Индивидуальный проект. Этап 5

Дисциплина: Основы информационной безопасности

Жибицкая Евгения Дмитриевна

Содержание

# 1 Цель работы

Завершение выполнения индивидуального проекта. Знакомство и освоение Burp Suite.

# 2 Выполнение лабораторной работы

Запустим сервер для работы с DVWA (рис. 1).



Рис. 1: Запуск mysql и apache2

Далее запускаем сам burpsuite.

Burp Suite представляет собой набор мощных инструментов безопасности веб-приложений, которые демонстрируют реальные возможности злоумышленника, проникающего в веб-приложения(рис. 2).

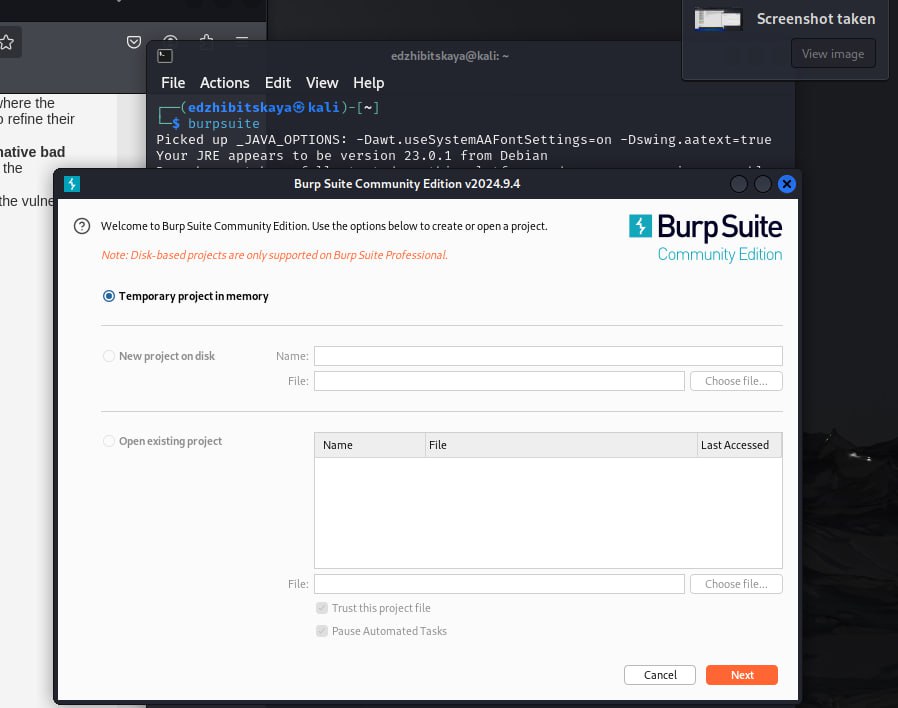


Рис. 2: Запуск burpsuite

После необходимо его настроить. Для этого в настройках соединения указываем 127.0.0.1 - наш сервер в http proxy(рис. 3), проверяем настройки приложения(рис. 4), ставим интерсепт в режим on(рис. 5).

Также устанавливаем на true параметр network.proxy.allow\_hijacking\_localhost(рис. 6).

