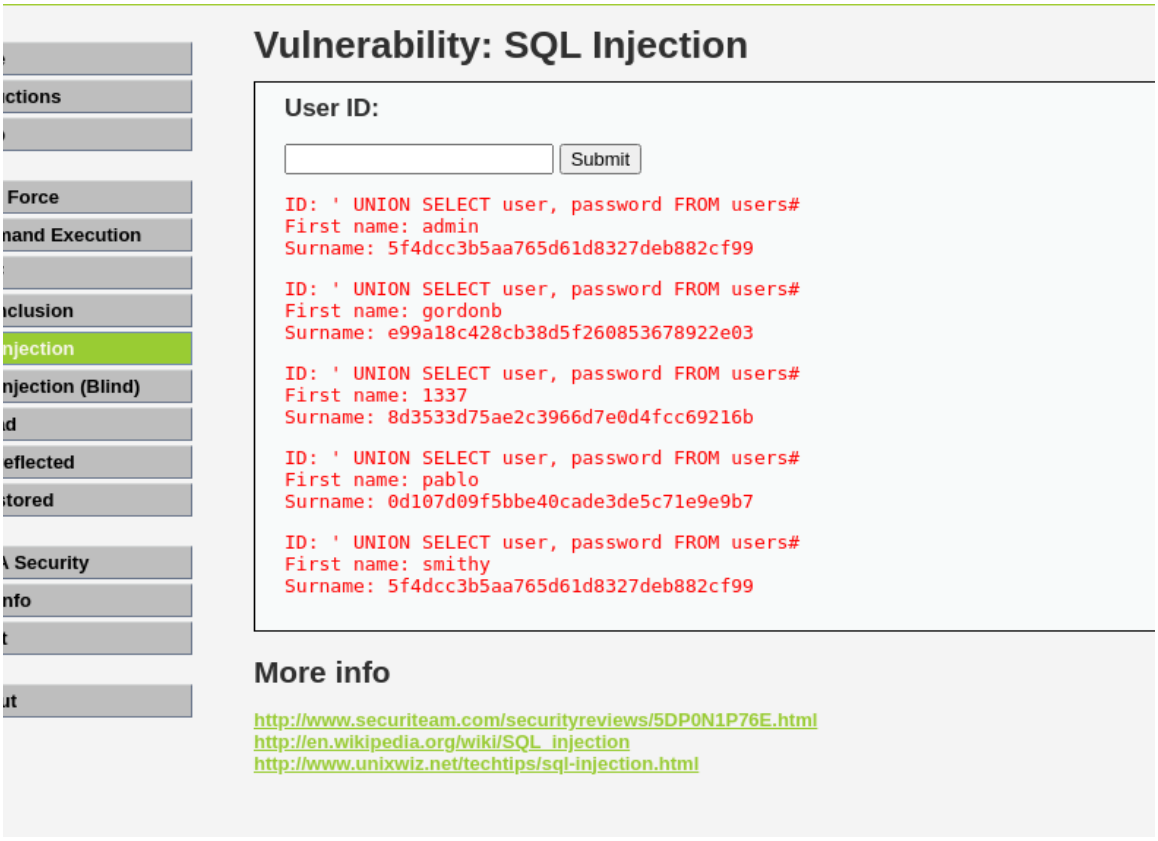
Traccia

Se guardiamo meglio le password, della lezione precedente, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5. Recuperate le password dal DB e provate ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro.

