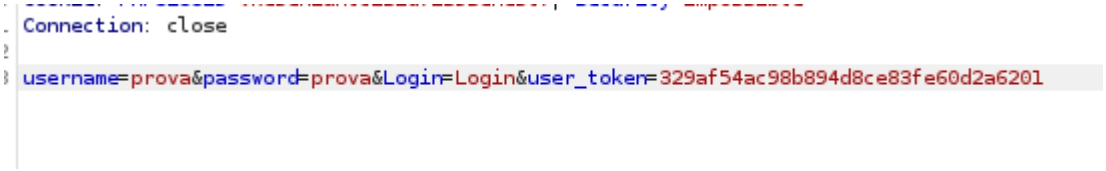
Gabriele Di giampietro **Data 09/11/2022**

Esercizio: Configurazione di una DVWA, vulnerable web application su Kali Linux

Nell'esercitazione di oggi abbiamo configurato un DVWA per simulare la vulnerabilità di un attacco su applicazione web con login e password. Per fare ciò abbiamo avviato una simulazione su kali di un database MySQL e un web serve Apache, e un file già impostato per i nostri servizi di DVWA (https://github.com/digininja/DVWA).

Attraverso Burpsuite, un tool per l'intercepting procy riusciamo a catturare le risposte tra client e server, cercando di individuare le credenziali del login, modificando la risposta e la richiesta http che il client manda al server. Modificando attraverso Burpsuite le credenziali che abbiamo catturato, possiamo notare utilizzando la funzione follow redirection che nel body dell'http response risulta login failed.

Come possiamo vedere dall'immagine seguenti:



In fine anche modificando il livello di sicurezza del DVWA, non riusciamo ad ottenere le credenziali di login. Il DVWA ha diversi livelli di sicurezza, di default parte da impossibile: