Отчет по четвертому этапу индивидуального проекта

Сканер nikto

Вакутайпа Милдред

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Научиться тестировать веб-приложений со сканером nikto.

2 Выполнение лабораторной работы

По скольку буду сканировать веб-приложение DVWA запускаю его.

Рис. 2.1: запуск сервера

Далее изменяю уровня безопасности на среднее.

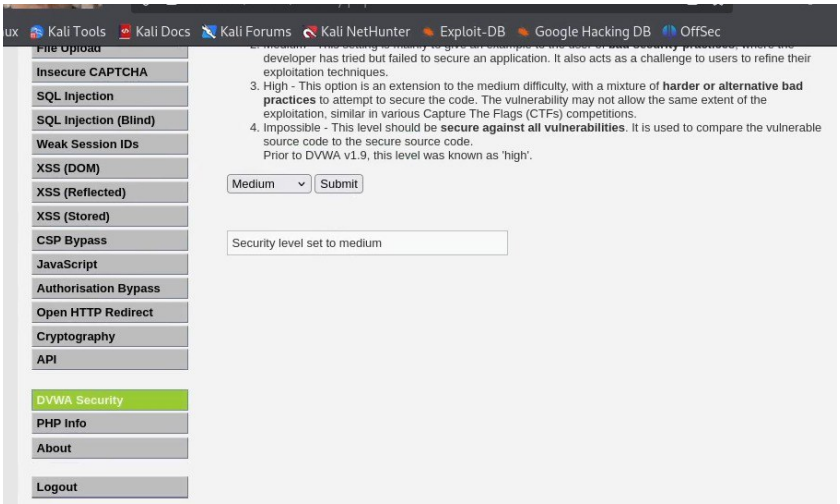

Рис. 2.2: Изменение уровня безопасности

Запускаю nikto используя #nikto и сканирую DVWA введя его польный URL без порта.

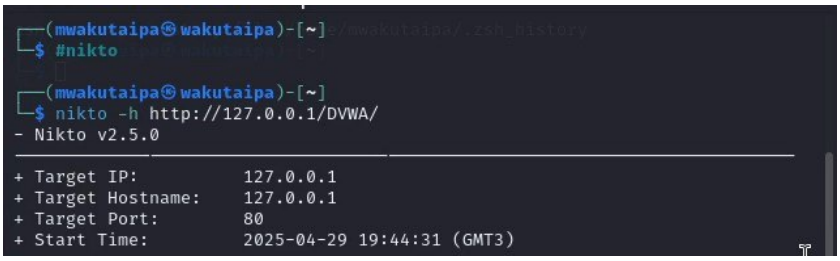

Рис. 2.3: Сканирование 1 с nikto

Сканирую второй раз введя польный URL DVWA с портом и заметила, что результаты не сильно отличаются.

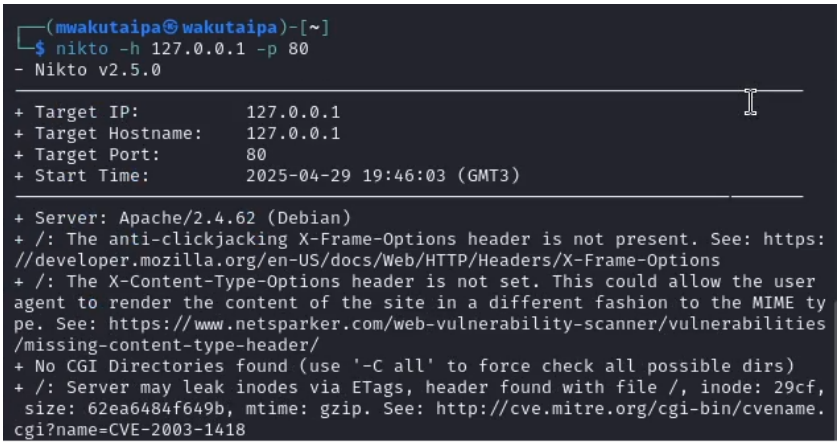

Рис. 2.4: Сканирование 2 с nikto

Кроме адреса хоста и порта веб-приложения, никто выводит инофрмацию о различных уязвимостях приложения как сервер: Apache/2.4.58 (Debian) /DVWA/: Заголовок X-Frame-Options, защищающий от перехвата кликов, отсутствует. /DVWA/: Заголовок X-Content-Type-Options не задан. Это может позволить пользовательскому агенту отображать содержимое сайта способом, отличным от MIME-типа. Корневая страница /DVWA перенаправляет на: login.php Каталоги CGI не найдены (используйте ‘-C all’, чтобы принудительно проверить все возможные каталоги) ОПЦИИ: Разрешенные HTTP-методы: GET, POST, OPTIONS, HEAD . /DVWA///etc/hosts: Установка сервера позволяет считывать любой системный

файл, добавляя дополнительный “/” к URL-адресу. /DVWA/config/: Найдена индексация каталога. /DVWA/config/: Информация о конфигурации может быть доступна удаленно. /DVWA/tests/: Найдена индексация каталога. /DVWA/tests/: Это может быть интересно. /DVWA/database/: Найдена индексация каталога. /DVWA/база данных/: Найден каталог базы данных. /DVWA/документы/: Найдена индексация каталога. /DVWA/login.php: Найдена страница входа администратора/раздел. /DVWA/.git/index: Индексный файл Git может содержать информацию о списке каталогов. /DVWA/.git/HEAD: Найден файл Git HEAD. Может содержаться полная информация о репозитории. /DVWA/.git/config: Найден конфигурационный файл Git. Может содержаться информация о деталях репозитория. /DVWA/.gitignore: найден файл .gitignore. Можно разобраться в структуре каталогов. /DVWA/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: Обнаружен файловый менеджер с бэкдором на PHP. /DVWA/wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: Обнаружен файловый менеджер с бэкдором на PHP. /DVWA/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: Найден файловый менеджер с бэкдором на PHP. /DVWA/wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: Найден файловый менеджер с бэкдором на PHP. /DVWA/wp-включает в себя/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: Найден файловый менеджер бэкдора PHP. /DVWA/wordpress/wp-включает в себя/js/tinymce/themes/modern/Meuhy.ph
Найден файловый менеджер бэкдора на PHP. /DVWA/assets/mobirise/css/meta.php?filesrc=: Найден файловый менеджер бэкдора на PHP. /DVWA/shell?cat+/etc/hosts: Обнаружен черный ход. /DVWA/.dockerignore: найден файл .dockerignore. Возможно, удастся разобраться в структуре каталогов и узнать больше о сайте.

Бэкдор — дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удалённому управлению операционной системой и компьютером в целом. Также в результатах nikto отображает код OSVDB 561 и дает ссылку на CVE-2003-1418. OSVDB — это аббревиатура базы данных уязвимостей с открытым исходным ко-

дом.

3 Выводы

Научилась тестировать веб-приложений со сканером nikto.

Список литературы