Индивидуальный проект. Этап 4

Использование nikto

Татьяна Александровна Буллер

Содержание

# 1 Цель работы

Знакомство со сканером уязвимостей nikto и тестирование его возможностей на примере DVWA.

# 2 Ход работы

nikto — базовый сканер безопасности веб-сервера. Он сканирует и обнаруживает уязвимости в веб-приложениях, обычно вызванные неправильной конфигурацией на самом сервере, файлами, установленными по умолчанию, и небезопасными файлами, а также устаревшими серверными приложениями.

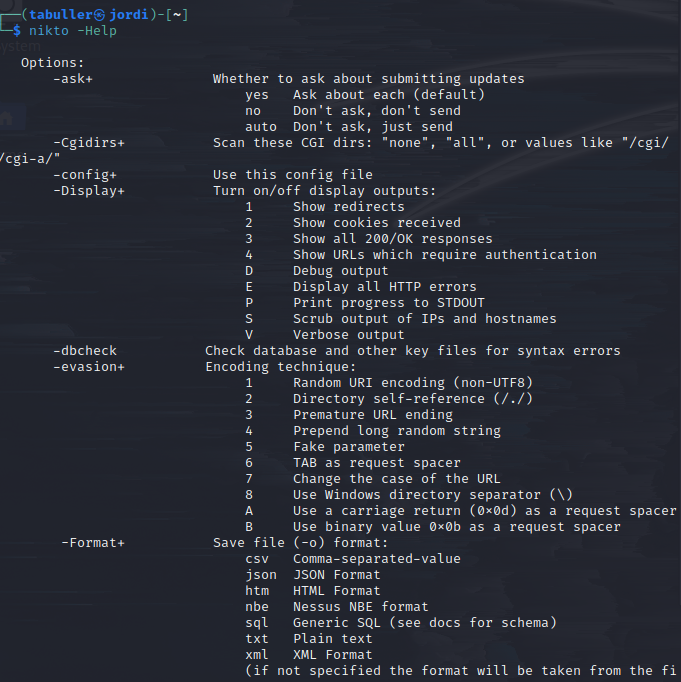


Рис. 1: Справка nikto

Основной параметр, который необходимо задать для nikto - -host, который принимает на вход адрес конкретной страницы либо машины. Для начала передадим адрес основной страницы DVWA и попробуем проанализировать вывод.

