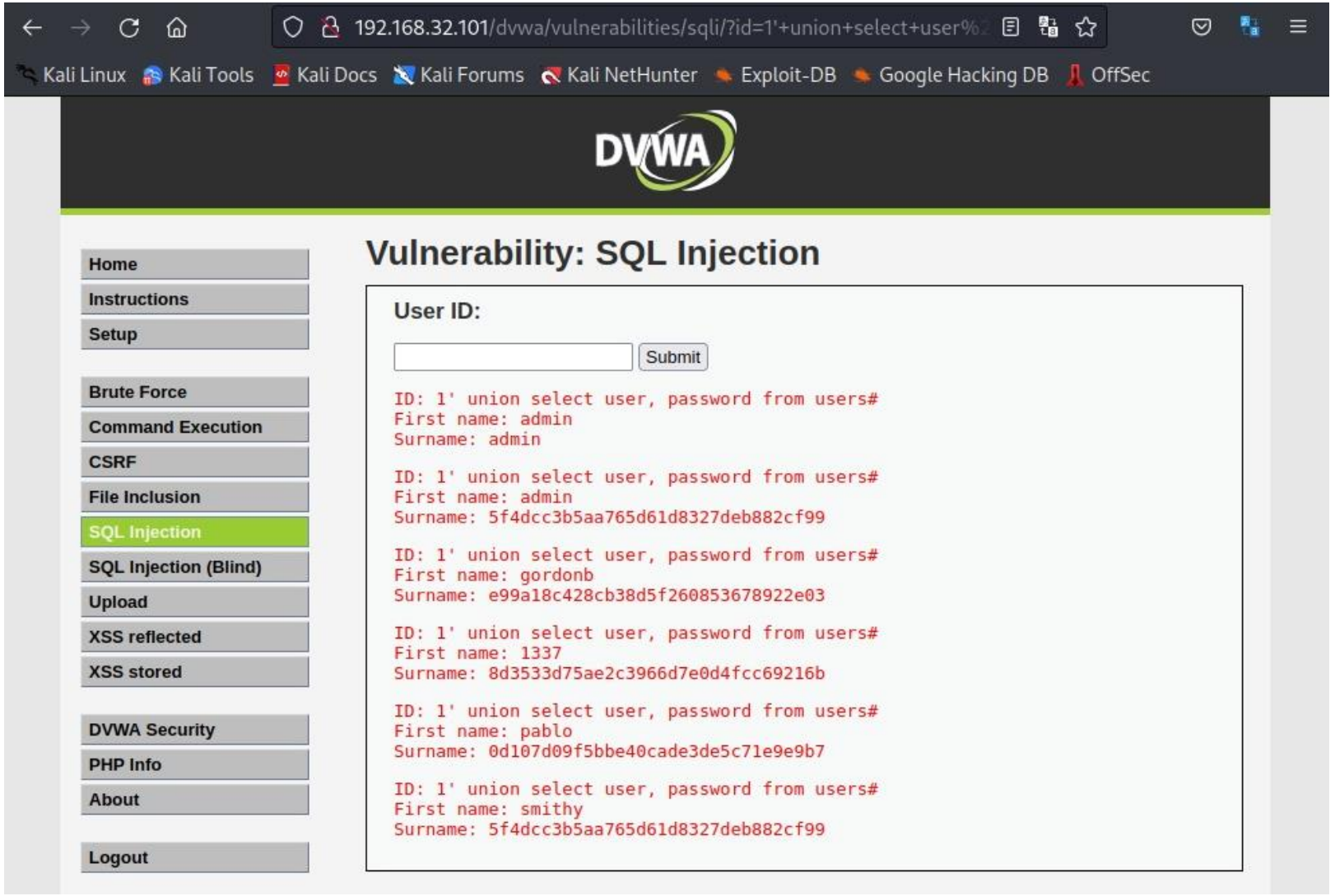
Password Cracking

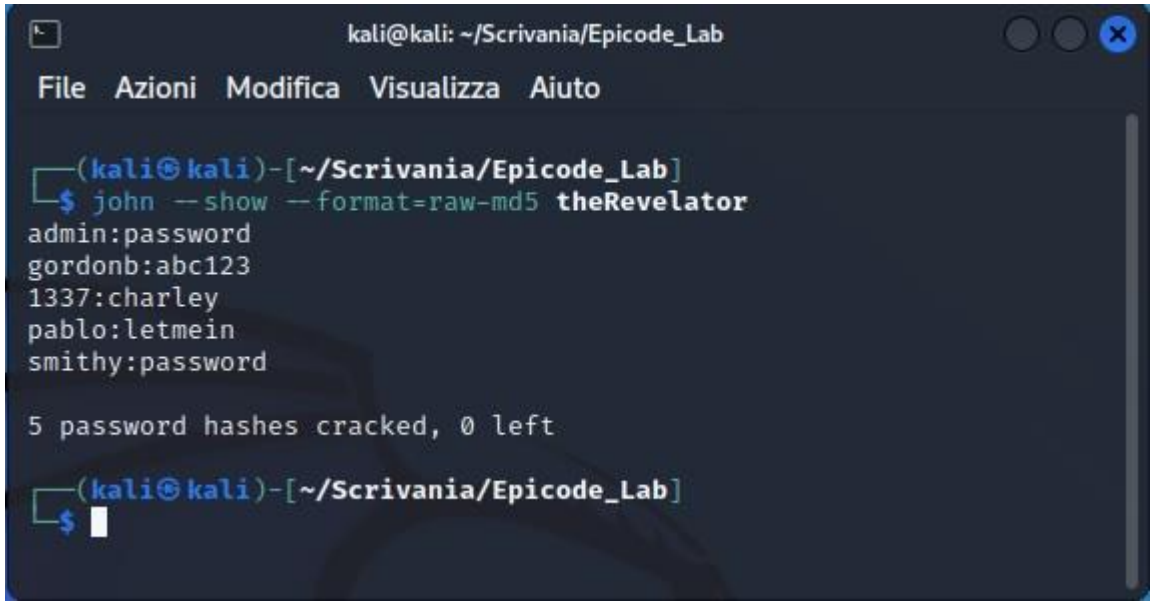
John the Ripper

Orlando Tangari



SQL Injection

Dalla VM Kali, accedendo alla DVWA della VM Metasploitable, nella sezione SQL Injection, digitando: *1' union select user, password from users#*, nel campo User ID, e cliccando il pulsante Submit, o premendo Invio, la Web App, sfruttando le vulnerabilità di SQL, restituisce le credenziali di tutti gli utenti ma, con le password criptate.



John the Ripper

Dalla VM Kali, tramite il tool di password cracking, John the Ripper, si decriptano le password trovate sfruttando la vulnerabilità SQL Injection ma, ha bisogno che nomi utenti e password siano in un unico file, rinominato, per l'occasione: *theRevelator*, come mostrato nell'immagine a sinistra.
Successivamente, come mostrato nell'immagine a destra, da terminale, eseguendo il comando: *john --format=raw-md5* –theRevelator, il tool ci decripta le password e, a brute force effettuato, eseguendo il comando: *john –show --format=raw-md5 –theRevelator*, il tool ci mostra le password recuperate in chiaro.