

# **Отчет по выполнению индивидуального проекта. Этап №4**

**Основы информационной безопасности**

Закиров Нурислам Дамирович

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>7</b>
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>9</b>
4.1	Выполнение основных действий . . . . .	9
4.2	Анализ результатов сканирования . . . . .	11
<b>5</b>	<b>Выводы</b>	<b>15</b>
	<b>Список литературы</b>	<b>16</b>

## Список иллюстраций

4.1	Запуск apache2 . . . . .	9
4.2	Запуск DVWA . . . . .	10
4.3	Запуск nikto . . . . .	10
4.4	Название рисунка . . . . .	11
4.5	Название рисунка . . . . .	11

## **Список таблиц**

# 1 Цель работы

Научиться тестированию веб-приложений с помощью сканера nikto

## 2 Задание

Использование nikto.

### 3 Теоретическое введение

*nikto* — базовый сканер безопасности веб-сервера. Он сканирует и обнаруживает уязвимости в веб-приложениях, обычно вызванные неправильной конфигурацией на самом сервере, файлами, установленными по умолчанию, и небезопасными файлами, а также устаревшими серверными приложениями. Поскольку *nikto* построен исключительно на LibWhisker2, он сразу после установки поддерживает кросс-платформенное развертывание, SSL (криптографический протокол, который подразумевает более безопасную связь), методы аутентификации хоста (NTLM/Basic), прокси и несколько методов уклонения от идентификаторов. Он также поддерживает перечисление поддоменов, проверку безопасности приложений (XSS, SQL-инъекции и т. д.) и способен с помощью атаки паролей на основе словаря угадывать учетные данные авторизации.

Для запуска сканера *nikto* введите в командную строку терминала команду: `# nikto`

По умолчанию, как ранее было показано в других приложениях, при обычном запуске команды отображаются различные доступные параметры. Для сканирования цели введите `nikto -h <цель> -p <порт>`, где — домен или IP-адрес целевого сайта, а — порт, на котором запущен сервис

Сканер *nikto* позволяет идентифицировать уязвимости веб-приложений, такие как раскрытие информации, инъекция (XSS/Script/HTML), удаленный поиск файлов (на уровне сервера), выполнение команд и идентификация программного обеспечения. В дополнение к показанному ранее основному сканирова-

нию `nikto` позволяет испытателю на проникновение настроить сканирование конкретной цели. Рассмотрим параметры, которые следует использовать при сканировании. - Указав переключатель командной строки `-T` с отдельными номерами тестов, можно настроить тестирование конкретных типов. - Используя при тестировании параметр `-t`, вы можете установить значение тайм-аута для каждого ответа. - Параметр `-D V` управляет выводом на экран. - Параметры `-o` и `-F` отвечают за выбор формата отчета сканирования.

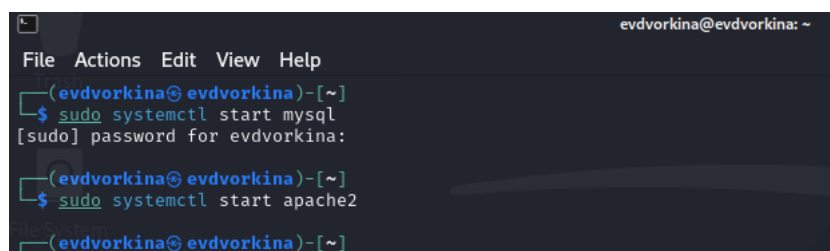
Существуют и другие параметры, такие как `-mutate` (угадывать поддомены, файлы, каталоги и имена пользователей), `-evasion` (обходить фильтр идентификаторов) и `-Single` (для одиночного тестового режима), которые можно использовать для углубленной оценки цели.



## 4 Выполнение лабораторной работы

### 4.1 Выполнение основных действий

Чтобы работать с nikto, необходимо подготовить веб-приложение, которое будем сканировать. Это будет DVWA. Для этого запустил apache2 (рис. 4.1).



```
evdvorkina@evdvorkina: ~  
File Actions Edit View Help  
(evdvorkina@evdvorkina)-[~]  
$ sudo systemctl start mysql  
[sudo] password for evdvorkina:  
(evdvorkina@evdvorkina)-[~]  
$ sudo systemctl start apache2  
(evdvorkina@evdvorkina)-[~]  
$
```

Рис. 4.1: Запуск apache2

Ввожу в адресной строке браузера адрес DVWA, перехожу в режим выбора уровня безопасности, ставлю минимальный (необязательно, nikto при обычном сканировании для режима impossible и low выдаст одинаковые потенциальные уязвимости, что логично, ведь они остаются, но изменяется сложность, с которой их можно использовать) (рис. 4.2).

