

# **Индивидуальный проект 4**

**Информационная безопасность**

Волчок Кристина Александровна НПМбд-02-21

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Задание</b>	<b>5</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>6</b>
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>8</b>
<b>5</b>	<b>Выводы</b>	<b>13</b>

## Список иллюстраций

4.1	Обновление системы и установка Nikto . . . . .	8
4.2	Установка Nikto . . . . .	9
4.3	Сканирование с помощью Nikto . . . . .	10
4.4	Целевое сканирование на устаревшие серверные программы . . .	11
4.5	Информационные утечки . . . . .	11
4.6	Проверка на конфигурационные уязвимости . . . . .	12

# 1 Цель работы

Цель данной работы — освоить использование базового сканера безопасности веб-сервера **Nikto** для выявления и анализа уязвимостей веб-приложений. Nikto позволяет обнаруживать потенциальные риски безопасности, которые могут возникнуть из-за неправильной конфигурации сервера, использования файлов по умолчанию, небезопасных файлов и устаревших серверных приложений. В ходе работы будет проведено сканирование веб-сервера с использованием различных опций и параметров Nikto, а также изучены результаты для последующего анализа и принятия мер по усилению безопасности веб-приложений.

## 2 Задание

1. Установить сканер безопасности веб-сервера **Nikto** на операционной системе Ubuntu.
2. Провести базовое сканирование уязвимостей на учебном веб-сайте (например, <http://testphp.vulnweb.com>) с помощью команды: `nikto -h http://testphp.vulnweb.com`

### 3 Теоретическое введение

С ростом использования веб-приложений в различных сферах деятельности безопасность веб-серверов и веб-приложений становится одним из ключевых аспектов информационной безопасности. Уязвимости в веб-серверах могут возникать из-за неправильной конфигурации, использования устаревших версий программного обеспечения, а также наличия небезопасных файлов и скриптов. Невнимательность к этим аспектам может привести к серьезным последствиям, включая утечку данных, взлом систем и компрометацию веб-приложений.

**Nikto** — это популярный инструмент для сканирования безопасности веб-серверов. Он позволяет быстро и эффективно находить уязвимости и слабые места на веб-серверах и веб-приложениях. Nikto выполняет проверку на наличие более чем 6700 потенциально опасных файлов и программ, проверяет конфигурацию веб-сервера на наличие уязвимостей, а также определяет устаревшие версии веб-серверов и их компонентов.

Nikto осуществляет следующие виды проверок: - Сканирование директорий и файлов, которые могут представлять угрозу (например, резервные копии или файлы, установленные по умолчанию). - Выявление потенциально уязвимых CGI-скриптов. - Проверка конфигурации веб-сервера на предмет наличия ошибок и неправильно настроенных параметров. - Определение устаревших серверных программ, которые могут содержать известные уязвимости. - Поиск информационных утечек, которые могут раскрывать чувствительную информацию злоумышленникам.

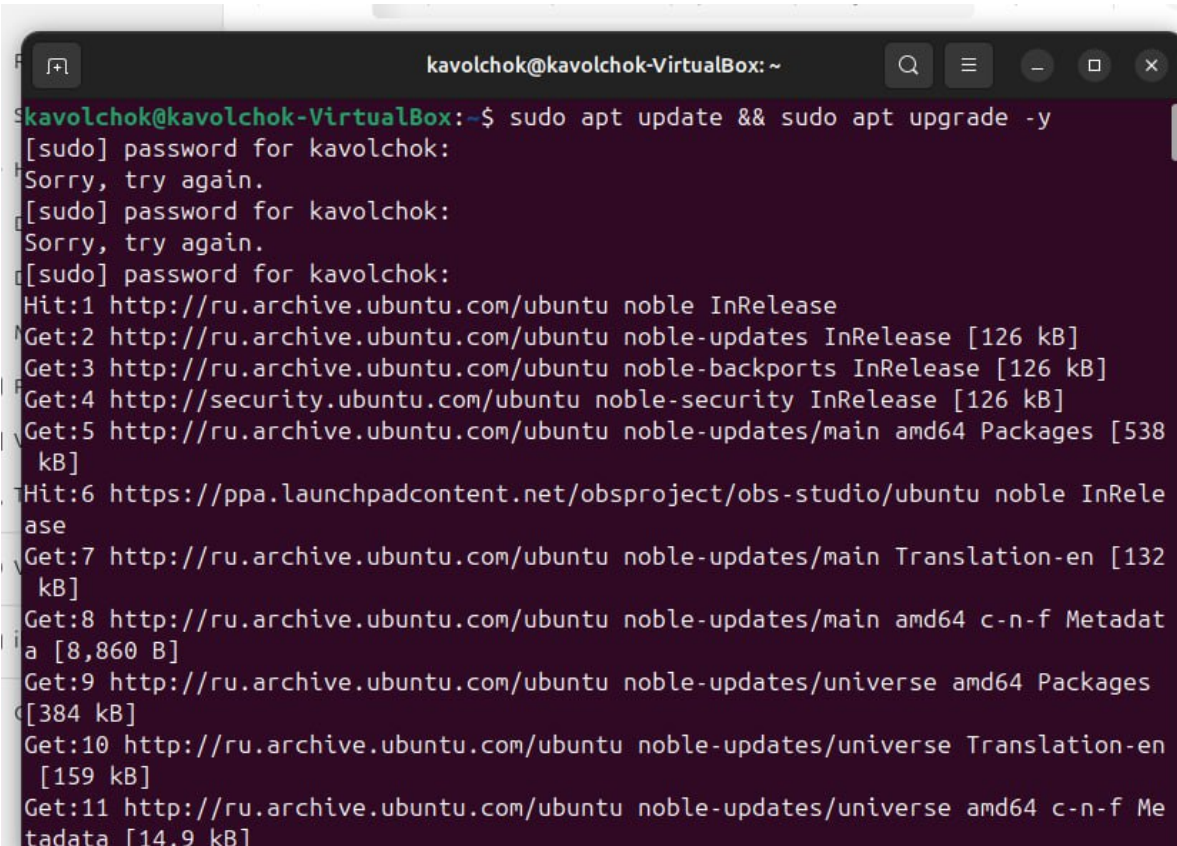
В процессе сканирования с помощью Nikto используется база данных уязви-