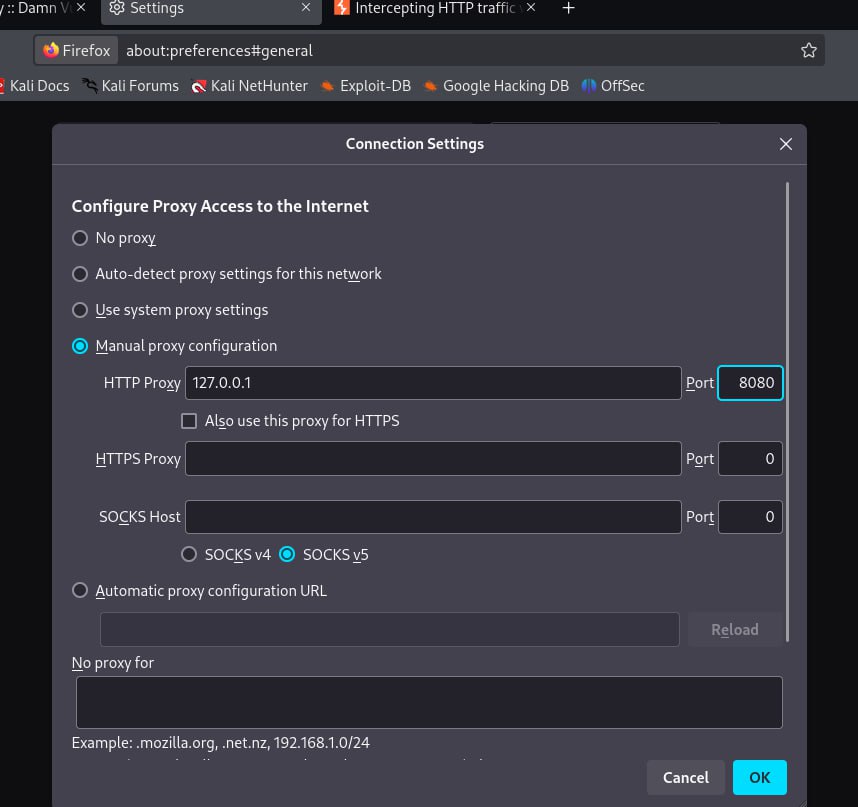


Рис. 3: Настройки соединения

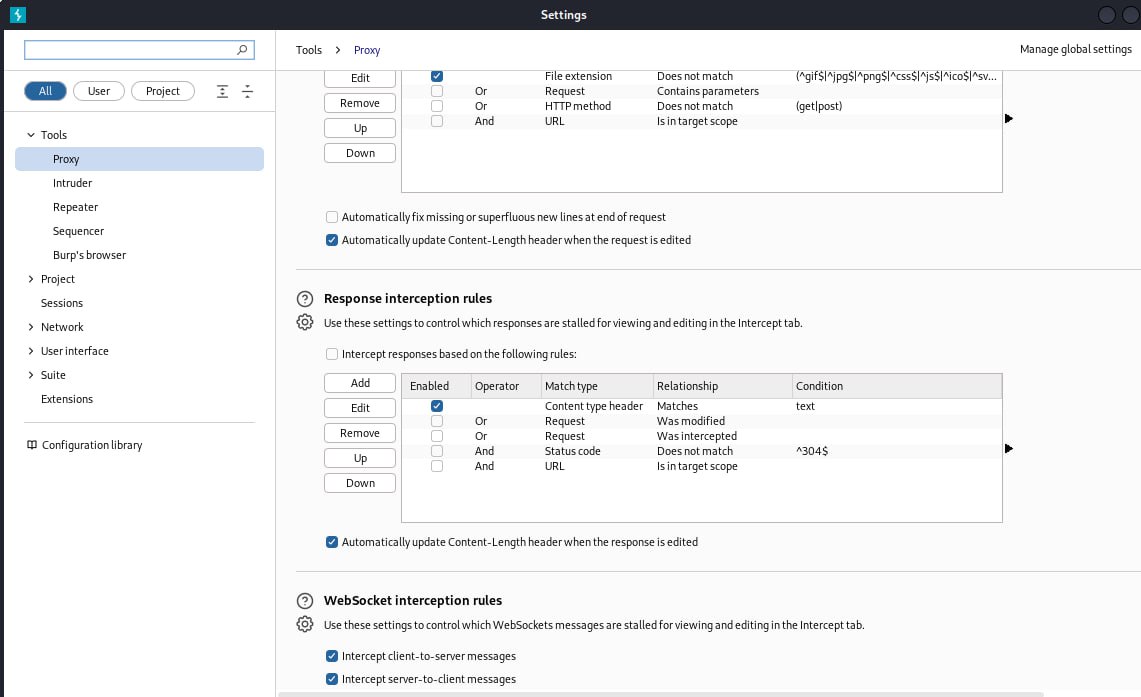


Рис. 4: Настройки приложения

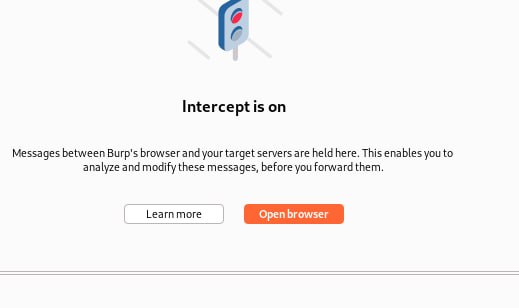


Рис. 5: Включение intercept

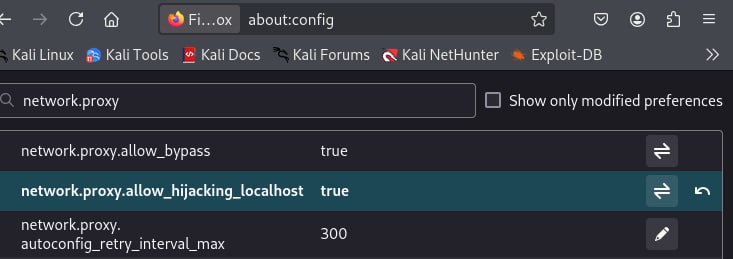


Рис. 6: Параметр network.proxy.allow\_hijacking\_localhost

Переходим непосредственно к работе.

Заходим на DVWA и смотрим, что появляется во вкладке Proxy(рис. 7). Видим, что запросы обновляются(также используем forward)(рис. 8).

