VULNERABILITIES:

The possibility to endlessly try potentially infinite rows of usernames and passwords makes it easy to find the correct credentials for that specific login form; it's just a matter of time for the program to execute the combinations and the compactness of the password. The absence of request controls and the lack of visual feedback for incorrect usernames create the means to find the correct credentials.

ATTACK:

The attack itself is trivial because it involves reading and comparing the two files selected by the user, trying the combinations in POST on the dedicated login form. When the feedback is positive, the attack stops and returns the found combinations to the user.

SOLUTIONS:

There can be multiple solutions:

1) Access Monitoring: Implementation of controls on requests from the same IP and consequently temporary blocking/banning of that particular IP.

2) Absence of Attempt Limitations: If a login page applies no limitations on access attempts, an attacker can perform an unlimited number of attempts without restrictions. This allows them to execute brute force attacks without hindrance.

3) Weak Passwords: If users use weak or easily guessable passwords, it becomes easier for an attacker to identify the correct combinations through a brute force attack.

4) Lack of Attack Detection Mechanisms: Login pages may lack brute force attack detection mechanisms, which could allow an attacker to execute the attack without being detected or blocked by the system.

5) Use of Multi-Factor Authentication (MFA): Using MFA, such as sending a verification code via SMS or using an authentication app, can make it more difficult for an attacker to gain access even if they manage to guess the password.