Индивидуальный проект 4

Генералов Даниил, 1032212280

Содержание

# 1 Цель работы

В этом этапе индивидуального проекта требуется использовать сканер уязвимостей nikto, чтобы найти какие-то уязвимости в DVWA.

# 2 Выполнение лабораторной работы

Сканер nikto уже идет в стандартной установке Kali Linux. Мы просто запускаем его, направляя его на адрес, где развернут DVWA, и получаем список потенциальных проблем (рис. 1).

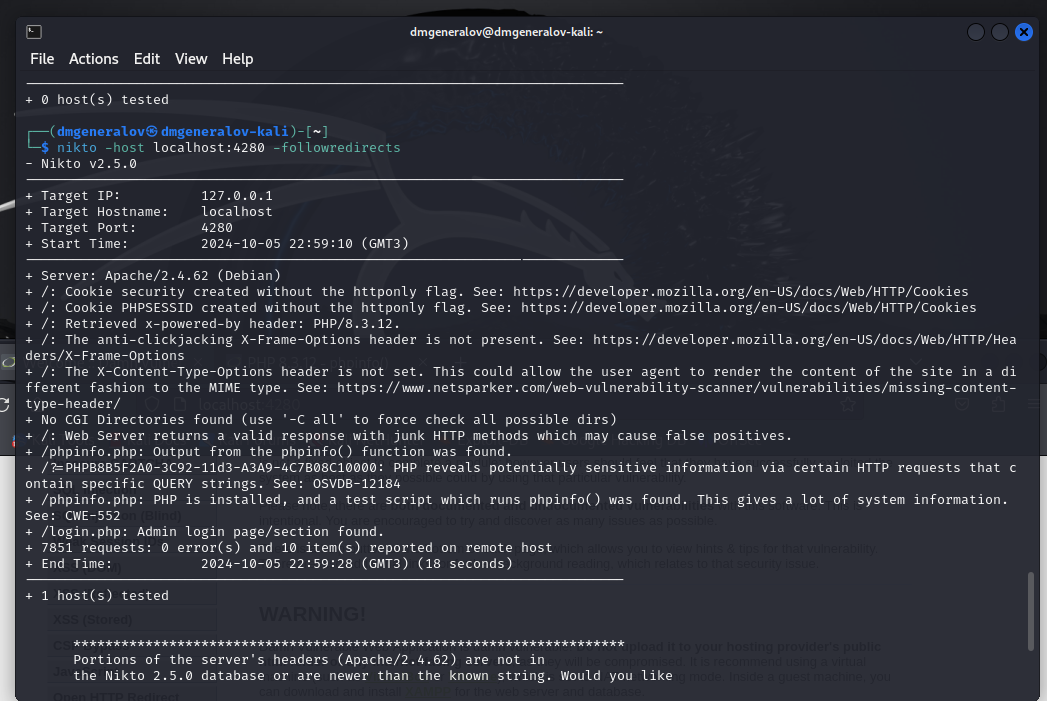


Рис. 1: nikto

К сожалению, большинство из этих проблем не слишком интересные, например тот факт что сервер раскрывает версию PHP на которой он работает.

Более интересный вывод можно получить, направив его на какую-то страницу, которая демонстрирует уязвимость. Например, на странице с SQL-инъекцией, он обнаружил, что может быть что-то интересное в скрипте, который используется для выдачи данных для формы (рис. 2).

