Основы информационной безопасности

Индивидуальный проект. Этап № 4. Использование Nikto

Демидова Екатерина Алексеевна

Содержание

Список иллюстраций

1 Постановка задачи

Целью данной работы является использование Nikto для сканирования уязвимостей веб-приложения.

2 Теоретические сведения

Damn Vulnerable Web Application (DVWA) – это веб-приложение PHP/MySQL, которое чертовски уязвимо[~ 1]. Его основная цель – помочь специалистам по безопасности проверить свои навыки и инструменты в правовой среде, помочь веб-разработчикам лучше понять процессы обеспечения безопасности веб-приложений, а также помочь студентам и преподавателям узнать о безопасности веб-приложений в контролируемом классе. обстановка помещения.

Цель DVWA – отработать некоторые из наиболее распространенных веб-уязвимостей различного уровня сложности с помощью простого и понятного интерфейса. В этом программном обеспечении существуют как задокументированные, так и недокументированные уязвимости.

DVWA имеет три уровня безопасности, они меняют уровень безопасности каждого веб приложения в DVWA:

- Невозможный — этот уровень должен быть безопасным от всех уязвимостей. Он используется для сравнения уязвимого исходного кода с безопасным исходным кодом.
- Высокий — это расширение среднего уровня сложности, со смесью более сложных или альтернативных плохих практик в попытке обезопасить код. Уязвимости не позволяют такой простор эксплуатации как на других уровнях.
- Средний — этот уровень безопасности предназначен главным образом для того, чтобы дать пользователю пример плохих практик безопасности, где разработчик попытался сделать приложение безопасным, но потерпел

неудачу.

- Низкий — этот уровень безопасности совершенно уязвим и совсем не имеет защиты. Его предназначение быть примером среди уязвимых веб приложений, примером плохих практик программирования и служить платформой обучения базовым техникам эксплуатации.

Nikto – бесплатный (open source) сканер для поиска уязвимостей в веб-серверах[~ 2].

В начале сканирования всегда отображается следующий блок с информацией:

- Target IP: IP адрес сканируемого домена.
- Target Hostname: имя хоста (доменное имя) сканируемого сайта;
- Target Port: порт, на котором находится сайт;
- Start Time: дата и время начала сканирования в формате год-месяц-день час:минута:секунда.

Вывод результатов сканирования имеет несколько форматов:

1. Формат: Тип компонента сайта: Наименование компонента. Пример: Server: nginx.
2. Описание: Nikto умеет определять, какие компоненты использует сайт. Сюда относят наименование веб-сервера, используемой СУБД, фреймворков, языков программирования, а также их версии. Формат: путь до файла/директории, где найдена уязвимость: описание уязвимости. Пример: /phpinfo.php: Output from the phpinfo() function was found.

3 Выполнение лабораторной работы

Проверим, что nikto установлен(рис. 3.1)

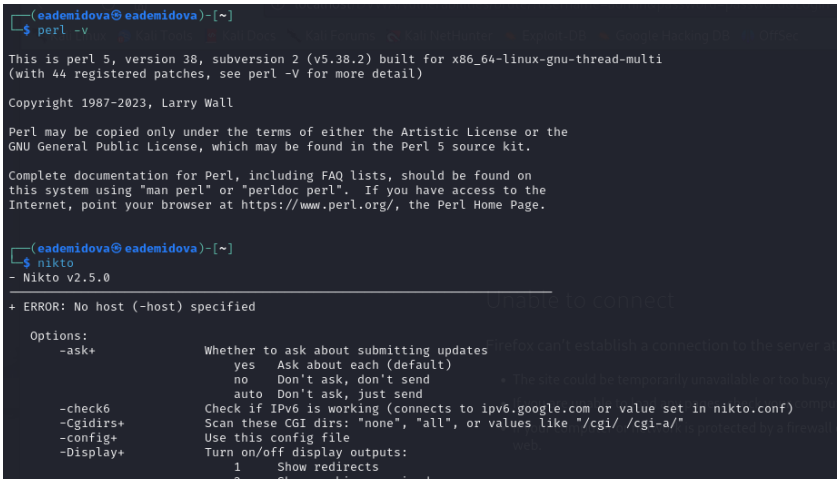

Рис. 3.1: Проверка установки ПО

Затем проверим сайт DVWA, указав опции для сохранения отчета в формате html(рис. 3.2,).

