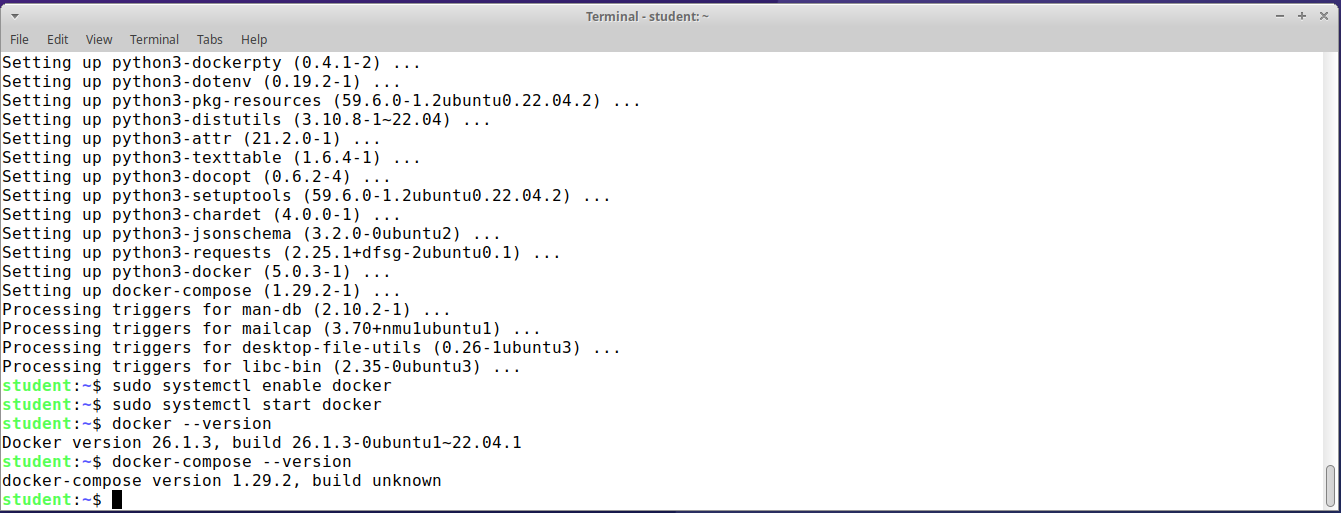
Реализация задания «Настройка системы защиты веб-приложений с использованием WAF»