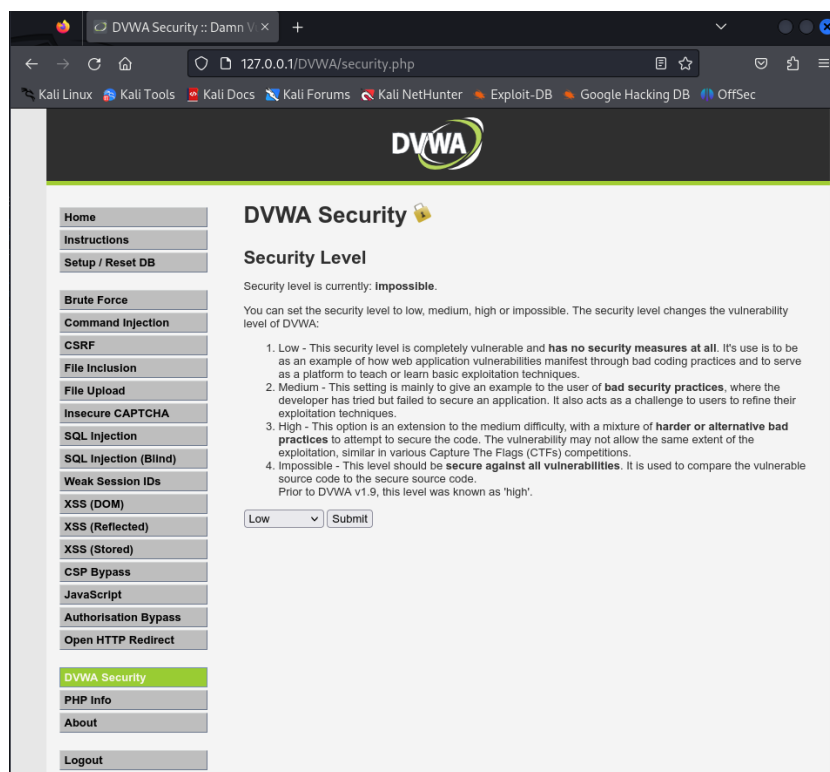


Рис. 4.2: Запуск DVWA

Запускаю nikto (рис. 4.3).

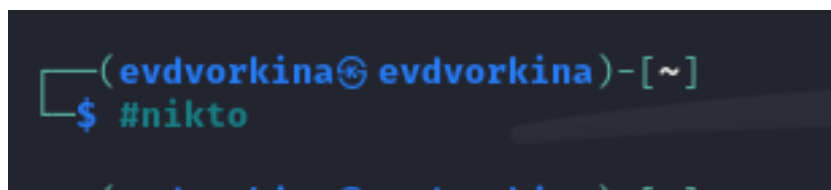


Рис. 4.3: Запуск nikto

Проверить веб-приложение можно, введя его полный URL и не вводя порт, по-пробывал просканировать так (рис. 4.4).

```
(evdvorkina@evdvorkina:~)
$ 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: 2024-04-27 17:34:23 (GMT3)

+ Server: Apache/2.4.58 (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: OPTIONS, HEAD, GET, POST
+ /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/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. Info 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/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/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/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=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/login.cgi?cli=32k28ak2?cat=0/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.
+ 8074 requests: 0 error(s) and 26 item(s) reported on remote host
+ End Time: 2024-04-27 17:35:22 (GMT3) (59 seconds)
```

Рис. 4.4: Название рисунка

Затем попробывал просканировать введя адрес хоста и адрес порта, результаты незначительно отличаются (рис. 4.5).

```
(evdvorkina@evdvorkina:~)
$ 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: 2024-04-27 17:38:00 (GMT3)

+ Server: Apache/2.4.58 (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 indices via ETags header found with file /, inode: 260, size: 4129635369, mime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /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 backdoor file manager was found.
+ /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 backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /login.cgi?cli=32k28ak2?cat=0/etc/hosts: Some D-link router remote command execution.
+ /Assets/mobirise/css/meta.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ 8074 requests: 0 error(s) and 26 item(s) reported on remote host
+ End Time: 2024-04-27 17:39:03 (GMT3) (63 seconds)

- 3 hosts(s) tested
```

Рис. 4.5: Название рисунка

## 4.2 Анализ результатов сканирования

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

Сервер: Apache/2.4.58 (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 пользователю 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/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?filesrc=/etc/hosts: 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.

## 5 Выводы

В ходе выполнения четвертого этапа индивидуального проекта я научился использовать сканер nikto для тестирования веб-приложений

## **Список литературы**