

# Презентация по индивидуальной проекте 4

## Основы информационной безопасности

---

Нджову Н.

26 апрель 2025

Российский университет дружбы народов, Москва, Россия

Научиться тестирование веб-приложений с помощью сканер nikto

1. Использование nikto
2. Анализ результатов

## Выполнение лабораторной работы

Чтобы работать с nikto(Nikto — это базовый сканер безопасности веб-сервера, который ищет уязвимости, вызванные неправильной конфигурацией, небезопасными файлами и устаревшими приложениями), необходимо подготовить веб-приложение DVWA, которое будем сканировать. Для этого запустила apache2(рис.1)

```
(nelianj@Nelianj)-[~]  
$ sudo systemctl start mysql  
[sudo] password for nelianj:  
  
(nelianj@Nelianj)-[~]  
$ sudo systemctl start apache2  
  
(nelianj@Nelianj)-[~]  
$
```

## Выполнение лабораторной работы

Я ввожу в адресной строке браузера адрес DVWA, перехожу в режим выбора уровня безопасности, ставлю минимальный-low(рис.2)

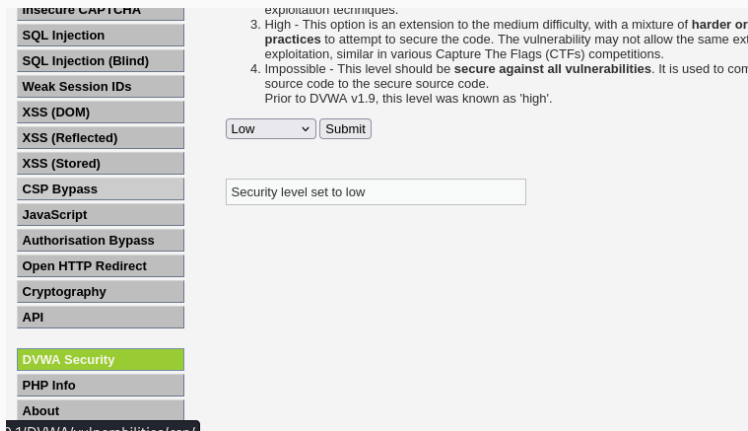
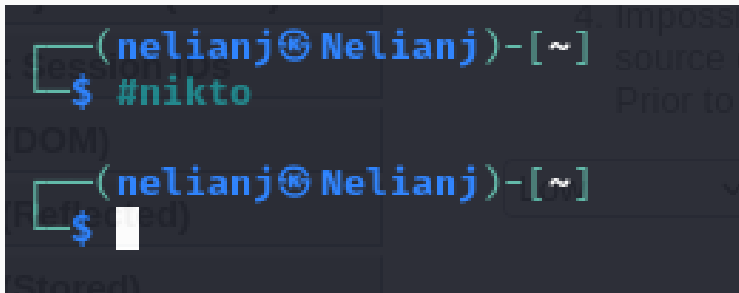


Рис. 2: Запуск DVWA

Запускаю nikto(рис.3)

A terminal window with a dark background. The prompt is '(nelianj@Nelianj)-[~]'. The command '#nikto' has been entered. The cursor is at the end of the command line.

```
(nelianj@Nelianj)-[~]  
$ #nikto  
  
(nelianj@Nelianj)-[~]  
$
```

Рис. 3: Запуск nikto

## Выполнение лабораторной работы

Я проверила веб-приложение, введя его полный URL-адрес и не вводя порт(рис.4 и рис.5)

```
(nelianj@Nelianj)-[~]
$ nikto -h http://127.0.0.1/DVWA/
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 80
+ Start Time: 2025-04-24 20:57:21 (GMT2)

+ Server: Apache/2.4.62 (Debian)
+ /DVWA/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /DVWA/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page /DVWA redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /DVWA///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ /DVWA/config/: Directory indexing found.
+ /DVWA/config/: Configuration information may be available remotely.
+ /DVWA/tests/: Directory indexing found.
+ /DVWA/tests/: This might be interesting.
+ /DVWA/database/: Directory indexing found.
+ /DVWA/database/: Database directory found.
```

```
+ /DVWA/docs/: Directory indexing found.
+ /DVWA/login.php: Admin login page/section found.
+ /DVWA/.git/index: Git Index file may contain directory listing information.
+ /DVWA/.git/HEAD: Git HEAD file found. Full repo details may be present.
+ /DVWA/.git/config: Git config file found. Infos about repo details may be present.
+ /DVWA/.gitignore: .gitignore file found. It is possible to grasp the directory structure.
+ /DVWA/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /DVWA/login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
+ /DVWA/shell?cat+/etc/hosts: A backdoor was identified.
+ /DVWA/.dockerignore: .dockerignore file found. It may be possible to grasp the directory structure and learn more about the site.
```



## Выполнение лабораторной работы

Затем попробовала просканировать введя адрес хоста и адрес порта, результаты незначительно отличаются(рис.6 и рис.7)

```
(nelianj@Nelianj)-[~]
$ nikto -h 127.0.0.1 -p 80
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 80
+ Start Time: 2025-04-24 21:01:43 (GMT2)

+ Server: Apache/2.4.62 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cf, size: 63270584880bc, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-561
```

```
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/host
s: A PHP backdoor file manager was found.
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc
=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP ba
ckdoor file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts
: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP b
ackdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/host
s: A PHP backdoor file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was fou
nd.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote comman
d execution.
+ /shell?cat+/etc/hosts: A backdoor was identified.
+ 8074 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time: 2025-04-24 21:01:51 (GMT2) (8 seconds)
```

Рис. 7: Запуск nikto-ввода порт

## Выполнение лабораторной работы

Кроме адреса хоста и порта веб-приложения, никто выводит информацию о различных уязвимостях приложения:

Сервер: Apache/2.4.62 (Debian) + /DVWA/: Заголовок X-Frame-Options, защищающий от перехвата кликов, отсутствует. Смотрите:

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

- /DVWA/: Заголовок X-Content-Type-Options не задан. Это может позволить пользовательскому агенту отображать содержимое сайта способом, отличным от MIME-типа.

Смотрите: <https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/>

- 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`  
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.php?filesrc=/etc/h`: Найден файловый менеджер бэкдора на PHP.

- `/DVWA/assets/mobirise/css/meta.php?filesrc=`: Найден файловый менеджер бэкдора на PHP.
- `/DVWA/login.cgi?cli=aa%20aa%27cat%20/etc/hosts`: Удаленное выполнение какой-либо команды маршрутизатором D-Link.
- `/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, тайный вход (от англ. back door — «чёрный ход», «лазейка», буквально «задняя дверь») — 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 кодом.

CVE-2003-1418 — это уязвимость в Apache HTTP Server 1.3.22–1.3.27 на OpenBSD, которая позволяет удалённым злоумышленникам получать конфиденциальную информацию через:

- Заголовок ETag, который раскрывает номерinode.
- Многочастную границу MIME, которая раскрывает идентификаторы дочерних процессов (PID).

В настоящее время эта проблема имеет среднюю степень тяжести.

Выполнив эту работу, я научилась тестирование веб-приложений с помощью сканер nikto