План

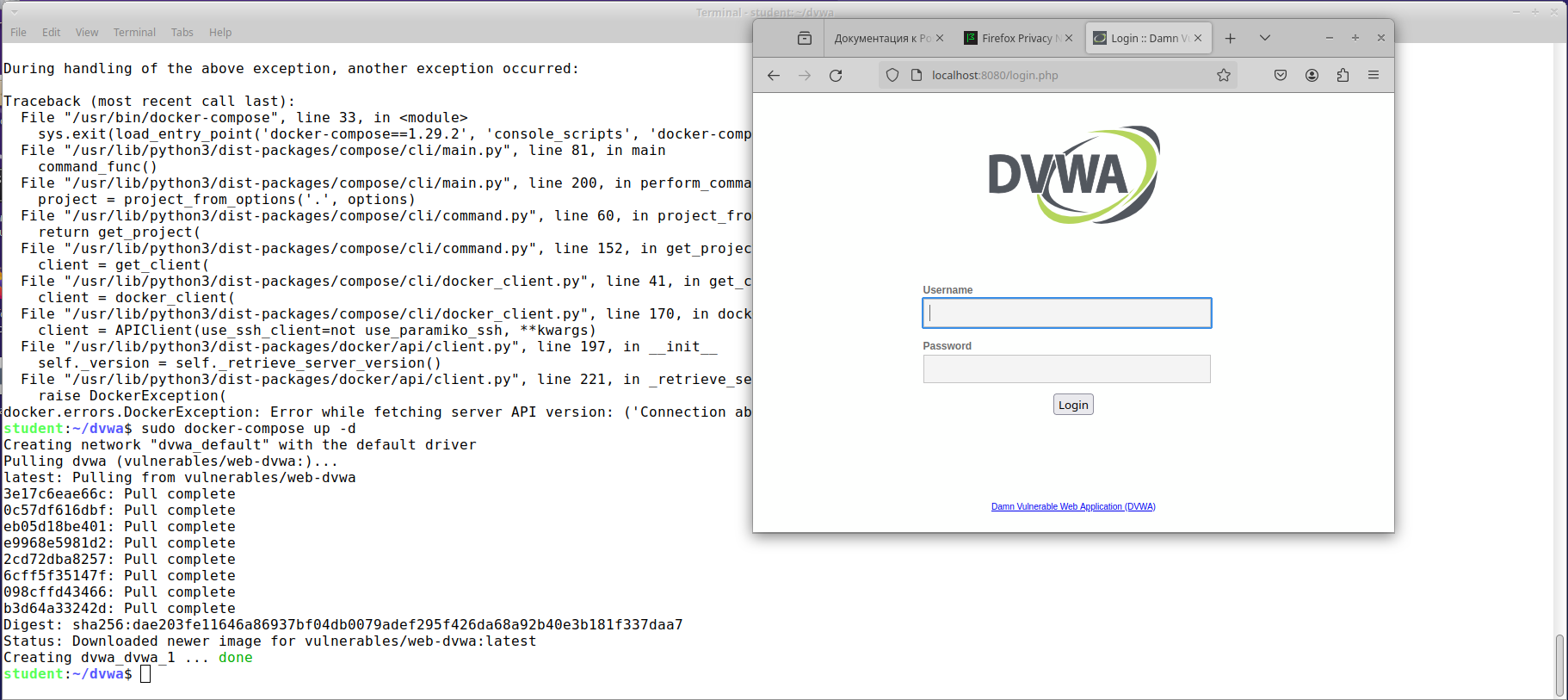
* Развертывание уязвимого веб-приложения DVWA
* Настройка Web Application Firewall при помощи ModSecurity для защиты от распространённых атак (SQL инъекции, XSS, RCE)
* Настройка мониторинга безопасности с использованием Kibana и Elastic Stack
* Анализ производительности приложения до и после внедрения WAF (производительность и ложные срабатывания)

