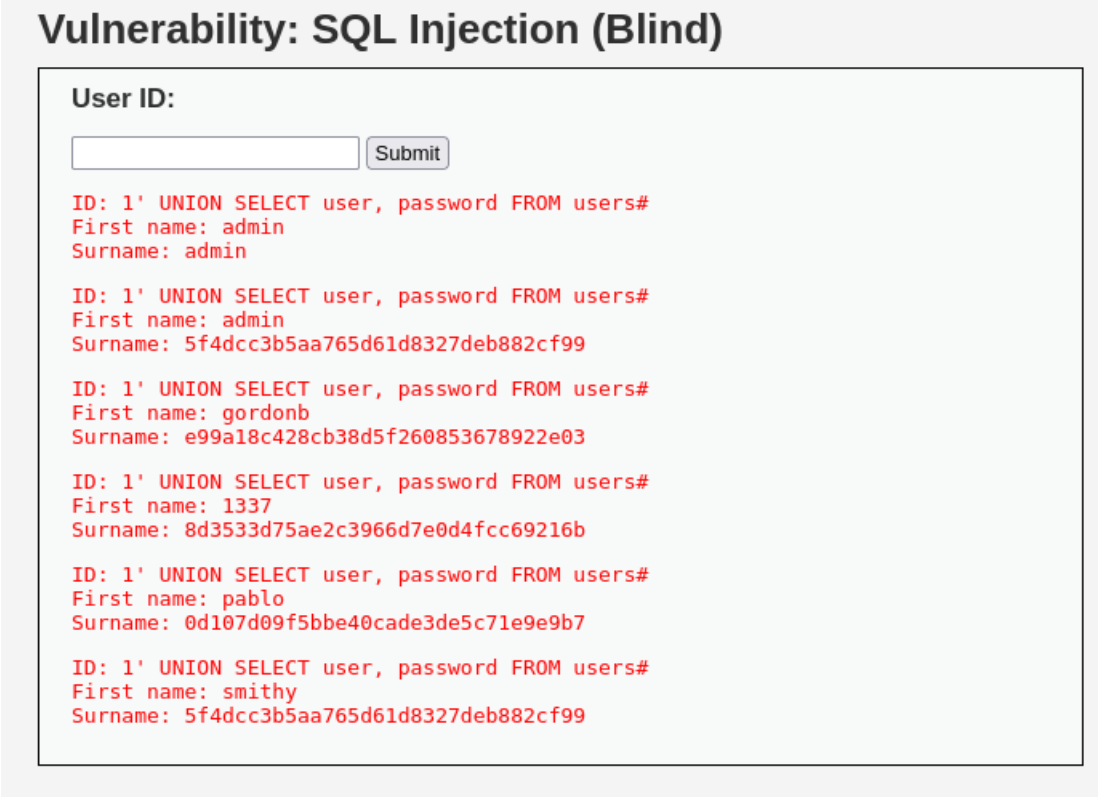
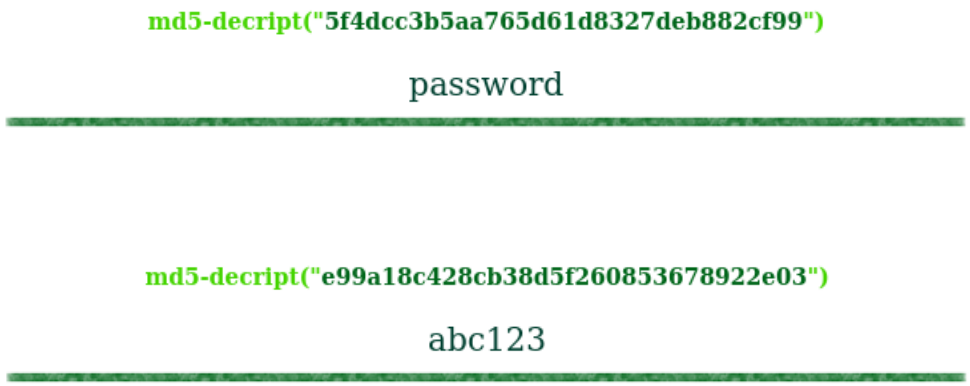
Dopo aver inserito il seguente script 1' UNION SELECT user, password FROM users# su DVWA, provare diversi tool per decifrare gli hash delle password.



Password con MD5

L'MD5 è una funzione crittografica di hash. Questa funzione prende in input una stringa di lunghezza arbitraria e ne produce in output. È diffuso anche come supporto per l'autenticazione degli utenti, infatti durante la registrazione di un utente su un portale internet, la password scelta durante il processo verrà codificata tramite MD5 e la sua firma digitale verrà memorizzata nel database. Dopo, durante il login la password immessa dall'utente verrà confrontata con la copia in possesso del database.



md5-decript("8d3533d75ae2c3966d7e0d4fcc69216b")

charley

md5-decript("0d107d09f5bbe40cade3de5c71e9e9b7")

letmein

md5-decript("5f4dcc3b5aa765d61d8327deb882cf99")

password

Password con John the reaper

John the Ripper è un software libero per la decrittazione forzata delle password. Agisce combinando diverse modalità di crack delle password, autorilevamento di password in hash e inclusione di un cracker impostabile.