VULNERABILITA':

La possibilità di provare senza fine potenzialmente infinite righe di username e password fa in modo di trovare facilmente le credenziali corrette per quel determinato form login, è solo questione di tempo del programma nell'eseguire le combinazioni e la compattezza della password.

L'assenza di controlli di richieste e il feedback visivo di nome utente errato crea il modo per trovare le credenziali corrette

ATTACCO:

L'attacco di per se è banale perché si vanno a leggere e a confrontare i due file selezionati dall'utente provando le combinazioni in POST sul form login dedicato.
Quando il feedback è positivo l'attacco si ferma e restituisce all'utente le combinazioni trovate.

SOLUZIONI:
Le soluzioni possono essere molteplici:
1) **Monitoraggio degli accessi**: Implementazione di controlli sulle richieste dallo stesso IP e di conseguenza un blocco temporaneo/ban di quel determinato IP
2**) Assenza di limitazioni di tentativi**: Se una pagina di login non applica alcuna limitazione ai tentativi di accesso, un attaccante può eseguire un numero illimitato di tentativi senza restrizioni. Questo consente loro di eseguire attacchi di brute force senza impedimenti.

3) **Password deboli**: Se gli utenti utilizzano password deboli o facilmente indovinabili, diventa più facile per un attaccante individuare le combinazioni corrette tramite un attacco di brute force.

4) **Mancanza di meccanismi di rilevamento degli attacchi**: Le pagine di login possono mancare di meccanismi di rilevamento degli attacchi di brute force, che potrebbero consentire a un attaccante di eseguire l'attacco senza essere rilevato o bloccato dal sistema.

5) **Utilizzare misure di autenticazione a più fattori (MFA)**: L'utilizzo di MFA, come l'invio di un codice di verifica via SMS o l'utilizzo di un'applicazione di autenticazione, può rendere più difficile per un attaccante ottenere l'accesso anche se riesce a indovinare la password.