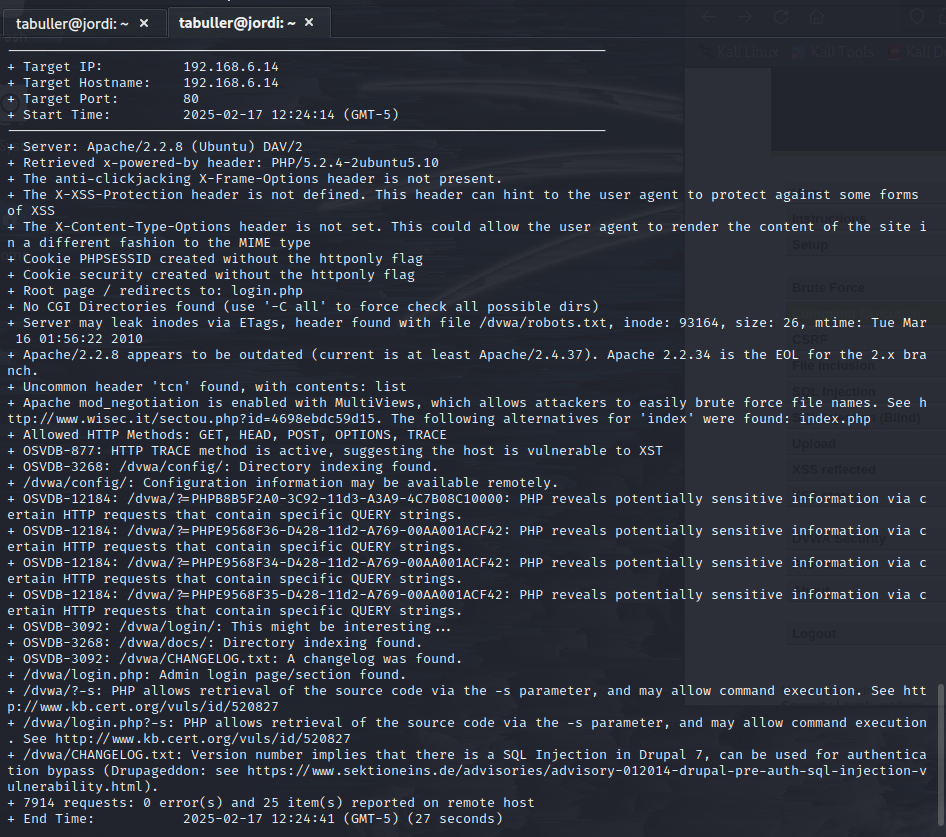


Рис. 2: Анализ основной страницы DVWA с помощью nikto

Видим, что nikto сразу определил версию веб-сервера Apache, на котором запущена страница, используемую версию php и отсутствующие заголовки в теле запроса, отсутствие которых позволяет так или иначе манипулировать страницей. Далее по отчету видим список HTTP-методов, которые принимает страница. Сканер обнаружил также файлы конфигурации php, страницу входа, лог изменений. Всегда следует обращать внимание на устаревшие версии тех или иных сервисов, так как нередки случаи того, что в них присутствуют доступные для эксплуатации уязвимости. Так, здесь nikto обращает внимание на устаревшую версию Apache и данные из лога изменений, из которых следует, что страница уязвима к SQLi. Кроме этого, сканер обнаруживает директории, ссылок на которые нет на главной странице DVWA. Это, например, директория /config, содержание которой, судя по названию, может представлять интерес для исследователя.



Рис. 3: Директория /config

Эта директория содержит единственный файл и перенаправление в корень - страницу, на которой мы были до этого. Открыв файл, лежащий в этой директории, мы не увидим никакого вывода, пока не добавим в конец адреса знак тильды. Действительно, этот файл хранит некоторые детали конфигурации базы данных:

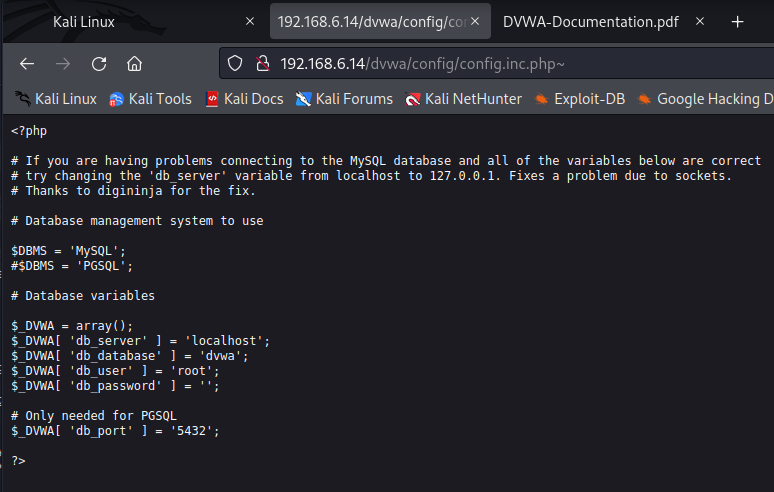


Рис. 4: config.inc.php

Кроме файла конфигурации nikto нашел еще и директорию /docs, где, судя по названию, хранится некоторая документация. И действительно - внутри находим .pdf файл с документацией DVWA.