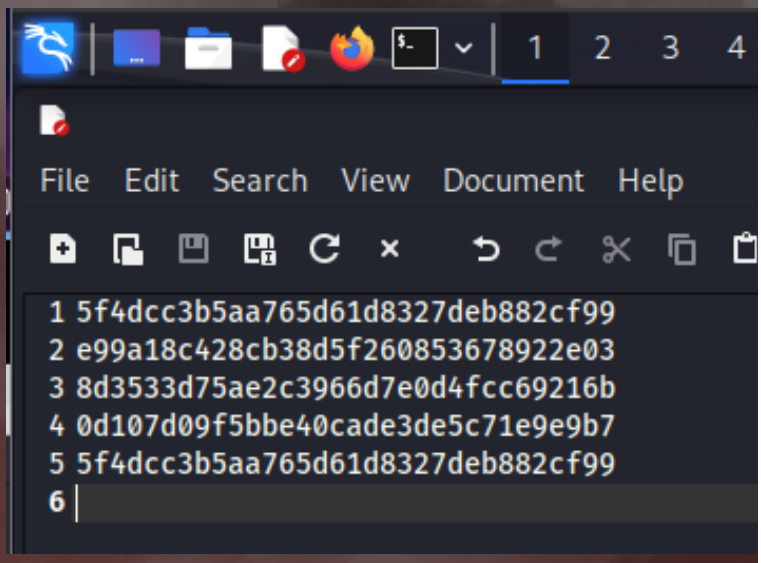
Sentitevi liberi di utilizzare qualsiasi dei tool visti nella lezione teorica.

L'obiettivo dell'esercizio di oggi è craccare tutte le password.

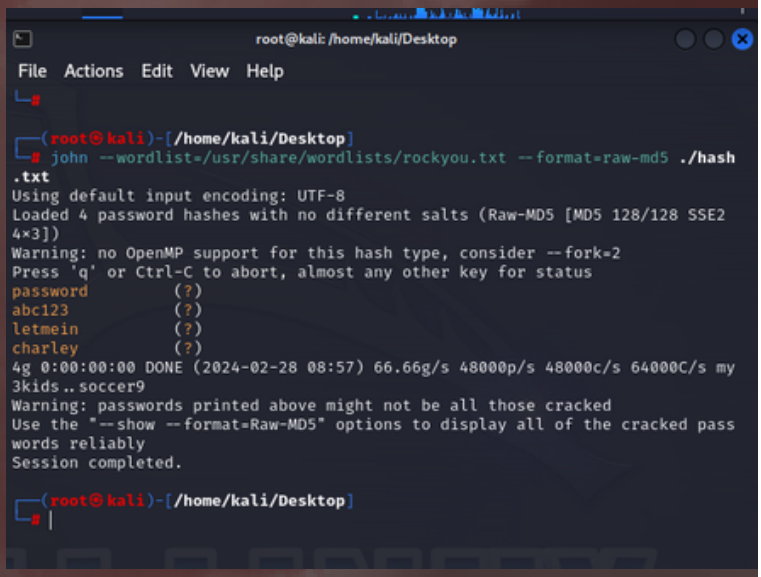
SQL INJECTION



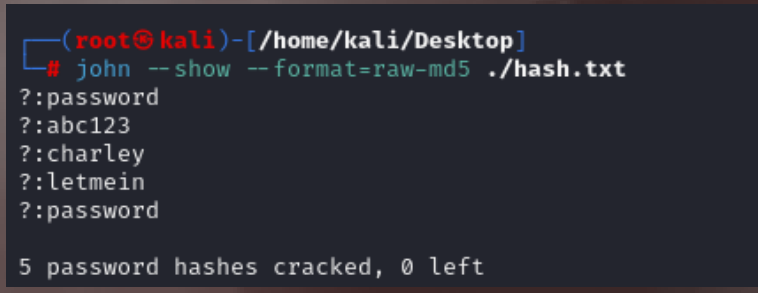
Andiamo ad inserire il sql injection per ricavare le password criptate.
Come vediamo la prima e l'ultima coincidono.