мостей, которая регулярно обновляется, обеспечивая актуальность проверки. Несмотря на свою эффективность, Nikto является инструментом пассивного сканирования, то есть он не производит активного тестирования безопасности, такого как внедрение вредоносного кода или эксплуатация обнаруженных уязвимостей. Однако даже такой подход может быть крайне полезен для выявления наиболее распространенных проблем безопасности и принятия своевременных мер по их устранению.

Таким образом, использование Nikto позволяет администратору веб-сервера или специалисту по безопасности получить общее представление о текущем состоянии защищенности веб-сервера и выявить области, требующие дальнейшей проработки и исправления.

## 4 Выполнение лабораторной работы

Для начала я обновила систему, чтобы убедиться, что все пакеты актуальны. Для этого я выполнила команду:



```
kavolchok@kavolchok-VirtualBox: ~  
$ sudo apt update && sudo apt upgrade -y  
[sudo] password for kavolchok:  
Sorry, try again.  
[sudo] password for kavolchok:  
Sorry, try again.  
[sudo] password for kavolchok:  
Hit:1 http://ru.archive.ubuntu.com/ubuntu noble InRelease  
Get:2 http://ru.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]  
Get:3 http://ru.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]  
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]  
Get:5 http://ru.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [538 kB]  
Hit:6 https://ppa.launchpadcontent.net/obsproject/obs-studio/ubuntu noble InRelease  
Get:7 http://ru.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [132 kB]  
Get:8 http://ru.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [8,860 B]  
Get:9 http://ru.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [384 kB]  
Get:10 http://ru.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [159 kB]  
Get:11 http://ru.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [14.9 kB]
```

Рис. 4.1: Обновление системы и установка Nikto

После этого система запросила мой пароль для sudo, и, после его успешного ввода, началось обновление списка пакетов. Затем я убедилась, что система полностью обновлена.



Затем я приступила к установке инструмента Nikto. Для этого я выполнила команду:

```
update-initramfs: Generating /boot/initrd.img-6.8.0-45-generic
kavolchok@kavolchok-VirtualBox:~$ sudo apt install nikto -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nikto is already the newest version (1:2.1.5-3.1).
The following package was automatically installed and is no longer required:
  pandoc-data
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
kavolchok@kavolchok-VirtualBox:~$ nikto -h http://testphp.vulnweb.com
- Nikto v2.1.5
-----
+ Target IP:          44.228.249.3
x_GAs_7.0.20 Hostname: testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2024-10-05 19:10:11 (GMT3)
-----
+ Server: nginx/1.19.0
+ Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
+ The anti-clickjacking X-Frame-Options header is not present.
+ /: Potential PHP MySQL database connection string found.
+ Server leaks inodes via ETags, header found with file /clientaccesspolicy.xml,
  fields: 0x5049b03d 0x133
```

Рис. 4.2: Установка Nikto

На моем компьютере Nikto уже был установлен (версия v2.1.5), поэтому система сообщила, что дополнительных действий по установке не требуется.

### **Базовое сканирование с помощью Nikto**

После установки я решила провести базовое сканирование тестового сайта, используя следующую команду:

```
[2] - Stopped nikto - http://testphp.vulnweb.com
kavolchok@kavolchok-VirtualBox:~$ nikto -h http://testphp.vulnweb.com -Tuning 2
- Nikto v2.1.5
-----
+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:       80
+ Start Time:        2024-10-05 19:28:28 (GMT3)
-----
+ Server: nginx/1.19.0
+ Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
+ The anti-clickjacking X-Frame-Options header is not present.
```

Рис. 4.3: Сканирование с помощью Nikto

В результате сканирования я получила информацию о целевом IP (44.228.249.3), порте (80), а также о версии веб-сервера (nginx/1.19.0). Nikto обнаружил следующие уязвимости:

Используемая версия PHP (5.6.40) устарела и может содержать известные уязвимости. Отсутствует заголовок X-Frame-Options, что делает сайт уязвимым к атакам типа clickjacking. Обнаружена утечка данных через ETag в файле clientaccesspolicy.xml. Этот результат показал мне, что сервер имеет несколько потенциальных проблем безопасности, требующих внимания.

