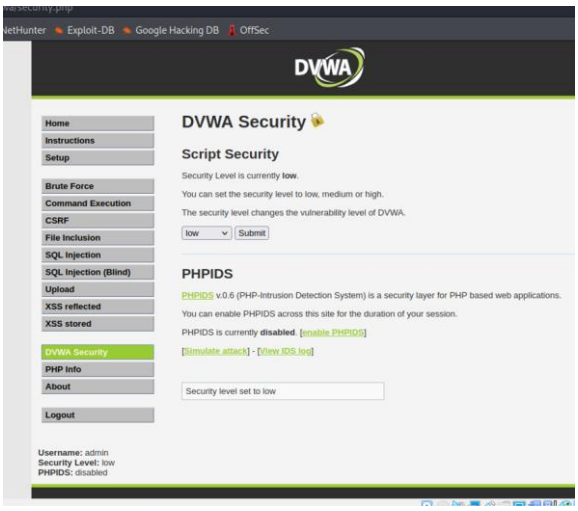
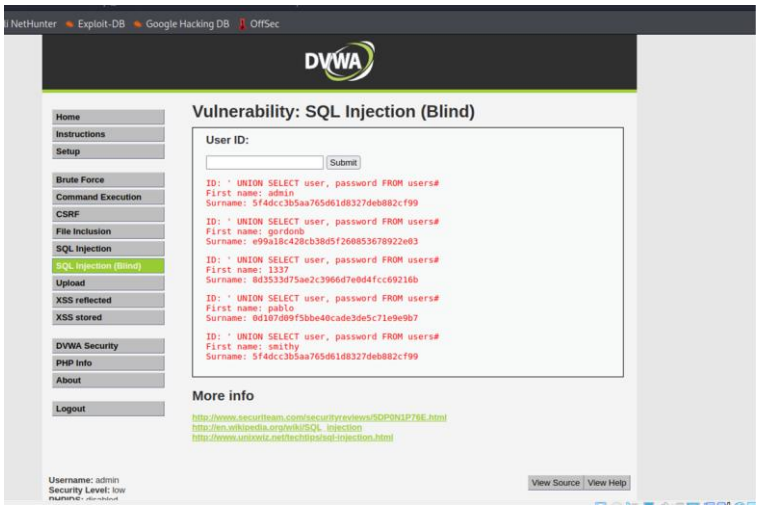
In questo esercizio andremo a recuperare le password degli utenti che sono registrati sulla pagina dvwa.



Per prima cosa andiamo a mettere la nostra sicurezza su “low”, andremo quindi a recuperare le nostre password che appartengono agli ID registrato con SQL Injection (blind), con il comando
' UNION SELECT user, password FROM users#



Dopo di che andremo a creare un file .txt dove inseriremo quindi gli user e le password ricavate in precedenza così da poterle decriptare con John The Ripper.

Abbiamo quindi decriptato le password (col comando john -format=raw-md5--) e poi con il comando seguente (john -format=raw-md5—show--)le abbiamo riportate in chiaro