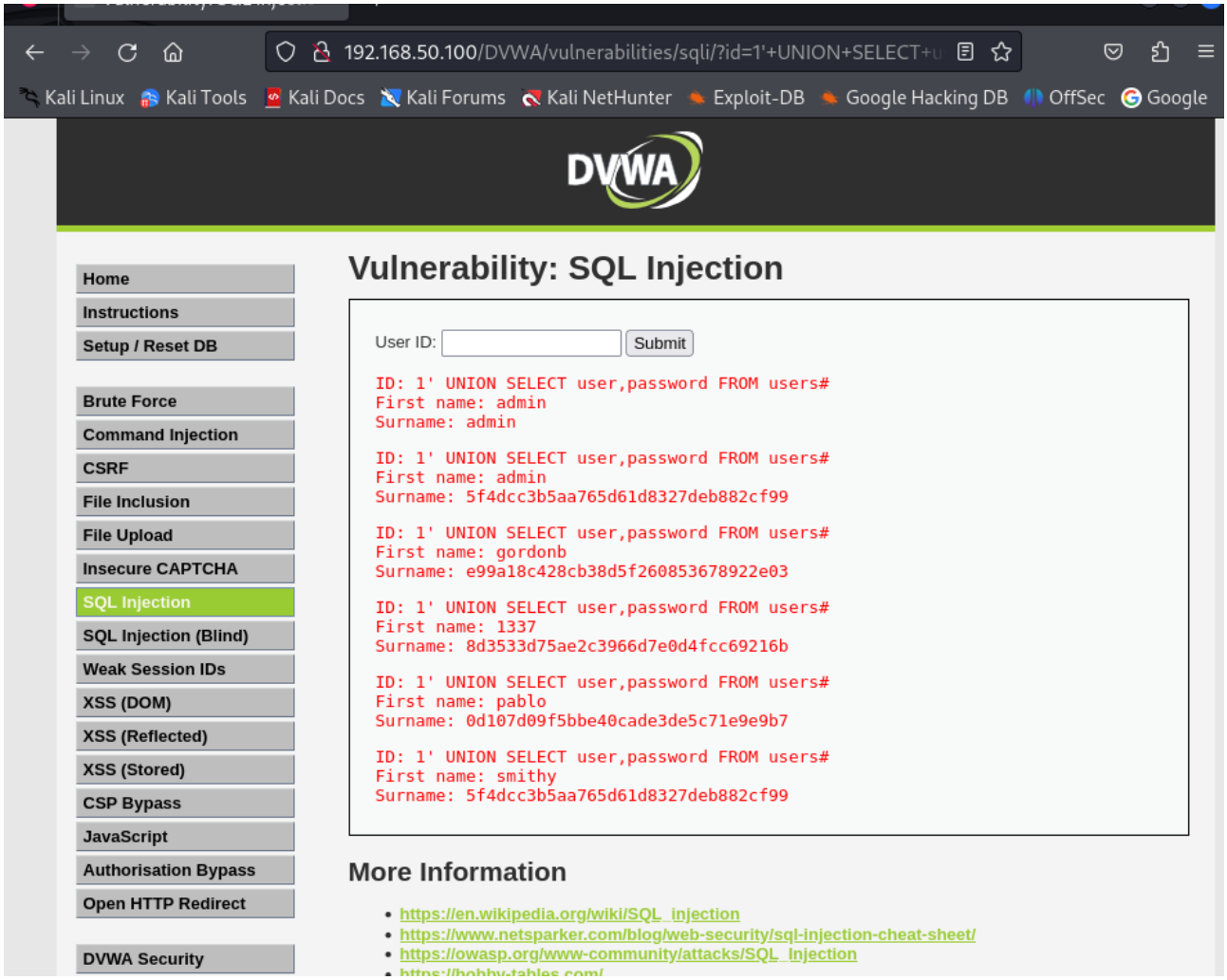
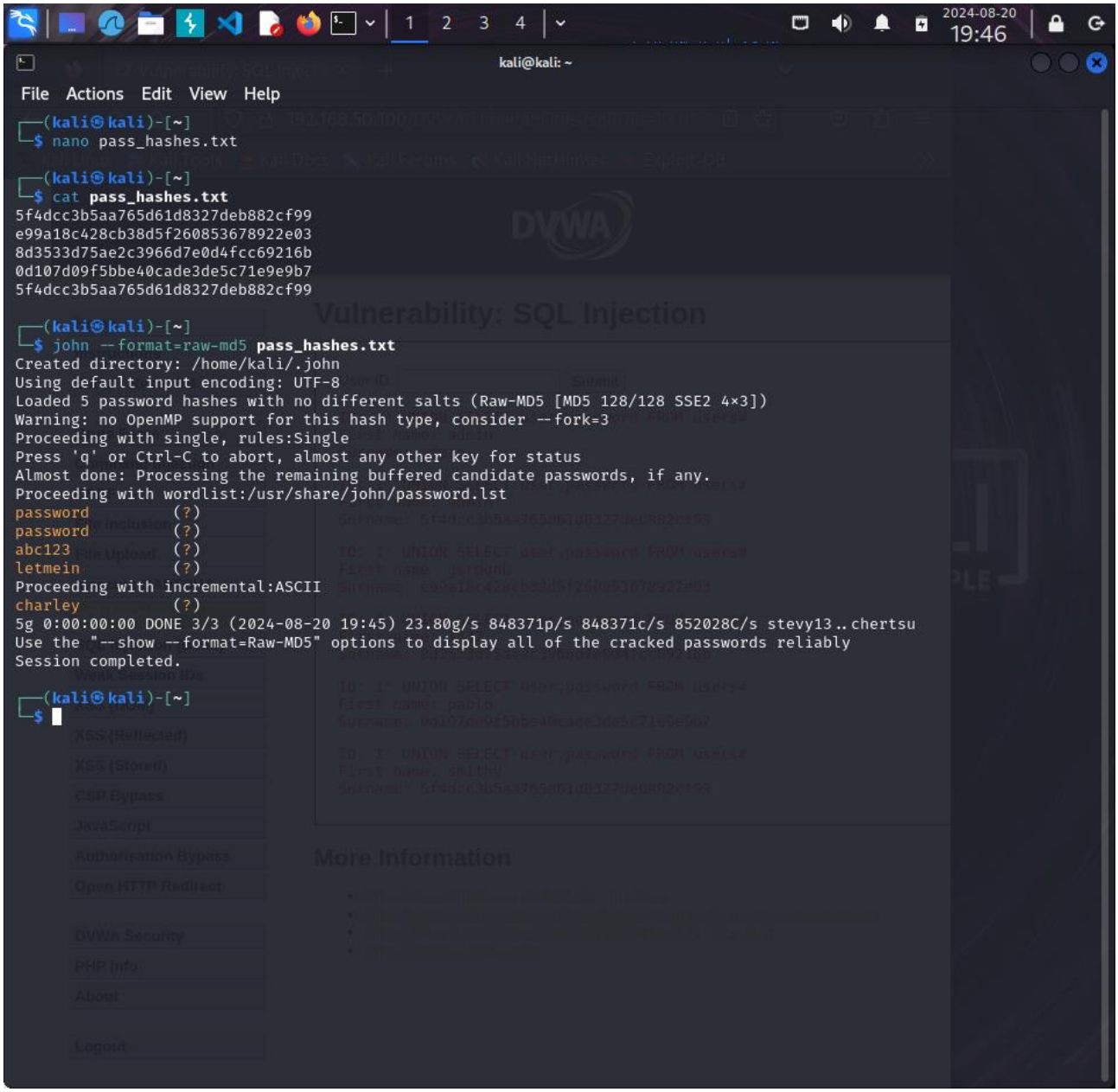
Screen con password trovate nel precedente esercizio con la SQL Injection