Развертывание уязвимого веб-приложения DVWA

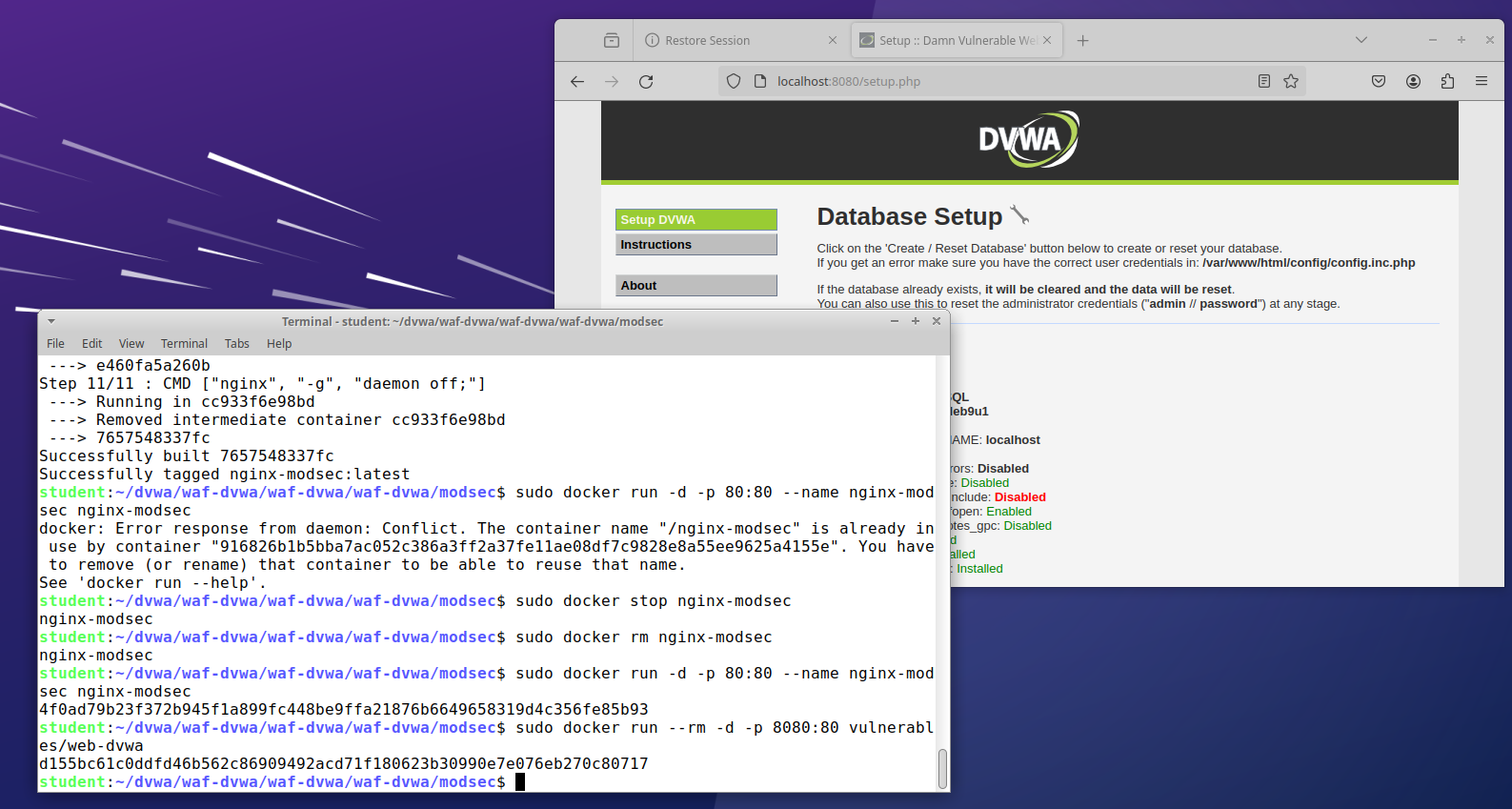


*Рис. 1, Установка и запуск Docker*

Развертывание DVWA с помощью Docker