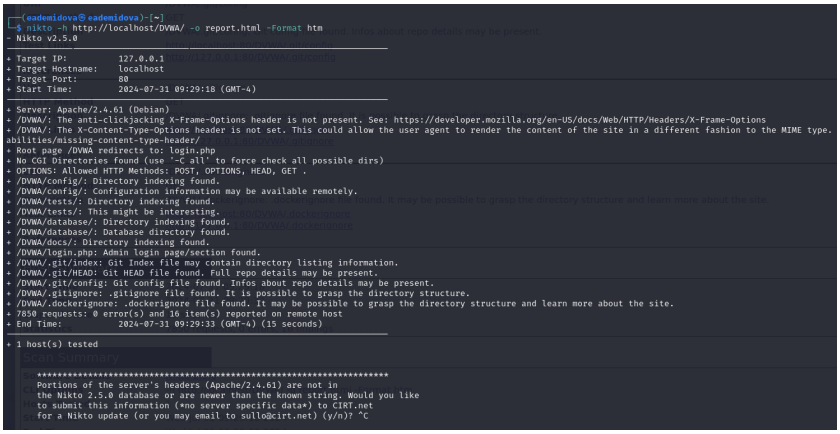

Рис. 3.2: Проверка уязвимостей по доменному имени

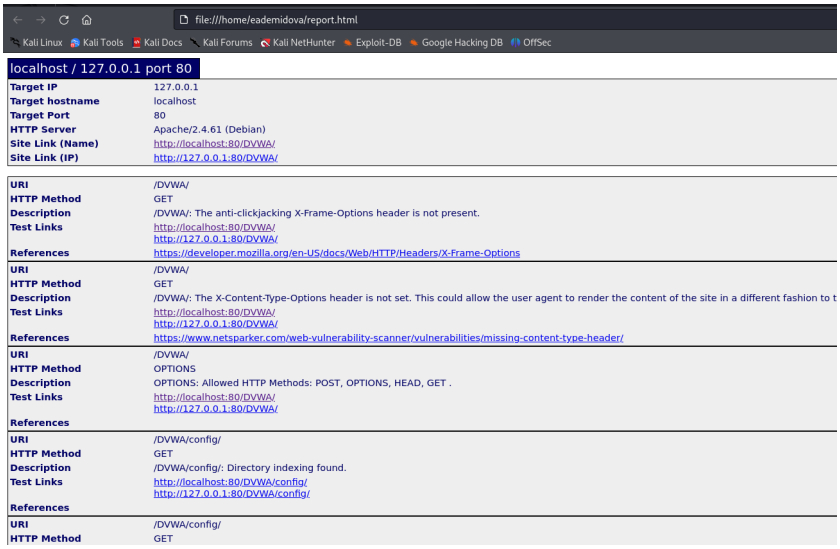

Рис. 3.3: Отчет об уязвимостях в формате html

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. Уязвимость типа `This might be interesting...` означает, что необходимо дополнительная ручная проверка(скорей всего это незначительная уязвимость

раскрытия информации – доступен просмотр файлов каталога). 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. 3.4).

Рис. 3.4: Проверка уязвимостей с указанием порта

4 Выводы

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

Список литературы

1. DVWA [Электронный ресурс]. GitHub, Inc, 2024. URL: https://github.com/digininja/DVWA.
2. Обзор сканера Nikto для поиска уязвимостей в веб-серверах [Электронный ресурс]. 2006–2024, Habr, 2023. URL: https://habr.com/ru/companies/first/articles/731696/.