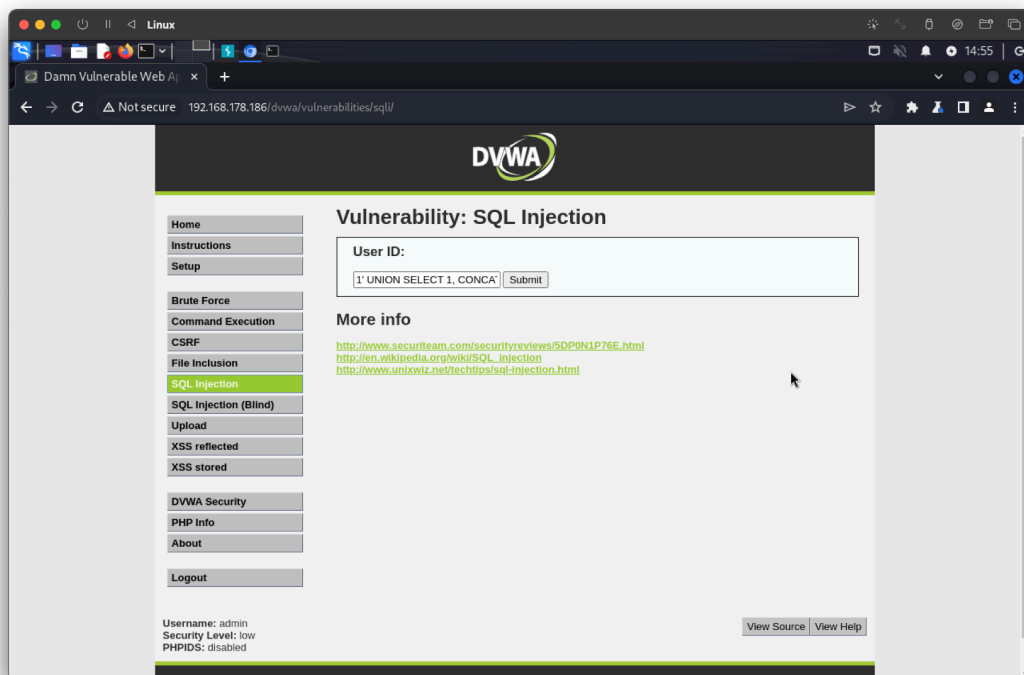
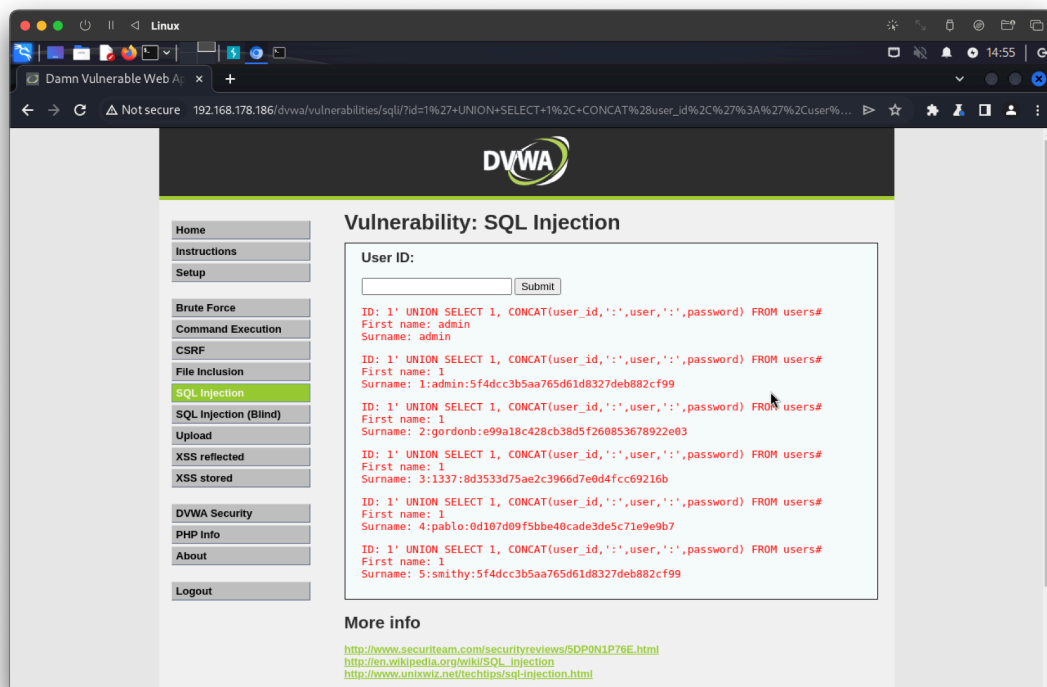


Consegna S6-L4



Una volta eseguito l'accesso su dvwa andiamo a testare la SQL Injection



Inserendo la stringa:

“1' UNION SELECT 1, CONCAT(user_id,',',user,',',password) FROM users# “

Otteniamo la lista delle password e dei nomi utenti in versione hash MD5
Possiamo procedere in due modi distinti, utilizzando un hash translator oppure utilizzando un tool che si chiama Jhon the ripper.



Nel primo caso otteniamo la stringa tradotta in formato di testo, nel secondo caso con il software otteniamo le varie combinazioni user/password.

