Отчёт по 4-ому этапу индивидуального проекта

Основы информационной безопасности

Бережной Иван Александрович

Содержание

Список иллюстраций

# 1 Цель работы

Научиться тестировать веб-приложения с помощью сканера nikto

# 2 Задание

Использовать nikto на DVWA

# 3 Теоретическое введение

Nikto – бесплатный сканер для поиска уязвимостей в веб-серверах. Утилита относиться к классу blackbox сканеров, т. е. сканеров, использующих стратегию сканирования методом черного ящика. Это значит, что заранее неизвестно о внутреннем устройстве программы/сайта (доступ к исходному коду отсутствует) и упор сделан на функциональность. Программа может обнаруживать более 6700 потенциально опасных файлов и уязвимостей. Новые уязвимости добавляются в базу данных программы по мере их возникновения. Помимо поиска уязвимостей, сканер производит поиск на наличие устаревших версий, используемых библиотек и фреймворков. Nikto не позиционируется как стелс сканер (стелс сканеры никогда не устанавливают TCP-соединения до конца, тем самым сканирование происходит скрытно) – при сканировании сайта в логах сайта или в любой другой системе обнаружения вторжений, если она используется, будет отображена информация о том, что сайт подвергается сканированию.

# 4 Выполнение задания

Для начала запустим зависимости (рис. 1), а затем и сам DVWA (рис. 2).

