Индивидуальный проект этап 5

Информационная безопасность

Ким Илья Владиславович НФИбд-01-21

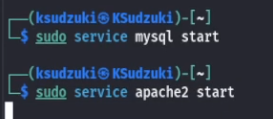
Содержание

# Цель работы

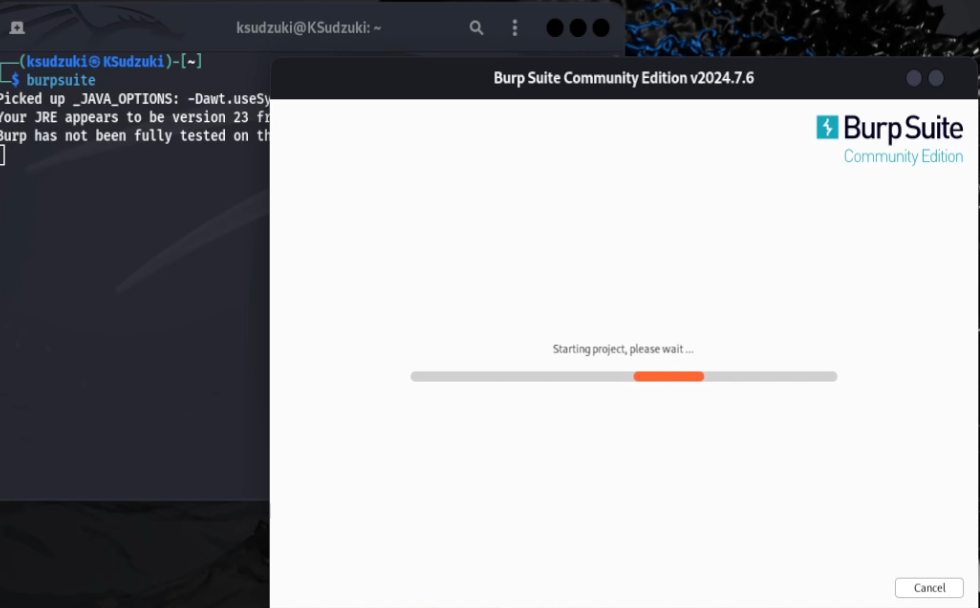
Научиться пользоваться Burp Suite

# Выполнение лабораторной работы

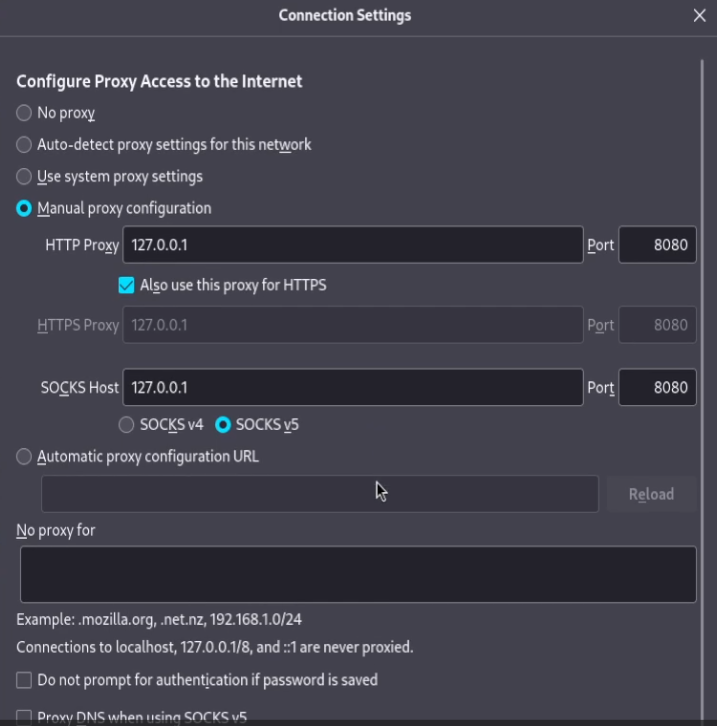
1. Запустил локальный веб-сервер (рис. [-@fig:001])



1. Запустил Burp Suite (рис. [-@fig:002])



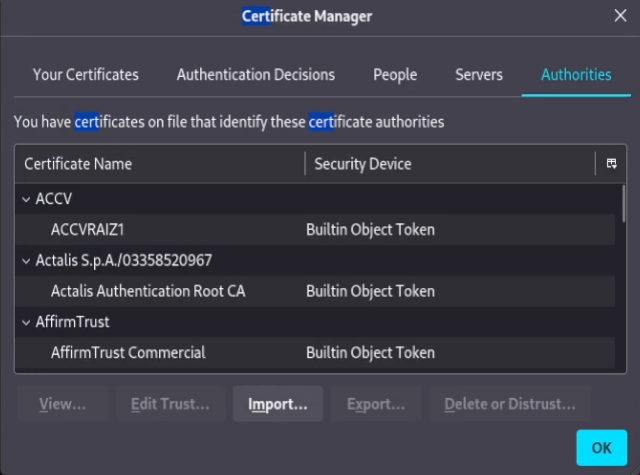
1. Настроил прокси в браузере (рис. [-@fig:003])



