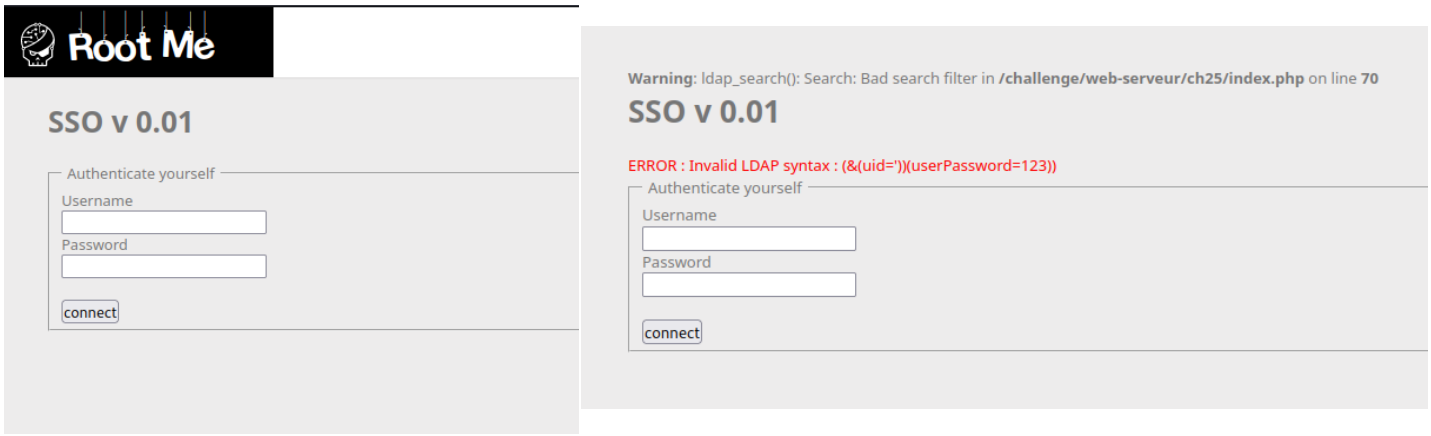
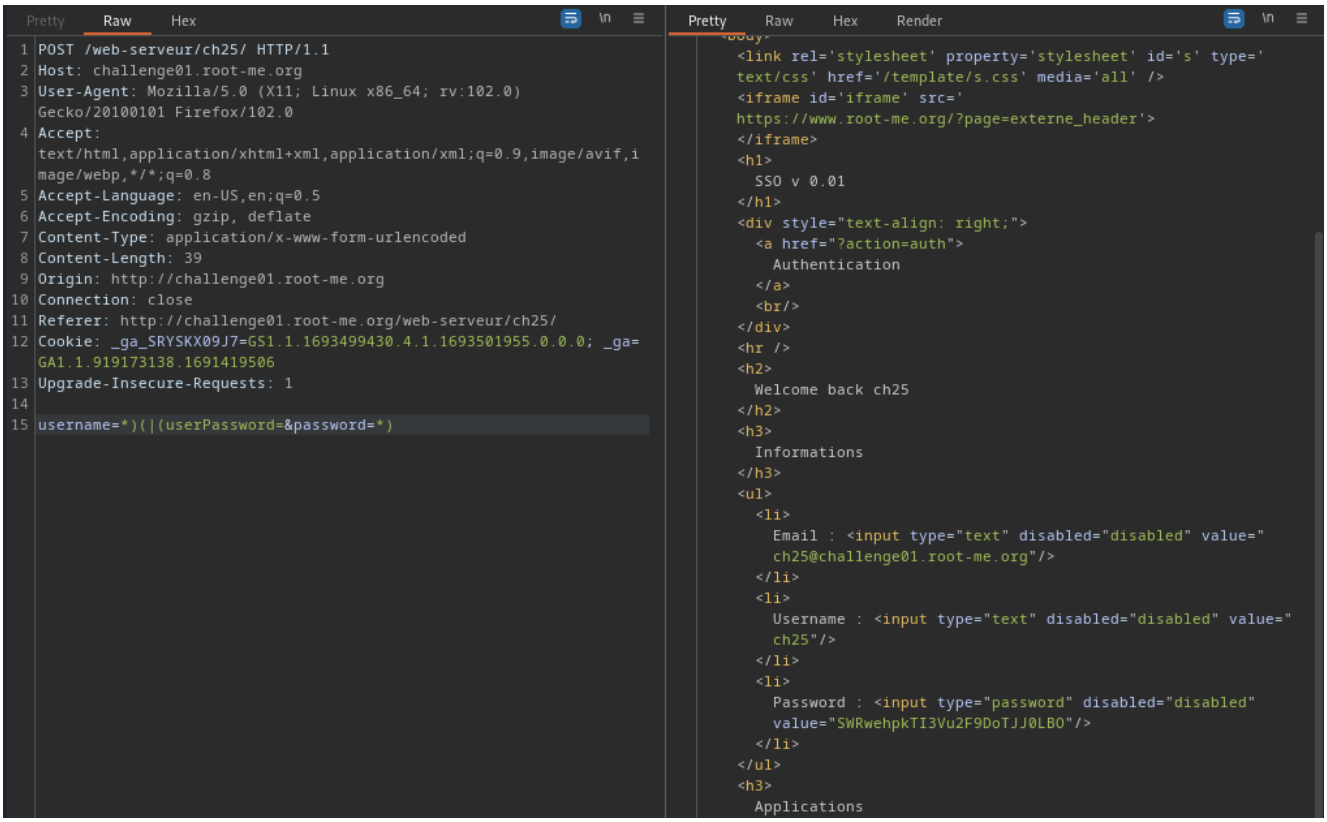
Выполнил Мешечкин Д. Инфобез-2837 (Ранее 2345)

