Основы информационной безопасности

Индивидуальный проект. Этап № 4. Использование Nikto

Подлесный Иван Сергеевич

Содержание

Список иллюстраций

Цель работы

Целью данной работы является сканирование уязвимостей с помощью приложения Nikto

Теоретические сведения

Damn Vulnerable Web Application (DVWA) — это намеренно уязвимое веб-приложение на PHP/MySQL. Цель проекта — помочь этичным хакерам и специалистам ИБ отточить свои навыки и протестировать инструменты.

DVWA также может помочь веб-разработчикам и изучающим ИБ, лучше понять процесс безопасности веб-приложений.

Ход работы

Проверим, что nikto установлен(рис. fig. 1)

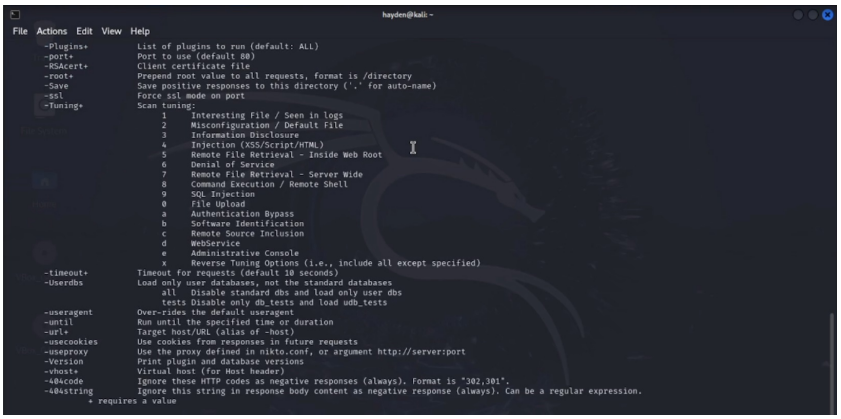

Рис. 1: Проверка установки ПО

Затем проверим сайт DVWA, указав опции для сохранения отчета в формате html(рис. fig. 2,).

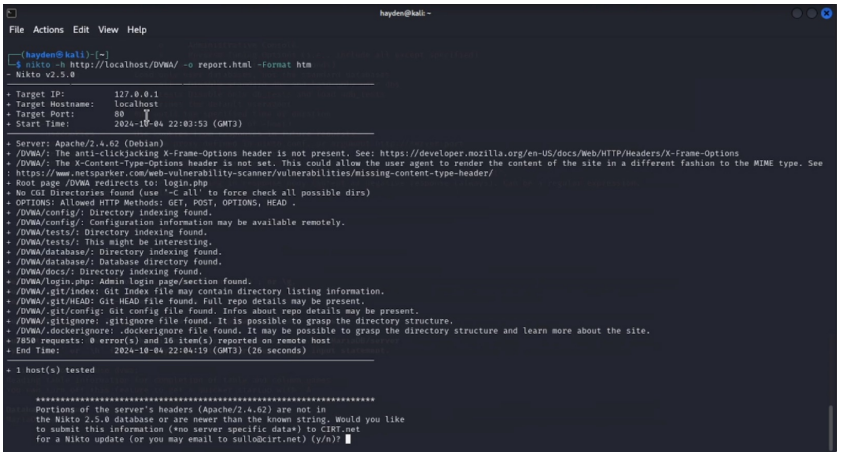

Рис. 2: Проверка уязвимостей по доменному имени

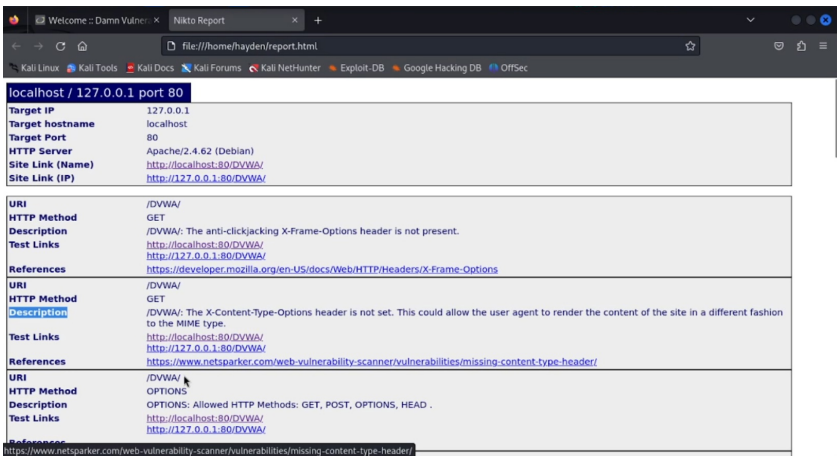

Рис. 3: Отчет об уязвимостях в формате html

Можем увидеть, что найдены такие уязвимости как отсутствие защиты от кликджекинга, не установлен заголовок X-Content-Type-Options(в связи с чем пользователь может выполнить вредоносный контент не того типа, который предполагает администратор), возможность удаленного доступа к файлам конфигураций, также найдена скрытая папка git, в которой хранятся данные о структуре сайта. В конце отчета указано, что найдено 16 уязвимостей.

Также можно посмотреть информацию об уязвимостях по конкретному порту(в нашем случае порт 80 для локального хоста)(рис. fig. 4).

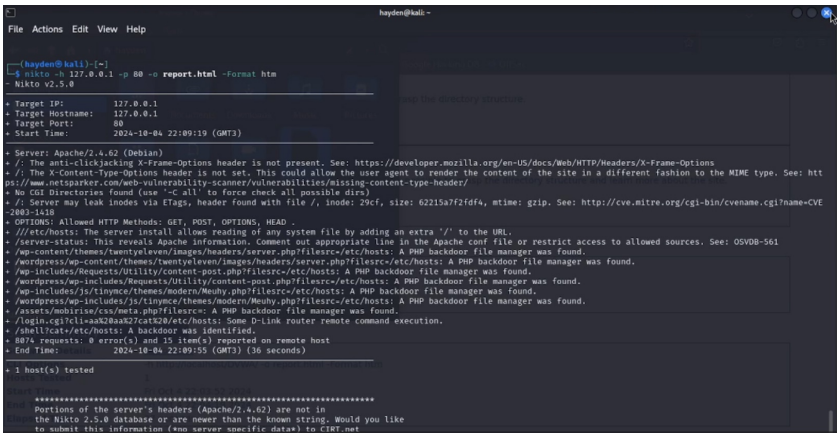

Рис. 4: Проверка уязвимостей с указанием порта

Выводы

В результате выполнения работы был использован сканер Nikto для сканирования уязвимостей веб-приложения.