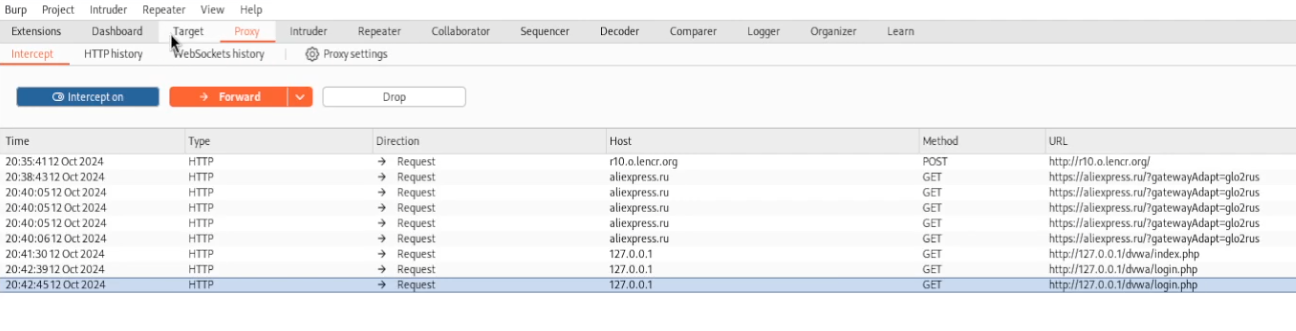
1. Зашёл на сайт burp и скачал сертификаты (рис. [-@fig:004])



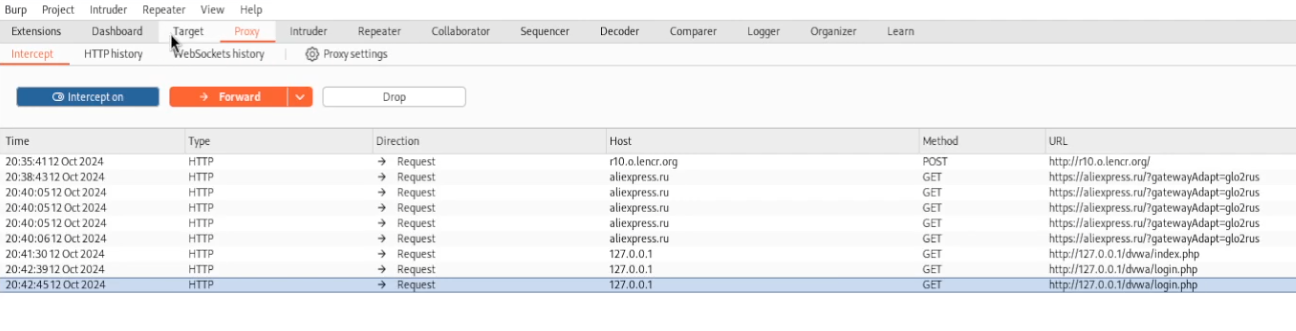
1. Установил сертификаты в браузер (рис. [-@fig:005])