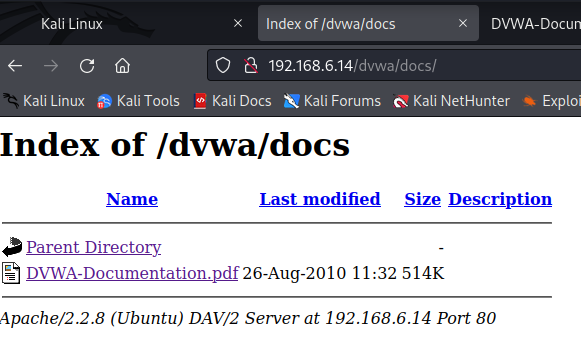


Рис. 5: Директория /docs

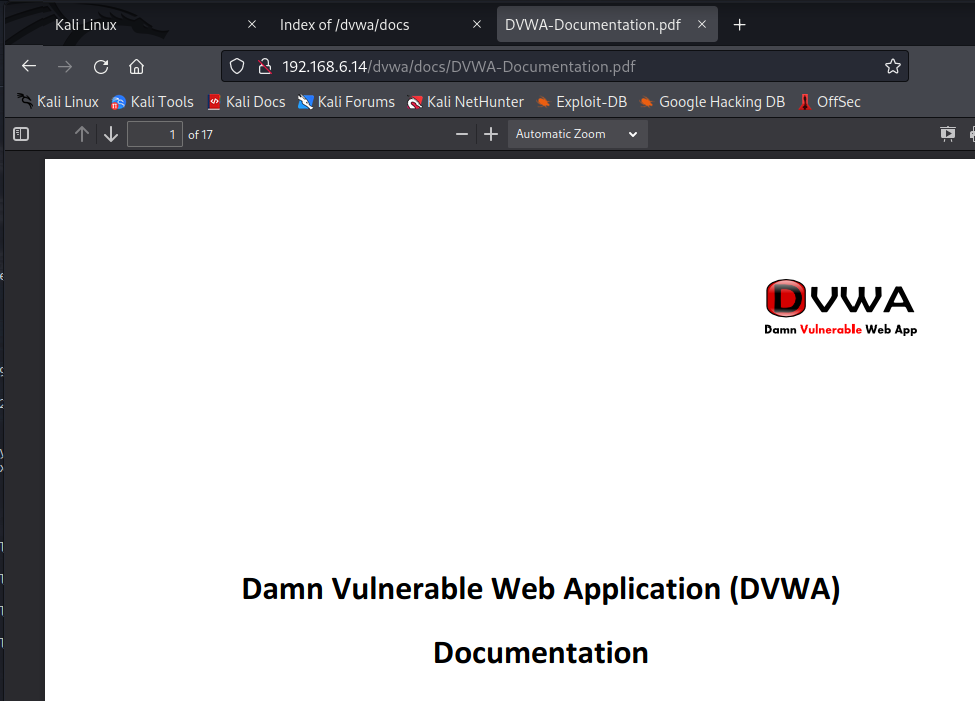


Рис. 6: Файл документации

Сканер также обращает внимание исследователя на то, что страница отвечает на запрос с параметром ?-s, возвращая исходный код. Это может быть крайне полезно в дальнейшем исследовании уязвимостей.

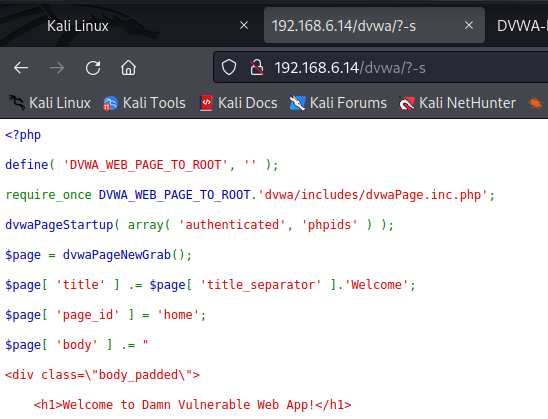


Рис. 7: Возвращение исходного кода страницы

Теперь попробуем просканировать страницу одной из уязвимостей. Кроме информации, аналогичной прошлому выводу, nikto обнаружил отдельные страницы с исходным кодом и помощью, которые, по его мнению, не должны быть доступны.

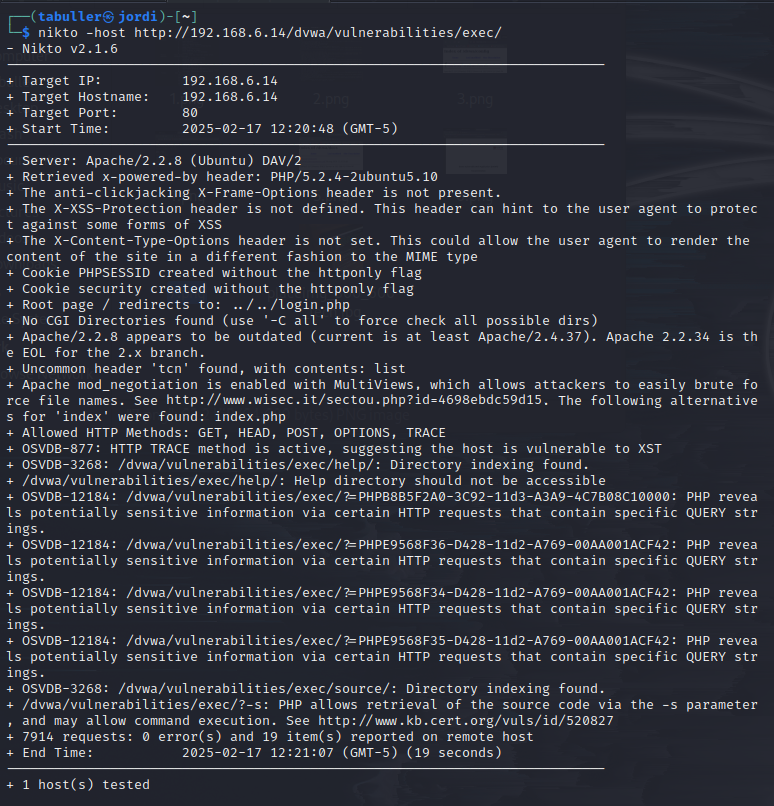


Рис. 8: Отчет по сканированию страницы уязвимости

# 3 Выводы

Было освноено применение сканера уязвимостей nikto и протестированы его возможности на примере заведомо уязвимой страницы DVWA.