ESERCITAZIONE W14D1 (1)

EPICODE

Esercizio
Password cracking

Traccia: password cracking

Abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema.

Se guardiamo meglio alle password trovate, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5.

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

Sentitevi liberi di utilizzare qualsiasi dei tool visti nella lezione teorica.

L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate precedentemente.

EPICODE

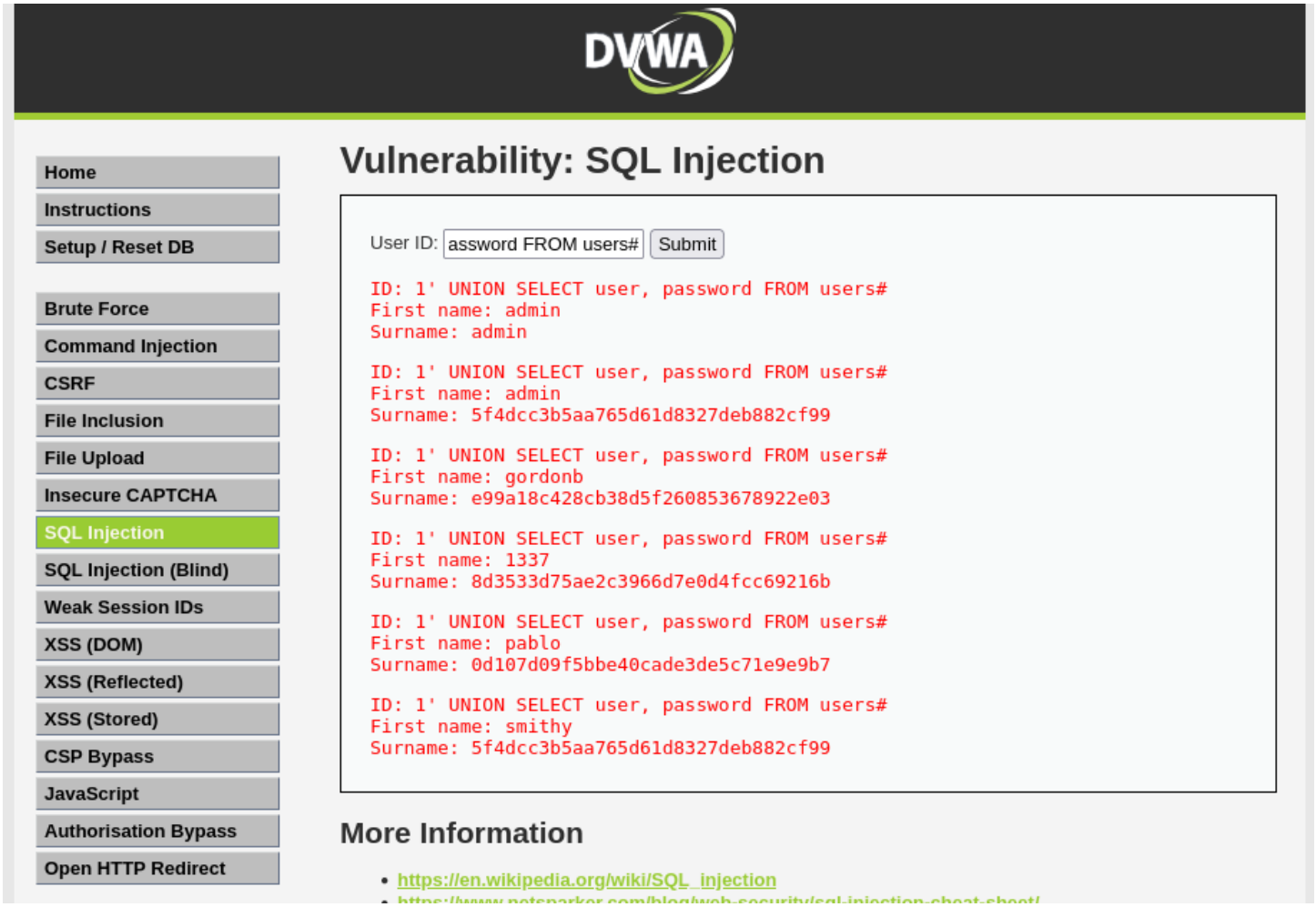
W14D1 - Pratica (1) PDF

Esercizio
Password cracking

Consegna:

1. Screenshot dell'SQL injection già effettuata
2. Due righe di spiegazione di cos'è **questo** cracking (quale tipologia / quale meccanismo sfrutta)
3. Screenshot dell'esecuzione del cracking e del risultato

1) Ho recuperato le password cifrate in hash con la SQL INJECTION (1' UNION SELECT user, password FROM users#)



2) Ho creato un file di testo con le cinque password cifrate in hash:

3) infine ho usato il programma John the Ripper per decifrare le password con questi comandi da terminale: