1) SQL injection già effettuata:

2) Il password cracking in questione si divide in due macro-categorie:
La prima e più semplice è un attacco al dizionario, che utilizza una lista di password comuni già presenti nella cartella /usr/share/john/password.lst
Le password in questione hanno decifrato la crittografia di
admin
smithy
gordonb
pablo
Poiché all'interno del documento sono già presenti, a John The Ripper sono serviti solo i tentativi necessari per provare a decriptare le password usando la lista a sua disposizione.
Cambia invece la metodologia per quanto concerne l'ultima password, "charley" che non è presente nel documento. Nell'immagine infatti si nota come JtR prova ad utilizzare il metodo di cui abbiamo parlato ma senza successo. Procede dunque a cambiare metodologia di attacco, passando ad un "bruteforce", ovvero prova in successione tutte le lettere (a,aa,aaa,aaaa e così via) prima di arrivare alla soluzione.
Di seguito il file con le password decifrate