Отчёта по индивидуальному проекту №4

дисциплина: Информационная безопасность

Кашкин Иван Евгеньевич

Содержание

[Цель работы](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab2\Lab_2_report.docx#_Toc177202532)

[Задание](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab2\Lab_2_report.docx#_Toc177202533)

[Теоретическое введение](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab2\Lab_2_report.docx#_Toc177202534)

[Выполнение лабораторной работы](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab2\Lab_2_report.docx#_Toc177202535)

[Выводы](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab2\Lab_2_report.docx#_Toc177202536)

[Список литературы](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab2\Lab_2_report.docx#_Toc177202537)

# Цель работы

Целью данной работы является изучение сканера уязвимостей nikto.

# Введение

**Nikto: Описание**

**Nikto** — это популярный сканер веб-серверов с открытым исходным кодом, который

проверяет веб-серверы на наличие уязвимостей, неправильных настроек, устаревших версий ПО и прочих проблем безопасности.

Основные задачи Nikto:

Поиск общих уязвимостей веб-серверов.

Проверка наличия опасных файлов и конфигураций.

Выявление устаревших версий веб-серверов и их компонентов. Определение серверных технологий и модулей.

Особенности:

Поддержка множества серверов и протоколов (HTTP, HTTPS, HTTP/2 и другие). Возможность добавления собственных правил для обнаружения уязвимостей. Регулярные обновления базы данных уязвимостей.

Nikto — это пассивный сканер, и он не пытается активно взламывать систему, а только собирает информацию о потенциальных уязвимостях.

Рекомендуется использовать Nikto в сочетании с другими инструментами безопасности, такими как Nmap и OpenVAS, для более полного анализа безопасности веб-сервера.

**Полезные параметры и примеры**

Nikto написан на Perl, и для его работы необходимо наличие Perl на системе. Сканирование веб-сервера

perl nikto.pl -h <URL>

Сканирование определенного порта

perl nikto.pl -h <URL> -p <port>

Вывод результатов в файл

perl nikto.pl -h <URL> -o output.txt

Дополнительные аргументы:

-ssl — принудительное использование SSL (HTTPS).

-no\_ssl — игнорирование SSL-сертификатов.

-Tuning — настройка интенсивности сканирования (например, отключение проверки директорий).

-Plugins — выбор определенных плагинов для сканирования.

-timeout — установка таймаута для запросов.

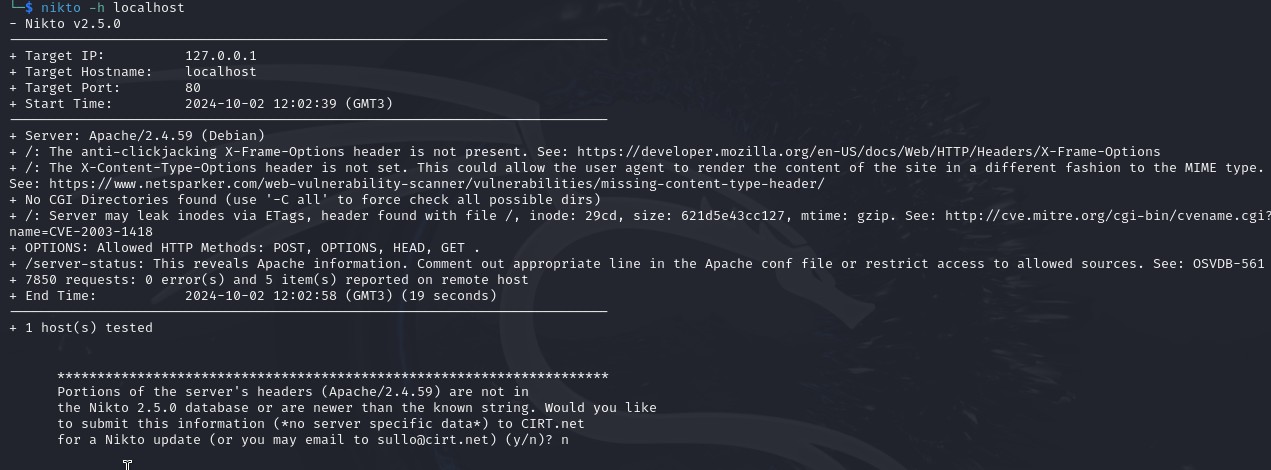
# Выполнение работы

Nikto может использоваться для пассивного сканирования DVWA, выявления базовых уязвимостей и проверок на неправильную конфигурацию.

Когда DVWA запущено, мы можем использовать Nikto для сканирования. Основной командой для сканирования будет:

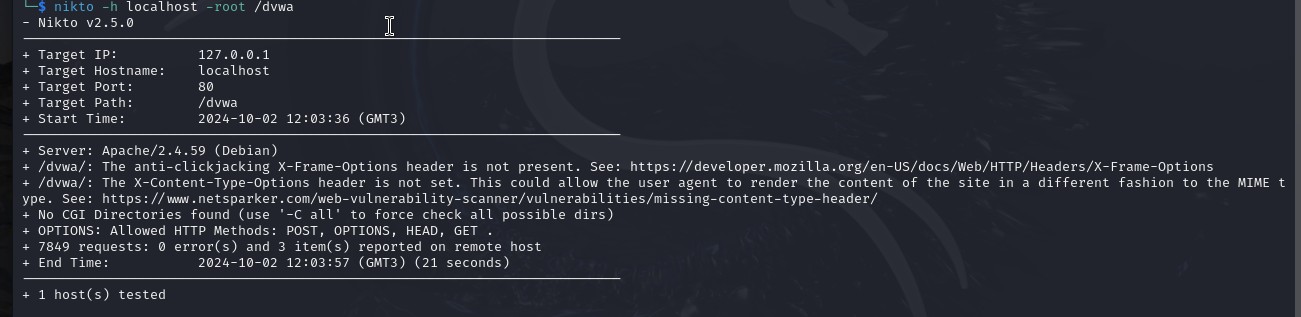
perl nikto.pl -h <http://localhost/dvwa/>

**Сканирование localhost**



#fig

**Сканирование localhost/dvwa/**



#fig

# Вывод

Мы изучили возможности сканера nikto.