REPORT ATTACCO

WEB APPLICATION

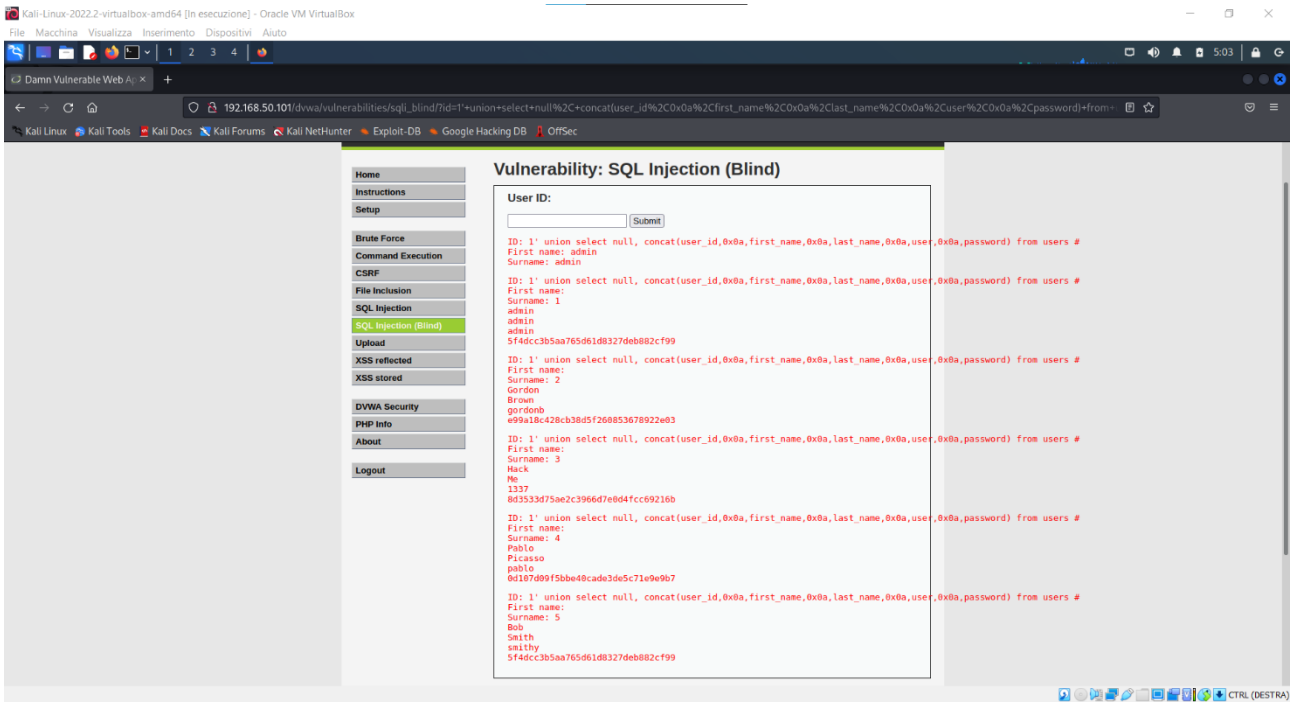
12/08/2022

SQLi BLIND

La SQLi (SQL injection) è una vulnerabilità che permette ad un utente non autorizzato di prendere il controllo sui comandi SQL utilizzati da un'applicazione web.

Attraverso una manipolazione della query sono riuscito ad ottenere dati sensibili, tra cui le password cifrate in hash md5 dei vari user, che andremo a crackare successivamente con un tool automatico.

Di seguito lo screen della query:

