SimpleLogin

罗承煜 523031910624

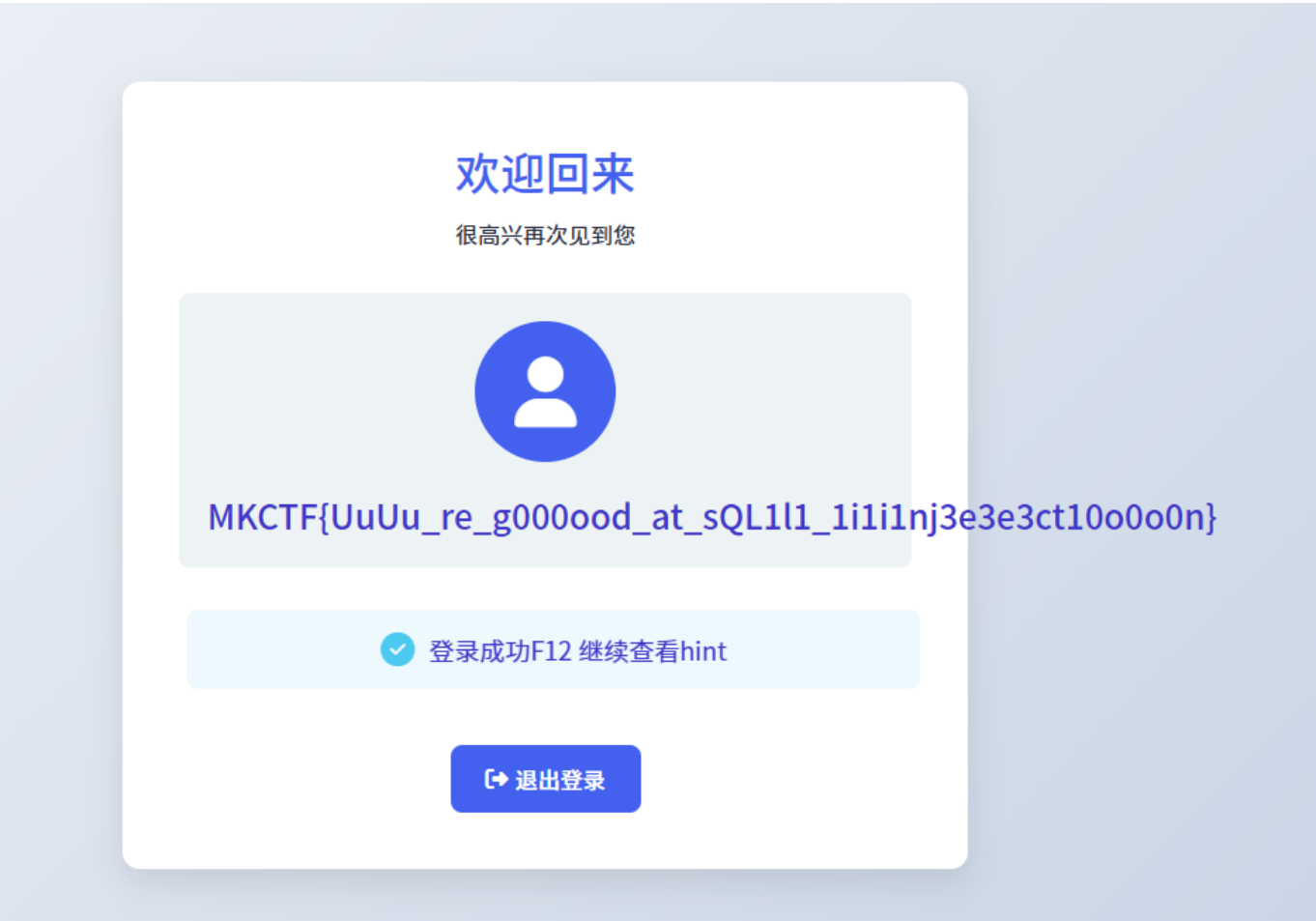
题目分析

本题只有一个登录界面，随便输点什么进去，发现登陆失败，但好消息是有hint，“本题采用的是弱密码”，那可以有如下三种方式成功登录 burp suite爆破，但鉴于他是弱密码，就不用这个方法了 用万能密码，几种常用的万能密码： `SELECT * FROM users WHERE name='$username' and password='$pwd'` 1、用户名：随意；密码：'or''=' 2、用户名：\；密码：or1# 3、用户名：admin'# ;密码：随意 本题禁用了单引号，那就用第二种万能密码 盲猜有个用户叫admin，在常用的弱密码里挑几个试一试，其实也容易，我第二次试admin123就成功登陆了

登录之后，发现本题登录成功的判断语句是 `SELECT * FROM users WHERE name='$username' and password='$pwd'` 此处存在注入点，如果输入username=\，就能对后面的单引号进行转义，相当于让 username=`' and password=`,此时把要查找的语句输入到password并在最后加个#，注释掉最后一个单引号，就能完成注入

为了用UNION SELECT查找flag信息，首先要知道users表有几列，于是可以在password中依次输入 `UNION SELECT 1#` `UNION SELECT 1,2#` 发现在输入到`UNION SELECT 1,2,3#`的时候不报错了，证明users有三列。

既然已知flag表里有我想要的数据，那只需要把他select出来即可，只是不知道flag表有几列，也只能慢慢尝试 `UNION SELECT * FROM flag#` 不对，加多一列呢？ `UNION SELECT *,1 FROM flag#` 欸？对了！



说明flag只有2列啊