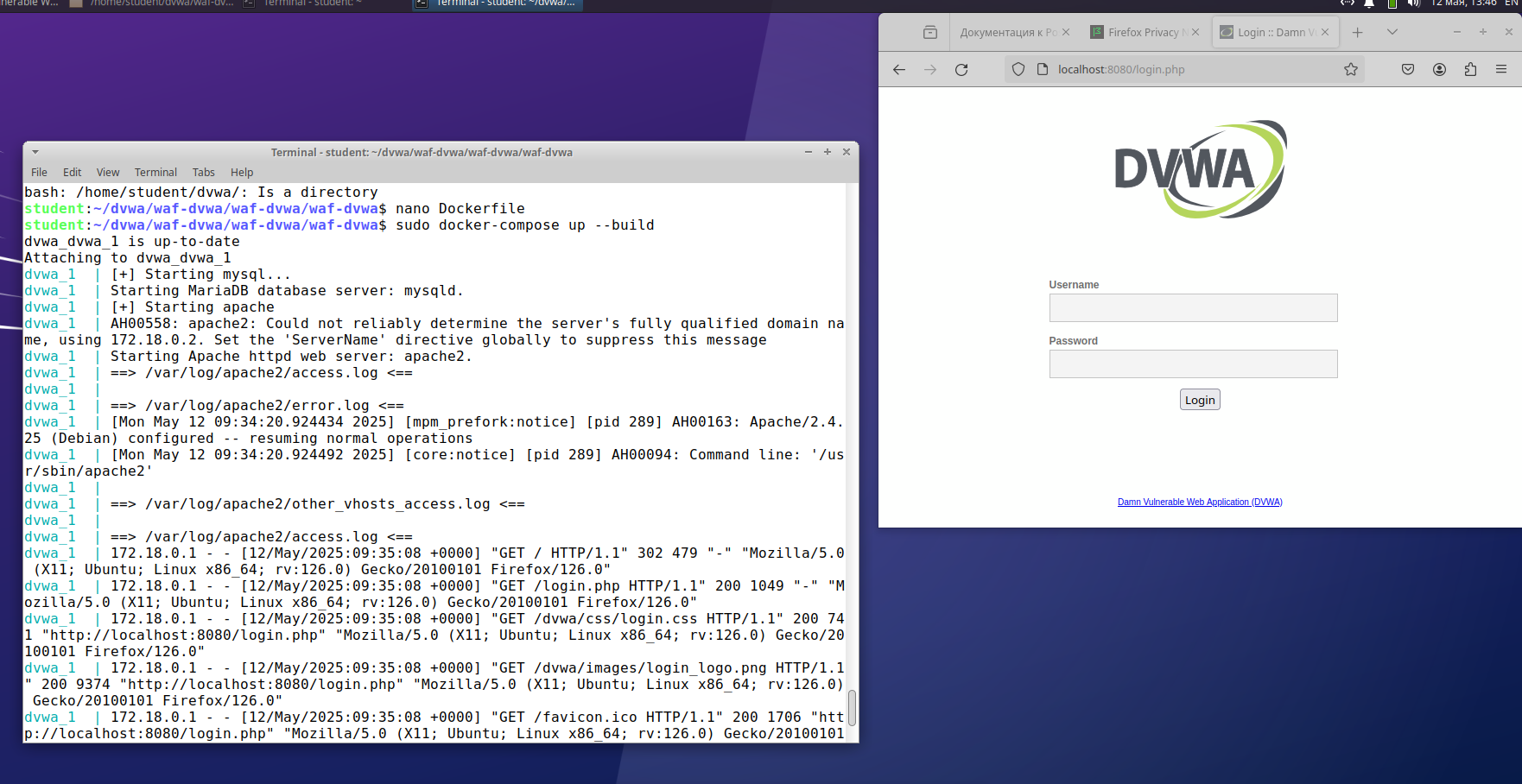


*Рис. 2, Развертывание DVWA с помощью Docker*

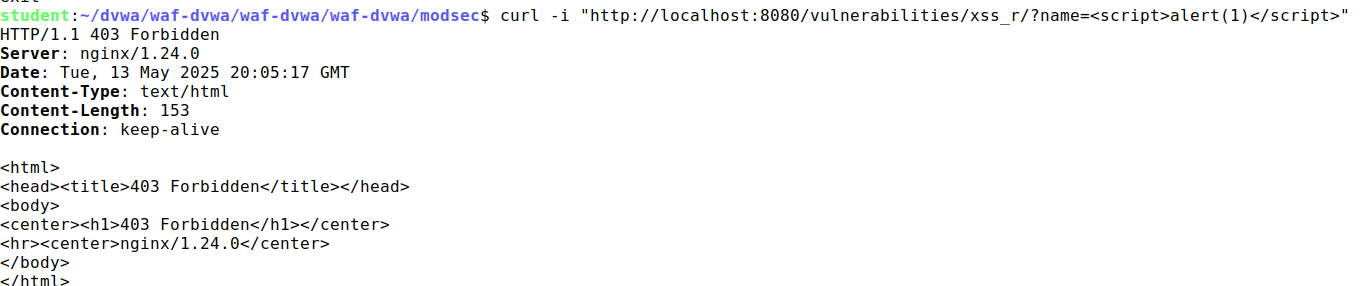


*Рис. 3, Демонстрация работоспособности DVWA*

