

# Индивидуальный проект 4

## Информационная безопасность

---

Волчок Кристина Александровна НПМбд-02-21

29 сентября 2024

Российский университет дружбы народов, Москва, Россия

## Информация

---

## Вводная часть

---

Nikto — это инструмент для базового сканирования безопасности веб-серверов, который позволяет обнаружить различные типы уязвимостей, включая устаревшие программные компоненты, конфигурационные ошибки и потенциальные информационные утечки. Этот инструмент широко применяется специалистами по информационной безопасности для анализа защищенности веб-приложений и серверов.

С ростом киберугроз и числа атак на веб-серверы, обеспечение безопасности веб-приложений становится крайне актуальным. Неправильная конфигурация серверов, использование устаревших программ и утечки информации могут быть использованы злоумышленниками для компрометации системы. Инструменты, такие как Nikto, позволяют своевременно выявить такие уязвимости и предпринять необходимые меры по их устранению.

Объектом исследования в данной работе является веб-сервер, на котором развернуто веб-приложение. Предмет исследования — уязвимости веб-сервера, такие как устаревшие версии программ, конфигурационные ошибки и утечки информации, которые могут возникать из-за неправильных настроек или слабой политики безопасности.

Целью данной работы является применение инструмента Nikto для сканирования веб-сервера с целью выявления и анализа различных уязвимостей. Основные задачи включают установку и настройку Nikto, выполнение базового и специализированного сканирования, анализ полученных результатов, а также предоставление рекомендаций по усилению безопасности.

В качестве материала был использован инструмент Nikto версии 2.1.5, установленный на операционной системе Ubuntu. Для анализа уязвимостей использовался тестовый веб-сайт (<http://testphp.vulnweb.com>). В ходе работы были проведены базовое сканирование и специализированные проверки на наличие устаревших программ, утечек информации и конфигурационных ошибок с помощью различных параметров Nikto.



## Результаты

---

В результате сканирования были обнаружены несколько уязвимостей, включая устаревшую версию PHP, отсутствие защитного заголовка X-Frame-Options и утечки данных через файл `clientaccesspolicy.xml`. Специализированные сканирования также показали конфигурационные проблемы и наличие файлов с недостаточной политикой безопасности. На основе полученных результатов были сделаны выводы о возможных мерах для повышения защищенности веб-сервера.

- Использование инструментов, таких как Nikto, жизненно важно для своевременного обнаружения уязвимостей веб-серверов и предотвращения потенциальных атак.
- Проведенное сканирование выявило критические области, требующие внимания, включая устаревшие версии ПО и ошибки конфигурации.
- **Главное сообщение:** Без регулярного мониторинга и анализа безопасности веб-серверов с помощью инструментов вроде Nikto, защита данных и работающих приложений оказывается под угрозой. Регулярное сканирование — ключ к безопасной и устойчивой работе веб-приложений.
- Помните, что безопасность — это процесс, а не разовое действие.

- Волчок Кристина Александровна, студентка кафедры прикладной информатики и теории вероятностей
- Российский университет дружбы народов
- [1032215007@rudn.ru]