Il cracking delle password è un processo utilizzato per recuperare password in chiaro partendo dai loro hash crittografici. In pratica, si tratta di trovare la corrispondenza tra un hash, che è una rappresentazione crittografica della password, e la password originale. Questo processo può essere eseguito attraverso vari metodi, come attacchi a dizionario, brute force, o utilizzando strumenti specializzati come John the Ripper.

Nel mio caso, ho utilizzato John the Ripper con il comando ‘john --format=raw-md5 pass_hashes.txt’ per craccare degli hash MD5 recuperati tramite un attacco SQL Injection. Questa tipologia di cracking, in particolare, è un attacco basato su dizionario e brute force. Il meccanismo principale consiste nel testare una serie di password comuni o generate automaticamente contro gli hash presenti nel file pass_hashes.txt.

John the Ripper esegue questi test utilizzando una combinazione di approcci: nel metodo a dizionario, prova password comuni prese da una lista predefinita, mentre con il metodo brute force, genera tutte le combinazioni possibili di caratteri, fino a trovare una corrispondenza. Questo approccio ha permesso di decodificare alcune delle password in chiaro. Il risultato finale dimostra quanto possa essere vulnerabile un sistema se le password non sono protette adeguatamente, ad esempio utilizzando hash salvati o password più complesse.




$dynamic_0$8d3535d75ae2c3966d7e0d4fcc69216b:charley
┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 pass_hashes.txt --show
?:password
?:abc123
?:charley
?:letmein
?:password
5 password hashes cracked, 0 left
┌──(kali㉿kali)-[~]
└─$