Настройка Web Application Firewall с ModSecurity

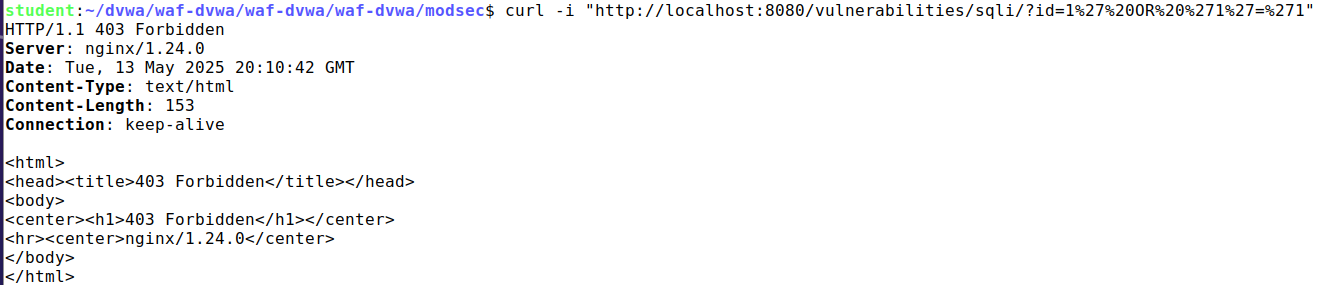
 *Рис. 4, Сборка Web Application Firewall с ModSecurity*