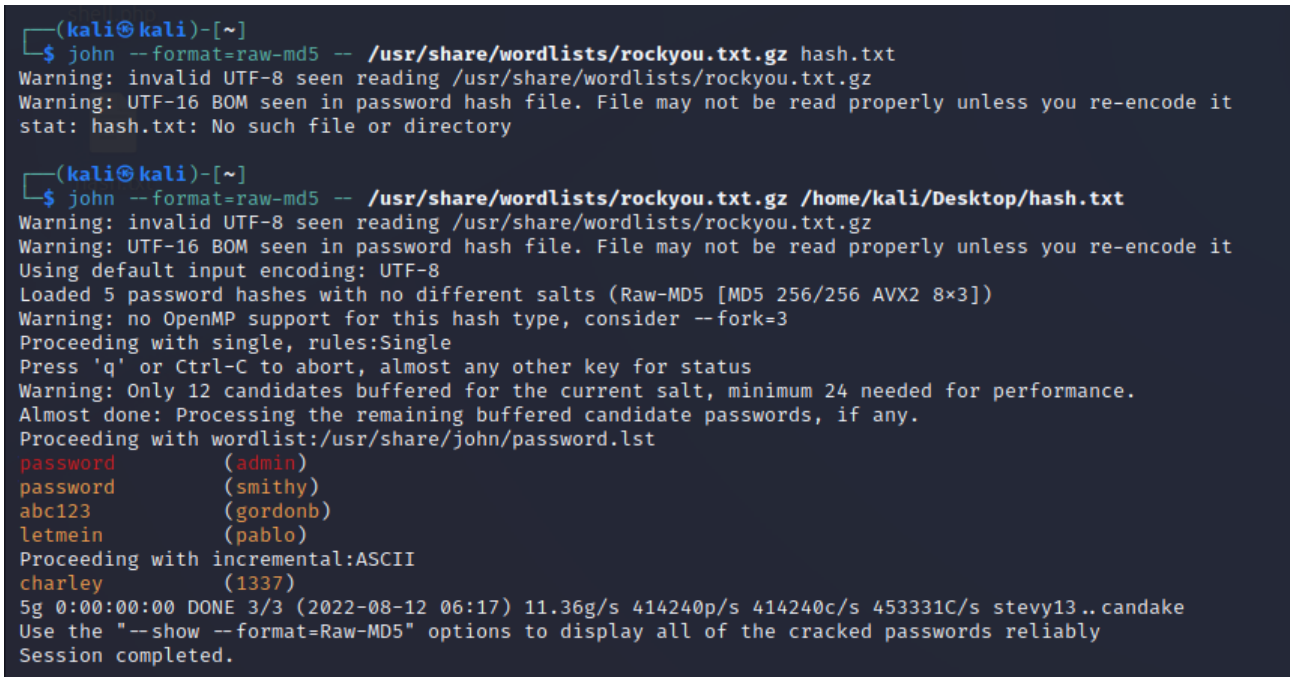


JOHN THE RIPPER 1.9.0

JTR (John The Ripper) è un tool automatico per il password cracking scritto per i sistemi operativi basati su Unix. L'ho utilizzato per risalire alle password in chiaro partendo dal codice in hash con formato md5. I codici hash sono stati recuperati tramite la SQLi blind.

L'hashing è la criptazione di una password in chiaro in senso univoco, ovvero una volta cifrata non si può tornare indietro.

Di seguito lo screen della risoluzione:

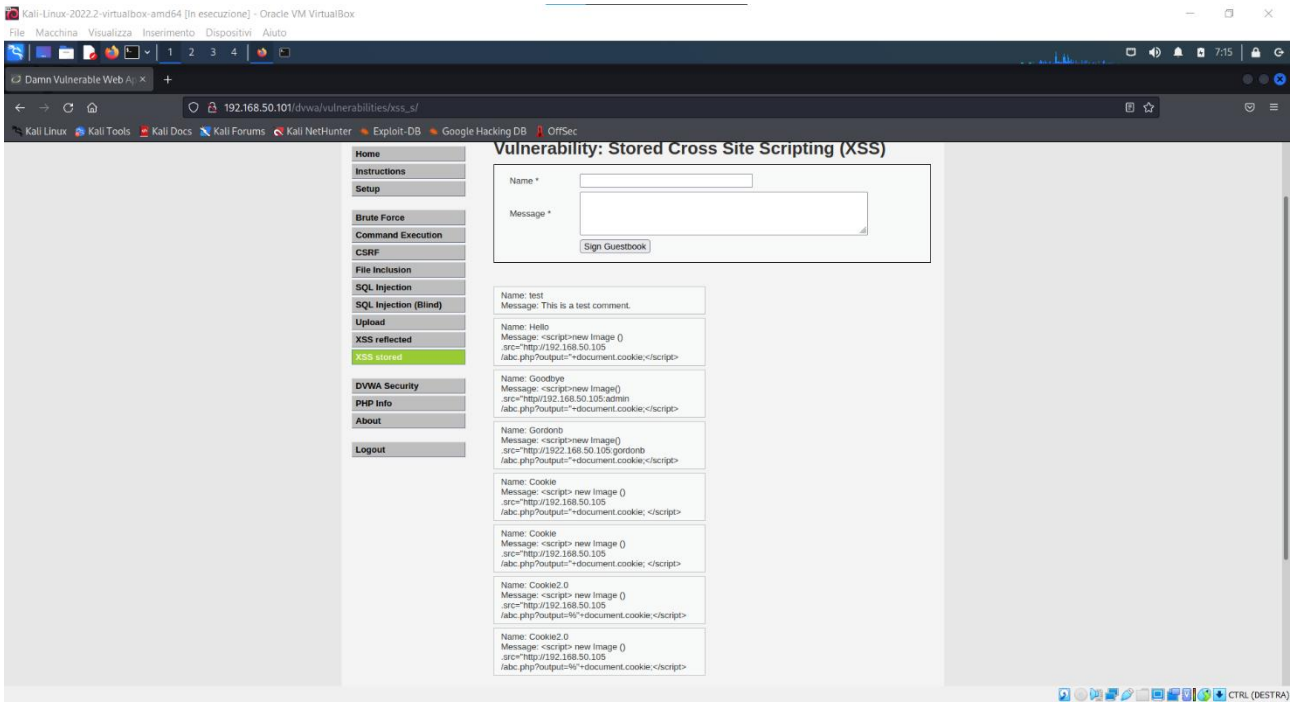


XSS STORED

XSS stored (Cross Site Scripting) è una vulnerabilità che permette di sfruttare errori di controllo nell'input utente lato client, e di conseguenza permette di modificare il codice HTML di una pagina web.

In questo caso ho iniettato un codice malevolo nella pagina che rubasse i cookie degli user che accedono alla web app, così da avere i loro SESSIONID legittimi per poterli impersonificare.

Di seguito il codice malevolo iniettato chiamato Cookie 2.0:



NETCAT 1.10

Netcat è un tool a riga di comando che permette sia connessioni TCP sia connessioni UDP. Può essere utilizzato sia come client che come server.

Nel nostro caso l'ho utilizzato come server e l'ho messo in ascolto sulla porta 80 (la porta di default del servizio http) per ricevere i cookie di sessione dei vari user presenti sulla DVWA.

Di seguito gli screen dei cookie di sessione di ogni user: