

# **Индивидуальный проект. Этап 4**

**Использование nikto**

Парфенова Елизавета Евгеньевна

# Содержание

|          |                                 |           |
|----------|---------------------------------|-----------|
| <b>1</b> | <b>Цель работы</b>              | <b>5</b>  |
| <b>2</b> | <b>Теоретическое введение</b>   | <b>6</b>  |
| <b>3</b> | <b>Выполнение этапа проекта</b> | <b>8</b>  |
| <b>4</b> | <b>Выводы</b>                   | <b>12</b> |
|          | <b>Список литературы</b>        | <b>13</b> |

## Список иллюстраций

|     |   |    |
|-----|---|----|
| 3.1 | Запуск веб-приложения DVWA . . . . .                        | 8  |
| 3.2 | Проверка наличия nikto . . . . .                            | 8  |
| 3.3 | Сканирование DVWA . . . . .                                 | 9  |
| 3.4 | Отчет в текстовом формате . . . . .                         | 9  |
| 3.5 | Отчет в формате html . . . . .                              | 10 |
| 3.6 | Команда для сканирования с отчетом в формате html . . . . . | 10 |
| 3.7 | Сканирование с помощью IP . . . . .                         | 11 |
| 3.8 | Команда сканирования с IP и портом . . . . .                | 11 |

## **Список таблиц**

# 1 Цель работы

Использование веб-сканера Nikto для сканирования уязвимостей веб-приложений.

## 2 Теоретическое введение

**Nikto** – веб-сканер, проверяющий веб-серверы на самые частые ошибки, возникающие обычно из-за человеческого фактора. Проверяет целевой веб-сервер на наличие опасных файлов и исполняемых сценариев, инструментов администрирования базами данных, устаревшего программного обеспечения. [1]

Он является бесплатным (open source) сканером. Утилита относится к классу blackbox сканеров, т. е. сканеров, использующих стратегию сканирования методом черного ящика. Это значит, что заранее неизвестно о внутреннем устройстве программы/сайта (доступ к исходному коду отсутствует) и упор сделан на функциональность. Программа может обнаруживать более 6700 потенциально опасных файлов и уязвимостей. Новые уязвимости добавляются в базу данных программы по мере их возникновения. Nikto не позиционируется как стелс сканер (стелс сканеры никогда не устанавливают TCP-соединения до конца, тем самым сканирование происходит скрытно) – при сканировании сайта в логах сайта или в любой другой системе обнаружения вторжений, если она используется, будет отображена информация о том, что сайт подвергается сканированию.

Первая версия Nikto под номером 1.00 была создана в 2001 году Американским инженером по информационной безопасности Крисом Сулло. На момент 2023 года последней актуальной версией является версия 2.1.6.

Среди функций Nikto можно выделить следующие:

- поддержка SSL,
- поддержка HTTP прокси;

- создание отчетов в текстовом формате, XML, HTML, NBE или CSV;
- возможность сканирования портов;
- поиск поддоменов;
- поддержка плагинов для расширения функционала сканирования. [2]

### 3 Выполнение этапа проекта

Для того, чтобы протестировать веб-приложение DVWA нам необходимо запустить его. Для этого мы запускаем сервер apache2 и базу данных с помощью команд *sudo service apache2 start* и *service mariadb start* (рис. 3.1).

```
(eeparfenova@eeparfenova)-[~]  
$ sudo service apache2 start  
  
(eeparfenova@eeparfenova)-[~]  
$ service mariadb start  
  
(eeparfenova@eeparfenova)-[~]  
$
```

Рис. 3.1: Запуск веб-приложения DVWA

Проверим наличие perl и nikto в нашей системе. Для этого последовательно введем команды *perl -v* и *nikto*. perl, по информации с источника [2], обязательно должен быть установлен перед nikto. В итоге, видим, что и то, и другое установлено в Linux (рис. 3.2).

```
(eeparfenova@eeparfenova)-[~]  
$ perl -v  
  
This is perl 5, version 38, subversion 2 (v5.38.2) built for x86_64-linux-gnu-thread-multi  
(with 44 registered patches, see perl -V for more detail)  
  
Copyright 1987-2023, Larry Wall  
  
Perl may be copied only under the terms of either the Artistic License or the  
GNU General Public License, which may be found in the Perl 5 source kit.  
  
Complete documentation for Perl, including FAQ lists, should be found on  
this system using "man perl" or "perldoc perl". If you have access to the  
Internet, point your browser at https://www.perl.org/, the Perl Home Page.  
  
(eeparfenova@eeparfenova)-[~]  
$ nikto  
- Nikto v2.5.0
```

Рис. 3.2: Проверка наличия nikto



Запрос в Nikto можно сделать через URL и через IP (с портом). В первом случае команда будет выглядеть следующим образом *nikto -h http://localhost/DVWA/ -output report.txt -Format text*. (рис. 3.3) Все что следует после опции output используется дополнительно для отчетов разных форматов. Я попробовала создать отчеты в текстовом формате (рис. 3.4) и в формате html (рис. 3.5). Для отчета в формате html команда немного изменится и будет выглядеть следующим образом (рис. 3.6). (В обоих вариантах report.txt(.html) - название файла, в котором отчет будет сохранен)

```
leapfenova@leapfenova:~$ nikto -h http://localhost/DVWA/ -output report.txt -Format text
Nikto v2.5.8

+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 80
+ Start Time: 2024-10-01 20:07:14 (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.net
tparker.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/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/action 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/.dockerignore: .dockerignore file found. It may be possible to grasp the directory structure and learn more about the site.
+ 7558 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time: 2024-10-01 20:07:28 (GMT3) (6 seconds)

+ 1 host(s) tested
```

Рис. 3.3: Сканирование DVWA

```
1 - Nikto v2.5.8/
2 - Target Host: localhost
3 - Target Port: 80
4 - GET /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/
5 - GET /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.net
tparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
6 - OPTIONS /DVWA/: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
7 - GET /DVWA/config/: Directory indexing found.
8 - GET /DVWA/config/: Configuration information may be available remotely.
9 - GET /DVWA/tests/: Directory indexing found.
10 - GET /DVWA/tests/: This might be interesting.
11 - GET /DVWA/database/: Directory indexing found.
12 - GET /DVWA/database/: Database directory found.
13 - GET /DVWA/docs/: Directory indexing found.
14 - GET /DVWA/login.php: Admin login page/action found.
15 - GET /DVWA/git/index: Git index file may contain directory listing information.
16 - GET /DVWA/git/HEAD: Git HEAD file found. Full repo details may be present.
17 - GET /DVWA/git/config: git config file found. Info about repo details may be present.
18 - GET /DVWA/.gitignore: .gitignore file found. It is possible to grasp the directory structure.
19 - GET /DVWA/.dockerignore: .dockerignore file found. It may be possible to grasp the directory structure and learn more about the site.
```

Рис. 3.4: Отчет в текстовом формате

| localhost / 127.0.0.1 port 80 |   |
|-------------------------------|---|
| Target IP                     | 127.0.0.1   |
| Target Hostname               | localhost   |
| Target Port                   | 80  |
| HTTP Server                   | Apache/2.4.62 (Debian)  |
| Site Link (Name)              | <a href="http://localhost:80/DVWA/">http://localhost:80/DVWA/</a>   |
| Site Link (IP)                | <a href="http://127.0.0.1:80/DVWA/">http://127.0.0.1:80/DVWA/</a>   |
| URI                           | /DVWA/  |
| HTTP Method                   | GET   |
| Description                   | /DVWA/ The anti-clickjacking X-Frame-Options header is not present.   |
| Test Links                    | <a href="http://localhost:80/DVWA/">http://localhost:80/DVWA/</a><br><a href="http://127.0.0.1:80/DVWA/">http://127.0.0.1:80/DVWA/</a>  |
| References                    | <a href="https://owasp.org/www-project-secure-headers/guidelines/section-http-headers/x-frame-options">https://owasp.org/www-project-secure-headers/guidelines/section-http-headers/x-frame-options</a>           |
| URI                           | /DVWA/  |
| HTTP Method                   | GET   |
| Description                   | /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.   |
| Test Links                    | <a href="http://localhost:80/DVWA/">http://localhost:80/DVWA/</a><br><a href="http://127.0.0.1:80/DVWA/">http://127.0.0.1:80/DVWA/</a>  |
| References                    | <a href="https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/">https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/</a> |
| URI                           | /DVWA/  |
| HTTP Method                   | OPTIONS   |
| Description                   | OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS.  |
| Test Links                    | <a href="http://localhost:80/DVWA/">http://localhost:80/DVWA/</a><br><a href="http://127.0.0.1:80/DVWA/">http://127.0.0.1:80/DVWA/</a>  |
| References                    |   |
| URI                           | /DVWA/config/   |
| HTTP Method                   | GET   |
| Description                   | /DVWA/config/ Directory indexing found.   |
| Test Links                    | <a href="http://localhost:80/DVWA/config/">http://localhost:80/DVWA/config/</a><br><a href="http://127.0.0.1:80/DVWA/config/">http://127.0.0.1:80/DVWA/config/</a>  |
| References                    |   |
| URI                           | /DVWA/config/   |
| HTTP Method                   | GET   |
| Description                   | /DVWA/config/ Configuration information may be available remotely.  |
| Test Links                    | <a href="http://localhost:80/DVWA/config/">http://localhost:80/DVWA/config/</a><br><a href="http://127.0.0.1:80/DVWA/config/">http://127.0.0.1:80/DVWA/config/</a>  |