Простая проверка XSS



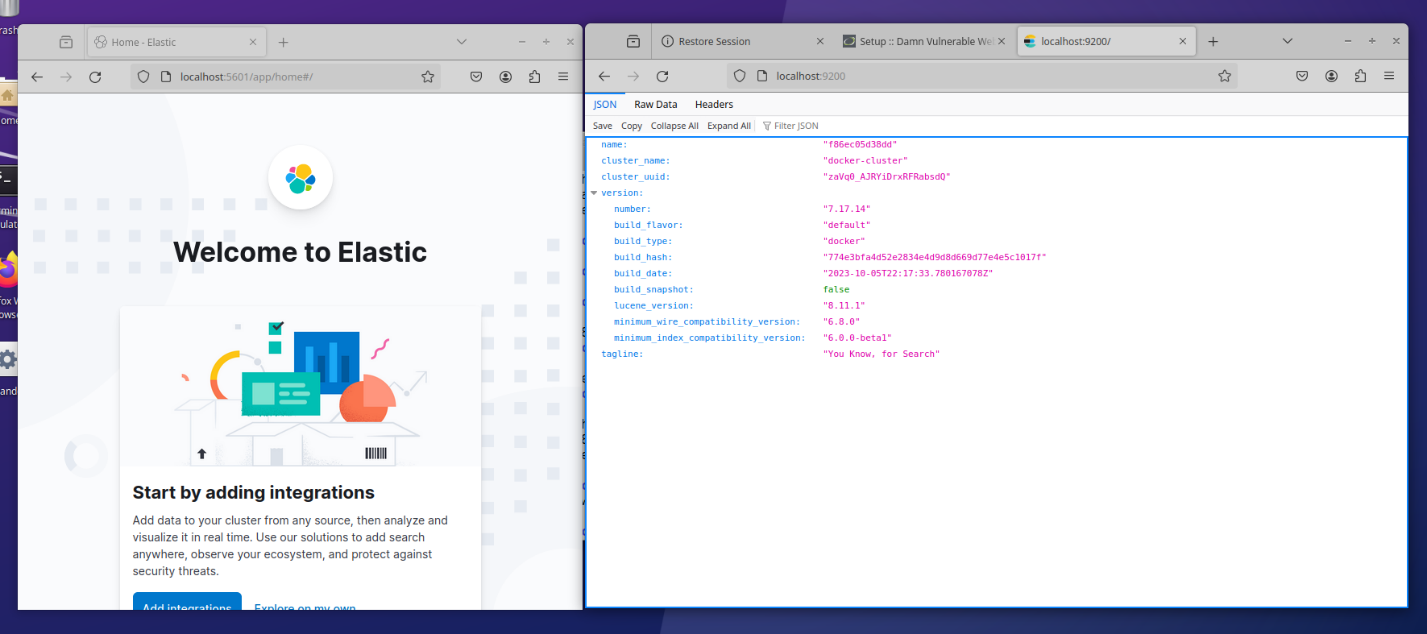
*Рис. 5, проверка защиты от XSS*

проверка SQL-инъекции



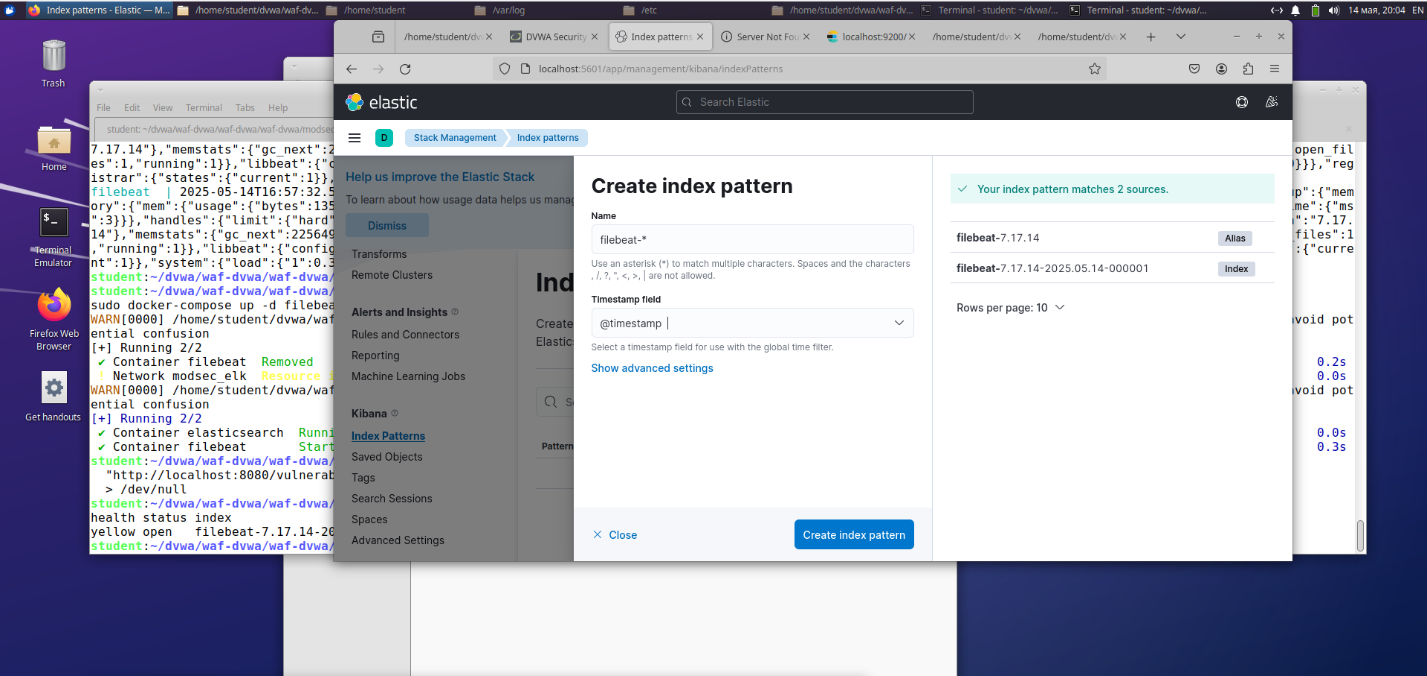
*Рис. 6, проверка защиты от SQL-инъекции*