Задание 1: Выполнить задание на LDAP injection https://www.root-me.org/en/Challenges/Web-Server/LDAP-injection-authentication

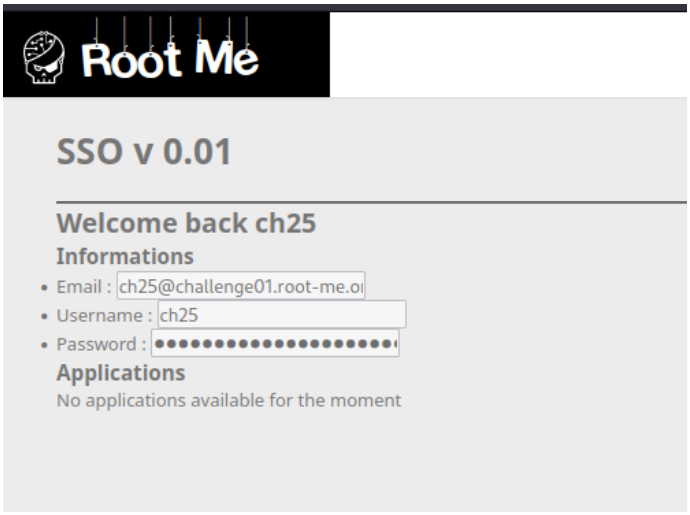
Изначально пробую нагрузку вида ') как логин и 123 как пароль.

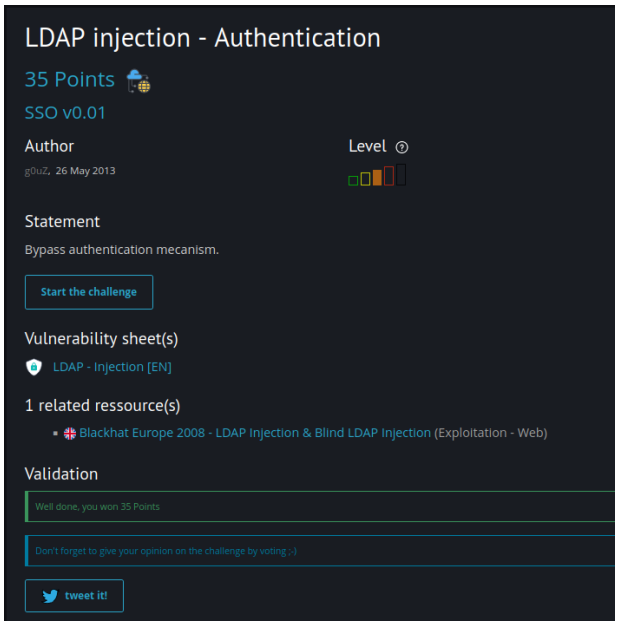


Отправляю перехваченный запрос в репитер и подставляю нагрузку в запрос username=*)(|(userPassword=&password=*)

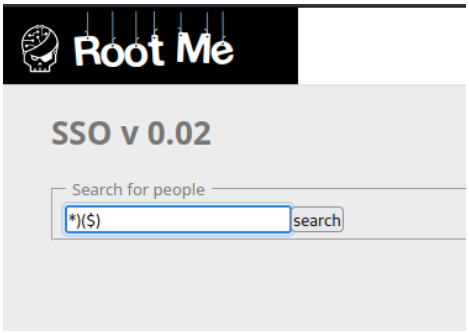


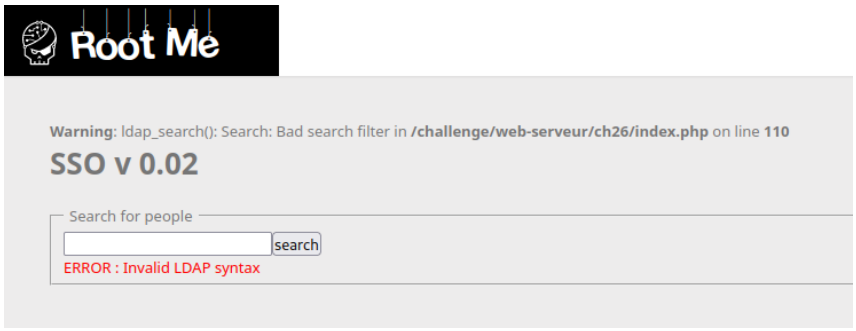
В результате получаю ответ в виде логина и пароля. Он используется как для логина на странице лабораторной машины, так и для сдачи лабораторной машины.



