Report sulla Bruteforce

Immagine che contiene testo

Descrizione generata automaticamente

Descrizione del codice di Bruteforce

Partendo dall’inizio, possiamo definire “import” come un comando di Python utilizzato per richiamare all’interno del codice delle funzioni esterne. In questo caso le funzioni richiamate da Import sono «http.client», «urllib.parse».

“Username\_ file” e “password\_file” sono le due variabili che andranno a contenere al loro interno i due file “.lst” con i nomi utente e le password più utilizzate. La funzione “open” è utilizzata per aprire i file all’interno delle variabile e restituisce ad esse il contenuto dei suddetti files.

“User\_list” e “pwd\_list” sono due variabili che verranno utilizzate per leggere il contenuto dei file .lst inseriti sopra.

«Readlines ()” è un comando di python che ci permette di leggere il contenuto dei file riga per riga, in questo caso dei nomi utente e delle password che andremo a scansionare.

I due cicli for vengono inseriti all’interno di questo codice per scansionare i vari file e le varie password, creando un ciclo nidificato.

Viene richiamata la variabile user\_list e il ciclo for andrà ad associare tutti i nomi utente della lista a tutte le password. Il punto di uscita di questo ciclo avviene nel momento in cui un nome utente della lista corrisponderà ad una password della seconda lista.

Nel “print(user, “-“, pwd)” verranno stampati in output il nome utente e la password corrispondente.

Con la variabile “post\_parameters” assegniamo la coppia username-password, associata alla combinazione realizzata nel for.

Poi andiamo ad inserire l’header, il quale contenuto è sempre lo stesso.

Con la variabile “conn” andiamo a creare la connessione, indicando l’indirizzo e la porta desiderati, per poi inviare una richiesta con il metodo POST all’url esplicitato all’interno della riga di codice.

Successivamente, assegniamo alla variabile “response” il valore ottenuto dal comando “conn.getresponse()”.

Infine, attraverso la funzione “if”, se rispettata la condizione assegnata, verrà stampato in output l’username e la password corrette.

Esito dell’attacco Bruteforce sulla pagina DVWA

Le password e gli username vengono combinate tra di loro all’interno dell’attacco bruteforce nei confronti della pagina di login: </dvwa/login.php> attraverso la richiesta http “POST”.

Il codice ha dato come esito le seguenti credenziali d’accesso:

Username: **admin**

Password**: password**