Report Brute Force

Il Brute Force è un metodo di attacco informatico dove vengono testate tutte le possibili combinazioni di valori per ottenere l’accesso non autorizzato ad un sistema o ad un account, generalmente è utilizzato per violare password.

Per eseguire l’attacco Brute Force abbiamo utilizzato il linguaggio Python innanzitutto importando le seguenti librerie:

* Il modulo http.client è utilizzato per creare richieste HTTP e interagire con server web tramite richieste come GET, POST.
* urllib.parse è un modulo di Python che fornisce funzionalità per lavorare con URL (Uniform Resource Locator) in modo semplice ed efficiente. È utile per analizzare, manipolare e costruire URL in applicazioni Python.

Questo modulo è particolarmente utile quando si lavora con richieste HTTP, parsing di HTML, creazione di script di web scraping e in generale per qualsiasi applicazione che coinvolga l'interazione con risorse online attraverso URL.

In particolare, il codice mira a una pagina di login /dvwa/login.php di un'applicazione web e prova tutte le possibili combinazioni di nomi utente e password presenti nei file usernames.txt e passwords.txt.

Principalmente nel codice viene importato il modulo http.client per effettuare richieste HTTP e urllib.parse per manipolare l’URL, successivamente viene aperto e letto il contenuto dei file usernames.txt e passwords.txt per ottenere i nomi utente e le password da utilizzare per l'attacco. Poi si richiede all'utente di inserire l'indirizzo IP e la porta del target. Dopodiché vengono provate tutte le possibili combinazioni di nomi utente e password, e per ciascuna combinazione viene effettuata una richiesta HTTP POST alla pagina di login dell'applicazione web, per ogni combinazione viene quindi controllata la risposta per vedere se l'accesso è riuscito. Se l'accesso riesce, il programma stampa le credenziali utilizzate.