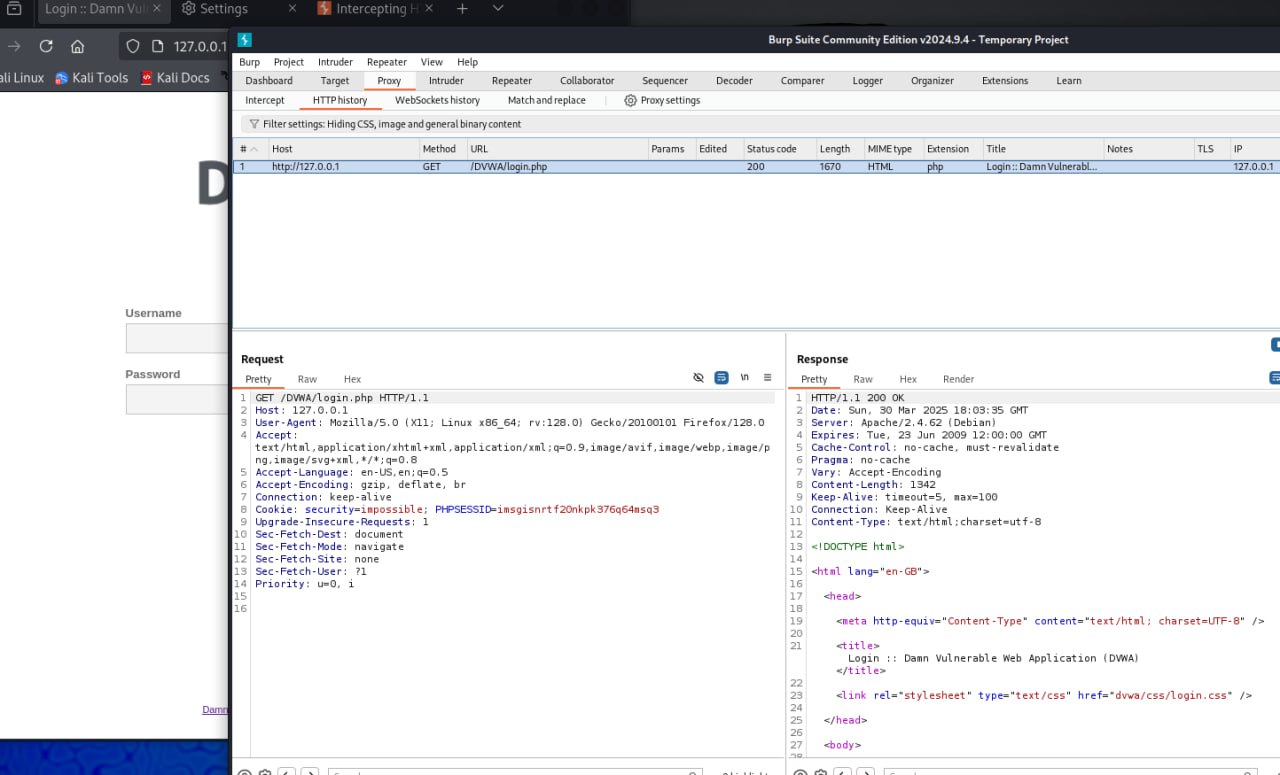


Рис. 7: Переход на DVWA

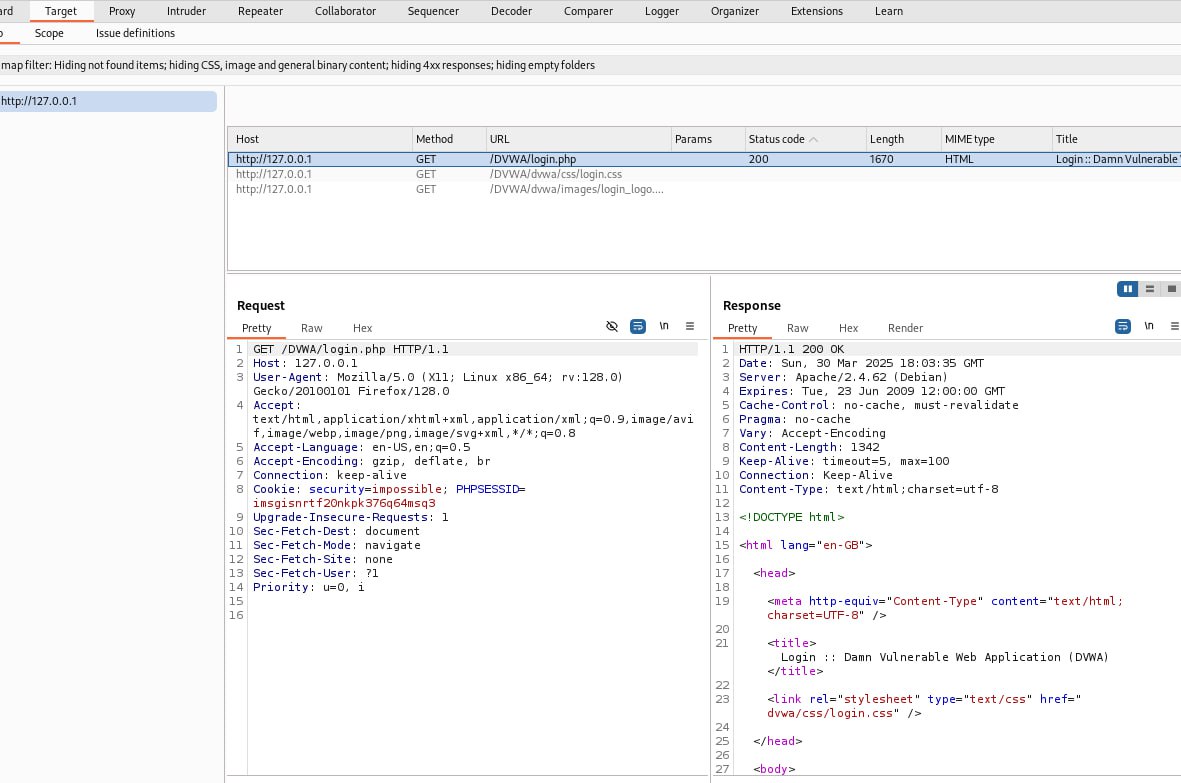


Рис. 8: Запросы

Пытаемся авторизоваться и видим внизу появляются введеные данные(рис. 9).



Рис. 9: Попытка авторизации