### **Целевое сканирование на устаревшие серверные программы**

Далее я решила просканировать сервер на наличие устаревших программных компонентов. Для этого я использовала флаг -Tuning 2:

```
nikto: command not found
kavolchok@kavolchok-VirtualBox:~$ nikto -h http://testphp.vulnweb.com -Tuning 4
- Nikto v2.1.5
-----
+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:       80
+ Start Time:        2024-10-05 19:29:38 (GMT3)
-----
+ Server: nginx/1.19.0
+ Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
+ The anti-clickjacking X-Frame-Options header is not present.
+ Server leaks inodes via ETags, header found with file /clientaccesspolicy.xml,
  fields: 0x5049b03d 0x133
+ /clientaccesspolicy.xml contains a full wildcard entry. See http://msdn.micros
  oft.com/en-us/library/cc197955(v=vs.95).aspx
+ lines
```

Рис. 4.4: Целевое сканирование на устаревшие серверные программы

Результаты сканирования подтвердили наличие устаревшей версии PHP (5.6.40-38). Кроме того, было отмечено отсутствие заголовка X-Frame-Options, что снова указало на возможную уязвимость для clickjacking.

**Проверка информационных утечек** Следующим этапом я решила провести сканирование на утечки информации, используя параметр -Tuning 4:

```
nikto: command not found
kavolchok@kavolchok-VirtualBox:~$ nikto -h http://testphp.vulnweb.com -Tuning 4
- Nikto v2.1.5
-----
+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:       80
+ Start Time:        2024-10-05 19:29:38 (GMT3)
-----
+ Server: nginx/1.19.0
+ Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
+ The anti-clickjacking X-Frame-Options header is not present.
+ Server leaks inodes via ETags, header found with file /clientaccesspolicy.xml,
  fields: 0x5049b03d 0x133
+ /clientaccesspolicy.xml contains a full wildcard entry. See http://msdn.micros
  oft.com/en-us/library/cc197955(v=vs.95).aspx
+ lines
```

Рис. 4.5: Информационные утечки

На этот раз Nikto обнаружил:

Отсутствие защитного заголовка X-Frame-Options. Утечку данных через ETag в файле clientaccesspolicy.xml. Файл clientaccesspolicy.xml с полным wildcard-разрешением, что может позволить злоумышленникам получить доступ к различным ресурсам сервера. Этот этап помог мне выявить потенциальные утечки информации, которые могли бы использоваться злоумышленниками.

### **Комбинированное сканирование на конфигурационные уязвимости и резервные файлы**

Для более комплексного анализа я выполнила комбинированное сканирование, чтобы проверить как конфигурационные уязвимости, так и наличие резервных файлов:



```
kavolchok@kavolchok-VirtualBox:~$ nikto -h http://testphp.vulnweb.com -Tuning 58
- Nikto v2.1.5
-----
+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Time:               2024-10-05 19:31:32 (GMT3)
-----
+ Server: nginx/1.19.0
+ Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
+ The anti-clickjacking X-Frame-Options header is not present.
+ Server leaks inodes via ETags, header found with file /clientaccesspolicy.xml,
  fields: 0x5049b03d 0x133
+ /clientaccesspolicy.xml contains a full wildcard entry. See http://msdn.micros
  oft.com/en-us/library/cc197955(v=vs.95).aspx
+ lines
```

Рис. 4.6: Проверка на конфигурационные уязвимости

В данном случае я использовала флаг -Tuning 58, который позволяет прове-  
сти сразу два вида сканирования: на конфигурационные уязвимости (5) и на  
резервные файлы (8). В результатах я увидела:

Отсутствие заголовка X-Frame-Options. Утечка данных через ETag в файле  
clientaccesspolicy.xml. Наличие файла clientaccesspolicy.xml с полным wildcard-  
разрешением. Этот комбинированный анализ позволил мне выявить как ошибки  
в конфигурации сервера, так и потенциально опасные файлы, доступные в си-  
стеме.

## 5 Выводы

- Инструмент Nikto был успешно установлен и использован для сканирования тестового веб-сайта на наличие различных типов уязвимостей.
- Проведены как базовое, так и специализированные сканирования для анализа устаревших серверных программ, информационных утечек и конфигурационных ошибок.
- Результаты сканирования показали наличие ряда уязвимостей на целевом веб-сервере, включая устаревшую версию PHP, отсутствие защитных заголовков, утечки данных и файлы с недостаточной политикой безопасности.
- На основе этих данных были получены важные сведения для принятия дальнейших мер по усилению безопасности веб-приложения. Этот процесс позволяет продемонстрировать, как с помощью Nikto можно выявить уязвимости и оценить уровень безопасности веб-сервера.