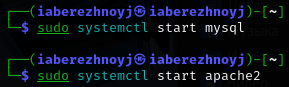


Рис. 1: Запуск mysql и apache

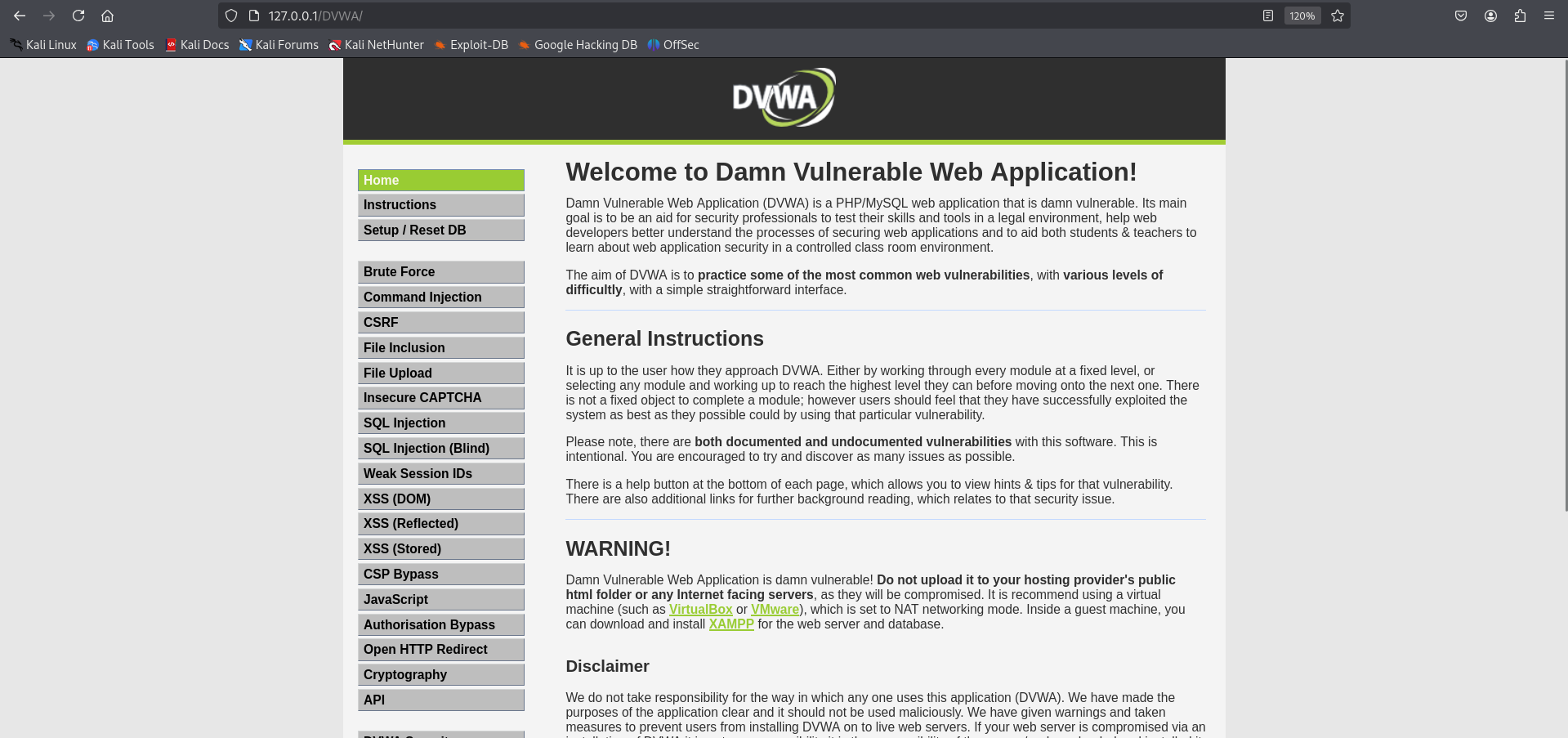


Рис. 2: Открытие DVWA

Теперь запустим nikto следующей командой: nikto -h http://127.0.0.1/DVWA/

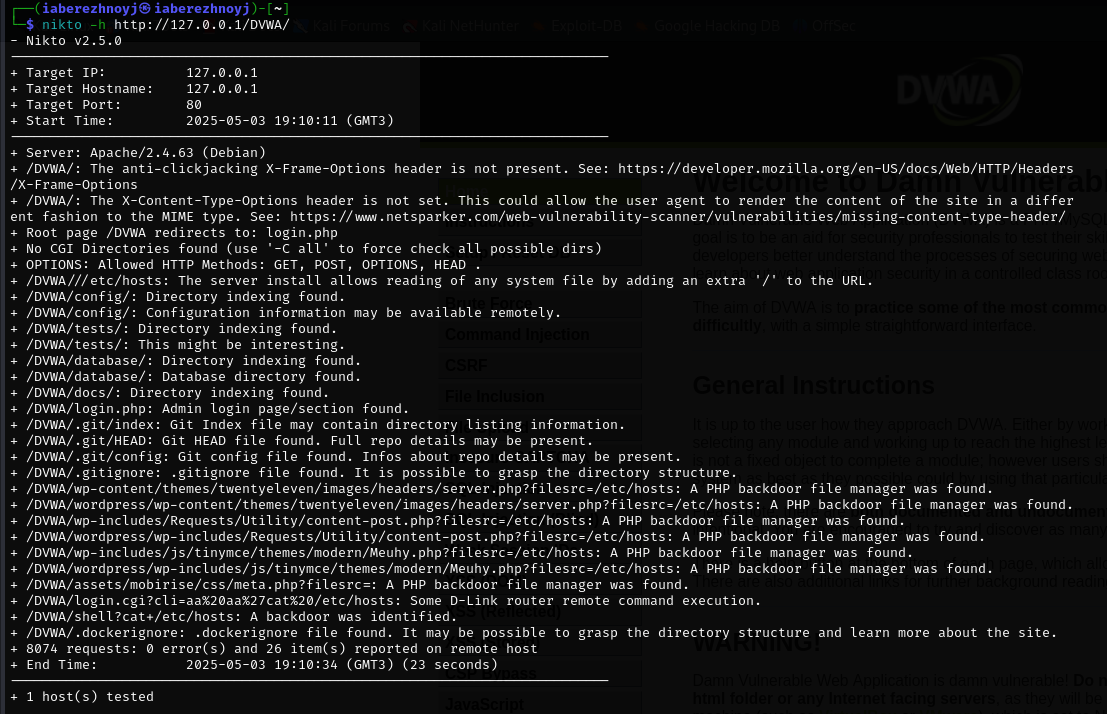


Рис. 3: Использование nikto

Из вывода в терминале можем заключить следующее:

Отчёт Nikto выявил несколько уязвимостей и проблем безопасности в DVWA.

1. Обнаружены несколько PHP-скриптов, позволяющих управлять файлами на сервере:
   * /DVWA/wp-content/themes/twent/vector/images/headers/server.php?filesrc=/etc/hosts
   * /DVWA/login.cgi?cli=a&z9aaxZ7catX20/etc/hosts (возможна RCE для D-Link роутеров)
   * /DVWA/shell?cat+/etc/hosts (подозрительный бэкдор).
2. Отсутствуют заголовки безопасности:
   * Нет X-Frame-Options (риск clickjacking).
   * Нет X-Content-Type-Options (возможна подмена MIME-типов).
3. Доступны директории с конфигурационными данными: /DVWAconfig/, /DVWA/database/, /DVWA/tests/ (индексация включена).

# 5 Выводы

В ходе выполнения этапа проекта мы научились исопльзовать nikto для сканирования веб-приложения на уязвимости