Рис. 3.5: Отчет в формате html

```
$ nikto -h http://localhost/DVWA/ -output report.html -Format html
- Nikto v2.5.0
```

Рис. 3.6: Команда для сканирования с отчетом в формате html

Итак, в результате сканирования было найдено 16 уязвимостей. В них входят:

- Отсутствие заголовка X-Frame-Options, что делает сайт уязвимым для атак типа clickjacking
- Отсутствие заголовка X-Content-Type-Options, что может позволить браузеру обрабатывать содержимое некорректно, не того MIME-типа, который был определен и не должен быть изменен
- Обнаружена индексация каталогов в /DVWA/config/, /DVWA/tests/, /DVWA/database/ и т.д., что может позволить доступ к конфиденциальной информации
- Найдены страницы для входа в административную панель и конфигурационные файлы Git (скрытая папка Git), которые могут содержать важную информацию о структуре проекта (сайта) и репозитории

Также было указано, что доступны 4 метода HTTP: OPTIONS, GET, POST, HEAD.

Во втором случае, сканирование будет выглядеть следующим образом (рис. 3.7).

При этом вывод команд `nikto -h 127.0.0.1` и `nikto -h 127.0.0.1 -p 80` (указание порта локального хоста) (рис. 3.8) идентичен

```
(eeparfenova@eeparfenova)-[~]
$ nikto -h 127.0.0.1
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 80
+ Start Time: 2024-10-01 20:14:37 (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: 622059c13b3c9, mtime: grip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1410
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
+ /etc/passwd: 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/passwd: A PHP backdoor file manager was found.
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meahy.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meahy.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /assets/modules/csl/meta.php?filesrc=/: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa28aa2catk20/etc/passwd: Some D-Link router remote command execution.
+ /bin/ls/etc/passwd: A backdoor was identified.
+ 90% requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time: 2024-10-01 20:14:44 (GMT3) (7 seconds)

+ 1 host(s) tested
```

Рис. 3.7: Сканирование с помощью IP

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

Рис. 3.8: Команда сканирования с IP и портом

При таком сканировании было найдено 15 уязвимостей. Помимо похожих с предыдущим случаем уязвимостей, были найдены:

- Утечка информации о файловой системе через ETags
- Уязвимость чтения системных файлов с помощью манипуляций с URL (/etc/passwd)
- PHP Backdoor file manager был обнаружен в нескольких местах, что свидетельствует о возможной зараженности системы бэкдором
- Уязвимость удаленного выполнения команд на роутерах D-Link

## 4 Выводы

Мы использовали веб-сканера Nikto для сканирования уязвимостей веб-приложений.

## Список литературы

1. Nikto [Электронный ресурс]. Wikimedia Foundation, Inc., 2024. URL: <https://ru.wikipedia.org/wiki/Nikto>.
2. Обзор сканера Nikto для поиска уязвимостей в веб-серверах [Электронный ресурс]. Habr, 2023. URL: <https://habr.com/ru/companies/first/articles/731696/>.