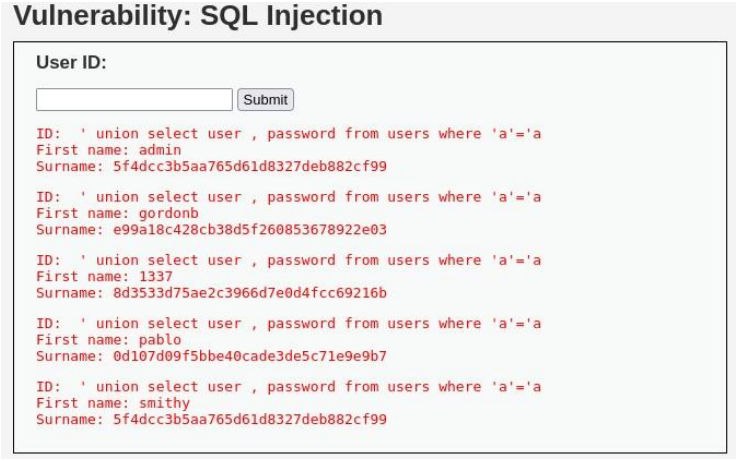
Progetto S6-L3

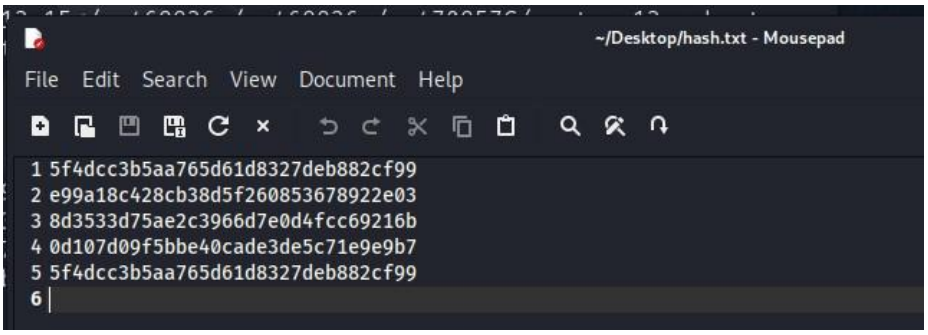
Studente: Simone Mininni

Task:Password cracking.

Dopo aver effettuato una SQL injection sulla web application DVWA e aver trovato quindi user e password(hash), proviamo a risolvere il codice hash delle password con un attacco a dizionario utilizzando in questo caso "John". Inoltre sappiamo che probabilmente il format dell' hash è md5.

Quindi estrapoliamo i codici hash e gli user dal sito e li inseriamo un file .txt:

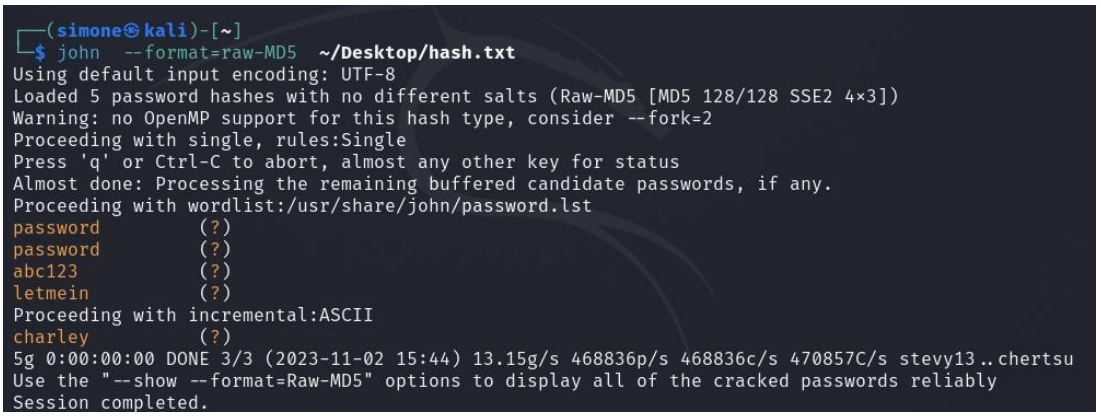




Successivamente utilizziamo John per trovare eventuali password in chiaro.
Nello specifico diamo in pasto a john una lista di password comuni e il tool le trasformerà in codice hash secondo dei formati che in questo

caso sappiamo essere md5 e poi li confronta con i codici hash della lista creata da noi con i codici hash delle password che vogliamo vedere in chiaro. Se john trova corrispondenza tra codici hash, allora vedremo la password in chiaro.

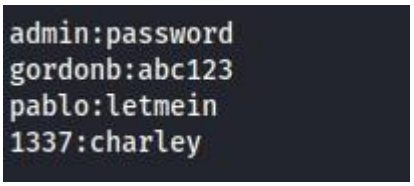
Eseguiamo l'operazione di password cracking…



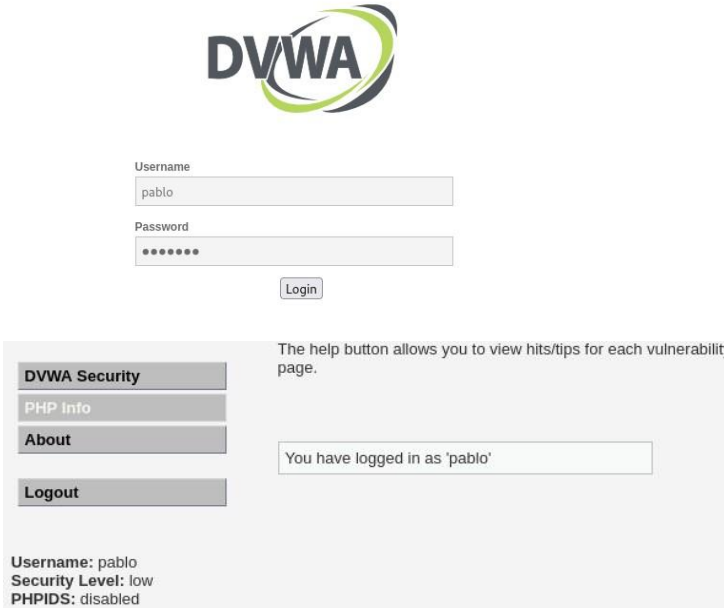
Come vediamo john trova quattro associazioni, quindi password, utilizzando una lista, e una associazione 'charley' utilizzando un attacco brute force puro.

Andiamo a vedere le associazione nel dettaglio presenti nel file john.pot…

Andiamo a definire l' associazione user:password



Testiamo ad esempio pablo:letmein



Sono riuscito a loggarmi con successo come ‘pablo’.
L’ attacco è andato a buon fine.

In conclusione notiamo come password deboli possono essere facilmente decifrate e quindi si riesce ad utilizzare un attacco a dizionario con successo.
Abbiamo visto come anche il pure brute force è stato efficace, riuscendo a trovare in poco tempo la combinazione.

Fine.