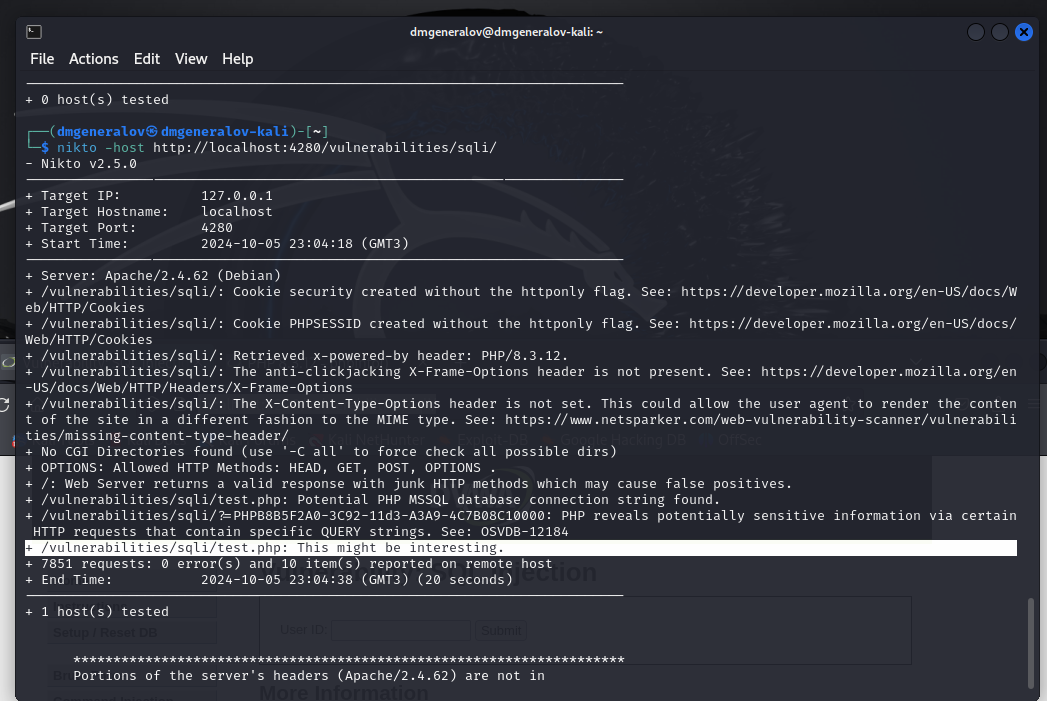


Рис. 2: nikto

Также можно найти уязвимость, связанную с подключением файлов: скрипт include.php может вернуть содержимое файлов в файловой системе (вроде /etc/passwd) и на HTTP-сайтах (рис. 3).

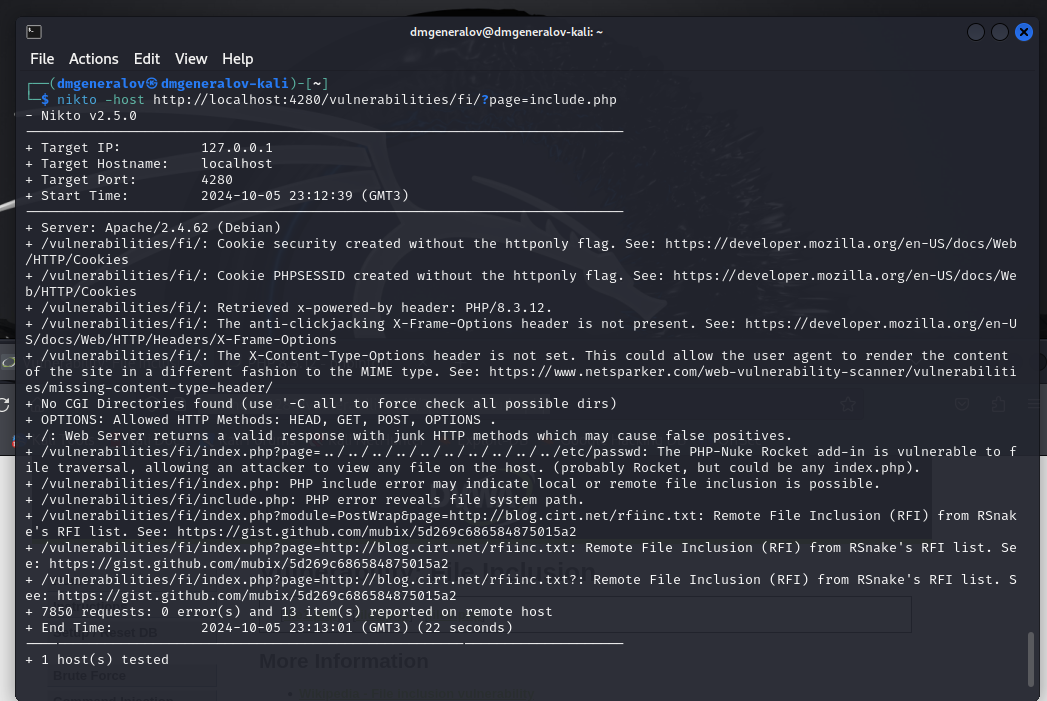


Рис. 3: nikto

Nikto не имеет автоматического рекурсивного сканирования, поэтому можно использовать другую программу, чтобы сгенерировать список всех страниц на сайте, а затем направить Nikto на каждую страницу и проверить ее; или в ручном режиме пробовать интересные страниуы.

# 3 Выводы

Мы успешно использовали Nikto, чтобы найти какие-то уязвимости в DVWA, определить их тип и получить ссылки на источники, где есть информация о том, как их можно исправить.