EPICODE

Esercizio S6 – L4

TRACCIA

Utilizzando l’attacco SQL Injection (non blind), andare a compromettere il database di DVWA.

Bonus: Noterete che le password sono in codice hash.Trovare il modo per rendere le password in chiaro.

SOLUZIONE

Scrivendo la seguente query:  
%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #  
si è potuto visualizzare tutte le informazioni di autenticazione presenti nel database.

Immagine che contiene testo, schermata, software, Pagina Web

Descrizione generata automaticamente

Segue

Le password di autenticazione vengono visualizzate in formato hash. Per poterle leggere in chiaro è possibile usare John the Ripper.  
Nello specifico si è prima creato un file di testo con al suo interno l’hash della prima password e lo si è salvato sul Desktop.

Immagine che contiene testo, Carattere, Software multimediale, schermata

Descrizione generata automaticamente

Successivamente, da root e da dentro la directory “Desktop”, si è utilizzato John the Ripper per vedere la lista dei formati e capire come vedere in chiaro un hash MD5 (l’hash utilizzato da DVWA).

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Segue

Dopo di che si è proceduto con il comando in grado di mettere in chiaro l’hash MD5 contenuto nel file. Nell’immagine sotto il comando viene ripetuto anche per una seconda password contenuta in un altro file.

Immagine che contiene testo, schermata, Carattere, design

Descrizione generata automaticamente

Segue

Come ultimo passaggio si è voluto dimostrare come, inserendo in un unico file diverse password in formato hash, John the Ripper sia in grado di mettere in chiaro diverse password con un solo comando.

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente