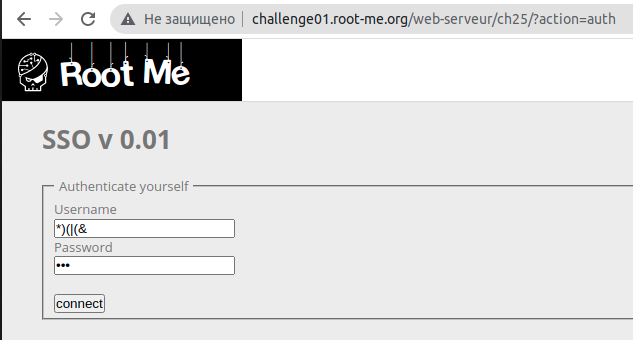
**Урок 7. LDAP injection**

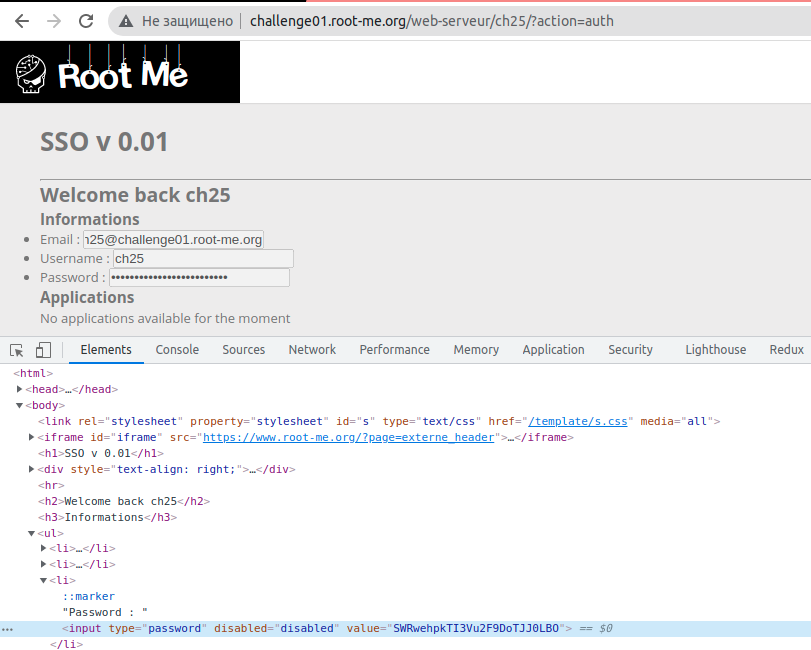
Задание 1:

Выполнить задание на LDAP injection   
 **https://www.root-me.org/en/Challenges/Web-Server/LDAP-injection-authentication**

Решение:

Воспользовался вложенным выражением:

 и результат:



Задание 2, 3\*, 4\*:

Выполнить задание на Blind LDAP injection  
 **https://www.root-me.org/en/Challenges/Web-Server/LDAP-injection-blind**

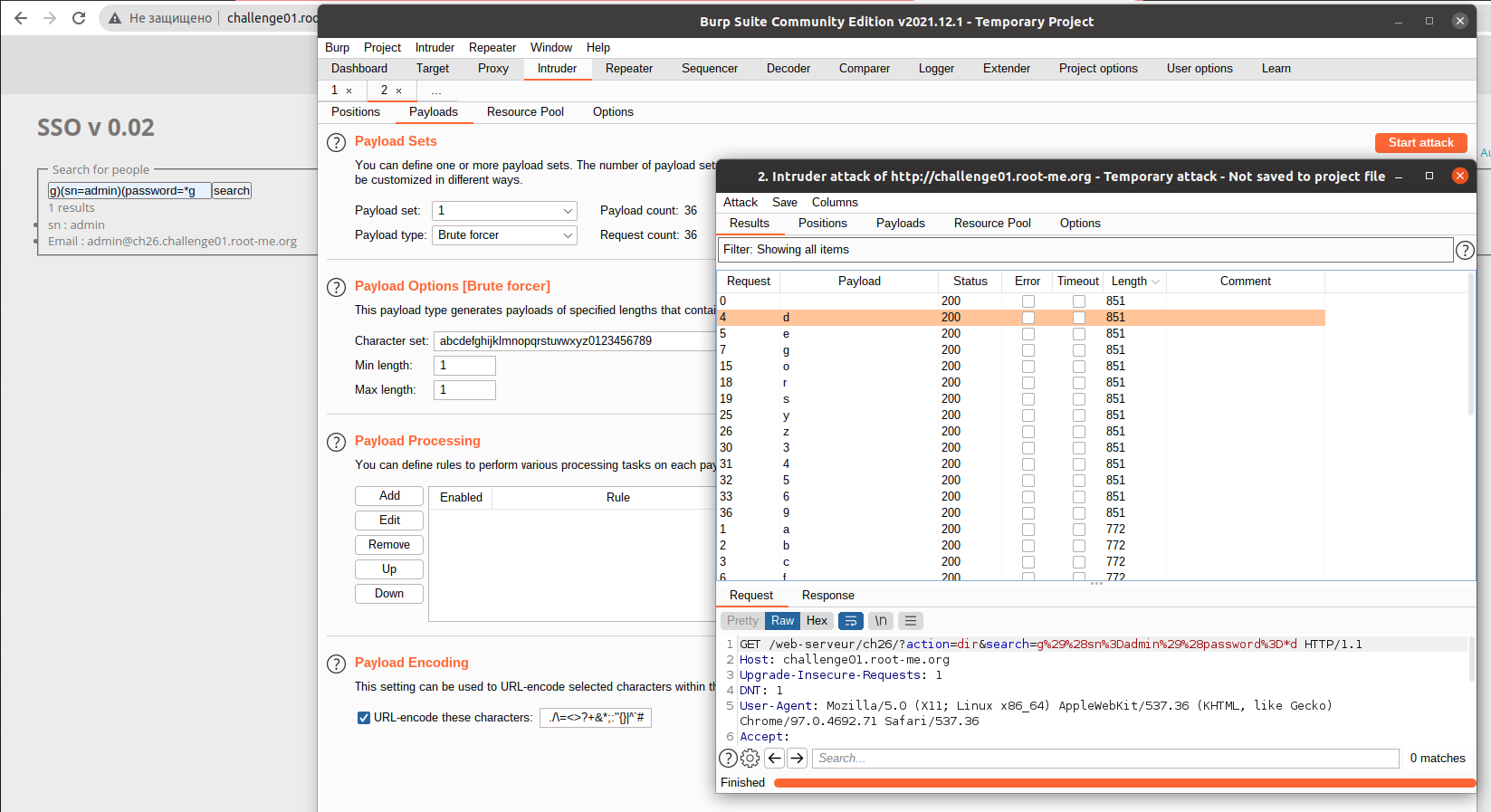
Решение:

К сожалению через Burp мне было сложнее выполнить это задание, чем через скрипт. Опыт в программировании у меня есть (Front-end), поэтому я выполнил это задание лишь через скрипт, но когда будет больше свободного времени разберусь как это делается и через Burp.

Что требуется для эксплуатации слепой LDAP-инъекции:

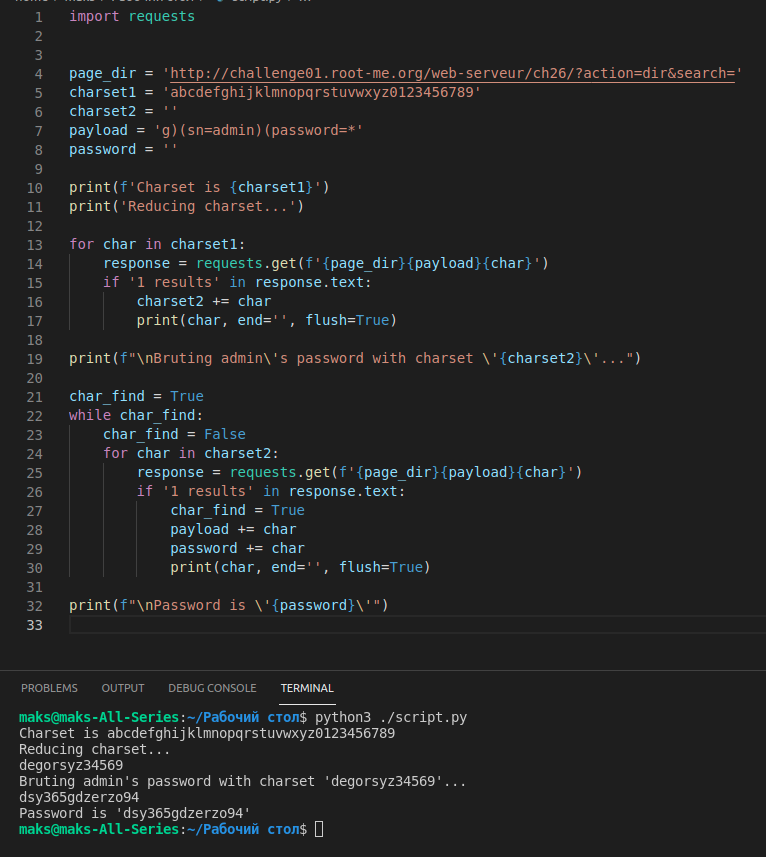
1. В патенциально уязвимом поле получить 3 статуса ответа:  
   ошибку, статус «не найдено» или же False и статус с результатом (True)
2. В нашем случае необходимо было определить по какому полю/параметру происходил поиск пользователя. У нас это поле E-mail.
3. На основе полученных данных построить валидное LDAP выажение для эксплуатации.

Вот попытки выполнить задание через Burp:



Дальше этого я не двинулся. Нашёл лишь из каких символов состоит пароль.

А вот собственно скриншот кода на Python:

Результат его работы можно видеть в терминале внизу.