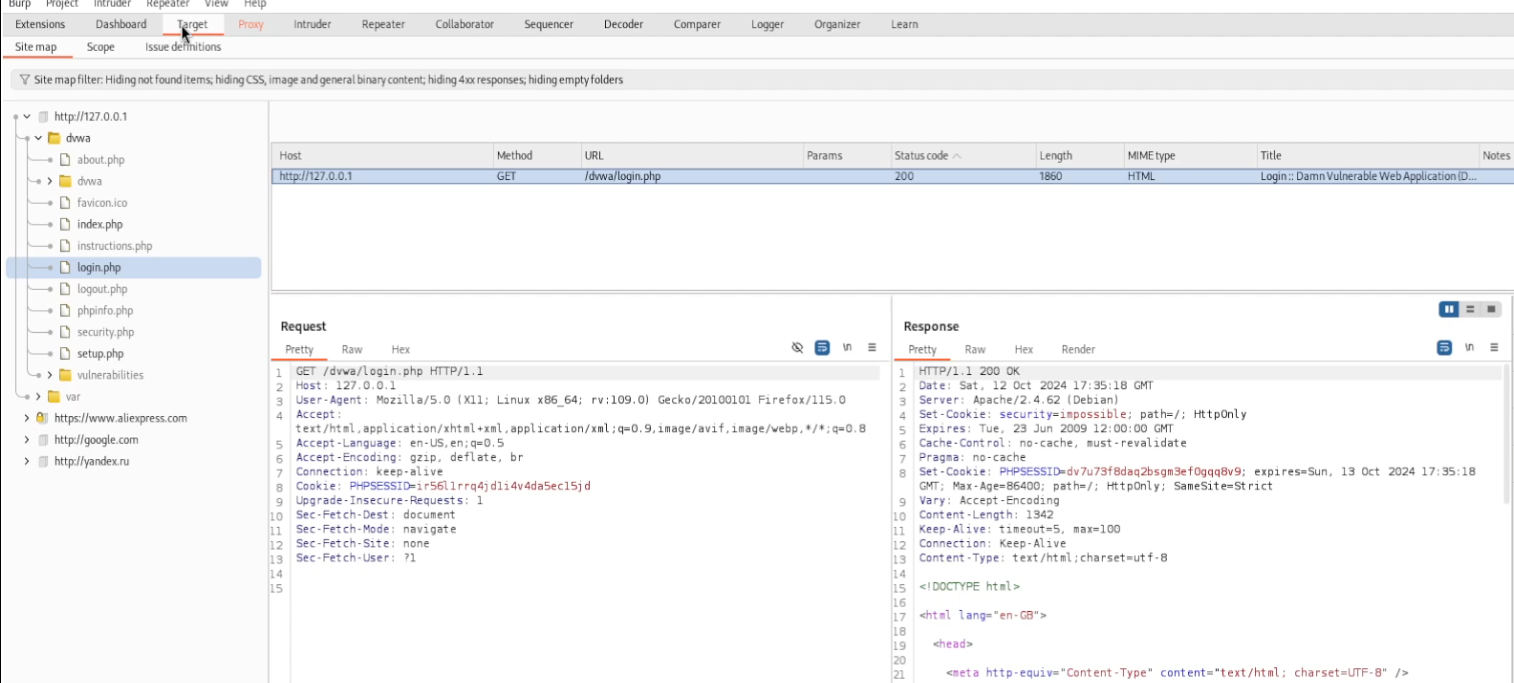
1. Перезапустил BurpSuite и зашёл на наш сайт dvwa/login.php (рис. [-@fig:006])



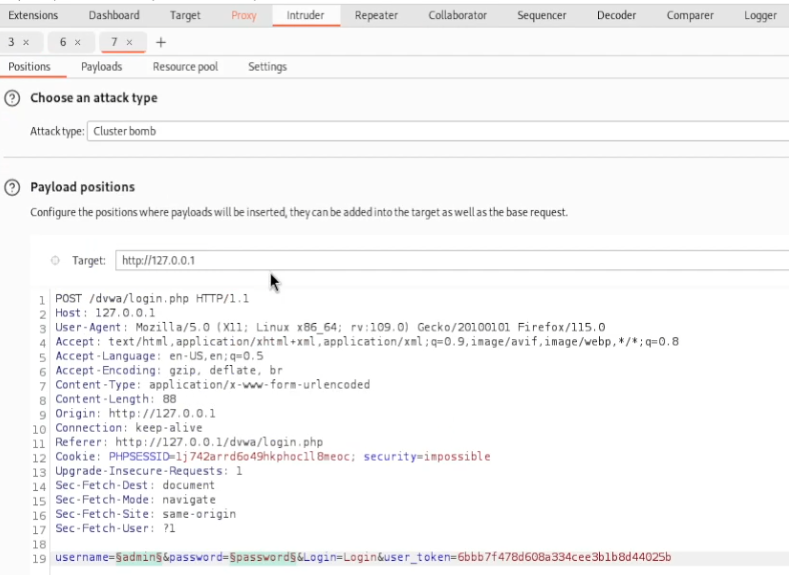
1. Во вкладке Proxy отображаются запросы на вход (рис. [-@fig:007])



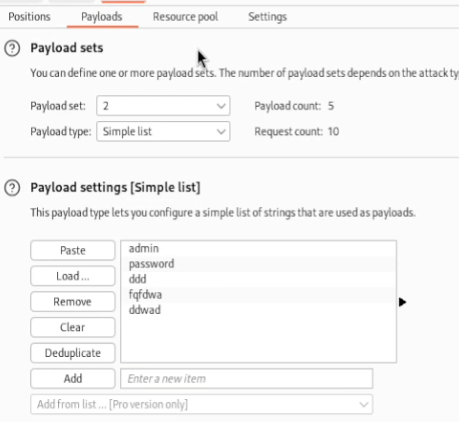
1. Во вкладке target мы можем посмотреть данные о цели (рис. [-@fig:008])



