

# **Индивидуальный проект - Этап 4**

**Основы информационной безопасности**

Чистов Даниил Максимович

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
1.1	Введение . . . . .	4
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>5</b>
<b>3</b>	<b>Выводы</b>	<b>8</b>
<b>4</b>	<b>Список литературы</b>	<b>9</b>

## Список иллюстраций

2.1	Запуск сервисов для DVWA . . . . .	5
2.2	DVWA: уровень защиты low . . . . .	5
2.3	Результат работы nikto . . . . .	6

# 1 Цель работы

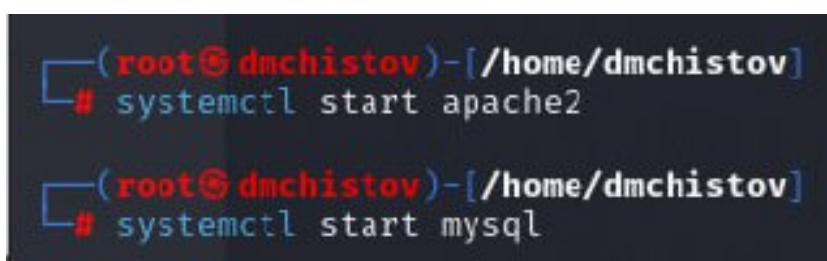
Получение навыков пользования nikto.

## 1.1 Введение

nikto - это базовый сканнер веб-приложений на уязвимости серверного уровня, т.е. ищет уязвимые файлы, скрипты, делает HTTP-запросы.

## 2 Выполнение лабораторной работы

Перед работой надо запустить apache2 и mysql, буду тестировать nikto на dvwa (рис. 2.1).



```
(root@dmchistov)-[/home/dmchistov]
# systemctl start apache2

(root@dmchistov)-[/home/dmchistov]
# systemctl start mysql
```

Рис. 2.1: Запуск сервисов для DVWA

В начале работы я думал протестировать dvwa на разных уровнях защиты, однако оказалось это бесполезно, ведь никто проверяет веб-приложения на уязвимости другого типа, а DVWA выставляет уровни защиты, которые проявляются в логике работы самого веб-приложения, а не его серверную структуру (рис. 2.2).

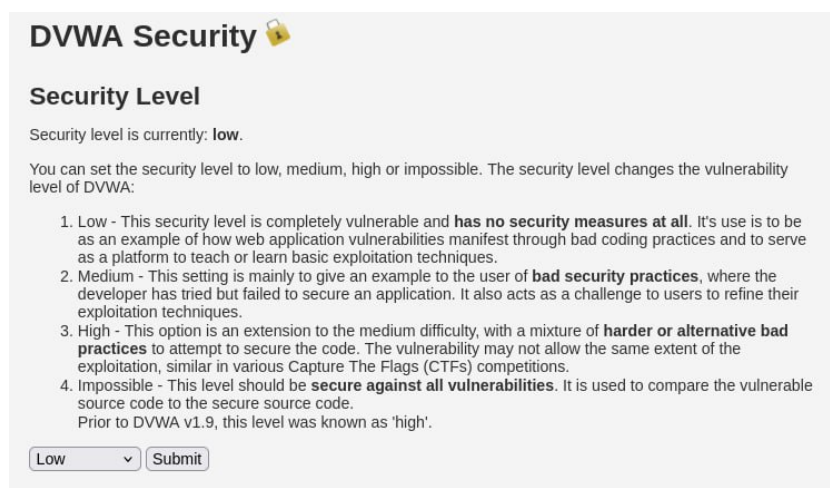


Рис. 2.2: DVWA: уровень защиты low

Пишем команду

```
nikto -h http://127.0.0.1/dvwa
```

Здесь -h - задаём хоста (кого будем анализировать), и дальше идёт URL нашего хоста. Также можно написать -o (имя) и после этого -F (формат) и это отправит результаты нашего сканирования в файл, чьё имя и формат мы сами задали

Команда вывела следующее: (рис. 2.3)

```
(dmchistov@dmchistov) [~]
$ 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: 2025-05-03 20:28:37 (GMT3)

+ 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/
+ 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/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.
+ 8073 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time: 2025-05-03 20:29:05 (GMT3) (28 seconds)

+ 1 host(s) tested
```

Рис. 2.3: Результат работы nikto

Здесь есть на что обратить внимание:

1. Можно узнать версию Apache, а это может помочь хакеру найти уязвимости, если уже известны уязвимости для этой версии
2. X-Frame-Options — отсутствие защиты от clickjacking (встраивание сайта в чужого сайта - т.е. так ввести в сайт свой функционал, который может принести вред пользователю)
3. X-Content-Type-Options — отсутствие от MIME-атаки (когда браузер может неадекватно интерпретировать тип файла, например подали серверу файл

txt, содержащий вредоносный код, а веб-приложение этот файл проинтерпретирует как раз как нам надо и этот код запустит.)

4. Nikto отправляет запросы к разным путям, подставляя ?filesrc=/etc/hosts и сервер возвращает содержимое файла hosts. Т.е. получается можно просматривать любые файлы. Такие скрипты часто называются “file manager backdoors”

## **3 Выводы**

При выполнении данной работы я успешно получил навыки работы с nikto.



## 4 Список литературы

Индивидуальный проект

Краткое введение в nikto (видео на английском)