Настройка мониторинга безопасности с использованием Kibana и Elastic Stack

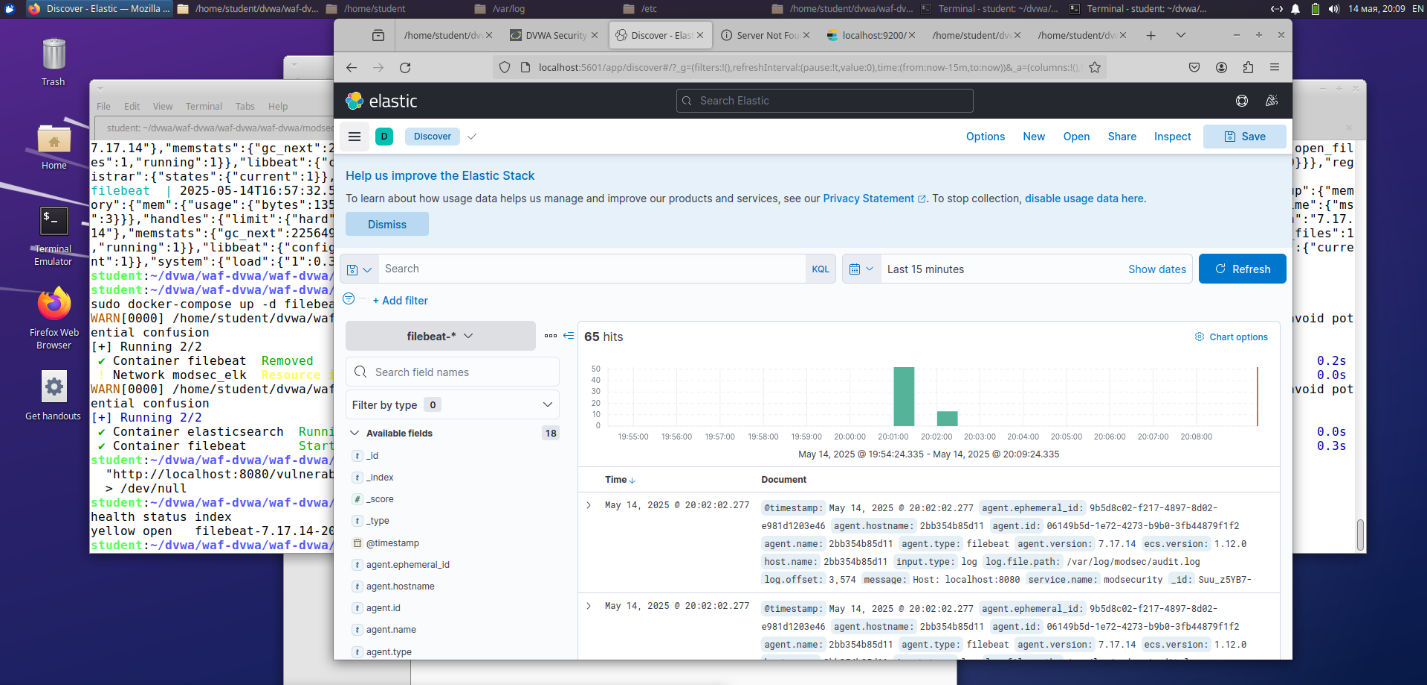
 *Рис. 7, Демонстрация работоспособности Kibana и Elastic Stack*