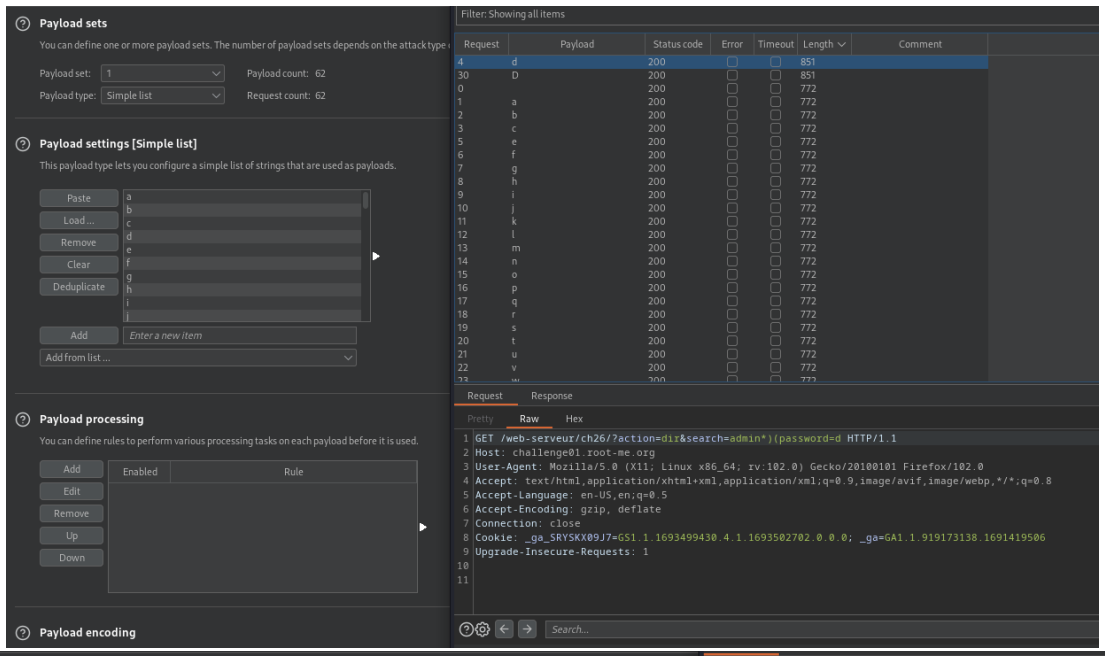


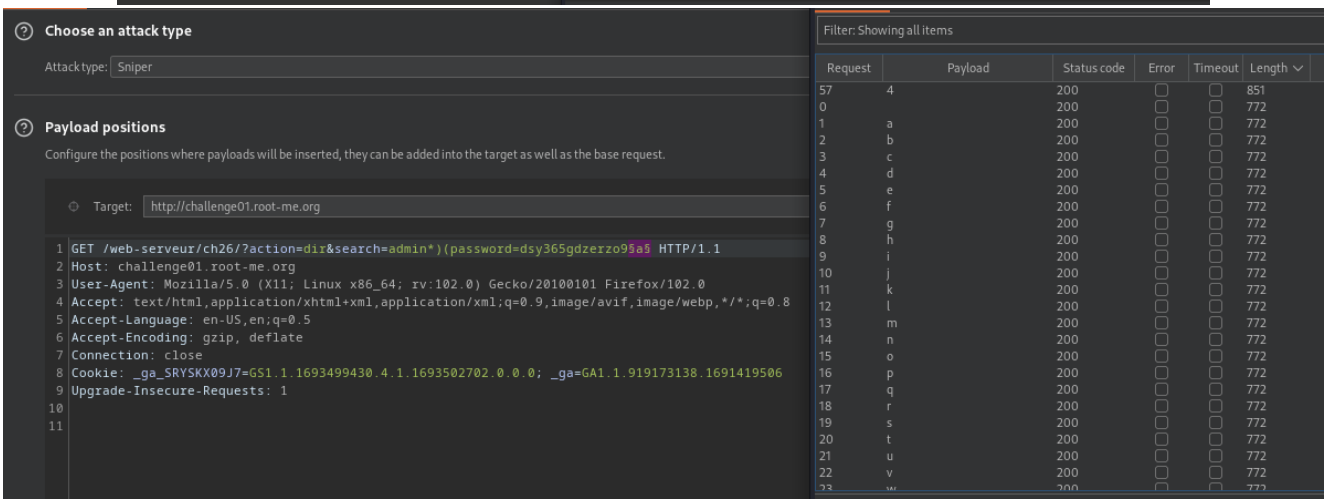
Задание 2: Выполнить задание на Blind LDAP injection https://www.root-me.org/en/Challenges/Web-Server/LDAP-injection-blind





На данном ресурсе есть форма аутентификации и поиска пользователей из БД. Для поиска пароля от логина admin будет использоваться форма поиска: ?action=dir&search=admin*)(password=





Таким образом брутфорсом подбираются результаты поиска, которые будут давать ответы отличные от "пустого ответа на запрос".
Собирается пароль dsy365gdzerzo94 используемый как для лабораторной машины, так и сдачи его на сайте.