

# **Отчет по четвертому этапу индивидуального проекта**

**Сканер nikto**

Вакутайпа Милдред

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>3</b>	<b>Выводы</b>	<b>10</b>
	<b>Список литературы</b>	<b>11</b>

## Список иллюстраций

2.1	запуск сервера . . . . .	6
2.2	Изменение уровня безопасности . . . . .	6
2.3	Сканирование 1 с nikto . . . . .	7
2.4	Сканирование 2 с nikto . . . . .	7

## **Список таблиц**

# 1 Цель работы

Научиться тестировать веб-приложений со сканером nikto.

## 2 Выполнение лабораторной работы

По сколько буду сканировать веб-приложение DVWA запускаю его.



```
mwakutaipa@wakutaipa: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/mwakutaipa/.zsh_history  
(mwakutaipa@wakutaipa)-[~]  
$ sudo systemctl start mysql  
[sudo] password for mwakutaipa:  
(mwakutaipa@wakutaipa)-[~]  
$ sudo systemctl start apache2  
(mwakutaipa@wakutaipa)-[~]  
$
```

Рис. 2.1: запуск сервера

Далее изменяю уровня безопасности на среднее.

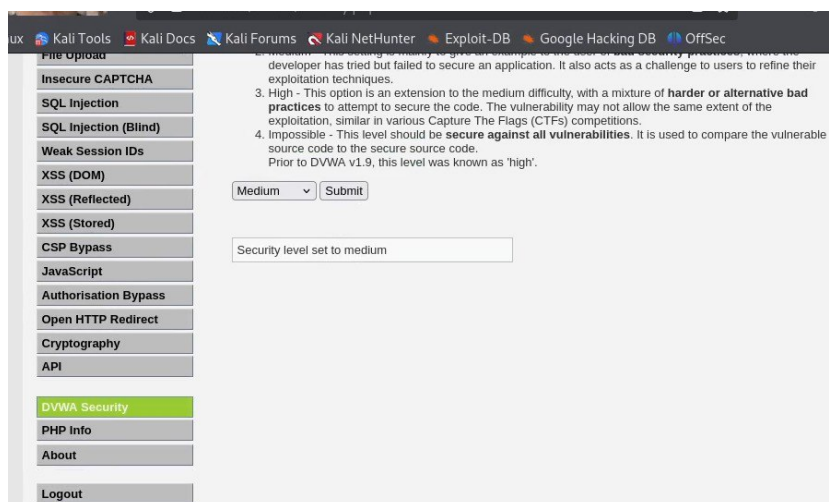


Рис. 2.2: Изменение уровня безопасности

Запускаю nikto используя #nikto и сканирую DVWA введя его полный URL без порта.

```
(mwakutaipa@wakutaipa)-[~]
$ #nikto
(mwakutaipa@wakutaipa)-[~]
$ 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:     2025-04-29 19:44:31 (GMT3)
```

Рис. 2.3: Сканирование 1 с nikto

Сканирую второй раз введя полный URL DVWA с портом и заметила, что результаты не сильно отличаются.

```
(mwakutaipa@wakutaipa)-[~]
$ 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:     2025-04-29 19:46:03 (GMT3)

+ 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: 62ea6484f649b, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
```

Рис. 2.4: Сканирование 2 с nikto

Кроме адреса хоста и порта веб-приложения, никто выводит информацию о различных уязвимостях приложения как сервер: Apache/2.4.58 (Debian) /DVWA/: Заголовок X-Frame-Options, защищающий от перехвата кликов, отсутствует. /DVWA/: Заголовок X-Content-Type-Options не задан. Это может позволить пользовательскому агенту отображать содержимое сайта способом, отличным от MIME-типа. 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/hosts: 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: Найден файловый менеджер бэкдора на PHP. /DVWA/assets/mobirise/css/meta.php?filesrc=: Найден файловый менеджер бэкдора на PHP. /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 — дефект алгоритма, который намеренно встраивается в него разрабатчиком 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 ко-



ДОМ.

## **3 Выводы**

Научилась тестировать веб-приложений со сканером nikto.

## **Список литературы**