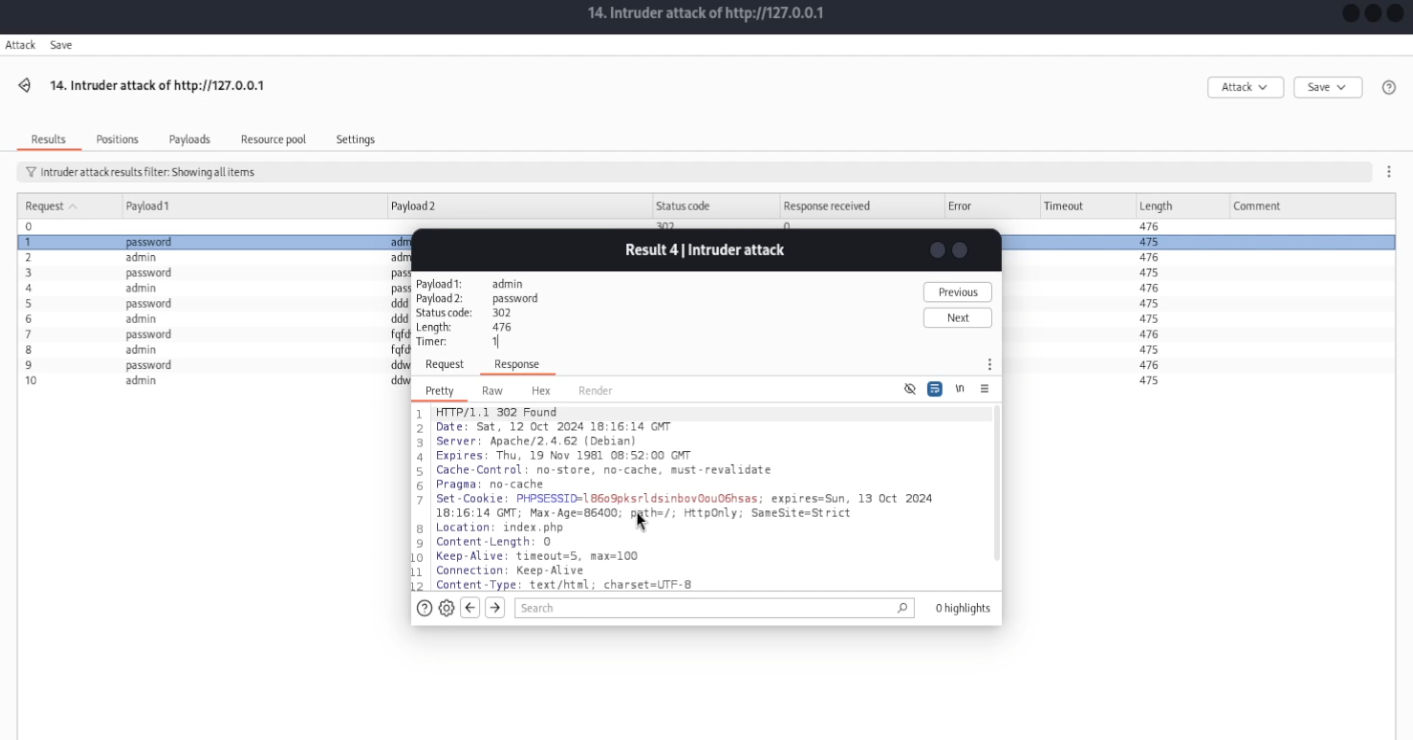
1. От туда мы можем отправить сайт во вкладку Intuder (рис. [-@fig:009])



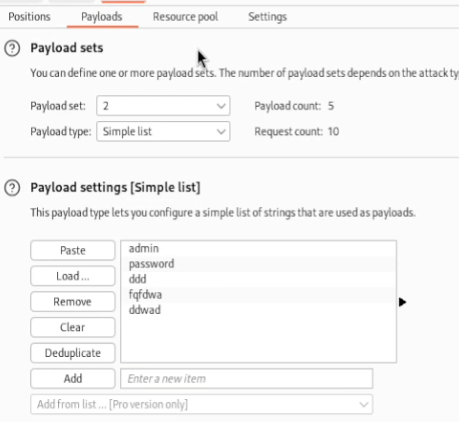
1. Здесь мы можем заполнить данные, которые будут посылаться на сайт, и произвести атаку (рис. [-@fig:010])



1. Произведя атаку, мы можем посмотреть данные, в которых можно увидеть где мы оказываемся. При комбинации admin и password, мы оказываемся на index.php, что означает успешные переход на другую страницу - вход (рис. [-@fig:011])



1. Здесь мы можем заполнить данные, которые будут посылаться на сайт, и произвести атаку (рис. [-@fig:012])



# Выводы

Попробовали применить инструменты Burp Suite на практике, использовали наш локальный веб-сервер для проверки атаки и исследовали полученные данные.