Отправялем запрос в Intruder(рис. 10).

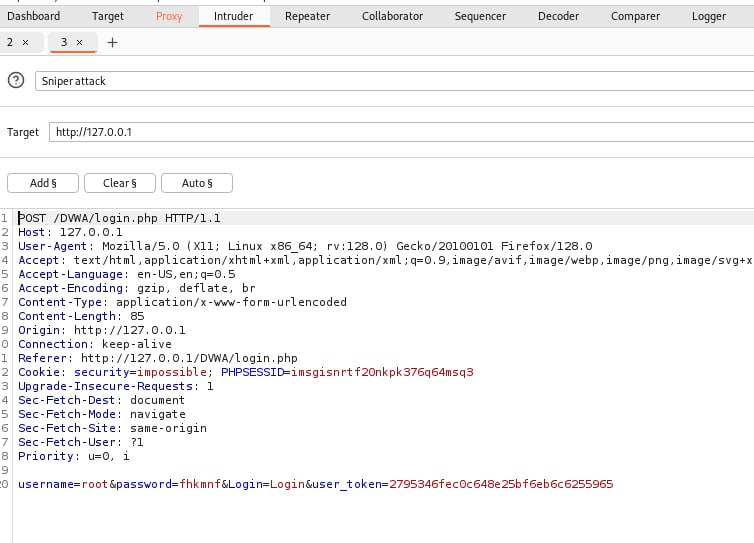


Рис. 10: Перенаправление в Intruder

Далее менеям тип атаки на Cluster bomb, меняем(убираем) данные о логине и пароле для дальнейшего подбора(рис. 11).