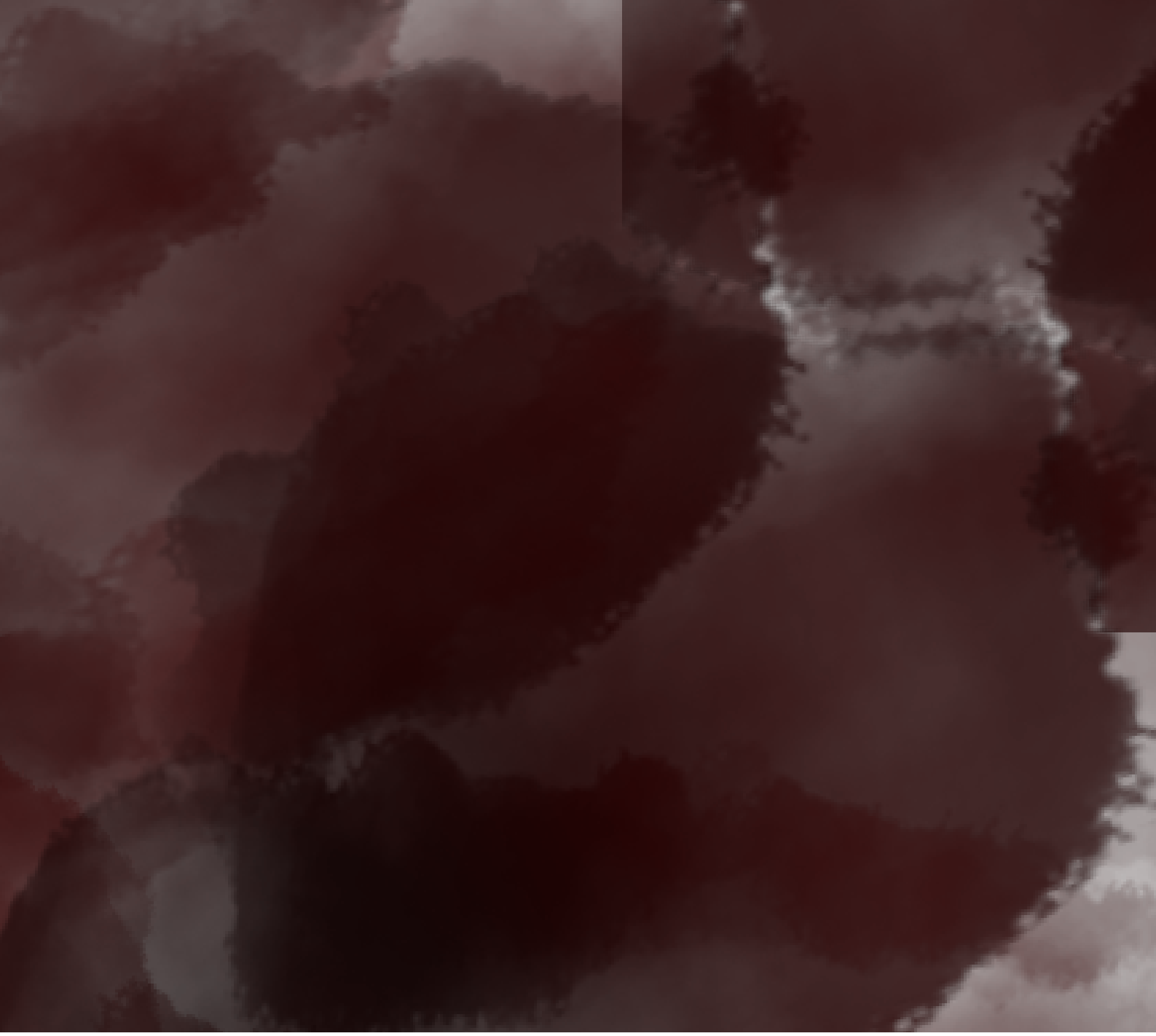
Salviamo le encrypted pwd in un file di testo.



Dopo aver unzippato il rockyou (file di testo che contiene le chiavi di lettura come la md5) diamo il relativo comando di **john** per svelare le pwd.



Infine col comando riportato nello screenshot osserviamo tutte le password inizialmente criptate, ora chiaramente leggibili.



Alessandro Marasca

Epicode

S6L3- CS0124

28 FEBBRAIO 2024