W14D1

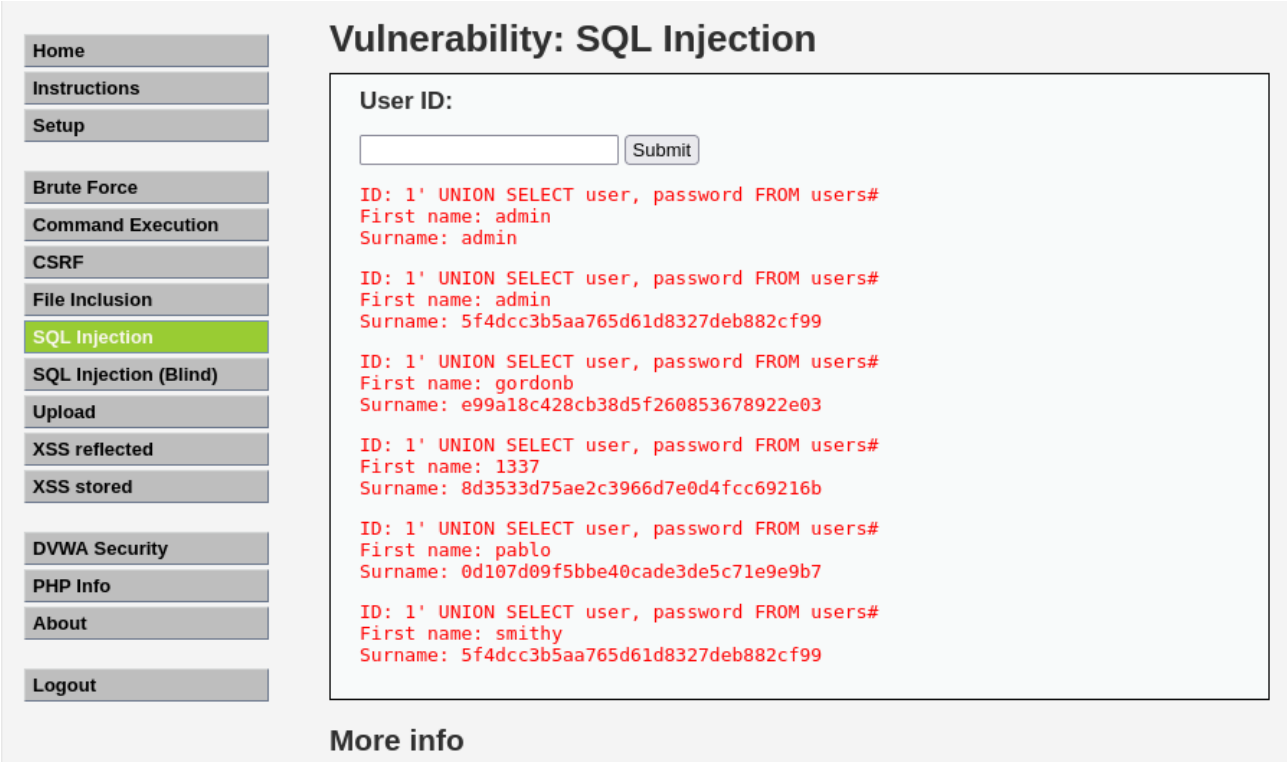
Recuperate le password dal DB come visto, e provate ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro.

Punto 1.

Screenshot dell'SQL injection già effettuata

1' UNION SELECT user, password FROM users#

La SQLI chiede al database (#) di estrarre gli users con le rispettive password.



Come vediamo tramite SQLI (visto che il sito non disinfetta l input)siamo riusciti ad ottenere la lista completa dei utenti con le loro rispettive password. Possiamo notare che le password sono criptografate in md5 (modello di criptografia hash) cosi sono inutilizzabili.

Per riuscire ad ottenere la password in "chiaro" abbiamo bisogno di crackarle .

Si puo utilizzare John the ripper .

John the Ripper è un tool di password cracking piuttosto popolare scritto per i sistemi operativi basati su Unix.Fa uso della parallelizzazione dei task per ridurre i tempi di cracking durante una sessione brute force, ed e altamente configurabile.

Quindi selezioniamo le password e inseriamole dentro un file .txt esempio Hash.txt

E scriviamo il comando john –format=RAW-MD5 <file.txt>

vediamo come il tool esamindo e confrontando le password in hash riesce a decriptarle e restituirle in chiaro.