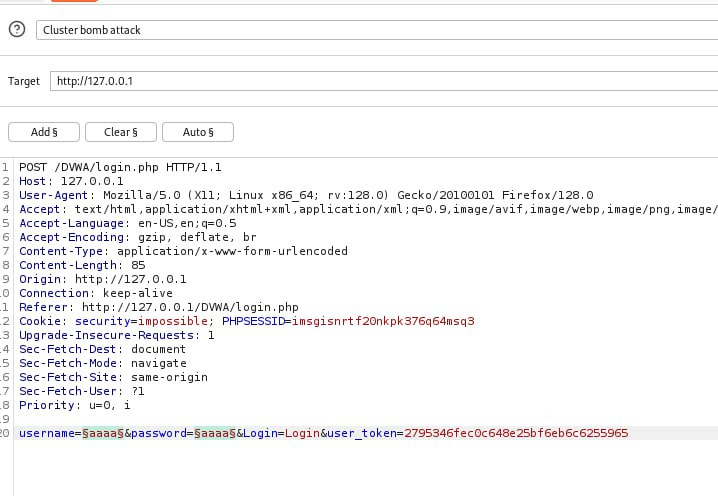
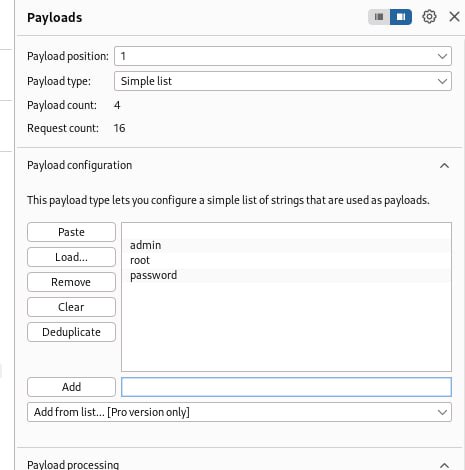


Рис. 11: Cluster bomb attack

Заполняем данными таблицы 1 и 2 - для логина и пароля(рис. **¿fig:012?**) и запускаем атаку(подбор и анализ)(рис. 12).

 .

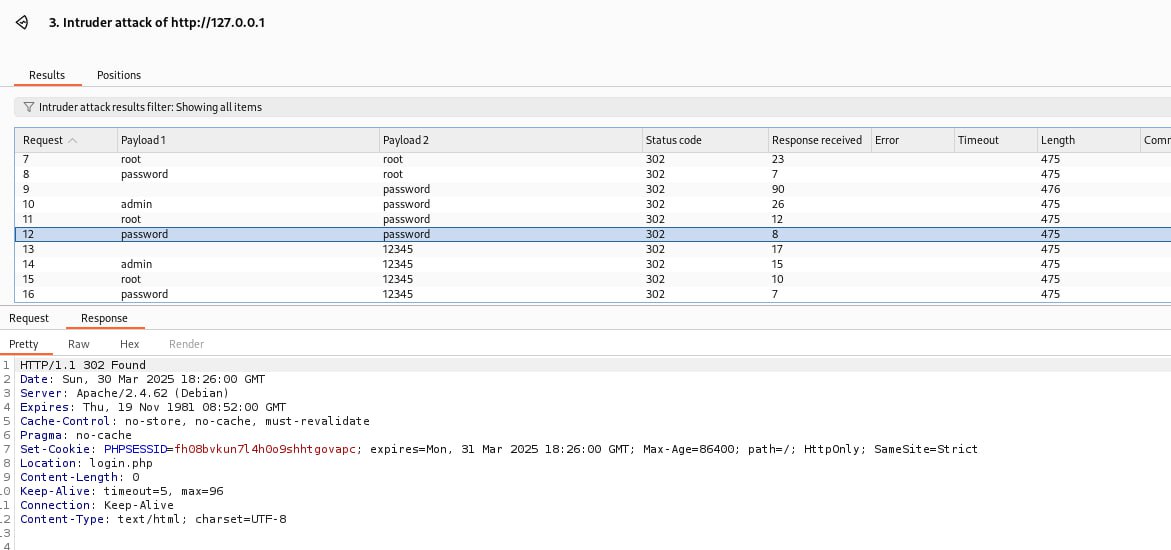


Рис. 12: Атака

На предыдщем рисунке видно, что местоположение не менятеся при неверных вариантах, а вот если посмотреть ниже, на подходящем наборе данных местоположение(location) уже меняется - происходит авторизация - вход успешный(рис. 13).