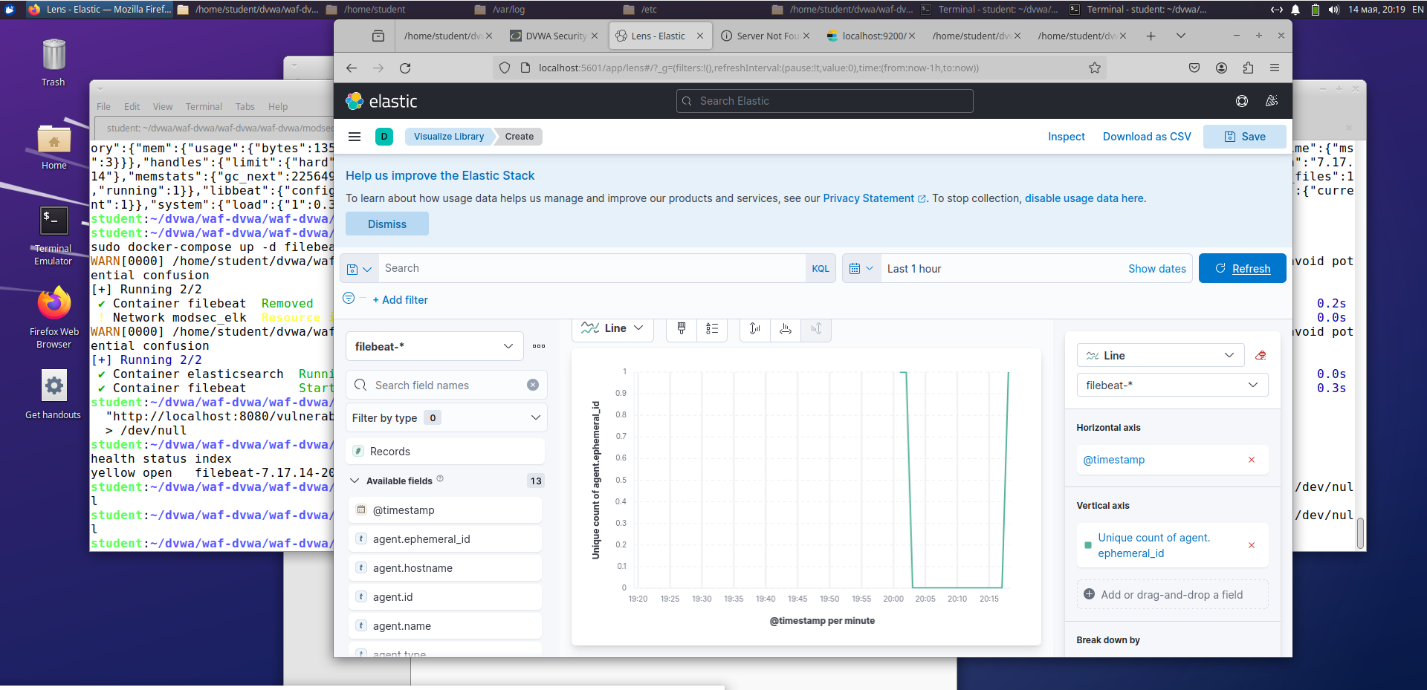
*Рис. 8, Настройка input на Modsec-audit*



*Рис. 9, Настройка Kibana*



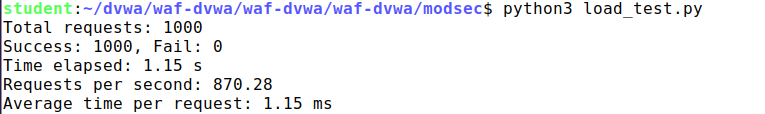
*Рис. 10, Просмотр событий в Discover*



*Рис. 11, Настройка визуализации линейного графика Kibana*

Проверки:

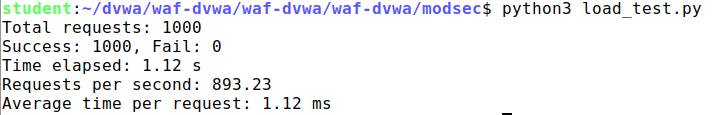
С WAF



*Рис. 12, Проверка работоспособности с WAF*

Отключение WAF

Без WAF



*Рис. 13, Проверка работоспособности без WAF*

Вывод

В ходе тестирования производительности уязвимого веб-приложения DVWA были проведены нагрузочные испытания с использованием 1000 HTTP-запросов при 50 параллельных соединениях. Тестирование проводилось в двух режимах: с включённым веб-фаерволом (ModSecurity) и без него. При включённом WAF средняя производительность составила 870 запросов в секунду, а среднее время обработки одного запроса — 1.15 миллисекунды. Без использования WAF производительность составила 893 запросов в секунду со средней задержкой 1.12 миллисекунды. Таким образом, включение WAF привело к незначительному снижению производительности примерно на 2.5%, что обусловлено дополнительной проверкой и фильтрацией входящих запросов. Несмотря на это, все запросы были успешно обработаны в обоих режимах, а разница в отклике оказалась минимальной. Это свидетельствует о том, что использование ModSecurity обеспечивает дополнительный уровень безопасности веб-приложения без существенного влияния на его производительность.