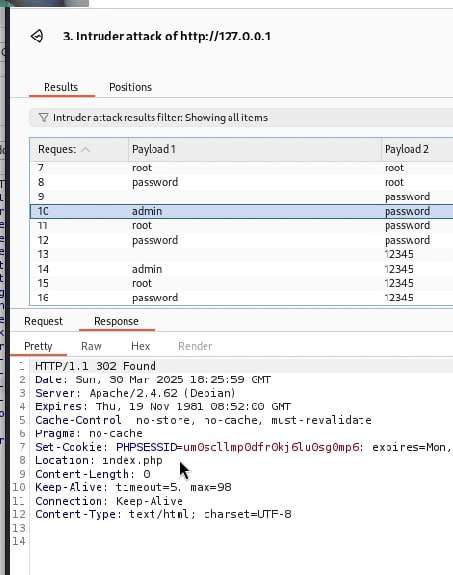


Рис. 13: Успешный подбор

Изучим также работы repeater. Перенаправим туда любой результат, посмотрим на его ответ в виде render - увидим страницу входа(рис. 14).

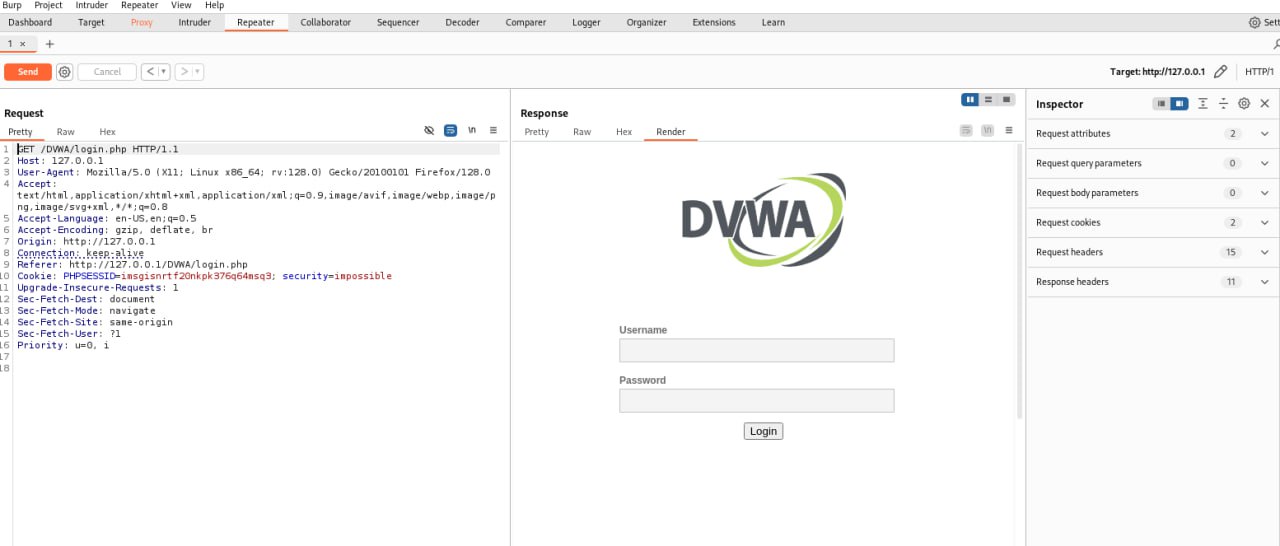


Рис. 14: Reapeter

# 3 Выводы

В ходе работы было произведена знакомство с Burp Suite, произведен анализ работы и принцип атаки подбора данных для входа

# Список литературы

* Парасрам, Ш. Kali Linux: Тестирование на проникновение и безопасность : Для профессионалов. Kali Linux / Ш. Парасрам, А. Замм, Т. Хериянто, и др. – Санкт-Петербург : Питер, 2022. – 448 сс.